Qualys Cloud Platform v3.x

Release Notes

Version 3.14

February 8, 2023 (Updated on April 19, 2023)

What’s New

CA

Cloud Agent

Updated the Upgrade Reattempt Interval Default Value

Remote Cloud Agent Log Collection

Configure Scan on Startup

MD

Web Malware Detection

Site Type Filter in Detections Tab

Administration

New Permissions for Container Security

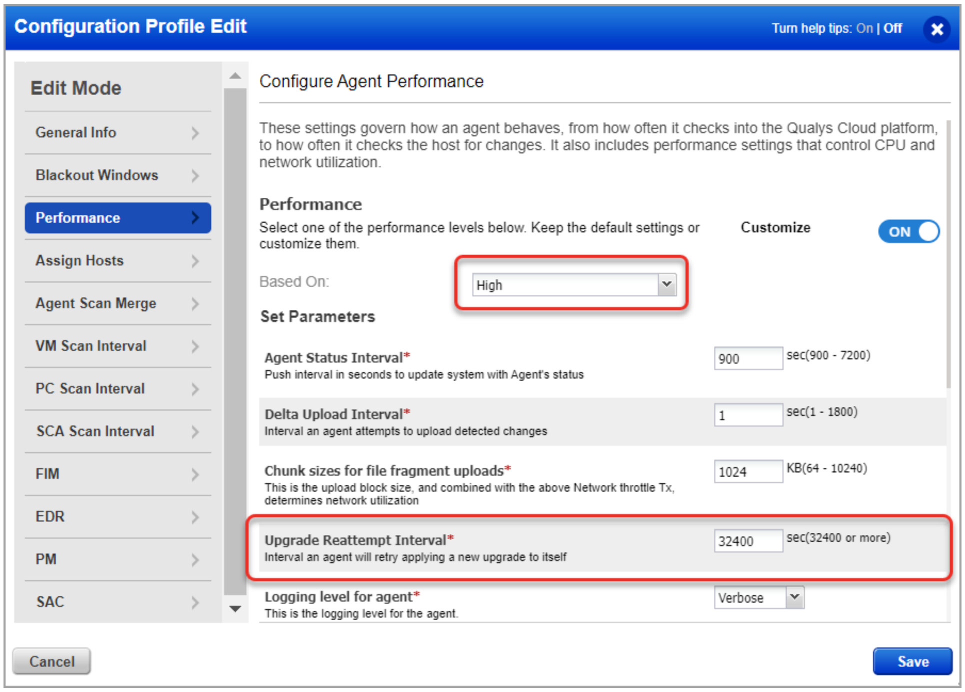
Qualys Cloud Platform 3.14 brings you many more improvements and updates! Learn more

CA Cloud Agent

Updated the Upgrade Reattempt Interval Default Value

With this release, the default value of the **Upgrade Reattempt Interval** field in the configuration profile is updated for different performance levels.

For High performance level, the default value is updated to 32400 seconds.



Configure Agent Performance

These settings govern how an agent behaves, from how often it checks into the Qualys Cloud platform, to how often it checks the host for changes. It also includes performance settings that control CPU and network utilization.

Performance

Select one of the performance levels below. Keep the default settings or customize them. Customize ON

Based On: High

Set Parameters

Agent Status Interval* 900 sec(900 - 7200)
Push interval in seconds to update system with Agent's status

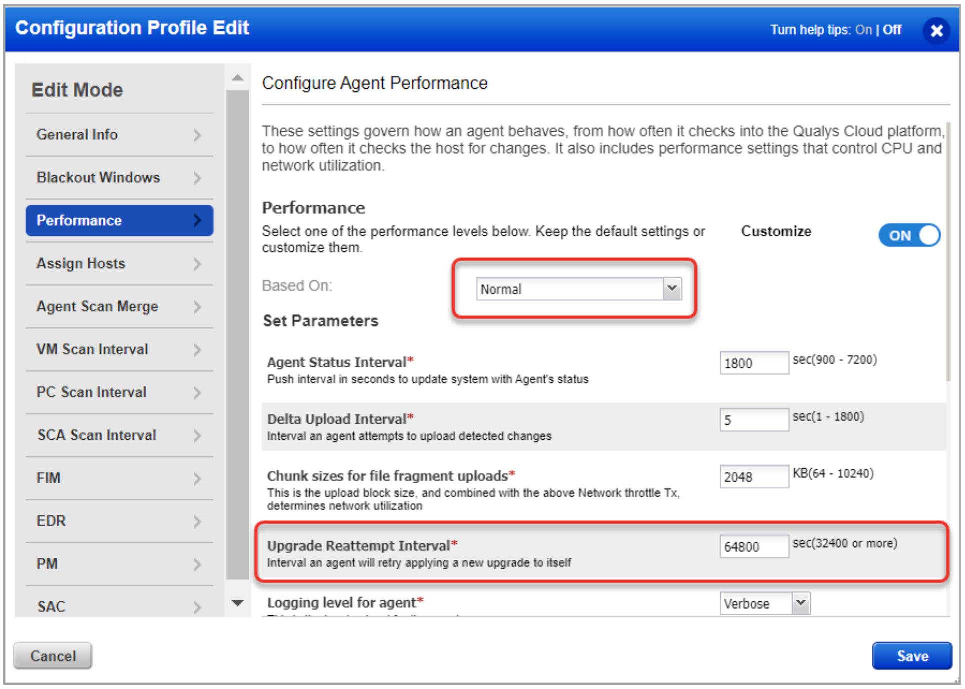
Delta Upload Interval* 1 sec(1 - 1800)
Interval an agent attempts to upload detected changes

Chunk sizes for file fragment uploads* 1024 KB(64 - 10240)
This is the upload block size, and combined with the above Network throttle Tx, determines network utilization

Upgrade Reattempt Interval* 32400 sec(32400 or more)
Interval an agent will retry applying a new upgrade to itself

Logging level for agent* Verbose
This is the logging level for the agent.

For Normal performance level, the default value is updated to 64800 seconds.



Configure Agent Performance

These settings govern how an agent behaves, from how often it checks into the Qualys Cloud platform, to how often it checks the host for changes. It also includes performance settings that control CPU and network utilization.

Performance

Select one of the performance levels below. Keep the default settings or customize them. Customize ON

Based On: Normal

Set Parameters

Agent Status Interval* 1800 sec(900 - 7200)
Push interval in seconds to update system with Agent's status

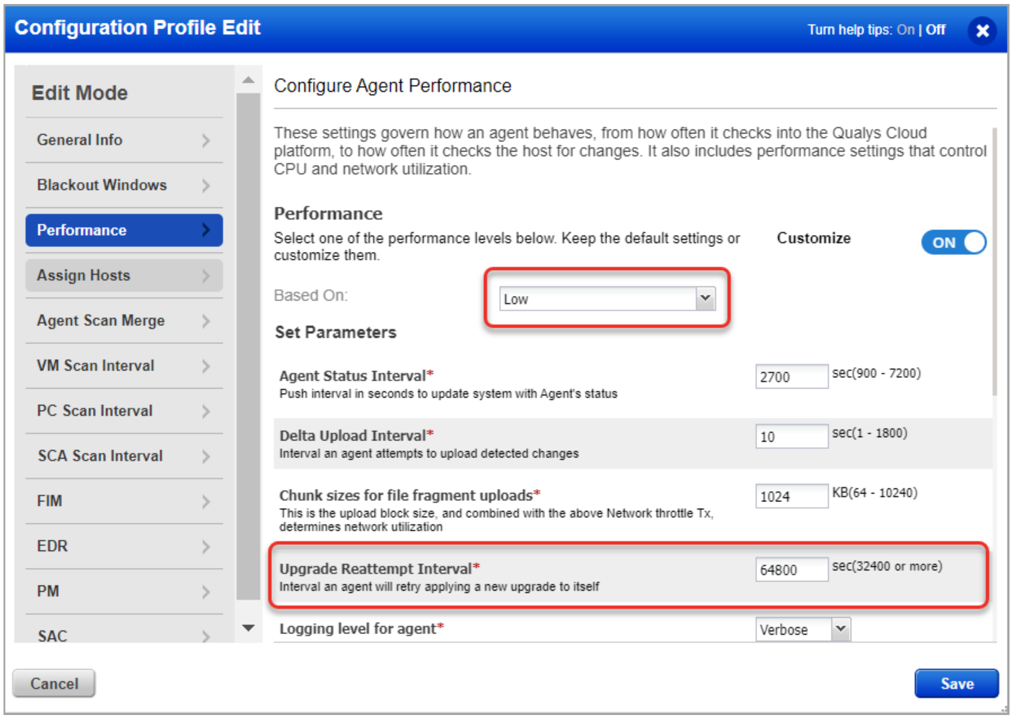
Delta Upload Interval* 5 sec(1 - 1800)
Interval an agent attempts to upload detected changes

Chunk sizes for file fragment uploads* 2048 KB(64 - 10240)
This is the upload block size, and combined with the above Network throttle Tx, determines network utilization

Upgrade Reattempt Interval* 64800 sec(32400 or more)
Interval an agent will retry applying a new upgrade to itself

Logging level for agent* Verbose

For Low performance level, the default value is updated to 64800 seconds.



Configure Agent Performance

These settings govern how an agent behaves, from how often it checks into the Qualys Cloud platform, to how often it checks the host for changes. It also includes performance settings that control CPU and network utilization.

Performance

Select one of the performance levels below. Keep the default settings or customize them.

Customize: ON

Based On: Low

Set Parameters

Agent Status Interval*: 2700 sec(900 - 7200)
Push interval in seconds to update system with Agent's status

Delta Upload Interval*: 10 sec(1 - 1800)
Interval an agent attempts to upload detected changes

Chunk sizes for file fragment uploads*: 1024 KB(64 - 10240)
This is the upload block size, and combined with the above Network throttle Tx, determines network utilization

Upgrade Reattempt Interval*: 64800 sec(32400 or more)
Interval an agent will retry applying a new upgrade to itself

Logging level for agent*: Verbose

Remote Cloud Agent Log Collection

With this release, Cloud Agent provides an opt-in feature—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\*` and `/var/log/qualys/*` directories.

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.

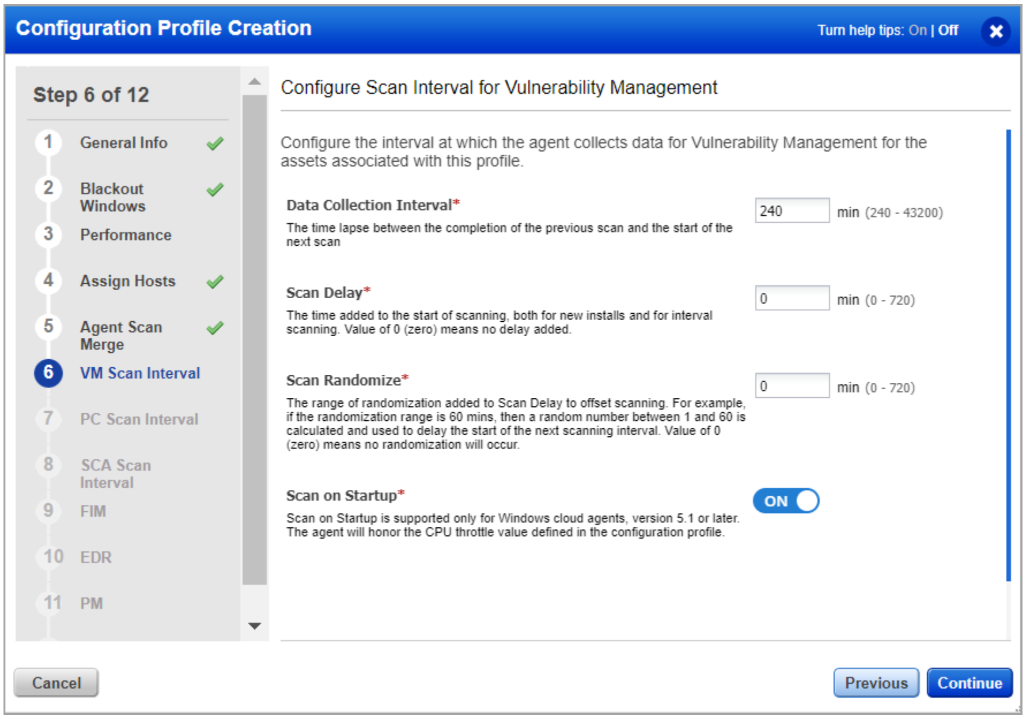
The required agent version is Qualys Cloud Agent Windows 5.0 or Qualys Cloud Agent Linux 5.6.

For more information, contact your Qualys representative.

Configure Scan on Startup

With this release, you can configure the agent to run the vulnerability scan when the agent service starts using the configuration profile.

You can configure the **Scan on Startup** option while creating or editing the **Configuration Profile** in the **VM Scan Interval** tab. By default, the **Scan on Startup** option is disabled.



Configure Scan Interval for Vulnerability Management

Configure the interval at which the agent collects data for Vulnerability Management for the assets associated with this profile.

Data Collection Interval* 240 min (240 - 43200)
The time lapse between the completion of the previous scan and the start of the next scan

Scan Delay* 0 min (0 - 720)
The time added to the start of scanning, both for new installs and for interval scanning. Value of 0 (zero) means no delay added.

Scan Randomize* 0 min (0 - 720)
The range of randomization added to Scan Delay to offset scanning. For example, if the randomization range is 60 mins, then a random number between 1 and 60 is calculated and used to delay the start of the next scanning interval. Value of 0 (zero) means no randomization will occur.

Scan on Startup* ON
Scan on Startup is supported only for Windows cloud agents, version 5.1 or later. The agent will honor the CPU throttle value defined in the configuration profile.

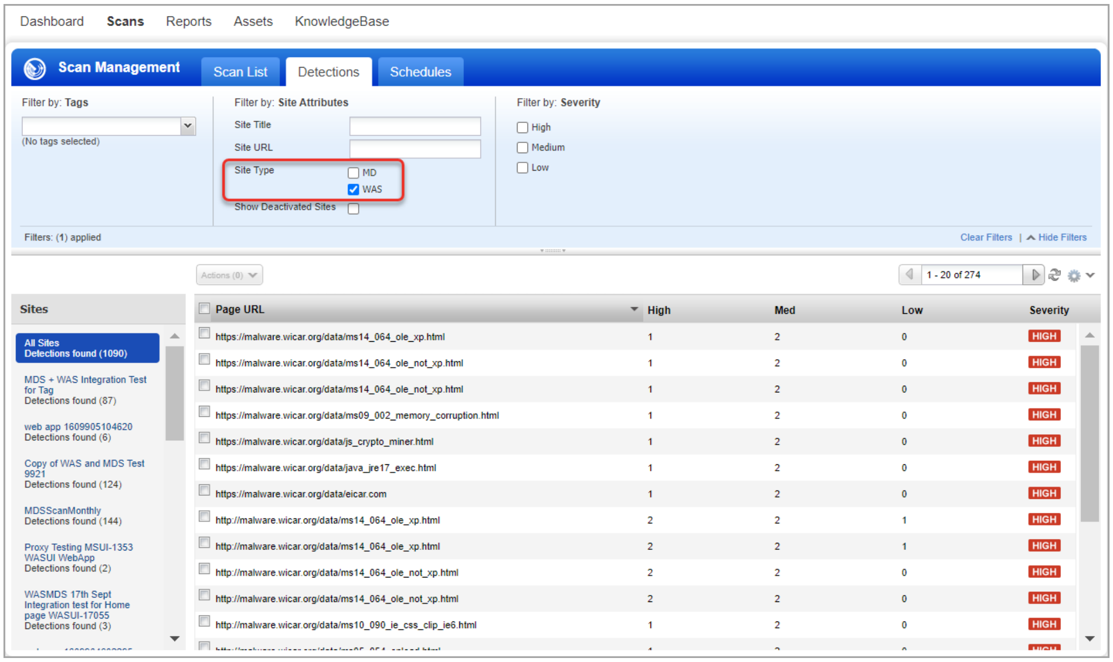
Note: This feature is not available by default. To enable the feature, contact your Qualys representative.

MD

Web Malware Detection

Site Type Filter in Detections Tab

With this release, a new filter— **Site Type**, is added to the **Site Attributes** filters in the **Scans** | **Detections** tab.



Filter by: **Tags**

(No tags selected)

Filter by: **Site Attributes**

Site Title

Site URL

Site Type ☐ MD ☑ WAS

Show Deactivated Sites ☐

Filter by: **Severity**

☐ High

☐ Medium

☐ Low

Filters: (1) applied

1 - 20 of 274

Sites

All Sites
Detections found (1090)

MDS + WAS Integration Test for Tag
Detections found (87)

web app 1609905104620
Detections found (6)

Copy of WAS and MDS Test 9921
Detections found (124)

MDSScanMonthly
Detections found (144)

Proxy Testing MSUI-1353 WASUI WebApp
Detections found (2)

WASMDS 17th Sept Integration test for Home page WASUI-17055
Detections found (3)

☐	Page URL	High	Med	Low	Severity
☐	https://malware.wicar.org/data/ms14_064_ole_xp.html	1	2	0	HIGH
☐	https://malware.wicar.org/data/ms14_064_ole_not_xp.html	1	2	0	HIGH
☐	https://malware.wicar.org/data/ms14_064_ole_not_xp.html	1	2	0	HIGH
☐	https://malware.wicar.org/data/ms09_002_memory_corruption.html	1	2	0	HIGH
☐	https://malware.wicar.org/data/js_crypto_miner.html	1	2	0	HIGH
☐	https://malware.wicar.org/data/java_jre17_exec.html	1	2	0	HIGH
☐	https://malware.wicar.org/data/eicar.com	1	2	0	HIGH
☐	http://malware.wicar.org/data/ms14_064_ole_xp.html	2	2	1	HIGH
☐	http://malware.wicar.org/data/ms14_064_ole_xp.html	2	2	1	HIGH
☐	http://malware.wicar.org/data/ms14_064_ole_not_xp.html	2	2	0	HIGH
☐	http://malware.wicar.org/data/ms14_064_ole_not_xp.html	2	2	0	HIGH
☐	http://malware.wicar.org/data/ms10_090_ie_css_clip_ie6.html	1	2	0	HIGH

The **Site Type** filter includes two values—**MD** and **WAS**. It filters the detections based on whether the assets are linked to MDS, WAS, or both applications.

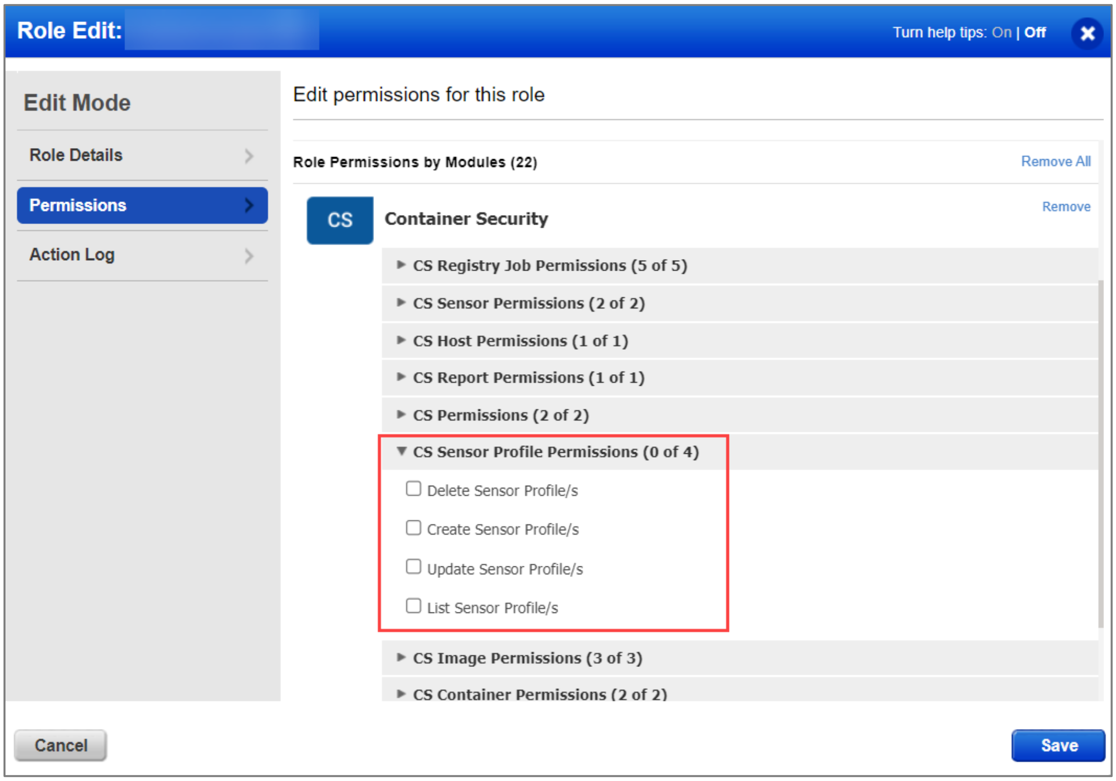
- If you select the **MD** check box, the detections for assets linked to the Web Malware Detection application are displayed.
- If you select the **WAS** check box, the detections for assets linked to the Web Application Scanning application are displayed.

Administration

New Permissions for Container Security

With this release, Manager users can now control access to Container Security sensor profiles. The users working on sensor profiles should get the sensor profile permissions configured for their roles.

The following new permissions are added:



Edit permissions for this role

Role Permissions by Modules (22)

CS Container Security

- ► CS Registry Job Permissions (5 of 5)
- ► CS Sensor Permissions (2 of 2)
- ► CS Host Permissions (1 of 1)
- ► CS Report Permissions (1 of 1)
- ► CS Permissions (2 of 2)
- ▼ CS Sensor Profile Permissions (0 of 4)
  - □ Delete Sensor Profile/s
  - □ Create Sensor Profile/s
  - □ Update Sensor Profile/s
  - □ List Sensor Profile/s
- ► CS Image Permissions (3 of 3)
- ► CS Container Permissions (2 of 2)

For more information about role permissions, see Qualys Administration Utility Online Help: Manage User Roles.

Issues Addressed

- With this release, the Reader role will now be unable to edit the Asset Name in Asset View and VMDR. This will be applicable only if Read Asset permission is given to users.
- We have fixed an issue where a user could not search for assets associated with tag names that included a special character using the tags.name QQL.
- The alignment for the package, installed version, and required version columns in the Detection Summary is now correctly realigned.
- Previously, in the VMDR application, when a user downloaded the CSV report, the data for IPv4 and IPv6 was displayed in the same column. This issue is now resolved.
- Previously, in the VMDR application, the Published Date column did not display the inputs on the VMDR Dashboard Widgets. With this release, while creating a Table widget, when you add a Published Date in the Columns to Display, the information is displayed correctly on the Dashboard widgets and in the Knowledgebase.
- We fixed an issue where customers could not upgrade the authentication type of access key type connectors. Now, they can edit and change the authentication type to ARN.
- We have fixed an issue where the v2 and v3 GET APIs were not fetching ARNs for connectors created through the Connector UI.
- We have fixed an issue where customers were unable to utilize the AWS GovCloud connector due to an error with the query fetching wrong values.
- We have fixed an issue where customers were experiencing failures/degradation on API calls that use unindexed search filters.
- We have now included the secure URL "https://www.qualys.com" instead of "http://www.qualys.com" below the copyright information in all the notifications (scan and report) that are sent to the customers.
- Despite being enabled or disabled for the user, the progressive scanning option was always observed to be enabled by default (checkbox is always selected/ticked). We have now fixed the issue to correctly reflect if the progressive scanning option is enabled or disabled for newly created web applications.
- The progression count did not reflect correct data when web application data was purged. We have now fixed this issue so that on the purge of web application data, the progression count is reset, and correct count is displayed.
- The authentication failed if the same selenium authentication record was used on multiple web applications. We have now fixed this issue so that the authentication is successful even if the same selenium authentication record is used on multiple web applications.
- If a new agent ID is provisioned with an instance ID that is already associated with an existing asset, then the manifest is assigned immediately.