Qualys Cloud Platform (VM, PC) 10.x

Release Notes

Version 10.24.2

December 21, 2023

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

What's New?

Qualys Policy Compliance (PC/SCAP/SCA)

Support for OS Authentication-based Technology- Verint Financial Compliance 9.x

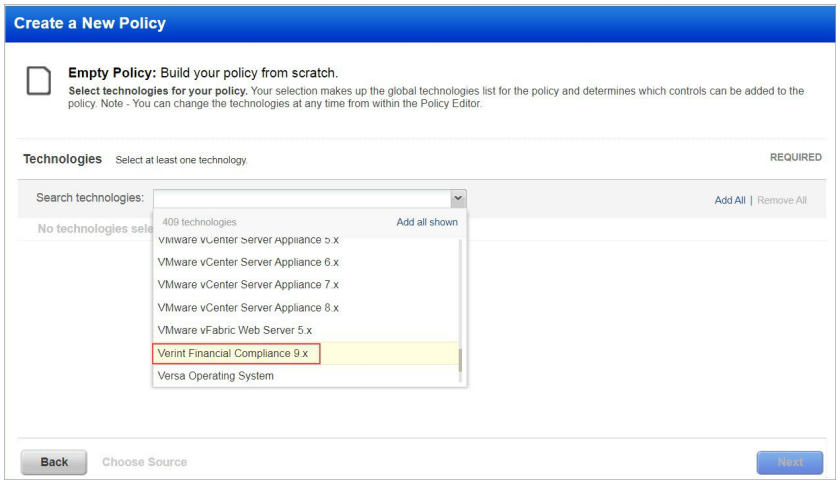
Qualys 10.24.2 brings you many more improvements and updates! Learn more

Support for OS Authentication-based Technology- Verint Financial Compliance 9.x

Our platform now offers support for OS-based authentication using Verint Financial Compliance 9.x technology.

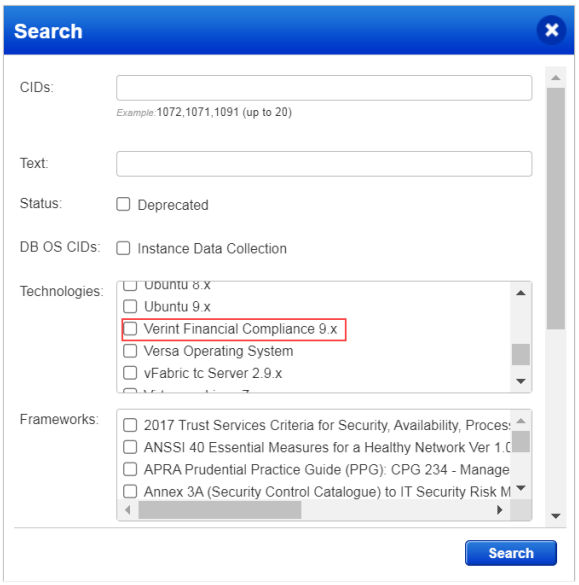
Policy Editor

When you create or edit a compliance policy, Verint Financial Compliance 9.x is now available in the list of supported technologies.



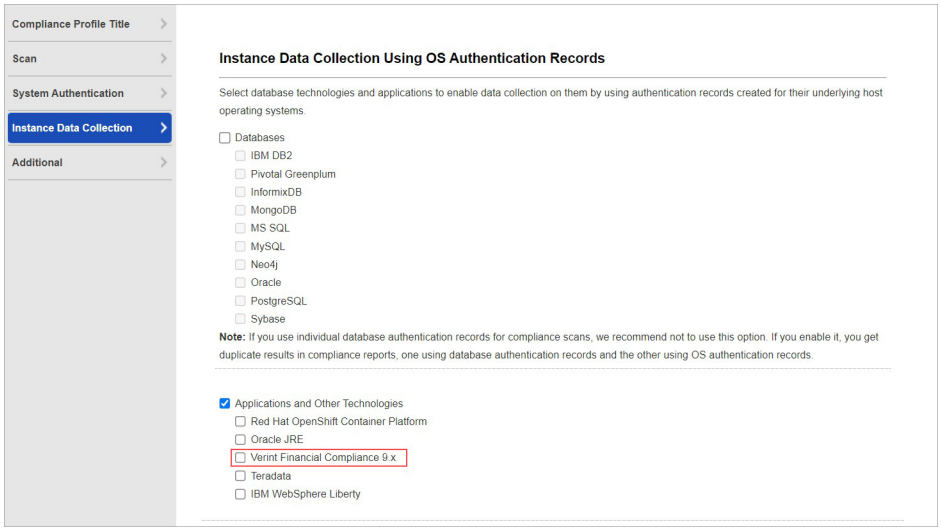
Search Controls

When you search controls, you see Verint Financial Compliance 9.x in the list of technologies. Go to **Policies > Controls > Search** and select **Verint Financial Compliance 9.x** in the list.



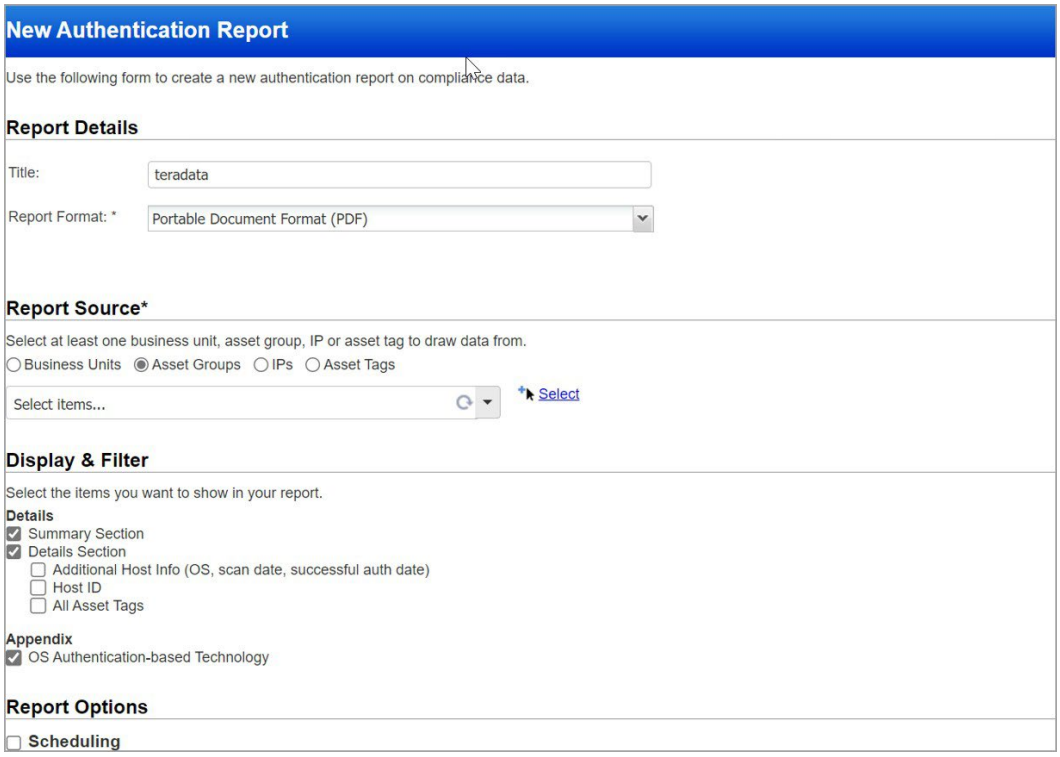
Option Profile

Select the option profile, go to **Instance Data Collection > Application and Other Technologies > Verint Financial Compliance 9.x**, and enable the OS Authentication-based Technology option.

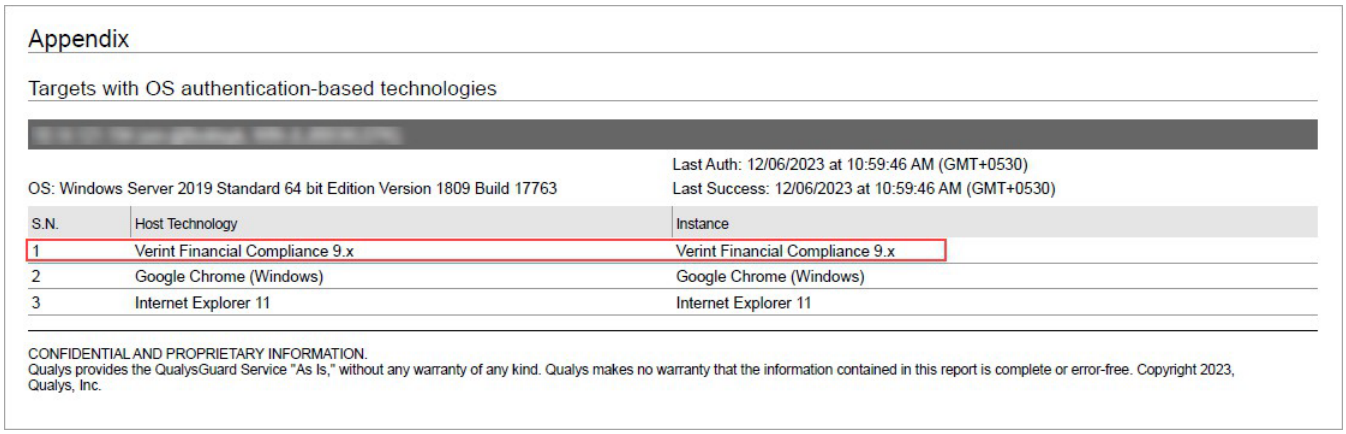


Authentication Reports

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



Scroll down to the **Appendix** section of your authentication report to see **Targets with OS authentication-based technologies**.



Appendix

Targets with OS authentication-based technologies

[redacted]

OS: Windows Server 2019 Standard 64 bit Edition Version 1809 Build 17763

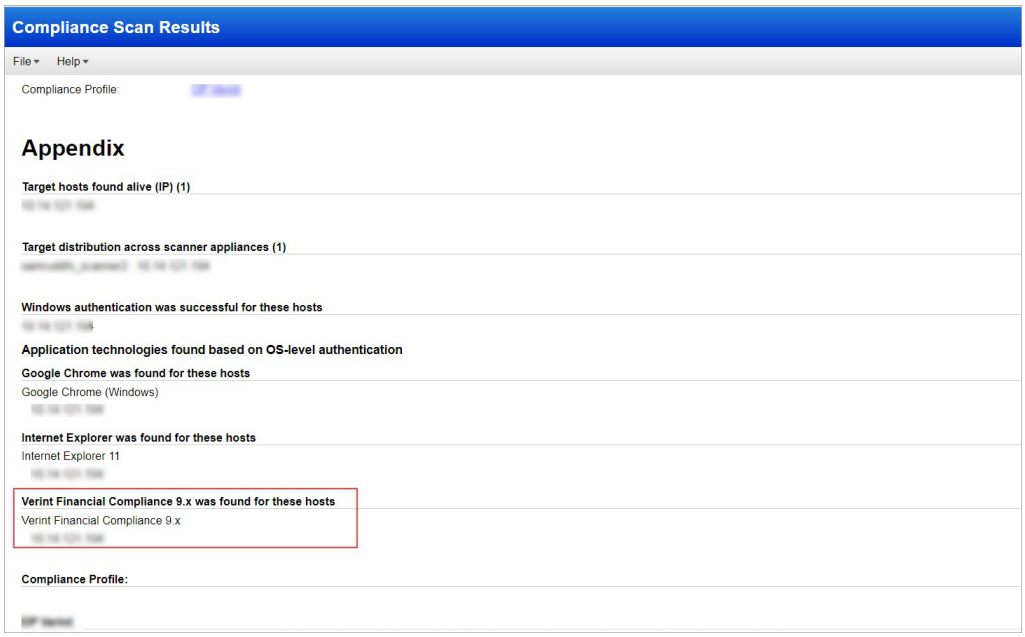
Last Auth: 12/06/2023 at 10:59:46 AM (GMT+0530)
Last Success: 12/06/2023 at 10:59:46 AM (GMT+0530)

S.N.	Host Technology	Instance
1	Verint Financial Compliance 9.x	Verint Financial Compliance 9.x
2	Google Chrome (Windows)	Google Chrome (Windows)
3	Internet Explorer 11	Internet Explorer 11

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.

Scan Results

You see Verint Financial Compliance 9.x listed under **Application technologies found based on OS-level authentication** in the **Appendix** section of a compliance scan result.



Compliance Scan Results

File Help

Compliance Profile: [redacted]

Appendix

Target hosts found alive (IP) (1)

[redacted]

Target distribution across scanner appliances (1)

[redacted]

Windows authentication was successful for these hosts

[redacted]

Application technologies found based on OS-level authentication

Google Chrome was found for these hosts

Google Chrome (Windows)

[redacted]

Internet Explorer was found for these hosts

Internet Explorer 11

[redacted]

Verint Financial Compliance 9.x was found for these hosts

Verint Financial Compliance 9.x

[redacted]

Compliance Profile:

[redacted]

Upcoming Improvements

Qualys released **View CPU, Memory, and Region Information of Scanners** feature in v10.22.1. This feature is temporarily inaccessible due to an unexpected issue requiring architectural adjustments. We are 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.

Issues Addressed

The following issues are fixed with this release:

Component/Category	Application	Description
PC – Reports	Policy Compliance	When creating or editing User Defined Controls (UDCs), special characters such as quotes and apostrophes were not getting saved correctly in the Remediation, Rationale, Statement, and Comment fields. The relevant code changes have been made to fix this issue. Now, these fields can accept special characters without any issues.
PC – Reports	Policy Compliance	Previously, when creating or editing the VMware Authentication record, there was no validation in place to check if the IP address was part of the Unix auth record or not. Validation was only available when the user selected the Disconnected ESXi check box. Now, validation has been added to the process of creating or editing VMware Authentication records to validate the IPs regardless of whether the user selects or deselects the Disconnected ESXi check box.
PC - Exceptions	Policy Compliance	While requesting bulk exceptions for large records, only 3987 records were created. Now the new limit on exception requests has increased to 4987 records.
VM - UI General	Vulnerability Management	While downloading the OVA image for the Virtual Scanner appliance using the Safari browser, the user encountered an issue. The relevant code changes have been made to fix this issue. Now OVA download works as expected on all the supported browsers, such as Chrome, Firefox, and Safari.
VM - Host List Detection API	Vulnerability Management	While executing Host List Detection API for a QID, an Incident signature occurred if the result section of QID contained "Fatal error: Allowed memory size of 134217728 bytes exhausted." The relevant code changes have been made to fix this issue. Now, the Host List Detection API is working as expected without returning the incident signature in the response.
VM - Scan Based Report	Vulnerability Management	While generating a scan on a large number of IPs and then downloading it in PDF format, the IPs overlapped in the Appendix

Component/Category	Application	Description
		section of the scan result. The relevant code changes have been made to fix this issue. Now, IPs do not get overlapped in the scan result.
VM - Asset Groups	Vulnerability Management	While downloading the asset groups, the users encountered an error. The relevant code changes have been made to fix this issue. Now the users can download their Asset Group.
VM - Purge Assets	Vulnerability Management	Users were able to purge the assets completely, but an error occurred when simultaneous purge activity got triggered. The issue has been fixed now.
VM - AGMS Integration	Vulnerability Management	When the user executed a scheduled scan on the Asset group, the scan result showed the Target group as No Group in the scan result email notification. Code changes have been made to fix this issue. Now, the email notification shows the target group as their Asset Group.
VM - AGMS Integration	Vulnerability Management	Users were facing issues with Qualys host list detection API and getting error 999 intermittently. The relevant code changes have been made to fix this issue.