Qualys Cloud Platform (VM, PC) v10.x

Release Notes

Version 10.7

January 8, 2021

This new release of the Qualys Cloud Platform (VM, PC) includes improvements to Vulnerability Management and Policy Compliance.

Qualys Vulnerability Management (VM)

Qualys 10.7 brings you more improvements and updates! Learn more

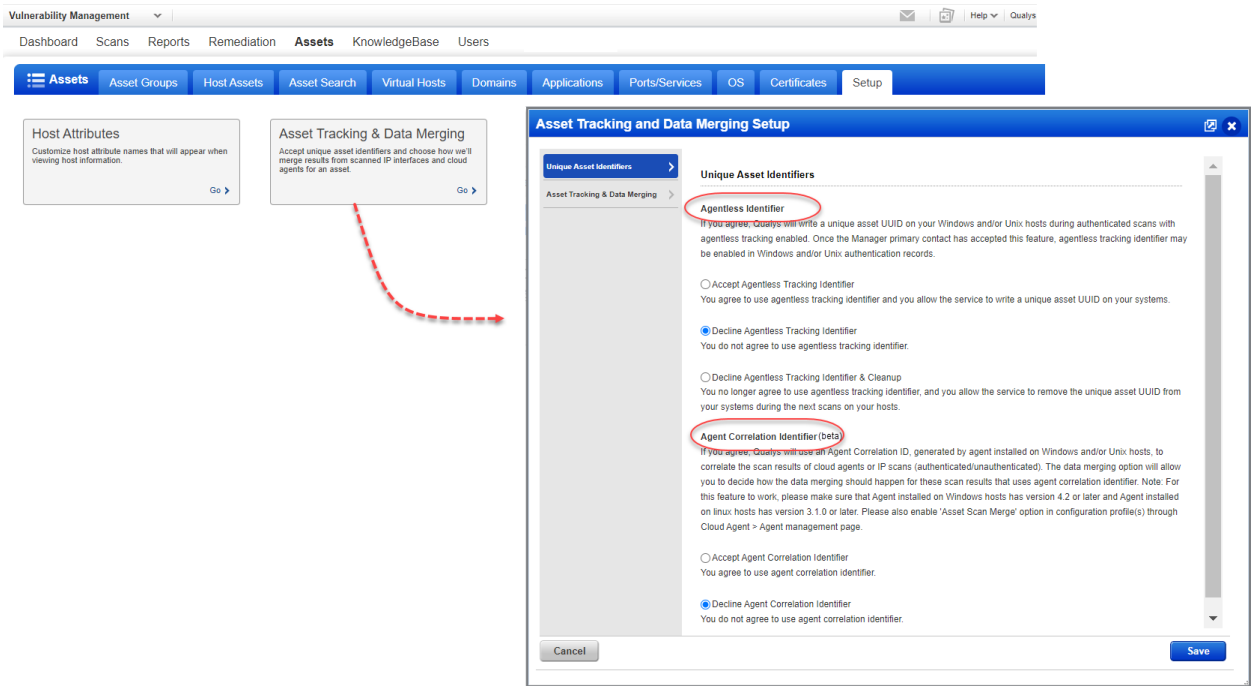
Qualys Vulnerability Management (VM)

New Agent Correlation Identifier (beta)

This release introduces a new Agent Correlation Identifier that allows you to merge *unauthenticated* and *authenticated* vulnerability scan results from scanned IP interfaces and agent VM scans for your cloud agent assets. The Agent Correlation Identifier is supported for VM only and is detected by QID 48143 "Qualys Correlation ID Detected". This new identifier is in addition to the existing Agentless Tracking Identifier (asset UUID), which allows you to merge *authenticated* scan results, and is supported for VM and PC.

When the Manager Primary Contact accepts this option for the subscription, this new identifier will also be used to identify the asset and merge scan results as per the selected merge option.

You'll see the new identifier option by going to **Assets** > **Setup** > **Asset Tracking and Data Merging**. In the Setup window, you'll notice that the tab Agentless Tracking Identifier has been renamed to **Unique Asset Identifiers** and you'll now have 2 options on this tab: **Agentless Identifier** (same as in previous releases) and **Agent Correlation Identifier** (new in this release).



Note that options on the Unique Asset Identifiers tab can only be enabled by the Manager Primary Contact for the subscription. Any Manager user can view and edit options on the Asset Tracking & Data Merging tab. The data merging options apply to both unique identifiers.

Prerequisites

- The Agent Correlation Identifier feature must be available on your Qualys Cloud Platform.
- Your agent hosts must have the minimum Cloud Agent version:
    - Windows Agent version 4.2 or later
    - Linux Agent version 3.1 or later

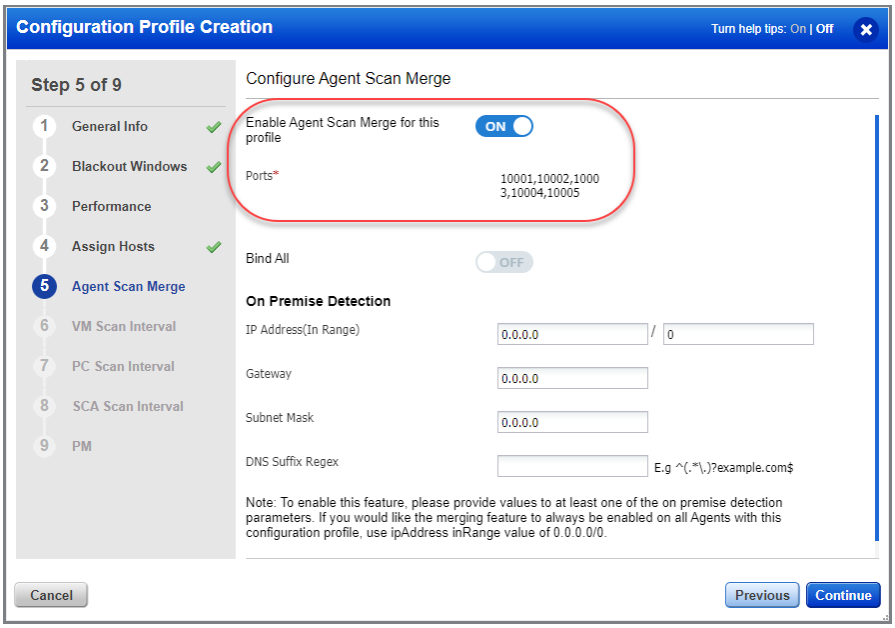
- The agent configuration profile must have the Agent Scan Merge option enabled. See steps below to learn how to enable this option in the Cloud Agent UI.
- The following TCP ports must not be blocked: 10001, 10002, 10003, 10004, 10005. These ports will be included in your vulnerability scans automatically when the agent correlation identifier option is accepted. We'll add these ports to the scanned ports list.
- Your vulnerability scans must include Information Gathered QID 48143 "Qualys Correlation ID Detected". A Full vulnerability scan will include this QID by default. If you run a custom scan using a search list, then you'll need to make sure this QID is included. Add the QID to a search list and add the search list to the scan option profile under Vulnerability Detection: Custom.

What are the steps?

Follow the steps below to start using the Agent Correlation Identifier.

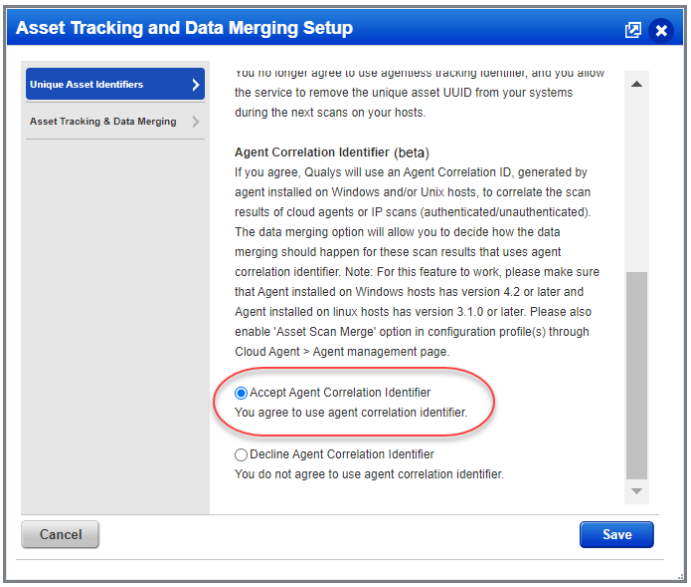
In Cloud Agent:

1) Toggle **On** the **Enable Agent Scan Merge for this profile** option in the configuration profile. Choose **Cloud Agent** from the app picker, then go to **Agent Management** > **Configuration Profiles**. Create a new profile (or edit an existing profile) and select this option.



In Vulnerability Management:

2) (Manager primary contact) Go to **Assets** > **Setup** > **Asset Tracking & Data Merging**. On the **Unique Asset Identifiers** tab, scroll down to **Agent Correlation Identifier** and select the option **Accept Agent Correlation Identifier**. Note that you can also accept Agentless Tracking Identifier on this tab, which was available in previous releases. The data merging options on the Asset Tracking & Data Merging tab apply to both unique identifiers.



3) Go to **Scans** > **Option Profiles**. Create a new option profile (or edit an existing profile) and make sure the scan is a Full scan or Custom scan with QID 48143 added.

4) Run new vulnerability scans to start gathering data for QID 48143.

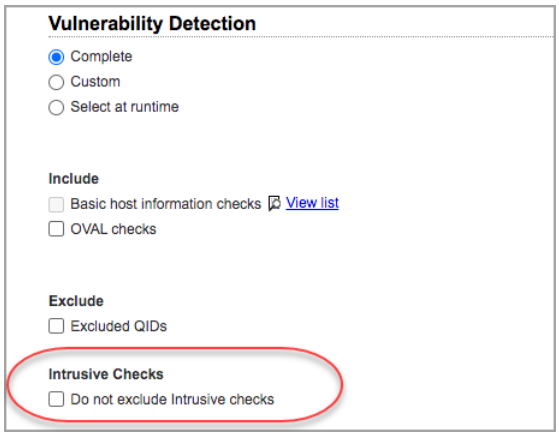
Introducing Intrusive QIDs

Our vulnerability signatures team will release new QIDs which are considered intrusive because these remote checks may cause harm or damage to a remote system. Some vulnerabilities can only be effectively detected by attempting to exploit the vulnerability. Qualys attempts to do this in a benign fashion, however we cannot guarantee this. These QIDs may leave the remote system in an unstable state.

All intrusive QIDs will be excluded from your scans automatically, even if you explicitly add them to a search list. This is to prevent the scanner from running QIDs against a remote system which could crash the remote system.

Want to scan an intrusive QID?

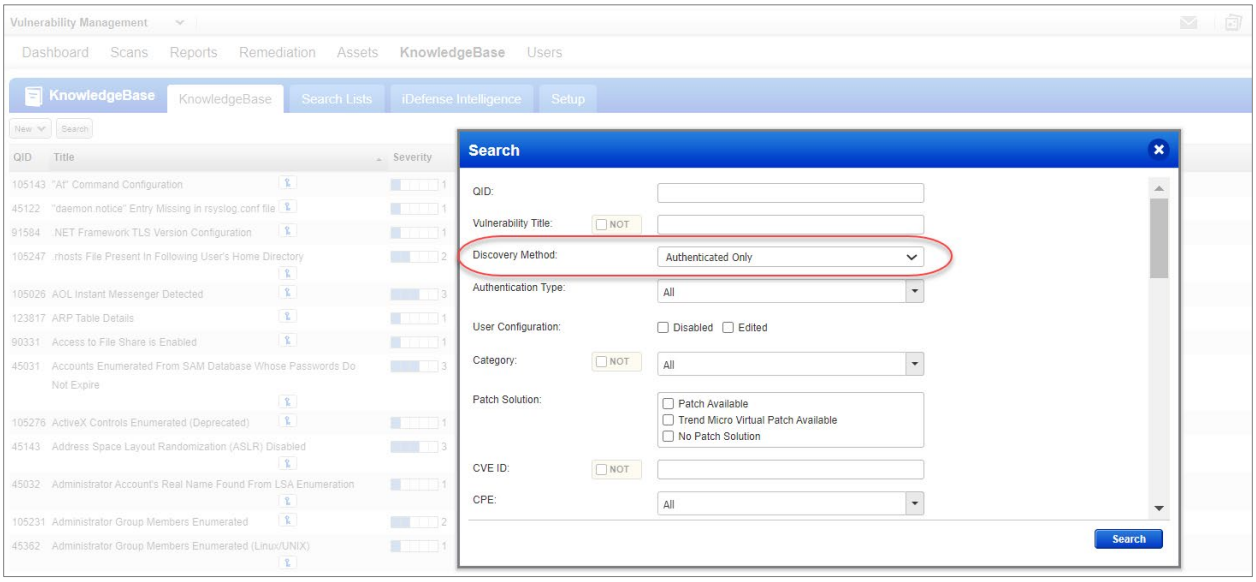
Intrusive QIDs will only be included in a scan if you select the new setting “Do not exclude Intrusive checks” in the scan option profile. Note that you will see a warning in the UI when this option is selected at the time you save the option profile. This will allow you to go back and change the setting if it was set unintentionally.



Change to Scan Results Processing for Authenticated Only Information Gathered QIDs

Certain Information Gathered QIDs require authentication or a cloud agent in order to be detected. Starting with this release, Information Gathered QIDs that require authentication will only be updated based on scan results from another authenticated scan or cloud agent scan. We will no longer update these QIDs when unauthenticated scan results are processed. Prior to this change, an authenticated only Information Gathered QID would be removed when an unauthenticated scan was processed because the unauthenticated scan could not detect it.

You can find Information Gathered QIDs that require authentication by searching the KnowledgeBase with **Discovery Method** set to **Authenticated Only**, as shown in the image below. You'll also want to pick the Information Gathered severity levels to include in the search.

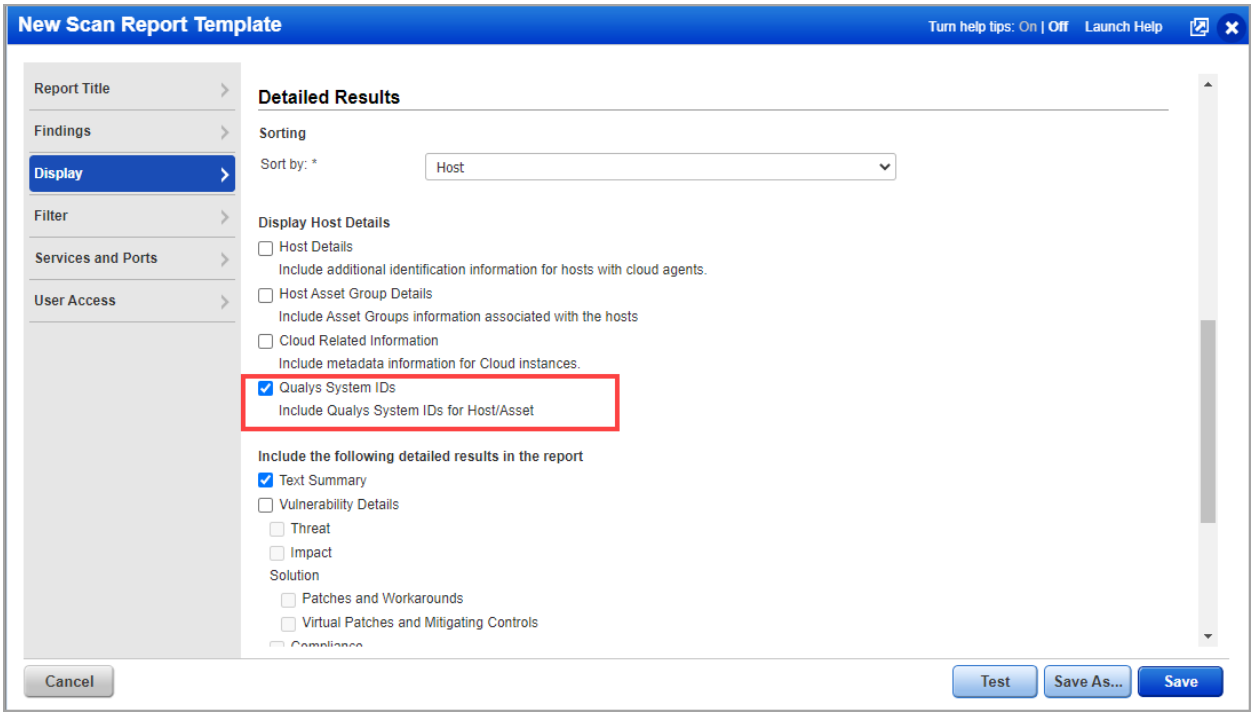


Host Identifiers in Host-Based Scan Report

We have now enhanced our scan report templates to include host identifiers such as host ID, asset ID in the host-based scan reports that you launch or download. We provide with an option to include or exclude asset/host ID details in scan report template. Once you enable the check box, the asset/host ID details are included in the scan report.

You can locate this option when you create a new scan report template or edit an existing scan report template. Go to Reports > Templates > New > Scan Template to create a new report template or edit an existing template.

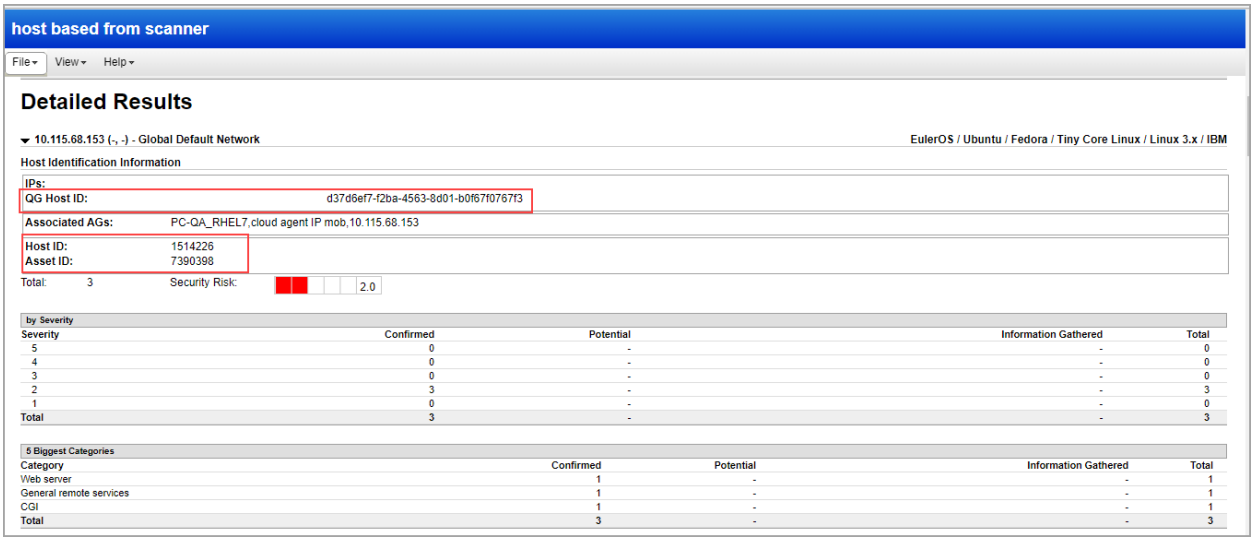
In the Display section of the left pane, under Display Host Details section, select Qualys System IDs checkbox.



When you enable the Qualys System IDs checkbox, the scan report includes the asset ID and host ID in the host-based scan report.

Note: We display the Qualys Host Id as QG Host ID (earlier: this was displayed as Asset ID) for reports in PDF, DOCX, HTML, MHT format to be consistent with reports in CSV, XML format.

Sample Report (HTML)



host based from scanner

File View Help

Detailed Results

10.115.68.153 (-, -) - Global Default Network — EulerOS / Ubuntu / Fedora / Tiny Core Linux / Linux 3.x / IBM

Host Identification Information

IPs:

QG Host ID: d37d6ef7-f2ba-4563-8d01-b0f67f0767f3

Associated AGs: PC-QA_RHEL7,cloud agent IP mob,10.115.68.153

Host ID: 1514226

Asset ID: 7390398

Total: 3 Security Risk: 2.0

by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	0	-	-	0
4	0	-	-	0
3	0	-	-	0
2	3	-	-	3
1	0	-	-	0
Total	3	-	-	3

5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
Web server	1	-	-	1
General remote services	1	-	-	1
CGI	1	-	-	1
Total	3	-	-	3

Sample Report (CSV)

Sample CSV	01/07/2021 at 17:42:34 (GMT+0530)												
Qualys Inc	919 E Hills	Foster City, CA	None										
John Doe	user_john	Manager											
Asset Group	IPs	Active H	Hosts	Trend Ana	Date Rang	Network	Asset Tags						
UM_New_A	NONE	2	1	Latest vul	01/01/199	Global De	NONE						
Total Vulner	Avg Secur	Business Risk											
196	3.4	23/100											
IP	Network	Total Vul	Security Risk										
10.115.68.15	Global De	196	3.4										
IP	Network	DNS	NetB	QG Host I	IP Interfac	Tracking M	OS	IP Status	QID	Title	Vuln Statu	Host ID	Asset ID
10.115.68.15	Global De	rhel7.0-unpatc		d37d6ef7-	10.115.68.	QAGENT	Red Hat Er	host scanr	236518	Red Hat U	Active	1350691	6227507
10.115.68.15	Global De	rhel7.0-unpatc		d37d6ef7-	10.115.68.	QAGENT	Red Hat Er	host scanr	238938	Red Hat U	Active	1350691	6227507
10.115.68.15	Global De	rhel7.0-unpatc		d37d6ef7-	10.115.68.	QAGENT	Red Hat Er	host scanr	238917	Red Hat U	Active	1350691	6227507
10.115.68.15	Global De	rhel7.0-unpatc		d37d6ef7-	10.115.68.	QAGENT	Red Hat Er	host scanr	238761	Red Hat U	Active	1350691	6227507
10.115.68.15	Global De	rhel7.0-unpatc		d37d6ef7-	10.115.68.	QAGENT	Red Hat Er	host scanr	238722	Red Hat U	Active	1350691	6227507
10.115.68.15	Global De	rhel7.0-unpatc		d37d6ef7-	10.115.68.	QAGENT	Red Hat Er	host scanr	238620	Red Hat U	Active	1350691	6227507
10.115.68.15	Global De	rhel7.0-unpatc		d37d6ef7-	10.115.68.	QAGENT	Red Hat Er	host scanr	238517	Red Hat U	Active	1350691	6227507
10.115.68.15	Global De	rhel7.0-unpatc		d37d6ef7-	10.115.68.	QAGENT	Red Hat Er	host scanr	238514	Red Hat U	Active	1350691	6227507

Issues Addressed

- We fixed an issue in the next launch date calculation for scheduled scans set to occur daily, weekly or monthly.
- We fixed an issue where the wrong Discovery Method was shown for VMware ESXi and vCenter QIDs in the Vulnerability KnowledgeBase.
- We fixed an issue where in certain cases the Certificates list (under VM/VMDR > Assets) was not loading.
- We fixed an issue where in certain cases the Applications list (under VM/VMDR > Assets) with the All asset group selected was resulting in an error when the list was downloaded to CSV format.