Qualys Cloud Agent Windows 5.0

December 2022 (Updated in February 2023)

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.

New Features

- Oracle Cloud Infrastructure – Bring Your Own License (OCI-BYOL): Added Bring your Own Licence (BYOL) support for Oracle Cloud Infrastructure (OCI) to enable VM scanning for instances on OCI. The OCI Vulnerability Scanning Service (VSS) takes care of Qualys Agent installation, configuration, and permissions required for scanning to detect vulnerabilities in both Qualys and OCI.

  Note: This feature has a dependency on the Oracle VSS portal. Ensure that Oracle has enabled the OCI BYOL features for your account.

  Required application version: Qualys Cloud Platform 3.13.1.0

- Self-Protection feature (SPF): The self-protection feature is introduced to prevent tempering with Qualys Cloud Agent files, directories, and registry entries, such as overwriting, deleting, renaming, modifying, and memory mapping. It prevents uninstallation of Cloud Agent and termination of Cloud Agent processes. The self-protection feature also prevents the user-defined scripts uploaded by Custom Assessment, Remediation, and Patch Management, from making changes to the protected files.

  Note: This feature is not enabled by default. To enable the feature, contact your Qualys representative.

  The self-protection feature can also be disabled if you want to access the agent data and artifacts required for debugging, such as log files. Disabling the self-protection feature can be initiated using the Cloud Agent application. For details, see Cloud Agent online help.

  Required application version: Qualys Cloud Platform 3.12.0.0

- Remote Cloud Agent log collection: Includes an opt-in feature for remote log collection, with which customers can permit Qualys Support to send the Cloud Agent log files to the Qualys Cloud Platform for debugging purposes.
  This feature helps to reduce time to resolution for the support cases, especially where the users are remote, and Qualys admins do not have access to the end systems on which Cloud Agent is installed.
  Qualys Cloud Agent sends only its Cloud Agent log files, such as logs in the `C:\ProgramData\Qualys\QualysAgent\*` directory.
  Note: This feature requires written consent from customers holding an active Qualys account over email. With the customer's consent, the Cloud Agent sends the log files to the Qualys Cloud Platform only once. A separate explicit consent is required from a customer for sending the agent log files to Qualys Cloud Platform each time.
  For more information, contact your Qualys representative.

Required application version: Qualys Cloud Platform 3.14.0.0

Enhancements

- Better handling of stale or terminated Cloud Assets: The AWS, Azure, and GCP instances discovered by a connector and have the Qualys Cloud Agent installed are merged in a single asset record.

  If the cloud instance is ephemeral, which is provisioned and terminated in the Cloud console between two successive connector runs, the asset state needs to be updated. However, the cloud provider APIs reflect the terminated assets only for a short time, and the Cloud Agent cannot report the asset status before the termination of an instance.

  With this release, you can better identify stale or terminated assets, as Qualys will start collecting the following information in the provisioning call.

  - For AWS instance – accountID
  - For Azure instances – subscriptionId
  - For GCP instances - projectId or project number

  For identifying stale assets, account reconciliation is performed in addition to the connector reconciliation to identify the stale assets for the account ID associated with the connector that was not discovered in the connector run.

  This helps in reporting up-to-date asset information to the Qualys Cloud Platform. This enhancement applies to assets created in AWS, Azure, and GCP environments.

  Required application version: Qualys Cloud Platform 3.13.1.0

- File Integrity Monitoring:
  - FIM can be configured to monitor files and folder changes at network shares or mapped drives.
    Required application version: FIM 3.6
  - For all FIM events, Cloud Agent provides the file size in the event details.

- Custom Assessment and Remediation:
  - Added support to pass Powershell Execution Policy through command manifest to CAR for executing Powershell scripts on an asset using Qualys CAR.
    Required application version: CAR 1.5

Behavior Changes

There are no behavior changes in this release.

Platform Coverage Support (Operating Systems)

Added support for the following platforms:

- Win 11 22H2
- Win 10 22H2 x86
- Win 10 22H2 x64

Fixed Defects

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

CRM-98209	Fixed an issue where the Cloud Agent used a WMI query that caused Windows Installer to reconfigure applications. Due to this, installation or restart of the agent led to a number of event logs - Event ID: 1035 under Application. With the fix, usage of the WMI query that was causing the Windows installer to reconfigure applications has been removed.
CRM-77150 CRM-97664 CRM-72329	Fixed issues in fetching provider information, such as instance ID, and account ID, from AWS instance metadata service (IMDS) v1 and v2.
CRM-95337	Fixed an issue in detecting CID 11211: Configure Windows spotlight on Lock Screen.
CRM-95377	Fixed an issue in handling large-size script output.
CRM-98168	Fixed an issue in uninstalling the agent when EPP is enabled.
CRM-90141	Fixed an issue where the agent files and HostID were not removed even after successfully uninstalling the agent with the Force=true parameter.

Known Limitations and Workarounds

- An interoperability issue may cause failure in Qualys Endpoint Protection initialization when Self-Protection is enabled.
  Note: For Windows Agent 5.0, the Self-Protection feature is not enabled by default.