Qualys 8.9.2 Release Notes

This new release of the Qualys Cloud Suite of Security and Compliance Applications includes improvements to Vulnerability Management and Policy Compliance.

Qualys Cloud Platform

EC2 Scanning Improvements

Qualys Policy Compliance (PC/SCAP)

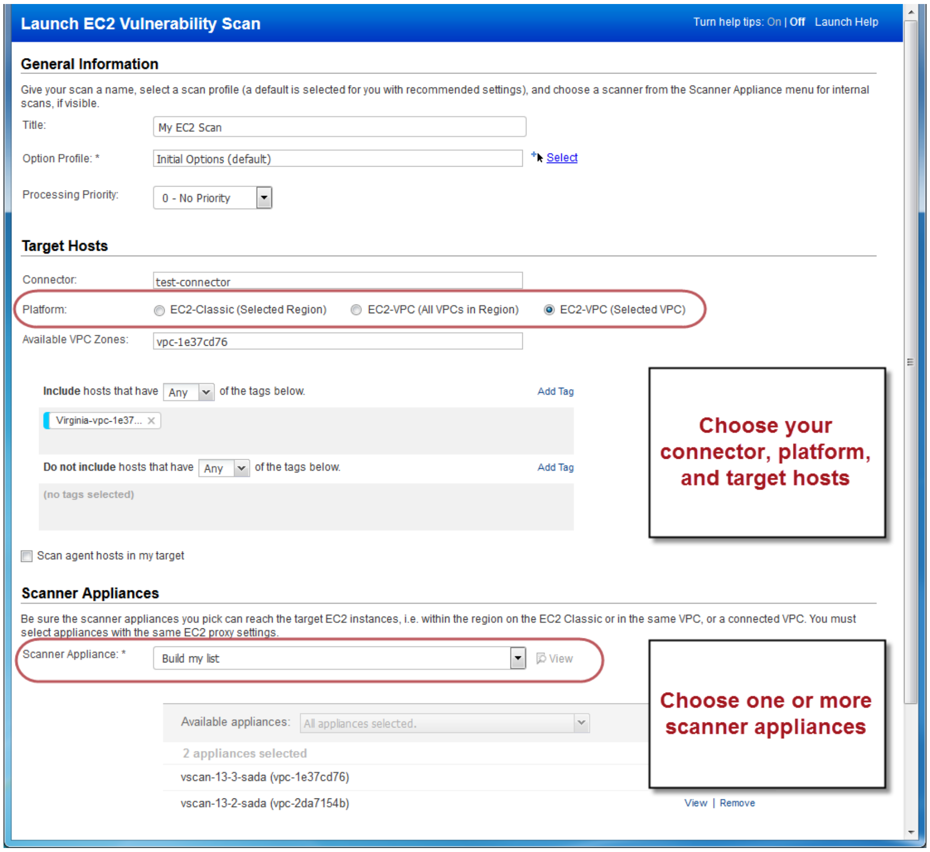
Microsoft SQL Server 2016 Support

Qualys 8.9.2 brings you many more Improvements and updates! Learn more

Qualys Cloud Platform

EC2 Scanning Improvements

When launching or scheduling EC2 scans you'll see a few changes to your scan options. A new Platform option lets you scan all the VPCs in a particular region. Also, you can now distribute your scan across multiple scanner appliances, so your scans will run faster. These options are supported for vulnerability scans and compliance scans. They're available using the UI only at this time.



Launch EC2 Vulnerability Scan

General Information

Give your scan a name, select a scan profile (a default is selected for you with recommended settings), and choose a scanner from the Scanner Appliance menu for internal scans, if visible.

Title: My EC2 Scan

Option Profile: * Initial Options (default) Select

Processing Priority: 0 - No Priority

Target Hosts

Connector: test-connector

Platform: ○ EC2-Classic (Selected Region) ○ EC2-VPC (All VPCs in Region) ● EC2-VPC (Selected VPC)

Available VPC Zones: vpc-1e37cd76

Include hosts that have Any of the tags below. Add Tag

Virginia-vpc-1e37... ×

Do not include hosts that have Any of the tags below. Add Tag

(no tags selected)

□ Scan agent hosts in my target

Scanner Appliances

Be sure the scanner appliances you pick can reach the target EC2 instances, i.e. within the region on the EC2 Classic or in the same VPC, or a connected VPC. You must select appliances with the same EC2 proxy settings.

Scanner Appliance: * Build my list View

Available appliances: All appliances selected.

2 appliances selected

vscan-13-3-sada (vpc-1e37cd76)

vscan-13-2-sada (vpc-2da7154b) View | Remove

Choose your connector, platform, and target hosts

Choose one or more scanner appliances

You now have 3 options for identifying the target platform and region/VPC.

EC2-Classic (Selected Region)
Scan EC2 classic hosts in a particular region. You'll notice that we removed the option "Only scan EC2 Classic Hosts in the region" because this is now the default behavior when EC2-Classic is selected.

EC2-VPC (All VPCs in Region)
Scan all of the VPCs in a particular region. Select this option ONLY if there is peering between all the VPCs in the region, or you could end up with Host not found errors for those instances where scanners cannot reach them.

EC2-VPC (Selected VPC)
Scan only the selected VPC.

Choose build my list to distribute your scan to a list of scanner appliances.

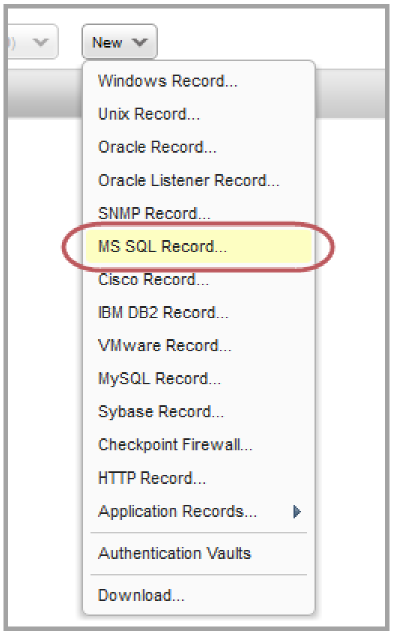
What do I need to know about building a list?
- You can choose appliances with a Connected status.
- Appliances must be able to reach hosts in the region or VPC
- Appliances must have the same EC2 proxy settings

Qualys Policy Compliance (PC)

Microsoft SQL Server 2016 Support

We’ve extended our support for MS SQL Server authentication to include Microsoft SQL Server 2016. These technologies are already supported: Microsoft SQL Server 2000, 2005, 2008, 2012 and 2014.

You’ll need a MS SQL Server record to authenticate to your Microsoft SQL Server 2016 database, and scan it for compliance.



How do I get started?

Go to Scans > Authentication, and choose New > MS SQL Record (as shown on the right). This authentication type is supported for compliance scans only.

Issues Addressed

- Fixed an issue in map results (graphic mode) where users were not able to add a large number of IPs from the map to a new or existing asset group.
- Fixed an issue where in some cases users were not able to change the host tracking method from IP address to NetBIOS hostname.
- Fixed an issue related to the filters on the Host Assets list (Assets > Host Assets). The filters “Cloud Agent Tracked Hosts” and “EC2 Tracked Hosts” were not returning the correct results.
- We will now correctly display user-provided comments in the Comments column on the Host Assets list.
- Improved performance while loading assets on the Host Assets list.
- When a report is generated with asset groups, the <HOST> section of <HOST_LIST> tag in XML scan report now correctly filters out CVSS tags based on template settings.
- The CVSS filter is no longer shown in the scan report template when CVSS scoring is disabled.
- CVSS environment text is now displayed correctly without any overlaps in the HTML, DOCX and MHT reports.
- We will no longer truncate long asset tag names displayed in your vulnerability scan reports. This fix applies to all report formats: CSV, PDF, HTML, DOCX.
- For scan reports in CSV format, we will now truncate data in a cell when it exceeds the cell-limit imposed by Microsoft Excel.
- Fixed vulnerabilities are now shown in CSV reports when trend is enabled in the scan report template and user selected Fixed vulnerabilities are enabled in the template.
- For vulnerability scan reports in CSV format, we fixed an issue that was causing some CSV reports to get stuck and not complete.
- For vulnerability scan reports, we will now show QID 38175 (Unauthorized Service Detected) and QID 82043 (Unauthorized Open Port Detected) in all report formats, when appropriate. These QIDs are reported when we detect services/ports that are flagged as unauthorized in your scan report template.
- Fixed a calculation error while plotting points on the “Vulnerability distribution by status” graph in VM Scorecard Reports with a certain set of vulnerability status counts.
- Made a fix to the CSS for HTML reports (VM and PC) to remove an extra horizontal line that was appearing in reports.
- Fixed a spelling error in the Compliance Scorecard Report Template.
- Users will no longer get an error when launching EC2 vulnerability scans with an option profile that has the “Select at runtime” vulnerability detection option enabled.
- The Scanner Capacity graph under General Information on the Scanner Appliance Information page is now displayed properly.
- When you perform a search on the Appliances list (Scans > Appliances) the default setting for Network was changed from “Global Default Network” to “All”.
- We now provide an option to set a date for the remediation tickets to be reopened for Ignored vulnerabilities from asset search page.

- We have fixed an issue and you can now successfully generate scan reports using the Scan based report template with Unit Manager.
- The Processing Priority scan option is supported for vulnerability scans only. We fixed an issue in the UI where the Processing Priority option appeared when scheduling compliance scans and we removed the Processing Priority column from the PC Scans data list.
- Fixed an issue where users could not start policy evaluation for locked policies using the Evaluate Now option. Also asset tags added to the locked policy were not being saved.
- Fixed an issue with compliance scan processing where completed scans were not being processed. Scans were stuck in Queued state.
- Fixed an issue where authentication record details were not being displayed when the Details link was clicked on the Authentication list.
- We've fixed issues with editing IPs in the Unix authentication record. Now if a user tries to add IPs already part of other Unix records, the user can close the error message and choose the remove option if needed.
- You'll now see an Error message when adding IPs to an authentication record and those IPs are not in your account.
- We have now removed the incorrect entry of "appliance added=[1]" from the Activity logs.
- We have now fixed the issue where GUI and API permission settings were being reset intermittently. You can now successfully create, activate new users and sub-users.
- You can now share your PCI scans even if API is enabled for the subscription and is expired.
- Qualys Express users will no longer see a blank page in place of their Home page after logging in to the Qualys GUI.
- Fixed an issue where Information Gathered QIDs were not being included in the output of the Host List Detection API v2 (resource /api/2.0/fo/asset/host/vm/detection/ with parameter action=list).
- Updated the Host List Detection API samples in the API v2 User Guide.
- Under Users > Setup > VeriSign Identity Protection (VIP) we updated the screen text to more clearly communicate that VIP two-factor authentication applies to UI access only, when logging into the Qualys GUI. It does not apply to API calls.
- Updated the API User Guides to clarify that users with VIP two-factor authentication enabled can use their accounts to access the API, however two-factor authentication will not be used when making API requests. Two-factor authentication is only supported when logging into the Qualys GUI.
- Made correction to the List Vendors and References section of the API V2 User Guide. Possible values for the action parameter are action=list_vendors and action=list_vendor_references.
- Updated the API V2 User Guide to rectify misspellings in the XPaths.
- Help is now updated to clarify distribution group permissions and we have also added information about the owner of a scheduled scan.
- Updated the View Host Information help file to clarify that the First Found date indicates when the host was first successfully scanned in VM or PC.

- Added a new help topic Vulnerability Status Levels to describe New, Active, Fixed and Re-Opened status.