



Qualys Cloud Platform (VM, PC) 10.x

Release Notes

Version 10.22.1

April 27, 2023

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

Qualys Cloud Platform

- [Password Never Expires for API Access](#)
- [Kerberos Authentication in Unix Authentication Records](#)
- [View CPU, Memory, and Region Information of Scanners](#)
- [Allow Only Primary Contact User to Access the Primary Contact Setting](#)
- [Auto Enablement of Preferences for VM and VMDR Subscriptions](#)
- [Qualys Knowledgebase: QIDs Change Log Consolidation](#)

Qualys Policy Compliance (PC/SCAP/SCA)

- [Support UDCs for Scanner on Mac OS X 12.x and 13.x](#)
- [Support New UDC Type for Agent on Ubuntu 18.x/20.x/22.x and RHEL 9.x](#)
- [Limit Posture Indexing](#)
- [Evaluate Script Result UDC only During Agent Scan](#)

Qualys 10.22.1 brings you many more improvements and updates! [Learn more](#)

What's New?

Password Never Expires for API Access

APIs are commonly used to integrate the Qualys platform with external tools and applications. To achieve this, API-only access accounts are often created.

Organizational security policies require that account passwords be set to expire periodically. This can be problematic for API accounts that are not monitored regularly, as it is difficult to know when a password has expired until the integration is broken.

To address this challenge, you can now set the password of API-only access accounts to never expire. The password of such accounts will never expire unless a password change request is initiated through the UI or the password change API.

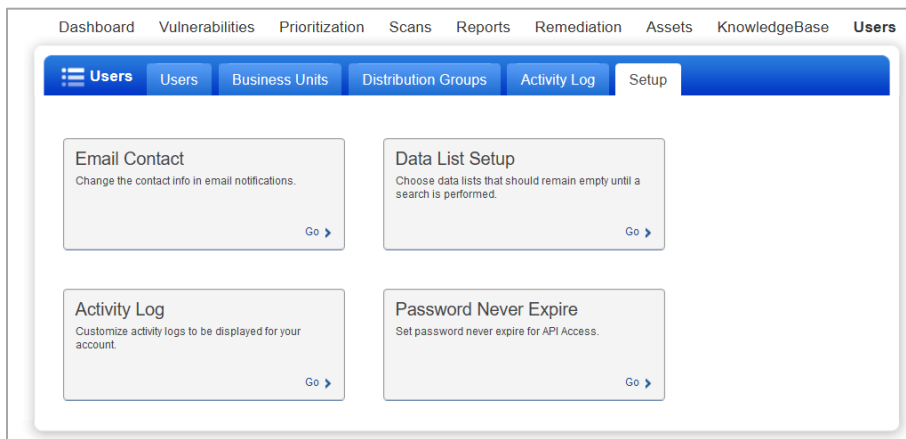
This may pose a security risk and you must accept an agreement acknowledging and accepting the risk to activate this feature. As per the organizational password security standards, Qualys recommends that account owners change the account password periodically. You can decline this agreement and opt out of this feature at any time.

Note: You must be a Manager POC user to access this feature.

How to activate this feature?

To activate this feature for your subscription, perform the following steps:

1. Contact your Technical Account Manager or Qualys support to activate this feature for your subscription.
2. After the activation, navigate to **Users > Setup**, and click **Password Never Expires**.



3. Read and accept the agreement detailing the associated security risk.
4. In the **Users** tab, edit the user account with API-only access.

- In the **Security** tab of the **Edit User** dialog box, under **Password Never Expires for API Access**, select the **Set the password of this account to “Never Expire”** check box.

The screenshot shows the 'Edit User' dialog box with the 'Security' tab selected. The 'Password Never Expire - API Access' section is highlighted with a red box, showing a checkbox that is currently unchecked. The checkbox text reads: 'Password for this account will never expire, unless a password change request is initiated via the Qualys UI or via the Qualys user password change API'. Other sections visible include 'Symantec™ VIP (Validation and ID Protection)' and 'Password'.

Kerberos Authentication in Unix Authentication Records

Kerberos is a network authentication protocol designed to provide secure and encrypted authentication for your systems and services.

You can now create Unix records with Kerberos authentication details and thus perform authenticated scans on Unix systems that have Kerberos (GSSAPI) enabled.

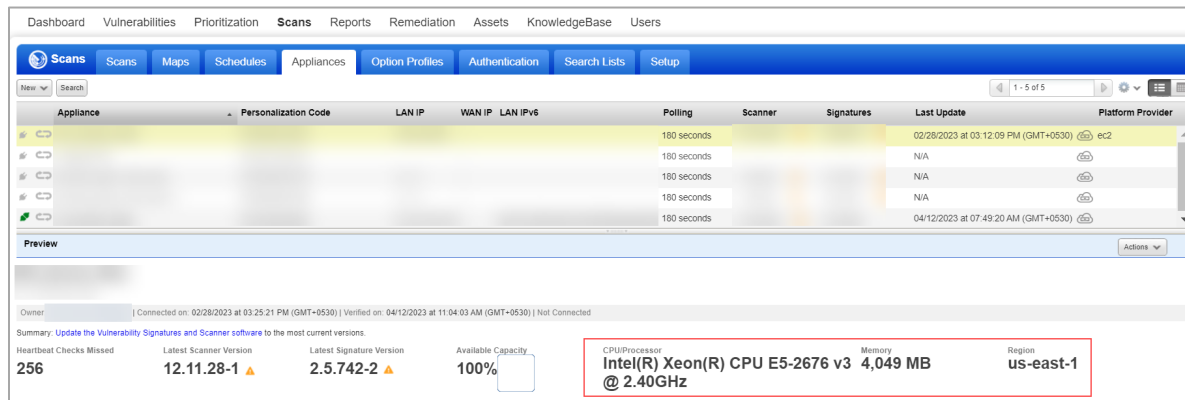
The screenshot shows the 'New Unix Record' dialog box with the 'Kerberos / GSSAPI' tab selected. The 'Use Kerberos' checkbox is checked (YES). The 'Authentication Type' is set to 'Basic'. Other fields include 'Realm Discovery' (Manual), 'User Realm *', 'User KDC', 'Service Realm', 'Service KDC', 'Password*', and 'Confirm Password*'. The 'Create' button is highlighted in blue.

For more information, see [Set Up Unix Authentication](#).

View CPU, Memory, and Region Information of Scanners

You can now view the CPU, memory, and region information of a scanner appliance in the appliance preview. This information helps you know the configuration and capacity of your scanner appliance and ensure the appliance is operating at its optimal level.

Note: To enable this feature for your subscription, contact your Technical Account Manager or Qualys support.



The screenshot displays the Qualys Scans interface. At the top, there are navigation tabs: Dashboard, Vulnerabilities, Prioritization, Scans, Reports, Remediation, Assets, KnowledgeBase, and Users. Below these are sub-tabs for Scans, Maps, Schedules, Appliances, Option Profiles, Authentication, Search Lists, and Setup. A table lists scanner appliances with columns for Appliance, Personalization Code, LAN IP, WAN IP, LAN IPv6, Polling, Scanner, Signatures, Last Update, and Platform Provider. Below the table is a 'Preview' section for a selected appliance, showing connection status and a summary of updates. A red box highlights the hardware specifications: CPU (Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.40GHz), Memory (4,049 MB), and Region (us-east-1).

Appliance	Personalization Code	LAN IP	WAN IP	LAN IPv6	Polling	Scanner	Signatures	Last Update	Platform Provider
					180 seconds			02/28/2023 at 03:12:09 PM (GMT+0530)	ec2
					180 seconds			N/A	
					180 seconds			N/A	
					180 seconds			N/A	
					180 seconds			04/12/2023 at 07:49:20 AM (GMT+0530)	

Preview

Owner: | Connected on: 02/28/2023 at 03:25:21 PM (GMT+0530) | Verified on: 04/12/2023 at 11:04:03 AM (GMT+0530) | Not Connected

Summary: Update the Vulnerability Signatures and Scanner software to the most current versions.

Heartbeat Checks Missed	Latest Scanner Version	Latest Signature Version	Available Capacity	CPU/Processor	Memory	Region
256	12.11.28-1 ▲	2.5.742-2 ▲	100%	Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.40GHz	4,049 MB	us-east-1

Allow Only Primary Contact User to Access and Edit the Primary Contact Setting

Starting this release, you have an option to let only a Primary Contact (POC) user assign a new Primary Contact. Once enabled, the following permissions are applied:

- Only the Primary Contact user can access the Primary Contact setting.
- If a manager user is not a primary contact, then they cannot view/edit the Primary Contact setting.

Contact your Technical Account Manager or Qualys Support to enable this feature for your subscription. If you do not opt for this feature, all Manager users are able to access the Primary Contact setting.

Auto Enablement of Preferences for VM and VMDR Subscriptions

Starting this release, new VM and VMDR subscriptions (Lite, Express, Enterprise, Community Edition, Consultant subscriptions, etc.) have the following four features enabled:

- **QID Data Services (QIDS)**

The Qualys KnowledgeBase (KB) comprises around 100K QIDs for vulnerability detections related to Infrastructure, Cloud, Web Application Scan (WAS), VMDT OT, VMDR for Mobile, etc. With these expansions, sometimes slowness is experienced in the Qualys KnowledgeBase (KB) GUI and KB APIs.

To resolve the slowness, Qualys is introducing QID Data Services (QIDS). This new dedicated microservice offers significant performance improvements for Qualys KnowledgeBase UI/API, VM Detection API, and the VM Scan Processing workflows.

Note: QIDS is default enabled and does not require any further activation.

- **Enable Close Vulnerabilities on Dead Hosts Setting**

Enable this Option Profile setting to close vulnerabilities or related tickets for hosts that are not found alive after a predefined number of scans. Navigate to **Scans -> Option Profiles** to enable/disable.

Here is an article about it – [Best Practice Subscription Maintenance: Opt-In Vulnerability Management Asset Housekeeping Subscription Support Options](#).

- **Enable Purge Old Host Data When OS is Changed Setting**

Enable this Option Profile setting to purge old host data when there is a significant change in the host OS vendor. In environments where a major OS change is detected (Windows to Linux etc.), enabling this option will purge and permanently remove the older host information. This prevents stale host data from being reported and saves any discrepancies.

Navigate to **Scans -> Option Profiles** to enable/disable.

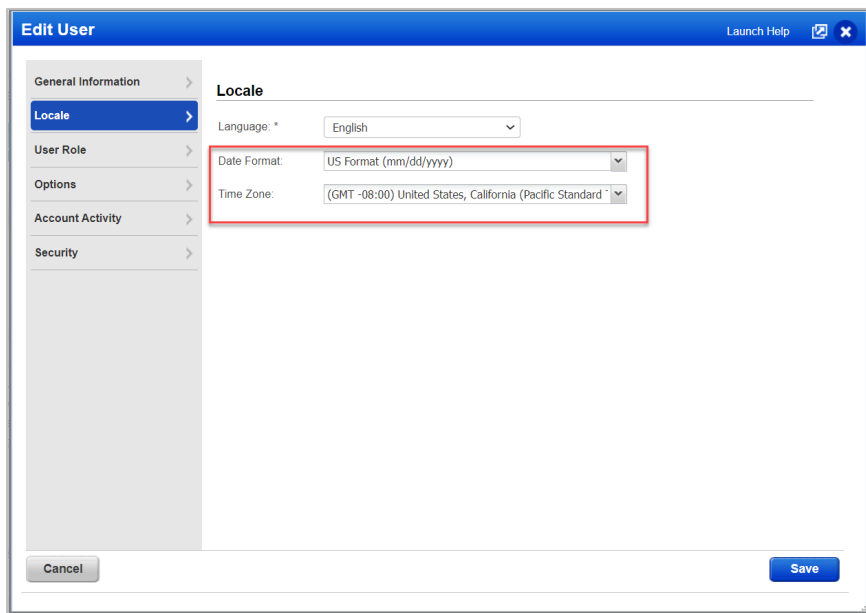
Find help for this setting [here](#). If you face any discrepancy in host data after setting **Purge old host data when OS is changed** in Option Profile, read this [article](#).

Note: Recommend this setting to be enabled only for the default Option Profile, where the required authentication record settings are enabled.

The screenshot shows a configuration page for an Option Profile. The 'Scan Dead Hosts' section has a checkbox for 'Include dead hosts in scans' which is unchecked. Below it, the 'Close Vulnerabilities on Dead Hosts' section is highlighted with a red box; it contains a checkbox for 'Close vulnerabilities when host is not found alive' (unchecked) and a text input field set to '3' times. The 'Purge old host data when OS is changed' section also has an unchecked checkbox. The 'Performance' section shows 'Overall Performance: Normal' with a 'Configure...' button. The 'Load Balancer Detection' section has an unchecked checkbox for 'Search for load balancers during scan'. The 'Password Brute Forcing' section is partially visible at the bottom.

- **Enable Date Format**

You can select your preference for Date & Time format from the User Account, **Locale-> Date Format**.



This Date & Time display format is then reflected in the UI and Reports. The supported Report formats for the Date Format setting are HTML, PDF, and DOC.

Qualys Knowledgebase: QIDs Change Log Consolidation

We have started publishing the QID change logs for 13 fields from June 2021. We also track the change dates in two date fields KB modified date and RTI modified date. The “service modified date” is using QID “insert date” and “modified date” instead of KB modified date and RTI modified date. We do not update QID “modified date” for all the 13 fields we are tracking as part of the change log.

To avoid the data discrepancy which is observed in the “service modified date” and “change log date,” we will update the QID Modified (Service Modified) date for 13 fields, and any future changes in these fields will capture the Service Modified field. This will accurately capture the QID-related fields that we are tracking as part of the change logs, and the customers will not see the mismatch between the change log date and the service modified date.

For more information refer: [Qualys Knowledgebase – QID Change Log Consolidation](#)

Below is the list of fields in the Change Log which will now be updated with “service modified date”.

- Authentication Type
- Category
- CVE
- CVSS
- Linked Exploits

- PCI Flags
- Impact
- Patch
- Patch Available
- Vendor Reference
- Remote Flags
- RTIs Changes
- Severity
- Solution
- Threat
- Title
- Workaround

Support UDCs for Scanner on Mac OS X 12.x and 13.x

Starting this release, the following UDC types are supported for Scanner on MacOS X 12.x and 13.x:

- File/Directory Existence
- File/Directory Permission
- File Integrity Check
- File Content Check
- Directory search

<input type="checkbox"/> Mac OS 11.x Use this section to create a Mac OS 11.x instance of this control.
<input type="checkbox"/> Mac OS 12.x Use this section to create a Mac OS 12.x instance of this control.
<input type="checkbox"/> Mac OS 13.x Use this section to create a Mac OS 13.x instance of this control.
<input type="checkbox"/> Mac OS X 10.10 Use this section to create a Mac OS X 10.10 instance of this control.
<input type="checkbox"/> Mac OS X 10.11 Use this section to create a Mac OS X 10.11 instance of this control.
<input type="checkbox"/> Mac OS X 10.12 Use this section to create a Mac OS X 10.12 instance of this control.

Support New UDC Type for Agent on Ubuntu 18.x/20.x/22.x and RHEL 9.x

Starting this release, a new UDC type, **Script Result Check**, is now available for Agent on Ubuntu 18.x/20.x/22.x and RHEL 9.x.

Qualys Cloud Platform

← New Control: **Script Result Check**

STEPS 2/3

- 1 Select Script
- 2 Control Information
- 3 Review And Confirm

- Ubuntu 14.x
- Ubuntu 16.x
- Ubuntu 18.x
- Ubuntu 20.x
- Ubuntu 22.x
- Ubuntu 8.x
- Ubuntu 9.x
- openSUSE 10.x

Qualys Cloud Platform

← New Control: **Script Result Check**

STEPS 2/3

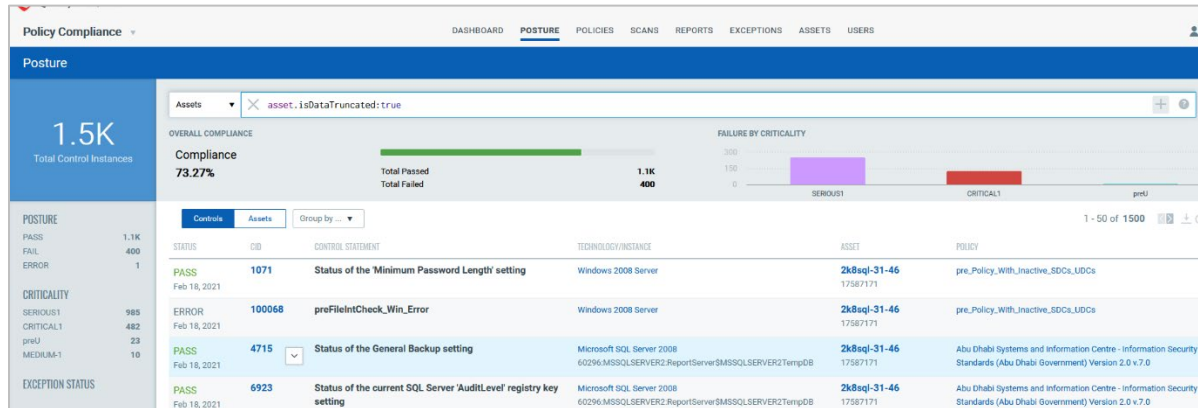
- 1 Select Script
- 2 Control Information
- 3 Review And Confirm

- Red Hat Enterprise Linux 6.x
- Red Hat Enterprise Linux 7.x
- Red Hat Enterprise Linux 8.x
- Red Hat Enterprise Linux 9.x
- SUSE Linux Enterprise 11.x
- SUSE Linux Enterprise 12.x
- SUSE Linux Enterprise 15.x

Limit Posture Indexing

Asset data is indexed as part of scan processing and policy evaluation. With this release, only up to 1500 postures are indexed for an asset, based on the most recent evaluation date.

Any additional postures are truncated and not included in the indexing. To view assets that have truncated postures, use the following search token: **asset.isDataTruncated: true**.



Evaluate Script Result UDC only During Agent Scan

Previously, when processing a script result for an asset, the script result UDC was unnecessarily evaluated for all assets that had policies associated with this UDC.

With this release, the script result UDC is no longer evaluated when a script result is processed. Instead, it is evaluated during the next agent scan (PC/UDC/Middleware).

Issues Addressed

The following issues are fixed with this release:

- We have fixed an issue where the policy list under the Scorecard Report was taking too long to load.
- We have fixed an issue where slowness was experienced in Asset Search with only one IP and **Include asset group titles in results** selected.
- We have fixed an issue with the VM auth tab Private Key while adding the new 2022 private key to the VM authentication tab; it was overwriting the old 2021 key instead of adding it to the new key.
- We have fixed an issue with the asset groups where the network, the owners, and the appliance list were not alphabetically displayed.
- We have fixed an issue where the user faced error in adding or editing the Apache authentication record even when the record was available in **Windows Authentication** record > **Domain type - Active Directory** or **NetBIOS, Service-Selected IPs**.
- We have fixed the issue where the user was redirected to the **Assets** tab of Policy Compliance when clicking the **Assets** tab from VM/VMDR.
- We have fixed an issue where the user got an error as tags are unavailable at this time in the **Tags** field on the **Scan Results** page when a scheduled scan was launched.
- We have fixed an issue where compliance scorecard reports (in both CSV and PDF formats) were interrupted or errored out in certain cases.
- We have fixed an issue where scan jobs remained in the QUEUED state and were not processed.
- We fixed an issue where the count of QIDs users requested to download from Knowledgebase exceeded the set limit. Now, the limit is increased to 2,00,000 and users can request to download more QIDs by contacting Qualys support. This change is only applicable to users with QID services enabled.
- We have fixed an issue where the asset count for **Hosts Not Alive** and **Scan Discontinued** under the **Hosts Not Scanned** section was displayed incorrectly.
- The email notification for delayed scheduled scan jobs contained unclear wording, leading to confusion. An example of the original message is "Schedule Task W_Amazon Web Services_10.191.64.0/18 was delayed before 00:05:07.". To improve clarity, the message has been revised to read "Schedule Task W_Amazon Web Services_10.191.64.0/18 was delayed by 00:05:07."
- We have fixed the issue where the **Assets > Address Management** tab did not load when the **Display Comments** check box was enabled. Also, we have disabled the sorting capability on the **Comments** column.