



# Qualys Cloud Platform (VM, PC) v10.x

## Release Notes

Version 10.2.1

August 4, 2020 (Updated August 14, 2020)

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

### **Qualys Policy Compliance (PC)**

[Dynamic Discovery & Assessment of Web Services via Cloud Agents](#)

**Qualys 10.2.1 brings you more improvements and updates! [Learn more](#)**

## Qualys Policy Compliance (PC)

### Dynamic Discovery & Assessment of Web Services via Cloud Agents

Qualys Policy Compliance now enables dynamic discovery and assessment of middleware technologies like web servers in your environment using PC agents. We provide you with two ways to quickly get started. You can either choose to enable all your agents to be activated for middleware assessment by default or you can have the assets listed in the Middleware Assets tab and activate it individually.

If you choose to enable by default, it will take away your need to monitor the asset list and then activate the asset. As soon as supported technology instances are discovered on the assets, they will be activated for assessment. As a part of activation process Middleware manifest will be installed on your agent.

In case you choose to activate the asset individually, the manifest is installed on the agent once you choose to activate the asset for assessment.

For assessment of middleware technologies minimum agent version installed must be:

- Windows Cloud Agent 4.0.x or later
- Linux Cloud Agent 2.8.x or later

The following middleware technologies are supported:

#### Linux Agent 2.8.x

Apache Tomcat 7.x  
Apache Tomcat 8.x  
Apache Tomcat 9.x  
Pivotal tc Server 3.x  
vFabric tc Server 2.9.x  
Docker 1.x  
Docker CE/EE

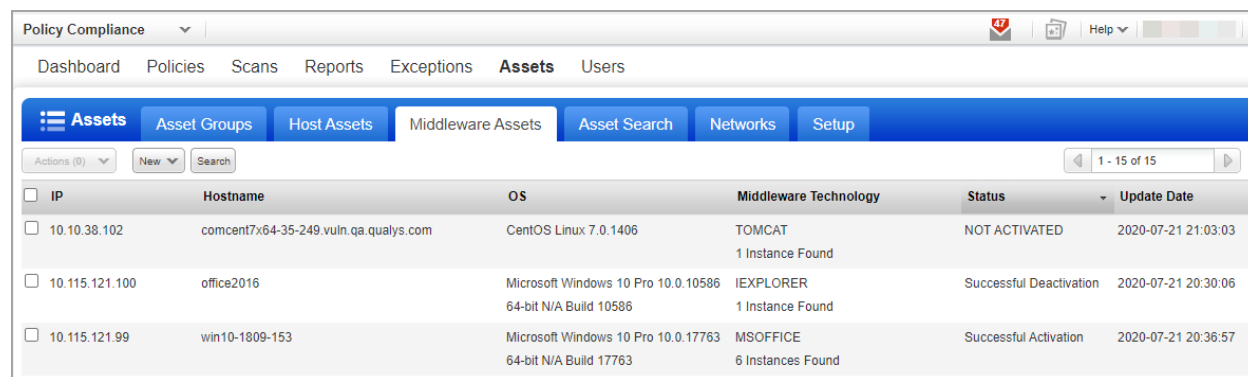
#### Windows Agent 4.0.x

Apache Tomcat 7.x  
Apache Tomcat 8.x  
Apache Tomcat 9.x  
MS IIS 10.x  
MS IIS 8.x  
MS IIS 7.x

### To Get Started

#### Identify Middleware Assets

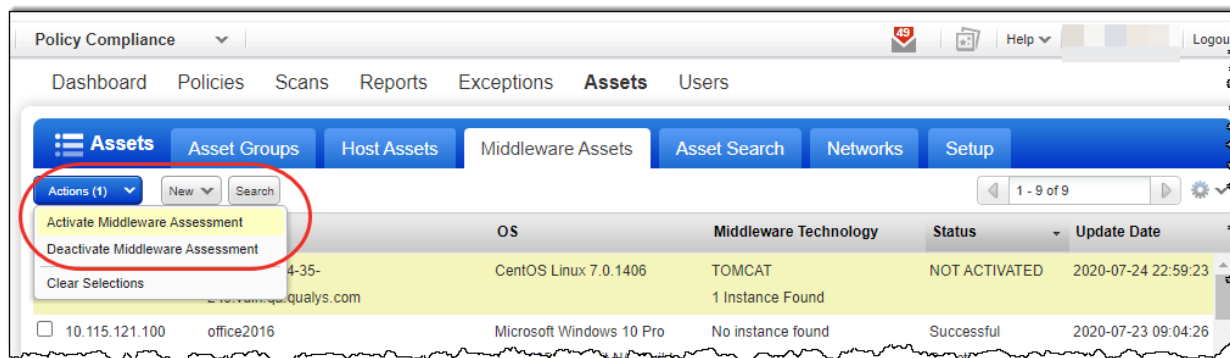
Set up Cloud Agent on the assets you want to scan for assessment of middleware technologies. Once the assets are scanned by the agents the middleware technology details of assets are listed in the Middleware Assets tab.



| Policy Compliance  |                |                                       |   |                               |                         |                     |
|--|----------------|---------------------------------------|---|-------------------------------|-------------------------|---------------------|
| Dashboard Policies Scans Reports Exceptions <b>Assets</b> Users                      |                |                                       |   |                               |                         |                     |
| Assets Asset Groups Host Assets <b>Middleware Assets</b> Asset Search Networks Setup |                |                                       |   |                               |                         |                     |
| Actions (0) New Search 1 - 15 of 15  |                |                                       |   |                               |                         |                     |
| <input type="checkbox"/>   | IP             | Hostname                              | OS  | Middleware Technology         | Status                  | Update Date         |
| <input type="checkbox"/>   | 10.10.38.102   | comcent7x64-35-249.vuln.qa.qualys.com | CentOS Linux 7.0.1406   | TOMCAT<br>1 Instance Found    | NOT ACTIVATED           | 2020-07-21 21:03:03 |
| <input type="checkbox"/>   | 10.115.121.100 | office2016                            | Microsoft Windows 10 Pro 10.0.10586<br>64-bit N/A Build 10586 | IEXPLORER<br>1 Instance Found | Successful Deactivation | 2020-07-21 20:30:06 |
| <input type="checkbox"/>   | 10.115.121.99  | win10-1809-153                        | Microsoft Windows 10 Pro 10.0.17763<br>64-bit N/A Build 17763 | MSOFFICE<br>6 Instances Found | Successful Activation   | 2020-07-21 20:36:57 |

## Activate Assets for Middleware Assessment

When a technology is identified by agent for first time on an asset, it is listed as Not Activated. To activate the asset, select the asset and from the Action menu choose Activate Middleware Assessment.

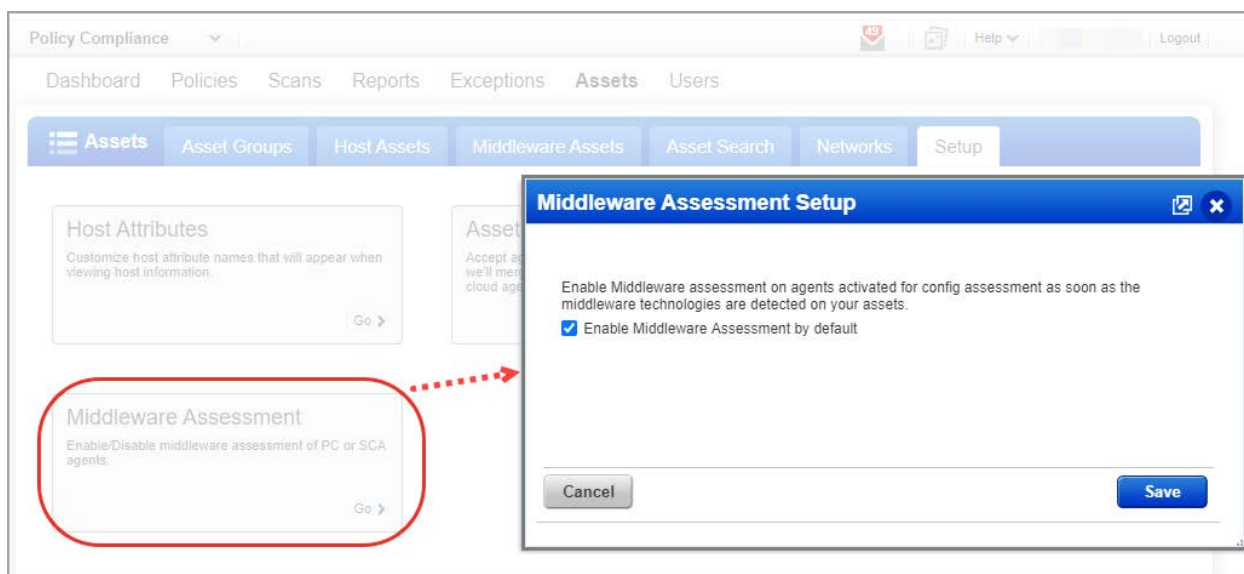


Once the asset is activated you can create policies and run compliance reports on these assets for the middleware technologies.

Similarly, you can deactivate an asset for assessment using the Deactivate Middleware Assessment option. Once deactivated, the data for technologies on assets will no longer be assessed and will not be displayed in the policy compliance report. However, data collected before deactivation can still be viewed in the report.

## Activate Assessment on Assets by Default

You can set the assets to be activated for assessment by default as soon as they are discovered. Navigate to Assets > Setup, click Middleware Assessment and select the Enable Middleware Assessment by default option.



## Issues Addressed

- Fixed an issue in the PC Scorecard Report for subscriptions with PC and SCA. There was an issue where the report did not show data for IP addresses that are in the SCA license but not in the PC license.
- Now we'll hide Oracle System Record Templates (and related options) in the UI and API in subscriptions that previously had PC but now PC is disabled. This template is only supported in accounts with PC/SCA.
- Fixed a minor typo on the Policy Report Template Information page.
- The USERNAME tag under HEADER in the asset\_data\_report DTD is now optional since the username doesn't always appear in the report.
- Fixed an issue where at times a custom severity level assigned to a QID was not showing correctly in the output for Host List Detection API.
- Updated the help to provide more information for the 4 data merging options under Assets > Setup > Asset Tracking & Data Merging.
- Added a new Authentication Technologies Matrix to the help to list VM/PC support for each authentication technology and details like whether Auto Discovery and Vaults are supported.
- Updated the Subscription Info API user guide to remove the INFO key user\_report\_quota\_usage since this key does not appear in the output when you export user preferences.
- The description for target type field in the login credentials for Unix authentication records is now updated in all relevant documents to mention that Auto is the default target type and more target types will be displayed in the list as they are made available.