



# Qualys Cloud Platform (VM, PC) 10.x

## Release Notes

Version 10.25

January 12, 2024

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

### What's New?

#### **Qualys Vulnerability Management (VM)**

[Support for adding Resource ID in Hitachi ID PAM Authentication Records](#)

[Addition of QDS Report Filter in Host-Based Scan Report Template](#)

[Support for Adding TCPS Configuration to Oracle Authentication Records](#)

[Addition of New Fields in the Excluded Host Setup](#)

[Integrate the Captcha on the Change Password Page](#)

[Addition of New Technology Tag for SCA QID](#)

[Display of QIDs that have Code Modified Date](#)

#### **Qualys Policy Compliance (PC/SCAP/SCA)**

[Policy Report Template Enhancements](#)

[Support for OS Authentication-based Technology - Enghouse Interactive Proteus Enterprise 8.x](#)

**Qualys 10.25 brings you many more improvements and updates! [Learn more](#)**

## Support for Adding Resource ID in Hitachi ID PAM Authentication Records

You can now provide resource ID information while creating or updating Hitachi ID PAM authentication records. This enhancement addresses the error that occurs during authenticated scans using Hitachi ID PAM authentication records due to the absence of resource ID information. As a part of this enhancement, the following changes have been made:

- **UI Changes:** A new Resource ID field has been added while creating or editing the Hitachi PAM authentication records. It is an optional field that allows you to provide the unique identifier of the authentication record to avoid errors while performing authenticated scans.

**Edit Unix Record** Turn help tips: On | Off Launch Help

**Record Title** >

**Login Credentials** >

**Kerberos / GSSAPI** >

**Private Keys / Certificates** >

**Root Delegation** >

**Policy Compliance Ports** >

**IPv4** >

**IPv6** >

**Comments** >

**Authentication**

Provide login credentials to use for authenticated scanning. You have the option to get the login password from a vault available in your account.

Username\*:

Get password from vault ☒ YES

Vault Type\*:

Vault Record\*:

Resource ID\*:

Target Type\*:

- **API changes:**
  - A new resource\_id parameter has been added to the following APIs. It is an optional parameter.
    - PostgreSQL Record
    - SAP IQ Record
    - Unix Record
    - Windows Record
    - Pivotal Greenplum Record
  - A new <VAULT\_RESOURCE\_ID> DTD tag is added.

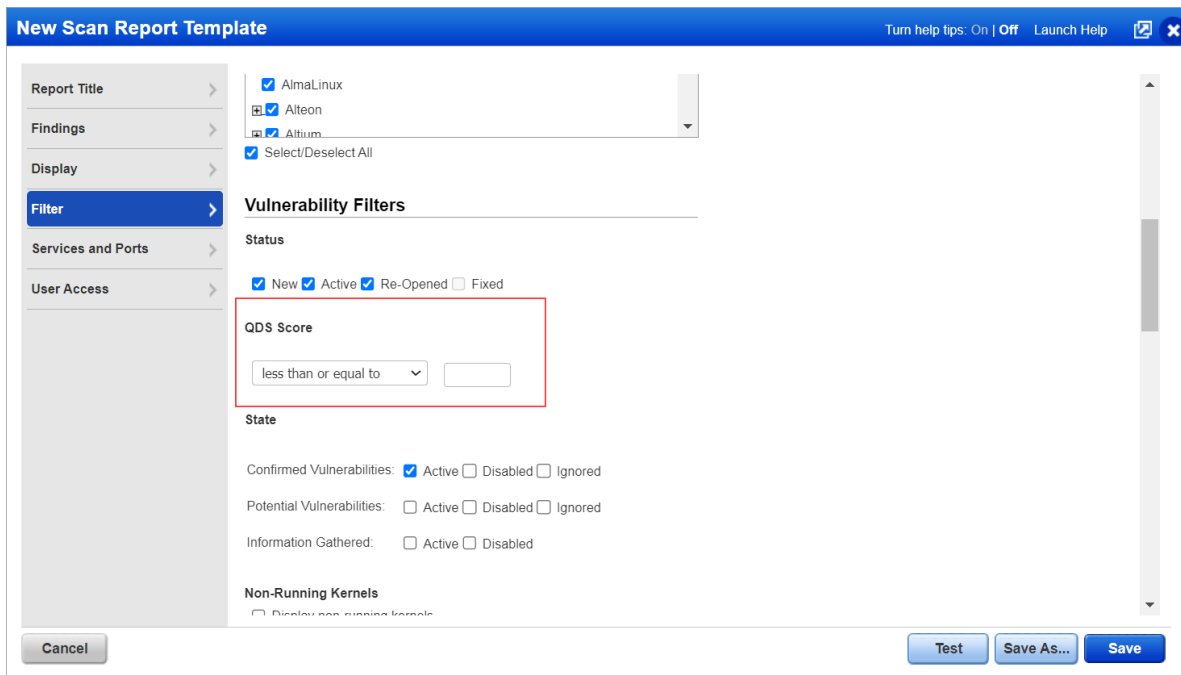
For more information, refer to Cloud Platform 10.25 API Release Notes.

## Addition of QDS Report Filter in Host-Based Scan Report Template

In addition to including TruRisk details (ACS, QDS) in your report, you can now use the QDS report filter to further refine the detection data in your report. QDS report filter provides you the ability to filter the detection data based on the QDS.

As a part of this enhancement, the following changes have been made:

- **UI Changes:** The **Filter tab** (Scans>Report>Templates>New or Edit>Filter tab) now has a QDS score filter while creating or updating the report template. The following two QDS filter parameters are now available for you to use to display detections in the report based on the selected QDS score filter.
  - greater than or equal to
  - less than or equal to



The screenshot shows the 'New Scan Report Template' dialog box with the 'Filter' tab selected. The 'Vulnerability Filters' section is expanded, and the 'QDS Score' filter is highlighted with a red box. The 'QDS Score' filter is set to 'less than or equal to'. The 'Status' section shows 'New', 'Active', and 'Re-Opened' checked, and 'Fixed' unchecked. The 'State' section shows 'Confirmed Vulnerabilities' with 'Active' checked, 'Disabled' and 'Ignored' unchecked. 'Potential Vulnerabilities' and 'Information Gathered' are all unchecked. The 'Non-Running Kernels' section is also visible.

- **API changes:** The following two new parameters are added to the report template API. For more information, refer to Cloud Platform 10.25 API Release Notes.
  - qds\_score\_min
  - qds\_score\_max

## Support for Adding TCPS Configuration to Oracle Authentication Records

You can now add a TCPS configuration while creating or editing the Oracle Authentication records. Once you have configured the TCPS connection protocol for your Oracle database, then you can add the same to the Oracle authentication records in the Qualys Platform. As a part of this enhancement, the following changes have been made:

### UI Changes:

- A new TCPS configuration tab (**Scan > Authentication > New/Edit > Databases > Oracle**) is added, as shown in the following images:

The screenshot shows the 'New Oracle Record' form with the 'TCPS Configuration' tab selected. The form includes a sidebar with navigation options: Record Title, Login Credentials, Target Configuration, TCPS Configuration (selected), Windows Configuration, Unix Configuration, IPs, and Comments. The main content area is titled 'TCPS Configuration' and contains the following sections:

- Wallets:** A text area for entering wallet contents. It includes a description: 'Wallets are intended for storing contents of client-side Oracle auto-login wallet files (CA certificate chains, client certificate, and client private key).' and a note: 'Cwallets are certificates intended for storing binary contents of cwallet.sso file. SSO file format is an Oracle proprietary.'
- Get passphrase from vault:** A toggle switch set to 'NO'.
- Passphrase:** A text input field with a masked password '\*\*\*\*\*'.
- SSL Verify:** A toggle switch set to 'NO'.

At the bottom of the form are 'Cancel' and 'Create' buttons.

The screenshot shows the 'Edit Oracle Record' form with the 'TCPS Configuration' tab selected. The form includes a sidebar with navigation options: Record Title, Login Credentials, Target Configuration, TCPS Configuration (selected), Windows Configuration, Unix Configuration, IPs, and Comments. The main content area is titled 'TCPS Configuration' and contains the following sections:

- Wallets:** A text area for entering wallet contents. It includes a description: 'Wallets are intended for storing contents of client-side Oracle auto-login wallet files (CA certificate chains, client certificate, and client private key).' and a note: 'Cwallets are certificates intended for storing binary contents of cwallet.sso file. SSO file format is an Oracle proprietary.'
- Get passphrase from vault:** A toggle switch set to 'NO'.

At the bottom of the form are 'Cancel' and 'Save' buttons.

- The Authentication Information of the Oracle authentication record has been enhanced to reflect information about TCPS configuration:

The screenshot shows a web interface titled 'Authentication Information'. On the left is a sidebar with tabs: 'General Information' (selected), 'Windows', 'Unix', 'IPs', and 'Comments'. The main area displays 'General Information' as a key-value list. A red rectangle highlights the 'Cwallet' and 'Ewallet' entries, both of which are set to 'installed'.

Field	Value
ID:	238513
Title:	ankittesttcps
Network:	Global Default Network
System Created:	No
Active:	Yes
Record Type:	Oracle
User Name:	[REDACTED]
SID:	[REDACTED]
Cwallet:	installed
Ewallet:	installed
Ewallet Passphrase:	yes
SSL verify:	true
Server DNs:	[REDACTED]
Vault Type:	Thycotic Secret Server
Vault Title:	[REDACTED]
Vault Info ID:	55010
Secret Name:	[REDACTED]
Port:	All Ports
Is CDB:	false

- **API changes:** The following new parameters have been added to Oracle Record API. For more information, refer to the Cloud Platform 10.25 API Release Notes.
  - o ssl\_verify
  - o use\_vault\_passphrase
  - o server\_dn
  - o cwallet,ewallet
  - o passphrase

## Addition of New Fields in the Excluded Host Setup

We have revamped the Excluded Host setting (**Scans > Setup > Excluded Host**) by adding new buttons and displaying the total excluded host count. There is also an Expiration column in various views of the dialog that displays the expiration date for excluded IP addresses.

The following fields are added to the Excluded Host Setup.

- Existing Excluded Hosts
- Excluded Hosts with an expiration
- Total Excluded Hosts

**Excluded Hosts Setup**

**Excluded Hosts**

Existing Excluded Hosts **View**

Excluded Hosts with an expiration date **View**

**Total Excluded Hosts: 20**

IPs:

8.8.9.1-8.8.9.5  
9.9.9.1-9.9.9.10  
10.10.9.2-10.10.9.6

**Close** **Edit** **History**

Using this setting, you can

- View the expiration date of the IP address on the history page.
- Search the IP address of the excluded hosts by downloading the CSV file.
- Remove the IPs from the excluded host based on the specified time period.

With the **Existing Excluded Hosts**, you can view all the existing hosts on a new page with the expanded IP address in each row. You can access the page by clicking on the View button.

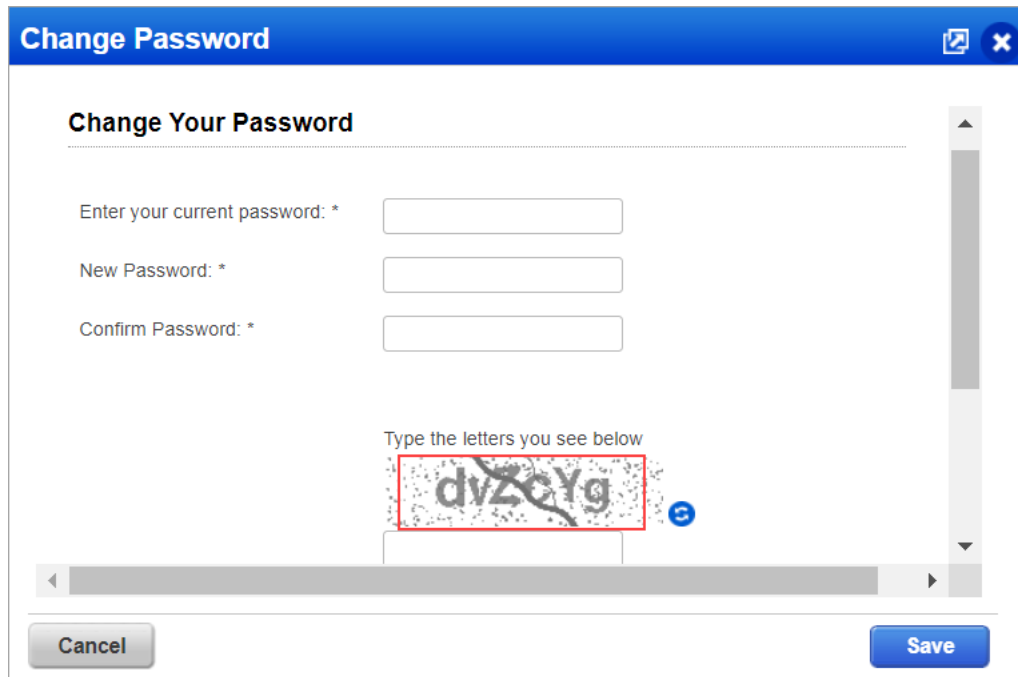
Excluded hosts					
Network	Edited	IPs	Expiration	Created By	Comments
Global Default Network	01/08/2024	10.10.9.2	01/10/2024		excluded hosts
Global Default Network	01/08/2024	10.10.9.3	01/10/2024		excluded hosts
Global Default Network	01/08/2024	10.10.9.4	01/10/2024		excluded hosts
Global Default Network	01/08/2024	10.10.9.5	01/10/2024		excluded hosts
Global Default Network	01/08/2024	10.10.9.6	01/10/2024		excluded hosts
Global Default Network	01/08/2024	8.8.9.1	01/10/2024		excluded hosts
Global Default Network	01/08/2024	8.8.9.2	01/10/2024		excluded hosts

Earlier **Excluded Hosts with an expiration date** was in the form of URL which was not user friendly. Now a **View** button is introduced where you can click **View** to see the hosts that have an expiration date. You can also view the count of excluded hosts from the list.

Excluded Hosts Expiration				
Search		1 - 3 of 3		
Info	Network	IPs	Expiration	Created By
	Global Default Network	9.9.9.1-9.9.9.10	01/10/2024	
	Global Default Network	8.8.9.1-8.8.9.5	01/10/2024	
	Global Default Network	10.10.9.2-10.10.9.6	01/10/2024	

## Integrate the Captcha on the Change Password Page

A new field is introduced on the VM/PC module to secure the users from brute forcing of passwords. We have added CAPTCHA to the Change password functionality. Captcha helps in strengthening password security against brute force logins. This field is mandatory while entering the new password.



The screenshot shows a 'Change Password' dialog box with a blue header bar containing the title 'Change Password' and a close button. Below the header, the section 'Change Your Password' is followed by three input fields labeled 'Enter your current password: \*', 'New Password: \*', and 'Confirm Password: \*'. Below these is a CAPTCHA field with the instruction 'Type the letters you see below'. The CAPTCHA image displays the letters 'dvZQYg' in a distorted font, with a red rectangular box highlighting the text. A small blue circular icon with a 'C' is located to the right of the CAPTCHA image. At the bottom of the dialog, there are two buttons: 'Cancel' on the left and 'Save' on the right. A vertical scrollbar is visible on the right side of the dialog content area.



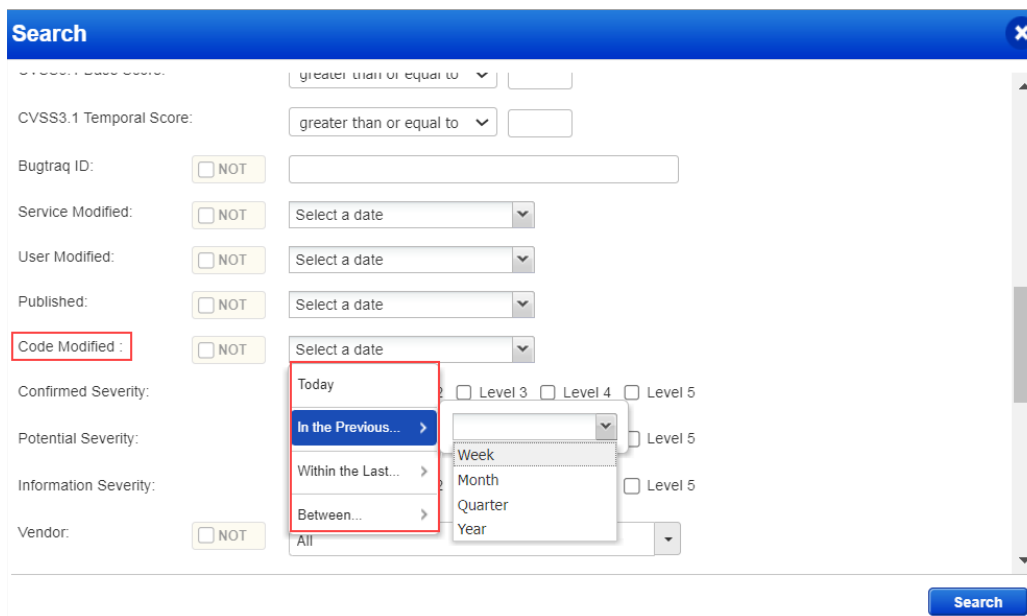
## Display of QIDs that have Code Modified Date

Code Modified has been added to the KnowledgeBase Search. Every QID has a signature code. When Qualys makes changes in the signature code, the Code Modified date gets displayed on the UI.

### UI Changes:

The Code Modified filter allows you to see code modified QIDs based on the following parameters:

- Between specific dates,
- Within the last few days
- In the previous week, month, quarter, or year
- Today



The screenshot shows the 'Search' window of the KnowledgeBase interface. The 'Code Modified' filter is highlighted with a red box, and its dropdown menu is open, also highlighted with a red box. The dropdown menu includes the following options: 'Today', 'In the Previous...' (with a right arrow), 'Within the Last...' (with a right arrow), 'Between...' (with a right arrow), 'Week', 'Month', 'Quarter', and 'Year'. The 'In the Previous...' option is currently selected. The background shows other search filters like 'CVSS3.1 Temporal Score', 'Bugtraq ID', 'Service Modified', 'User Modified', 'Published', 'Confirmed Severity', 'Potential Severity', 'Information Severity', and 'Vendor'.

You can view the QIDS with code modified dates on the following places:

- Preview window of KnowledgeBase listing page
- Vulnerability Information page of a selected QID

### API Changes:

- The following new parameters have been added to KnowledgeBase API. These parameters are optional.
  - Code\_modified\_after
  - Code\_modified\_before
- A new DTD `<CODE_MODIFIED_DATETIME>` DTD tag is added.

For more information, refer to Cloud Platform 10.25 API Release Notes.

## Addition of New Technology Tag for SCA QID

Multiple technology types can now be associated with a single QID. We have added a new field called Technology in the Vulnerability Information - QID, Vulnerability Edit, and KnowledgeBase Preview windows that display the technology type related to an SCA QID to detect vulnerabilities based on technology type.

**Vulnerability Information - QID** Launch Help

**General Information**

- Details**
- Software
- Threat
- Impact
- Solution
- Exploitability
- Associated Malware
- Search Lists
- Compliance
- Change Log

**Details**

QID:

Category: SCA

**Technology:** Python

CVE ID: [CVE-2023-20898](#)

Vendor Reference: [GHSA-qvh6-3j7x-3hg7](#)

Bugtraq ID: -

Patch Available: Yes

Virtual Patch Available: No

**Detection Information**

PCI Reasons: Reasons for failing PCI compliance are below.  
[The QID adheres to the PCI requirements based on the CVSS basescore.](#)

Supported Modules: CA-Windows Agent,CA-Linux Agent,SCA

CVSS Base: 5.4 [1]  
AV:A/AC:M/Au:M/C:N/I:C/A:P

CVSS Temporal: 4.0 E:U/RL:OF/RC:C

CVSS Access Vector: Adjacent Network

CVSS3.1 Base: 7.8  
AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

Close Edit

**Note:** This field is visible only if QID has a technology associated with it, otherwise it is not visible on the UI.

### API Changes:

A new DTD <TECHNOLOGY> is added to the Knowledgebase API. For more information, refer to Cloud Platform 10.25 API Release Notes.

## Policy Report Template Enhancements

We added the following new features in the **Compliance Policy Report Template > Layout**. This feature is available in CSV format:

- **Asset Tag For CSV Reports Only:** Using this option, you can now include or exclude asset tag information associated with the assets in the Policy Compliance report.

The screenshot shows the 'Edit Compliance Policy Report Template' window. On the left is a sidebar with tabs: General Information, Layout (selected), Display, Trending, Frameworks, and User Access. The main area is divided into 'Sections' and 'Layout' panels. In the 'Sections' panel, under the 'Report' section, the 'Asset Tag For CSV Reports Only' checkbox is checked and highlighted with a red box. Other checked options include 'Control Statistics', 'Host Statistics', and 'Report Details'. The 'Layout' panel shows a preview of the report template with sections like 'Report Title', 'Report Summary', 'Percentage of Hosts Passed per Control', 'Percentage of Controls Passed per Host', and 'Detailed Results'. The 'Hosts' section is expanded, showing 'Host: IP, DNS, NetBIOS' and 'Operating System'.

### Notes:

- To use this feature, it is necessary to have Cloud Platform v10.25 and installed.
- For existing Policy Compliance report templates, this option is not selected by default. If you generate a report using an existing template, the asset tag information will be shown in the CSV report. However, if you modify the existing template for different settings and leave the Asset tag option unselected, and save the template, the CSV report will not include asset tag information when you generate a report using this modified template.
- For new templates, this option is selected by default.

- **Timeframe selection:** You now have the option only to show the compliance data for hosts evaluated within a certain timeframe. The report summary, host statistics, and detailed results sections of your report will be based on the timeframe you specify.

**Edit Compliance Policy Report Template** Launch Help

**General Information** **Layout** **Display** **Trending** **Frameworks** **User Access**

### Timeframe Selection

Show only hosts that have been scanned during the specified period of time.

Timeframe ☒ No Time Limit  
Limit Timeframe

Show only hosts that have been evaluated during the specified period of time. For CSV Reports Only

Timeframe ☐ No Time Limit  
Limit Timeframe

### Report Layout

Choose a grouping method for the report's detailed results section, and select the components to be included in the report.

Group By: \*

Status: \* ☒ All ☒ Passed ☒ Failed ☒ Error

Criticality: \* ☒ All ☒ UNDEFINED ☒ MINIMAL ☒ MEDIUM ☒ SERIOUS ☒ CRITICAL ☒ URGENT

☐ Do Not Include Criticality

## Support for OS Authentication-based Technology - Enghouse Interactive Proteus Enterprise 8.x

### Policy Editor

When you create or edit a compliance policy, Enghouse Interactive Proteus Enterprise 8.x is now available in the list of supported technologies.

**Create a New Policy**

**Empty Policy:** Build your policy from scratch.  
Select technologies for your policy. Your selection makes up the global technologies list for the policy and determines which controls can be added to the policy. Note - You can change the technologies at any time from within the Policy Editor.

**Technologies** Select at least one technology. REQUIRED

Search technologies: Add All | Remove All

No technologies selected

410 technologies Add all shown

- Docker CE/EE
- Docker Containers/Images
- Elasticsearch 6.x/7.x
- Enghouse Interactive Proteus Enterprise 8.x**
- EulerOS 2.x
- Extreme Networks BOSS 5.x
- Extreme Networks ERS 5.x

Back Choose Source Next

### Search Controls

When you search controls, you see Enghouse Interactive Proteus Enterprise 8.x in the list of technologies. Go to **Policies > Controls > Search** and select Enghouse Interactive Proteus Enterprise 8.x in the list.

**Search**

CIDs:   
Example: 1072, 1071, 1091 (up to 20)

Text:

Status: ☐ Deprecated

DB OS CIDs: ☐ Instance Data Collection

Technologies:

- ☐ Docker Containers/Images
- ☐ Elasticsearch 6.x/7.x
- ☒ Enghouse Interactive Proteus Enterprise 8.x
- ☐ EulerOS 2.x
- ☐ Extreme Networks BOSS 5.x

Frameworks:

- ☐ 2017 Trust Services Criteria for Security, Availability, Process
- ☐ ANSSI 40 Essential Measures for a Healthy Network Ver 1.0
- ☐ APRA Prudential Practice Guide (PPG): CPG 234 - Manager
- ☐ Annex 3A (Security Control Catalogue) to IT Security Risk M

Search

## Authentication Reports

To display all OS auth-based instance technologies per host, including Enghouse Interactive Proteus Enterprise 8.x in your authentication report, go to **Reports > Compliance Report > Authentication Report**, and enable the OS Authentication-based Technology option under the Appendix.

### New Authentication Report

[Launch Help](#)

Use the following form to create a new authentication report on compliance data.

#### Report Details

Title:

Report Format: \* Portable Document Format (PDF)

#### Report Source\*

Select at least one business unit, asset group, IP or asset tag to draw data from.

☐ Business Units ☒ Asset Groups ☐ IPs ☐ Asset Tags

[Select](#)

#### Display & Filter

Select the items you want to show in your report.

##### Details

☒ Summary Section

☒ Details Section

☐ Additional Host Info (OS, scan date, successful auth date)

☐ Host ID

☐ All Asset Tags

##### Appendix

☒ OS Authentication-based Technology

Scroll down to the **Appendix** section of your authentication report to see Enghouse Interactive Proteus Enterprise 8.x mentioned under **Targets with OS authentication-based technologies**.

Appendix		
Targets with OS authentication-based technologies		
Network: Global Default Network		Last Auth: 12/27/2023 at 03:08:36 PM (GMT+0530)
OS: Windows Server 2022 Standard Version 21H2		Last Success: 12/27/2023 at 03:08:36 PM (GMT+0530)
S.N.	Host Technology	Instance
1	Google Chrome (Windows)	Google Chrome (Windows)
2	Microsoft Edge Chromium (Windows)	Microsoft Edge Chromium (Windows)
3	Enghouse Interactive Proteus Enterprise 8.x	Enghouse Interactive Proteus Enterprise 8.x
4	Internet Explorer 11	Internet Explorer 11
5	Microsoft SQL Server 2017	MSSQL 2017 (Instance Name: PROTEUS, Port: 49761)
CONFIDENTIAL AND PROPRIETARY INFORMATION. Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2023, Qualys, Inc.		

## Option Profile

Make sure you have enabled the OS Authentication-based Technology option. Under **Scans**, select **Option Profiles > Instance Data Collection**. The Enghouse Interactive Proteus Enterprise 8.x is available under **Application and Other Technologies**.

**New Compliance Profile**

Compliance Profile Title >

Scan >

System Authentication >

**Instance Data Collection >**

Additional >

**Instance Data Collection Using OS Authentication Records**

Select database technologies and applications to enable data collection on them by using authentication records created for their underlying host operating systems.

☐ Databases

- ☐ IBM DB2
- ☐ Pivotal Greenplum
- ☐ InformixDB
- ☐ MongoDB
- ☐ MS SQL
- ☐ MySQL
- ☐ Neo4j
- ☐ Oracle
- ☐ PostgreSQL
- ☐ Sybase

**Note:** If you use individual database authentication records for compliance scans, we recommend not to use this option. If you enable it, you get duplicate results in compliance reports, one using database authentication records and the other using OS authentication records.

☒ Applications and Other Technologies

- ☐ Red Hat OpenShift Container Platform
- ☐ Oracle JRE
- ☐ Teradata
- ☐ Verint Financial Compliance 9.x
- ☐ IBM WebSphere Liberty
- ☒ Enghouse Interactive Proteus Enterprise 8.x

Restore Defaults

Save Save As... Cancel

## Scan Results

Enghouse Interactive Proteus Enterprise 8.x is now listed under **Application technologies found based on OS- level authentication** in the **Appendix** section of a compliance scan result.

**Compliance Scan Results**

File Help

**Target distribution across scanner appliances (1)**

Windows authentication was successful for these hosts

**Application technologies found based on OS-level authentication**

**Enghouse Interactive Proteus Enterprise 8.x was found for these hosts**

Enghouse Interactive Proteus Enterprise 8.x

**Google Chrome was found for these hosts**

Google Chrome (Windows)

**Internet Explorer was found for these hosts**

Internet Explorer 11

**Microsoft Edge Chromium (Windows) was found for these hosts**

Microsoft Edge Chromium (Windows)

**Compliance Profile:**

enhouse OP

**Scan Settings**

## Issues Addressed

The following issues are fixed with this release.

Component/Category	Application	Description
VM - Feature Request	Vulnerability Management	The Excluded Hosts list (Scans > Setup > Excluded Hosts) did not display all the details about the excluded hosts and the count of excluded hosts. Now, the Excluded Hosts feature has been improvised to display details like the number of excluded hosts, edited date, expiration date, and added by. Users can also download the list for their convenience.
SCA Reports	Policy Compliance	When a sub-user selected <b>Select Asset Tag</b> (tags assigned to the user) as the report source while executing a policy compliance report, the compliance data pie chart did not appear. The relevant code changes have been made to fix this issue. However, if a sub-user assigned to only asset tags generates a report for a policy with only asset groups and no associated tags by selecting All Assets in Policy as the report source, the report will be generated as blank. This is an expected behavior.
VM - Reports General	Vulnerability Management	When generating a Patch report in XML format with special characters in the VENDOR_ID tag, page parsing errors occurred due to illegal characters. To resolve this issue, the XML format has been modified from <VENDOR_ID>text here</VENDOR_ID> to <VENDOR_ID><![CDATA[ text here ]]></VENDOR_ID>.
CompSig - Policies	Policy Compliance	While creating and saving a policy, CDATA tagging was missing in controls having multiple dps. This issue is now fixed, and the policy is now getting saved
VM - Assets	Vulnerability Management	While viewing netblock ranges (click <b>Asset&gt;Domain&gt;Quick Actions&gt;Info</b> ), the scrolling functionality was not working as expected. The user was unable to scroll down the list to view additional IP ranges. The relevant code changes have been made to fix this issue.
VM - User Management	Vulnerability Management	Qualys does not support receiving Scanner Appliance Heartbeat Check notifications for the Contact user role. However, during the creation or modification of the Contact user role, the user setting option to receive this notification was still available on the UI under Other Notification. This



Component/Category	Application	Description
		option has been removed from the UI.
VM - Reports General	Vulnerability Management	While generating a scan based report in PDF format that contained QIDs with a large result section, the user encountered an error. This issue is now fixed.
VM - Scans	Vulnerability Management	When a user tried to search the scan list in the search panel by a particular word or character in the scan tab. The search panel was displaying only the latest scan result, and the page count was also not correctly seen. Now, the search panel displays the correct list and page count on the scan listing page.
VM - Scan Based Report	Vulnerability Management	When the user was downloading the scan report in CSV format, it was stuck at 80% of download. There was an interrupted error on the browser window. Relevant code changes are made to fix this issue. Now, the users can generate the scan report properly.
PC scans	Policy Compliance	IP addresses like x.x.x.x/32 to the asset group were not getting saved. We have resolved this issue by extending our support to CIDR /32 IP address format.
VM Scan	Vulnerability Management	Users could not view installed Scanner Trusted CAs under VM DR > Setup > Scanner Trusted CA. Clicking any of the trusted CAs resulted in a loading message, but no information was loaded. We improved our VM Scan logic to resolve this issue.
VM Assets	Vulnerability Management	We have resolved the issue of vulnerability data not loading correctly on the Host info page.
VM Report	Vulnerability Management	"Exploitability" and "Associated Malware" columns were displayed in the scan report (CSV format) despite both options were not selected in the "Scan Report Template" when a user was creating the scan template using the Scan Template API (/api/2.0/fo/report/template/scan/?action=create).