

Qualys Cloud Platform (VM, PC) 10.x

Release Notes

Version 10.22.1 April 27, 2023 (updated on December 4, 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**.

Users Users Business Units	Distribution Groups Activity Log Setup
	Distribution Groups Activity Log Setup
Email Contact Change the contact info in email notifications.	Data List Setup Choose data lists that should remain empty until a search is performed.
Go >	Go >
Activity Log	Password Never Expire
Customize activity logs to be displayed for your account.	Set password never expire for API Access.
G0 >	Go 🗲

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

5. 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.

Edit User	Launch Help	2	×
General Information	Symantec™ VIP (Validation and ID Protection)		
Locale	> Endin Not Registered		
User Role	Symantec VIP two-factor authentication		
Asset Groups	Note: This option enables Symantec VIP two-factor authentication for users to login into Qualys GUI.		
Permissions	This setting impacts UI access only.		
Options	Password	_	
Account Activity	This will automatically generate a new password. It will not go into effect until you confirm the change.		
Security	Password Never Expire - API Access		
User Status	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		
Cancel	Sav	'e	

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.

		Turn help tips: On Off Lau	nch Help
>	Kerberos / GSSAPI		
>	Provide Kerberos Authenticati	n details to use for authentication.	
>	Use Kerberos:	YES	
>	Realm Discovery:	Manual 👻	
>	User KDC:		
>	Service Realm:		
>	Service KDC:		
>	Authentication Type:	Basic	
	Password*:		
	Confirm Password*:		
	> > > > > > >	 Provide Kerberos Authenticatio Use Kerberos: Realm Discovery: User Realm *: User KDC: Service Realm: Service KDC: Authentication Type: Password*: 	Kerberos / GSSAPI Provide Kerberos Authentication details to use for authentication. Use Kerberos: YES Realm Discovery: Manual User Realm *: User KDC: Service Realm: Service KDC: Authentication Type: Basic Password*:

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: This feature is temporarily inaccessible due to an unexpected issue requiring architectural adjustments. Qualys is actively working to enhance the feature for a better user experience that we plan to release in the upcoming quarters. We appreciate your patience as we work to bring an improved version of the feature.

Dashboard Vulnerabilities	Prioritization Scans	Reports Remediat	ion Assets Knowledge	Base Users					_
Scans Scans Ma	aps Schedules App	liances Option Profile	s Authentication Sear	ch Lists Setup					
w 🗸 Search		-					4 1	- 5 of 5 🛛 👂 🗸	=
Appliance	 Personalization 0 	Code LAN IP	WAN IP LAN IPv6	Polling	Scanner	Signatures	Last Update	Platform Pro	ovide
C				180 seconds			02/28/2023 at 03:12:09 PM	(GMT+0530) 🙆 ec2	
- CD				180 seconds			N/A	ŝ	
⇔				180 seconds			N/A	6	
CD				180 seconds			N/A	æ	
(c)				180 seconds			04/12/2023 at 07:49:20 AM	(GMT+0530) 📾	
review				7 1000 F				Actions	~
			11:04:03 AM (GMT+0530) Not Connecter						
mmary: Update the Vulnerability Signatur			г						
		atest Signature Version 2.5.742-2 A	Available Capacity	Intel(R) Xeon(R) @ 2.40GHz	CPU E5-2	676 v3 4,049		s-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.

By default dead ho	osts are ignored. Including them may increase scan time, and is not suggested for Class C or larger networks.
Include dead here	anta in pages
Close Vulner	abilities on Dead Hosts
When selected, we status will be upda	e'll take this action if a host is found not alive after a set number of scans. Tickets will be marked Closed/Fixed and vulnerability sted to Fixed.
Close vulnerab	times.
Purge old ho	st data when OS is changed
When selected, we	e'll take this action if a scan detects a major change in host OS vendor from the previous scan. Old host data (vulnerabilities, tickets)
will be purged and	permanently removed, and new host data related to new OS only will be saved.
Purge old host	data when OS is changed
Performance	
Configure performa	ance options for scanning your network.
Overall Performan	ce: Normal Configure
Load Balance	er Detection
With this option en	habled, the scanner will attempt to identify load balancers and the number of Web servers behind them.

• Enable Date Format

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

lit User			Launch Help 🛛 🖉
General Information	Locale		
_ocale	Language: *	English	
Jser Role	> Date Format:	US Format (mm/dd/yyyy)	
Options	> Time Zone:	(GMT -08:00) United States, California (Pacific Standard -	
Account Activity	>		
Security	>		

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

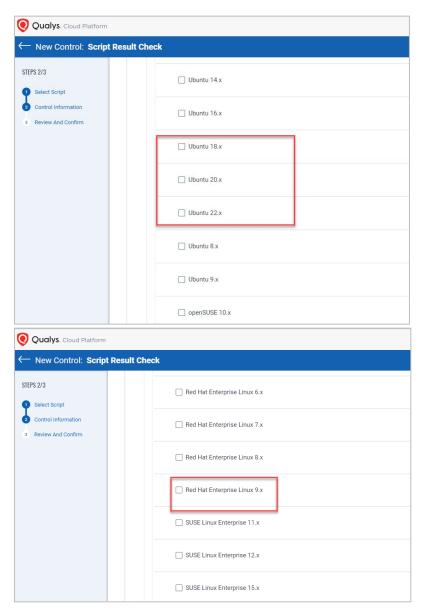
Starting this release, the following UDC types are supported for Scanner on MacOS X 12.x and 13.x:

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

Mac OS 11.x Use this section to create a Mac OS 11.x instance of this control.	
Mac OS 12.x Use this section to create a Mac OS 12.x instance of this control.	
Mac OS 13.x Use this section to create a Mac OS 13.x instance of this control.	
Mac OS X 10.10 Use this section to create a Mac OS X 10.10 instance of this control.	
Mac OS X 10.11 Use this section to create a Mac OS X 10.11 instance of this control.	
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.



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**.

Policy Compliane	ce ×			DASHBOARD POSTURE	POLICIES SCANS REP	PORTS EXCEPTIONS ASSET	'S USERS		
Posture									
		Assets •	× asset.isDat	taTruncated:true					+ 0
1.5K Total Control Insta	-	OVERALL COMPLIAN Compliance 73.27%	(CE	Total Passed Total Fasied	1.1K 400	FAILURE BY CRITICALITY	10US1	CRITICALI	preU
POSTURE	1.16	Controls	Assets Group	by 🔻					I - 50 of 1500
FAIL	400	STATUS	CID CC	INTROL STATEMENT	TECHNOLOGY/INSTANCE		ASSET	POLICY	
ERROR	1	PASS Feb 18, 2021	1071 Si	tatus of the 'Minimum Password Length' setting	Windows 2008 Server		2k8sql-31-46 17587171	pre_Policy_With_Inactive_SDCs_UD	Cs
SERIOUS1 985 ER CRITICAL1 482 Feb preU 23 MEDIUM-1 10		ERROR Feb 18, 2021	100068 pr	reFileIntCheck_Win_Error	Windows 2008 Server		2k8sql-31-46 17587171	pre_Policy_With_Inactive_SDCs_UDCs	
		PASS Feb 18, 2021			Microsoft SQL Server 2008 2k8sgl-31-46 60296.MSSQLSERVER2.ReportServer\$MSSQLSERVER2TempDB 17587171			6 Abu Dhabi Systems and Information Centre - Information Se Standards (Abu Dhabi Government) Version 2.0 v.7.0	
EXCEPTION STATUS		PASS Feb 18, 2021		tatus of the current SQL Server 'AuditLevel' registry key etting	Microsoft SQL Server 2008 60296:MSSQLSERVER2:Report	tServer\$MSSQLSERVER2TempDB	2k8sql-31-46 17587171	Abu Dhabi Systems and Informatio Standards (Abu Dhabi Government	

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.