Qualys Cloud Platform (VM, PC) v10.x

Release Notes

Version 10.12

June 24, 2021 (Updated on July 6, 2021)

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

Qualys Vulnerability Management (VM)

Automated Updates to QID Change Logs

Closed/Ignored Tickets Automatically Updated as Closed/Fixed After Fix

Qualys Policy Compliance (PC/SCAP/SCA)

MS SQL Server Authentication Now Supported for Unix

Qualys 10.12 brings you more improvements and updates! Learn more

Qualys Vulnerability Management (VM)

Automated Updates to QID Change Logs

The QID change log has been enhanced in this release to show customers more updates. Currently, the change log includes log entries when there's a change to the detection logic. Now the change log will also include log entries when key values change, including linked exploits, the addition or removal from RTI lists, and signature code changes. This will give customers a more complete view into how a QID has been modified. Please note that only QID changes made after this release will result in new change log entries.

Qualys tracks many variables related to each vulnerability signature, and change log entries will be automatically created whenever risk-relevant fields are modified:

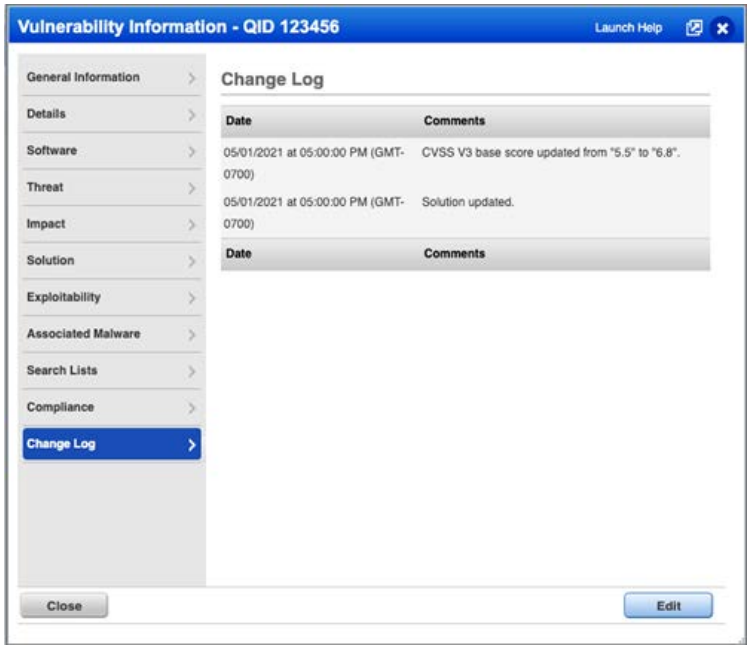
- Addition or removal from RTI lists
- Severity
- CVSS scores
- Title
- Solution
- Linked CVEs
- Linked exploits
- PCI flag
- Remote flag
- Authentication types

Changes to other components such as detection logic can also be recorded by the Vulnerability Signatures team. For each change, you will see the date of the change and comments provided by the team. The modified date for a QID would change if there is a change in one of the fields for a QID in the KnowledgeBase. For example, if the severity of a QID was updated.

How to view change logs

Go to the **KnowledgeBase** and choose **Info** or **Edit** for any QID. Then go to the **Change Log** section to see the change log entries. Please note that only changes made by Qualys will be included in the change log. This section will not include changes made by users.

Note that you can also get change log information when you download a list of vulnerabilities using the KnowledgeBase API.



Closed/Ignored Tickets Automatically Updated as Closed/Fixed After Fix

Starting in this release, a remediation ticket will directly move from Closed/Ignored state to Closed/Fixed state when the vulnerability associated with the ticket is remediated and the fix is verified by a scan. In previous releases, a ticket that was in Closed/Ignored state had to first be reopened (either automatically or manually) before it could be verified as fixed and moved to Closed/Fixed state. With this change, we save you the effort of having to first reopen ignored tickets. You still have the option to reopen tickets, in case your workflow requires it.

Qualys Policy Compliance (PC/SCAP/SCA)

MS SQL Server Authentication Now Supported for Unix

We're expanding MS SQL Server authentication support to allow authentication to MS SQL Server database accounts on Unix hosts. We already support this type of authentication on Windows hosts. You'll see new options in the MS SQL Server authentication record for identifying the OS authentication type (Windows or Unix) and for specifying the Unix instance directory path and Unix configuration file path on your Unix hosts. MS SQL Server authentication is supported for compliance scans only.

Good to Know

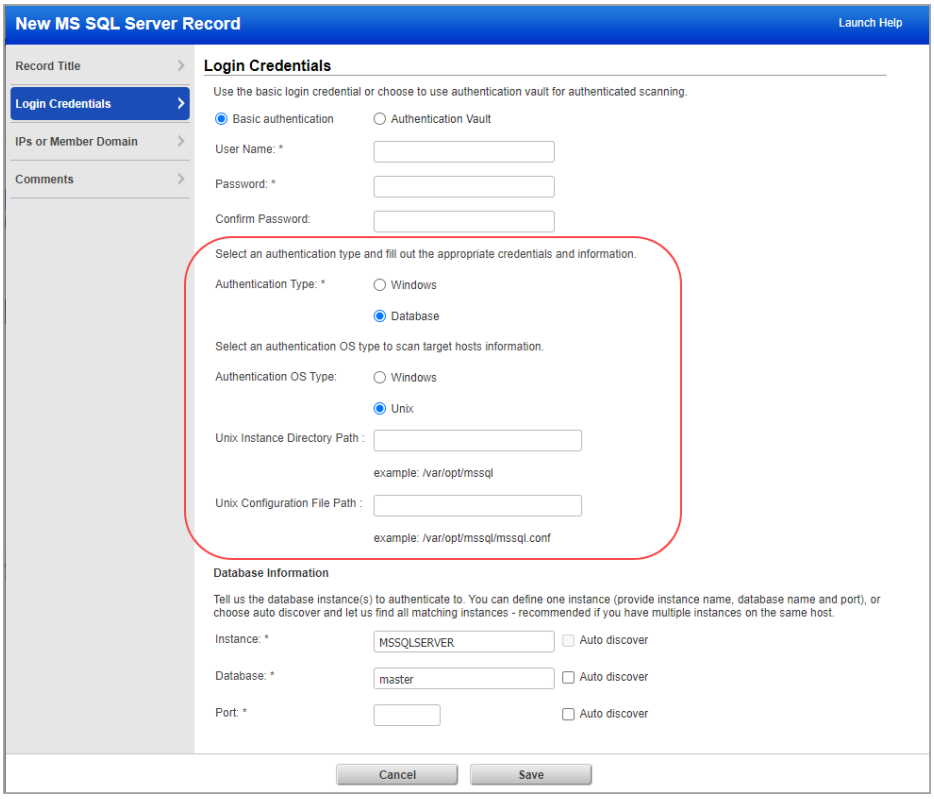
- We support these MS SQL technologies for Unix: MS SQL Server 2017 and MS SQL Server 2019

- Certain fields in MS SQL records only apply to the Windows OS type and not the Unix OS type, including Domain, Member Domain and Authentication Protocols (Kerberos, NTLMv2, NTLMv1)

- For Unix, we support Auto discover options for Database and Port. You are required to provide the Instance name. If you select Auto discover for Port, then Unix authentication is also required. Make sure the IPs assigned to the MS SQL record are also configured for a Unix record.

Updates to the MS SQL Server Record

You'll see new options in the MS SQL Server authentication record. When Database is selected for the Authentication Type, then you'll also need to pick the Authentication OS Type: Windows or Unix. When you pick Unix, you'll see additional fields for entering the path to the MS SQL Server instance directory on your Unix hosts and the path to the MS SQL Server configuration file on your Unix hosts. Please refer to the online help for help configuring your record.



Issues Addressed

- Fixed an issue where changes made to the Summary section of the Consultant Report template were not being saved.
- Fixed an issue where the database compliance scan data was getting overwritten by agent scan.
- Fixed an issue that occurred when trying to run a Policy report on an instance string that has more than 64 characters.
- Fixed an issue where you could not choose to include “any” or “all” of the selected tags in the edit section of SCA and PC policy.
- Fixed an issue where the Compliance Option Profile had duplicate entries for SAP IQ Database Check.