Qualys Cloud Platform (VM, PC) 10.x

Release Notes

Version 10.18

April 4, 2022 (Updated April 6, 2022)

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

Qualys Cloud Platform

Qualys Policy Compliance (PC/SCAP/SCA)

Qualys Vulnerability Management (VM)

Qualys 10.18 brings you many more improvements and updates! Learn more

Qualys Cloud Platform

Update to EC2 Scan Workflows and Recommended AWS Scanner Image

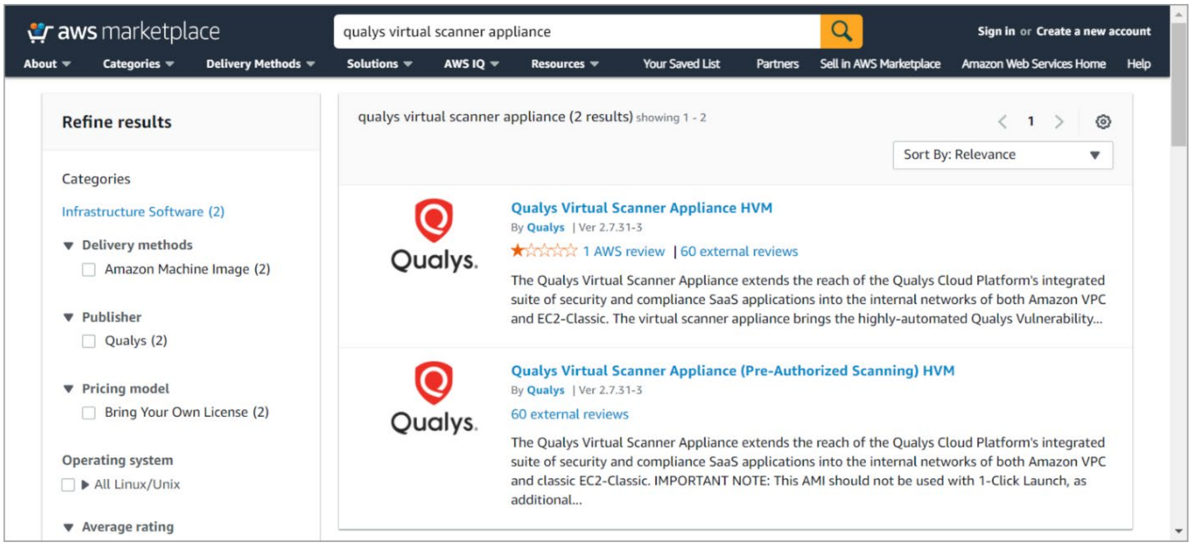
With this release, we have updated the EC2 scan workflows within the Qualys UI/API to allow customers to use a single scanner for cloud security assessments and instance-based scanning.

Users are no longer required to download the **Qualys Virtual Scanner Appliance (Pre-Authorized Scanning) HVM image** for EC2 instance-based scanning in VM, PC and SCA.

For new scanner deployments in AWS, we recommend downloading the **Qualys Virtual Scanner Appliance HVM** image from the Amazon AWS Marketplace. We plan to remove the Qualys Virtual Scanner Appliance (Pre-Authorized Scanning) HVM image from the marketplace at a future date.

For existing scanner deployments in AWS, your virtual scanner appliances deployed using the **Qualys Virtual Scanner Appliance (Pre-Authorized Scanning) HVM** image will continue to show up in EC2 scan workflows in the UI and API. Starting in this release, the virtual scanner appliances deployed in AWS using the **Qualys Virtual Scanner Appliance HVM** image will also be listed in your EC2 scan workflows. This includes any existing scanners and new scanner deployments.

To save costs, if you already have 2 scanners (1 scanner for cloud scans & 1 scanner for instance-based scans) deployed where only 1 scanner is required now, you can decommission one of your scanners. You will save on the cost of the virtual scanner license and save on AWS costs for running the appliance as an EC2 instance.



qualys virtual scanner appliance (2 results) showing 1 - 2

Qualys Virtual Scanner Appliance HVM
By Qualys | Ver 2.7.31-3
1 AWS review | 60 external reviews
The Qualys Virtual Scanner Appliance extends the reach of the Qualys Cloud Platform's integrated suite of security and compliance SaaS applications into the internal networks of both Amazon VPC and EC2-Classic. The virtual scanner appliance brings the highly-automated Qualys Vulnerability...

Qualys Virtual Scanner Appliance (Pre-Authorized Scanning) HVM
By Qualys | Ver 2.7.31-3
60 external reviews
The Qualys Virtual Scanner Appliance extends the reach of the Qualys Cloud Platform's integrated suite of security and compliance SaaS applications into the internal networks of both Amazon VPC and classic EC2-Classic. IMPORTANT NOTE: This AMI should not be used with 1-Click Launch, as additional...

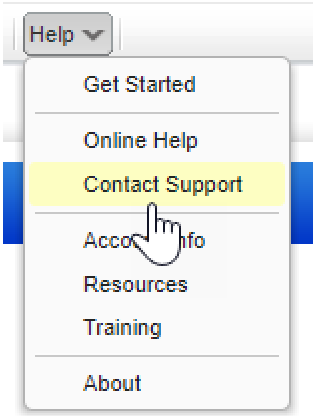
Change in Email Notification Address

To strengthen Qualys' email security posture, we are now using qualys.net as a dedicated email domain for our platform emails. As a result, the domain used for account management emails, scan notifications, and daily vulnerability feed emails will change from '@qualys.com' to '@qualys.net'.

Note: You may require to add '@qualys.net' to the approved senders' lists and domains to avoid any quarantine or incorrect categorization of Qualys emails.

For more information on this change, refer to Qualys Email Notification Change.

Separate Customer Support Portal URL for Federal Customers



As a Qualys customer, you log into the Customer Support Portal (CSP) via single sign-on from your Qualys subscription by clicking **Help** > **Contact Support** in the Qualys UI. You'll continue to access the Customer Support Portal in this way, but now if you have a Federal subscription type, we'll direct you to a different CSP URL. Having separate CSP URLs for Federal vs. Non-Federal subscription types allows us to implement additional standards required for Federal customers.

Customer Support Portal for Non-Federal accounts:
https://success.qualys.com/support/s/

Customer Support Portal for Federal accounts:
https://fed.success.qualys.com

If you are a Federal customer and you are not redirected to the Federal CSP URL when you choose **Contact Support**, then please reach out to your Technical Account Manager.

If your Qualys subscription is not enabled for Customer Support Portal access, please reach out to Qualys Support at https://www.qualys.com/support/ to request it.

Qualys Policy Compliance (PC/SCAP/SCA)

Enhanced Policy Compliance Capabilities

The following enhanced capabilities are now available in the Policy Compliance module:

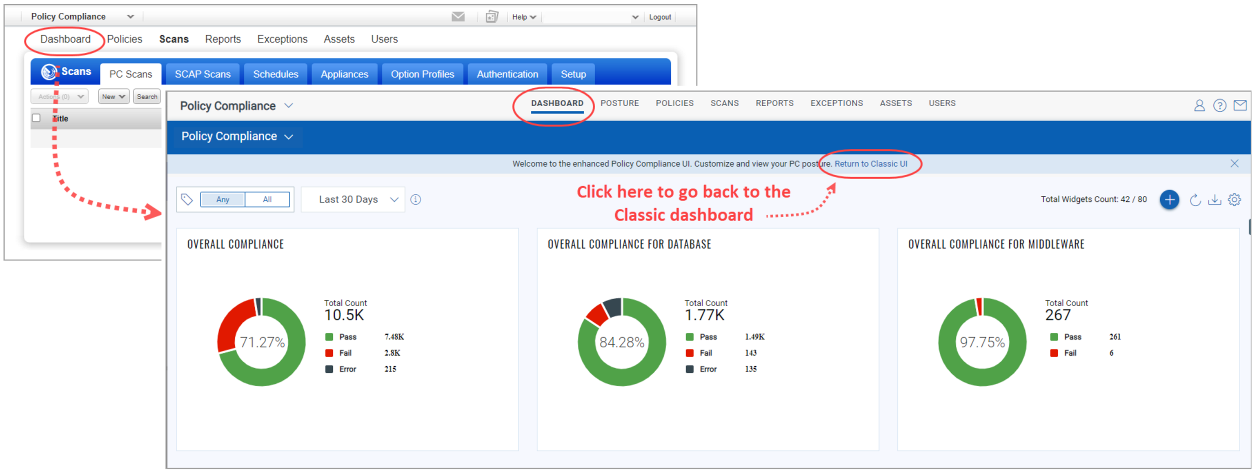
- Support for Unified Dashboard for PC in the Dashboard tab
- Security Posture management and Compliance in the new Posture tab
- Enhanced UI for better usability and user experience

With this release, you'll get capabilities for continuous risk reduction, configuration management, detection while prioritizing remediation to prevent security threats, and maintain security compliance. Qualys PC has a revamped user interface and enhanced dashboarding capabilities to help you with a faster and more dynamic way to visualize compliance and risk posture data.

New PC Dashboard

Integrated with Unified Dashboard, the easily customizable and dynamic PC Dashboard provides real-time insights into security and compliance posture of assets. The flexibility of customizable widgets makes it easier to drill down into posture of assets, identify compliance drift from best practices and prioritize remediation action to fix misconfigurations based on criticality and other factors. The dashboarding capabilities in Policy Compliance have been enhanced to help you with real-time insights into the current security and compliance posture of your asset system.

Once your subscription has been migrated, PC users will be directed to the new PC dashboard automatically when they choose the **Dashboard** option in the PC module.



Welcome to the enhanced Policy Compliance UI. Customize and view your PC posture. Return to Classic UI

Click here to go back to the Classic dashboard

The newly designed Dashboard is enhanced with customizable dynamic dashboards and widgets for visualizing and tracking security and compliance.

- Executive and operational dashboards
- Drill-down widgets

The new Dashboard enables you to visually monitor your organization's compliance by providing insights into:

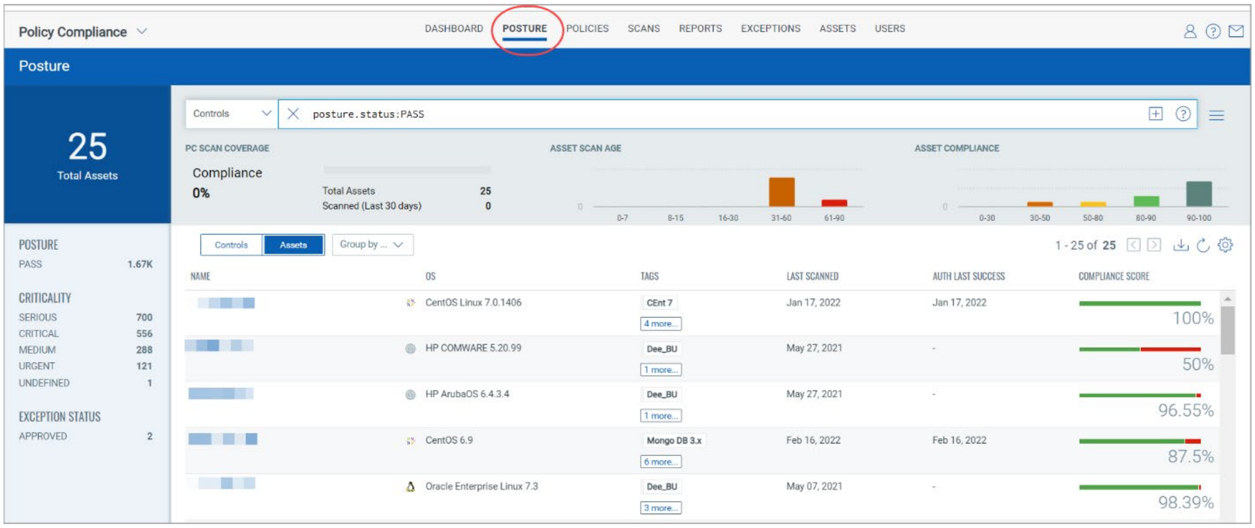
- 'Failure by Operating Systems' to monitor the compliance posture at any time
- Compliance posture for top failing controls organized by category and sub-category
- Compliance posture by OS category and sub-category

Security Posture Management and Compliance

The **Posture** tab enables you to peek into granular level details for each failing control or high-risk asset. Using Qualys Query Language (QQL) with its advanced search capabilities, makes it easier to search for compliance posture of assets without having to run the reports. In addition, you can filter evaluation results based on Assets, Technology, Criticality, and other factors to prioritize and remediate high risk assets.

The **Posture** tab helps you with:

- Faster data searches using QQLs
- Have access to failed controls posture for assets by last scan date
- Switch between the Assets and Controls view and drill down to a specific asset for granular information
- Pre-defined quick access cards to show overall compliance, failure by criticality
- View posture data grouped by Assets or Controls
- Several Group by options including control, technology, policy, criticality and more
- Drill down posture details to quickly get to the most important assets



posture.status:PASS

25 Total Assets

PC SCAN COVERAGE

Compliance 0%

Total Assets	25
Scanned (Last 30 days)	0

POSTURE	
PASS	1.67K
CRITICALITY	
SERIOUS	700
CRITICAL	556
MEDIUM	288
URGENT	121
UNDEFINED	1
EXCEPTION STATUS	
APPROVED	2

1 - 25 of 25

NAME	OS	TAGS	LAST SCANNED	AUTH LAST SUCCESS	COMPLIANCE SCORE
[redacted]	CentOS Linux 7.0.1406	CEnt 7 4 more...	Jan 17, 2022	Jan 17, 2022	100%
[redacted]	HP COMWARE 5.20.99	Dee_BU 1 more...	May 27, 2021	-	50%
[redacted]	HP ArubaOS 6.4.3.4	Dee_BU 1 more...	May 27, 2021	-	96.55%
[redacted]	CentOS 6.9	Mongo DB 3.x 6 more...	Feb 16, 2022	Feb 16, 2022	87.5%
[redacted]	Oracle Enterprise Linux 7.3	Dee_BU 3 more...	May 07, 2021	-	98.39%

Which subscriptions will get enhanced PC capabilities?

All subscriptions with the Policy Compliance (PC) module and/or PC Agent will be migrated to start using the enhanced PC UI capabilities. Once migrated, you'll see your assets and data represented in the new PC Dashboard and Posture tabs.

When will my subscription be migrated?

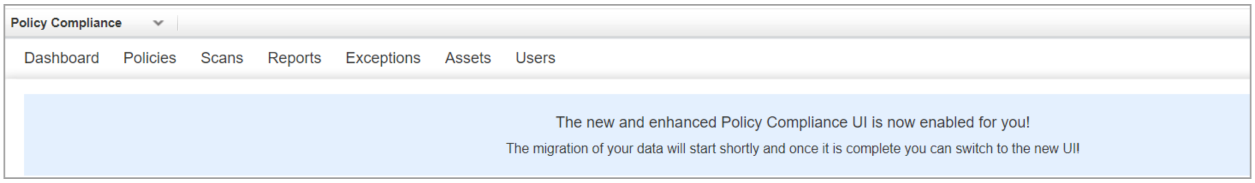
We are in the process of migrating customers on each platform and once migration is completed, the new PC Dashboard and Posture tabs will show up in your account. If you have any questions, please reach out to your Technical Account Manager or Qualys Support.

Will my SCA assets/data be migrated?

No. Only PC assets/data will be migrated. For subscriptions with both PC and SCA, only the PC assets/data in the subscription will be migrated. The SCA assets/data will not be migrated.

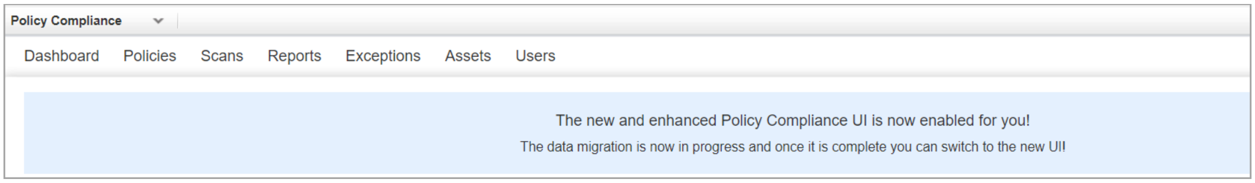
How will I know when migration has started?

The Manager Primary Contact (POC) for the subscription will see a notification on their PC Dashboard when the subscription is queued for migration.



The new and enhanced Policy Compliance UI is now enabled for you!
The migration of your data will start shortly and once it is complete you can switch to the new UI!

The notification message will change once migration has started.



The new and enhanced Policy Compliance UI is now enabled for you!
The data migration is now in progress and once it is complete you can switch to the new UI!

Can I continue to work while migration is in progress?

Yes, users can continue to work normally, including running scans and updating policies while migration is in progress.

How long will migration take?

This will vary depending on the number of PC assets and data in the subscription.

How will I know when migration is complete?

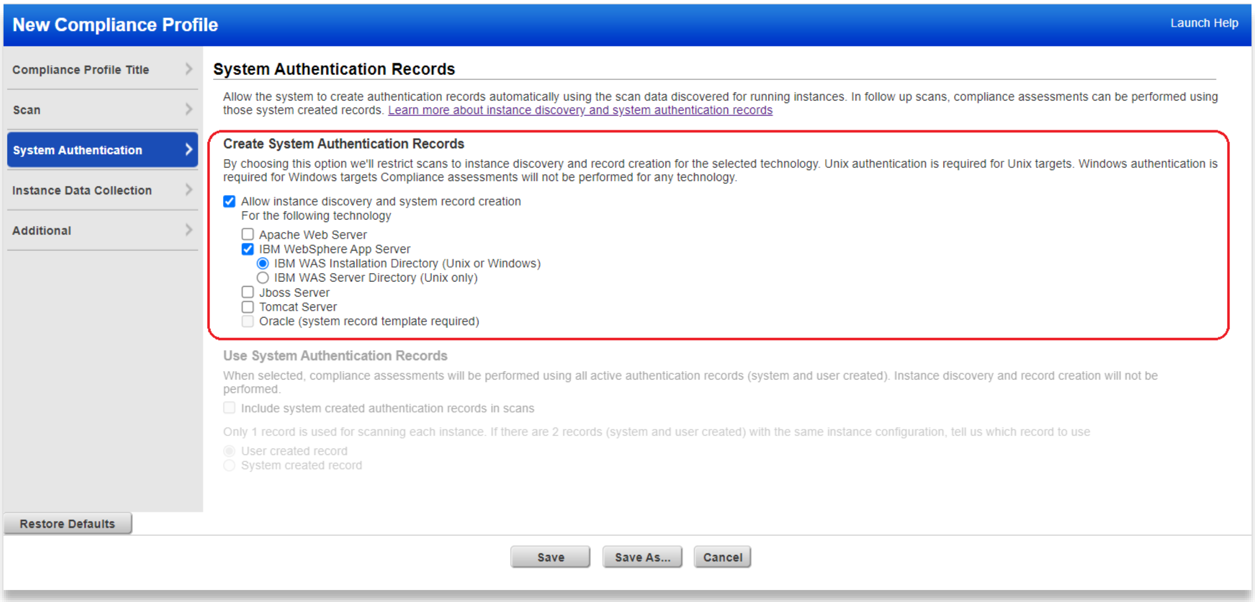
When migration is complete, all PC users in the subscription will start seeing the new PC Dashboard and Posture tab automatically.

After migration is complete, can I return to my old dashboard?

Yes. Individual users can switch between the new PC dashboard and the classic UI dashboard. Click the “Return to Classic UI” link from the new dashboard. Then, after returning to the Classic dashboard, click the “Switch to New PC Dashboard” link to go back to the new PC dashboard.

Auto Discover IBM WebSphere Application Server on Windows

Starting this release, Qualys PC enables auto-discovery and creation of system authentication records for IBM WebSphere Application Server on Windows. Now you can automatically discover all instances of IBM WebSphere Application Server on each Windows host. This new support ensures that you don't have to create a separate authentication record for compliance scans on each IBM WebSphere Application Server in your environment.



System Authentication Records

Allow the system to create authentication records automatically using the scan data discovered for running instances. In follow up scans, compliance assessments can be performed using those system created records. Learn more about instance discovery and system authentication records

Create System Authentication Records

By choosing this option we'll restrict scans to instance discovery and record creation for the selected technology. Unix authentication is required for Unix targets. Windows authentication is required for Windows targets Compliance assessments will not be performed for any technology.

☑ Allow instance discovery and system record creation
For the following technology
- □ Apache Web Server
- ☑ IBM WebSphere App Server
  - ● IBM WAS Installation Directory (Unix or Windows)
  - ○ IBM WAS Server Directory (Unix only)
- □ Jboss Server
- □ Tomcat Server
- □ Oracle (system record template required)

Use System Authentication Records

When selected, compliance assessments will be performed using all active authentication records (system and user created). Instance discovery and record creation will not be performed.

□ Include system created authentication records in scans

Only 1 record is used for scanning each instance. If there are 2 records (system and user created) with the same instance configuration, tell us which record to use

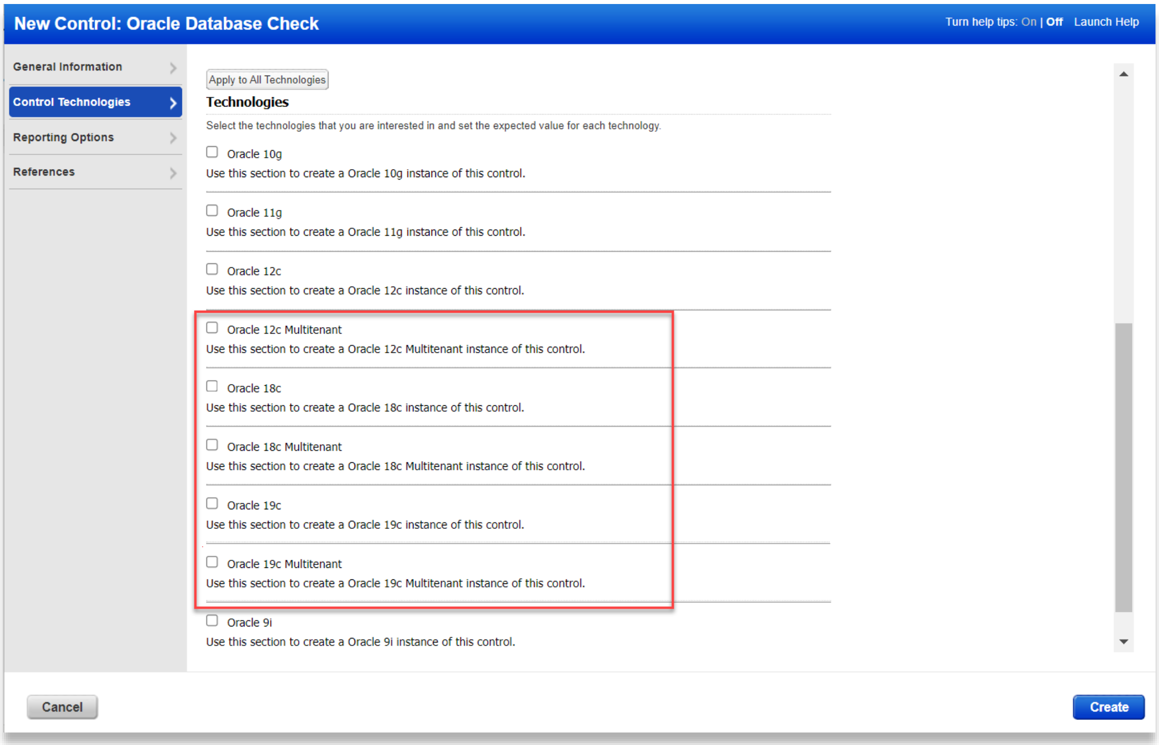
○ User created record
○ System created record

Currently, only the installation directory is supported for Windows.

Multitenant Databases are Now Supported for Oracle UDCs

With this release, Qualys PC adds support for the following technologies in the existing Oracle database UDCs:

- Oracle 12c Multitenant
- Oracle 18c Multitenant
- Oracle 19c Multitenant



Technologies

Select the technologies that you are interested in and set the expected value for each technology.

□ Oracle 10g
Use this section to create a Oracle 10g instance of this control.

□ Oracle 11g
Use this section to create a Oracle 11g instance of this control.

□ Oracle 12c
Use this section to create a Oracle 12c instance of this control.

□ Oracle 12c Multitenant
Use this section to create a Oracle 12c Multitenant instance of this control.

□ Oracle 18c
Use this section to create a Oracle 18c instance of this control.

□ Oracle 18c Multitenant
Use this section to create a Oracle 18c Multitenant instance of this control.

□ Oracle 19c
Use this section to create a Oracle 19c instance of this control.

□ Oracle 19c Multitenant
Use this section to create a Oracle 19c Multitenant instance of this control.

□ Oracle 9i
Use this section to create a Oracle 9i instance of this control.

Support for New OCA Technology

We now support the following new technology on assets for which data is collected using Out-of-Band Configuration Assessment (OCA) tracking.

- Extreme Networks VOSS 10.x

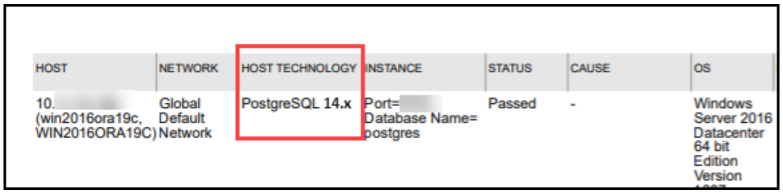
Using the OCA module, upload the corresponding configuration or command output for the assets. Then navigate to **Policy Compliance** > **Reports** tab to run the Policy Compliance Report for these technologies to view the compliance posture.

Support New Technology: PostgreSQL 14.x

With this release, we have added a new feature to extend our support for PostgreSQL authentication to include PostgreSQL 14.x. We already support PostgreSQL 9.x, 10.x, 11.x, 12.x, and 13.x on linux and windows platforms to make it easier to deploy data-backed applications.

You'll need a PostgreSQL authentication record to authenticate to a PostgreSQL database instance running on a host and scan it for compliance.

Authentication to the host is required, so you'll also need a Unix/Windows record for the host running the database. The PostgreSQL record type is only available in accounts with PC or SCA and is only supported for compliance scans.



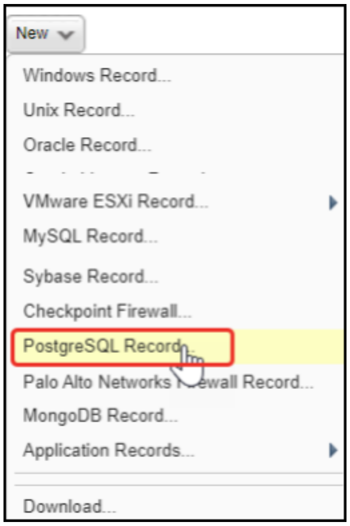
HOST	NETWORK	HOST TECHNOLOGY	INSTANCE	STATUS	CAUSE	OS
10.[redacted] (win2016ora19c, WIN2016ORA19C)	Global Default Network	PostgreSQL 14.x	Port=[redacted] Database Name= postgres	Passed	-	Windows Server 2016 Datacenter 64 bit Edition Version

How do I get started?

- Go to **Scans** > **Authentication**.

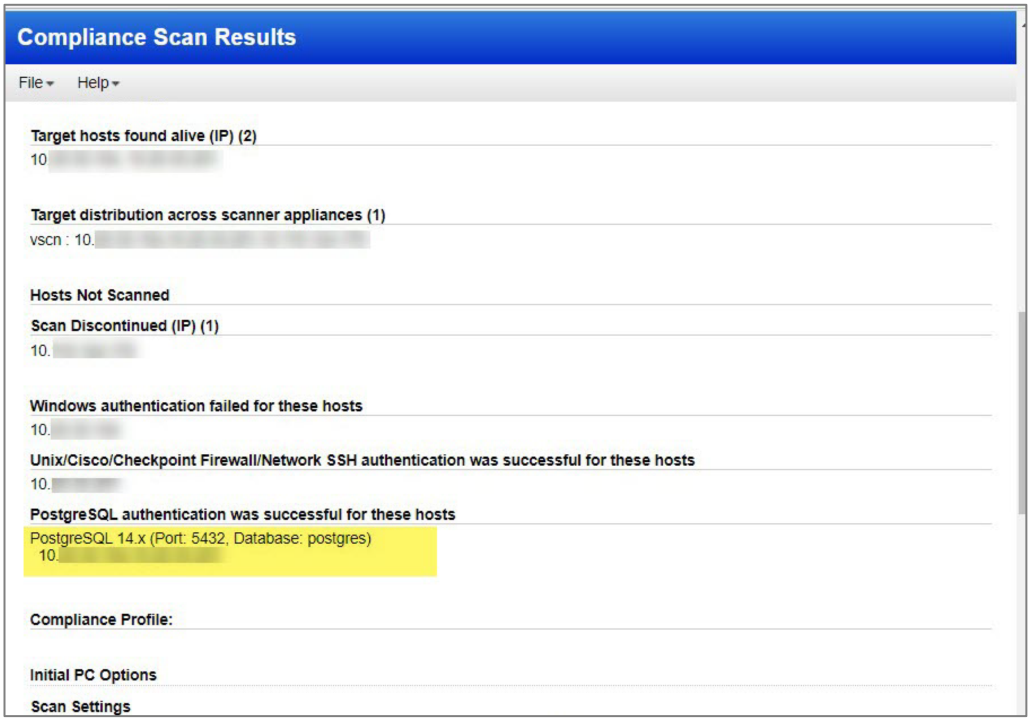
- Check that you have a Unix/Windows record already defined for the host running the database.

- Create a PostgreSQL record for the same host. Go to **New** > **PostgreSQL Record**.



Sample UI Report Changes

You'll see the PostgreSQL 14.x technology in compliance reports and in compliance scan results.



Compliance Scan Results

Target hosts found alive (IP) (2)
10[redacted]

Target distribution across scanner appliances (1)
vscn : 10.[redacted]

Hosts Not Scanned

Scan Discontinued (IP) (1)
10.[redacted]

Windows authentication failed for these hosts
10.[redacted]

Unix/Cisco/Checkpoint Firewall/Network SSH authentication was successful for these hosts
10.[redacted]

PostgreSQL authentication was successful for these hosts
PostgreSQL 14.x (Port: 5432, Database: postgres)
10.[redacted]

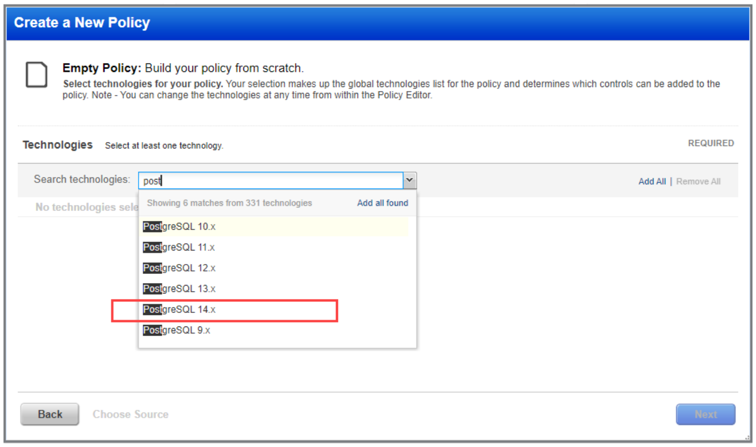
Compliance Profile:

Initial PC Options

Scan Settings

Policies and Controls

You’ll see PostgreSQL 14.x in the technologies list when creating a new policy.



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

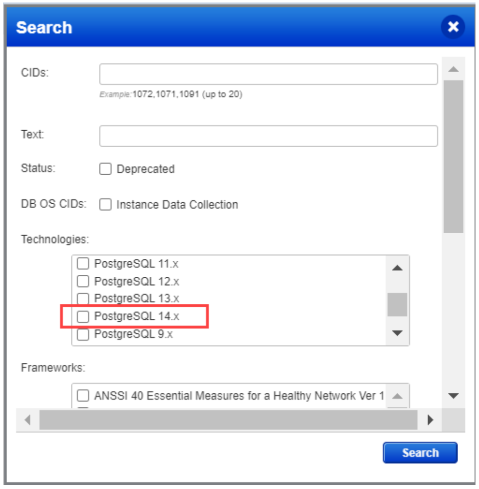
Search technologies: post

Showing 6 matches from 331 technologies

- PostgreSQL 10.x
- PostgreSQL 11.x
- PostgreSQL 12.x
- PostgreSQL 13.x
- PostgreSQL 14.x
- PostgreSQL 9.x

No technologies sele

You’ll also see it when searching controls.



Search

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

Text:

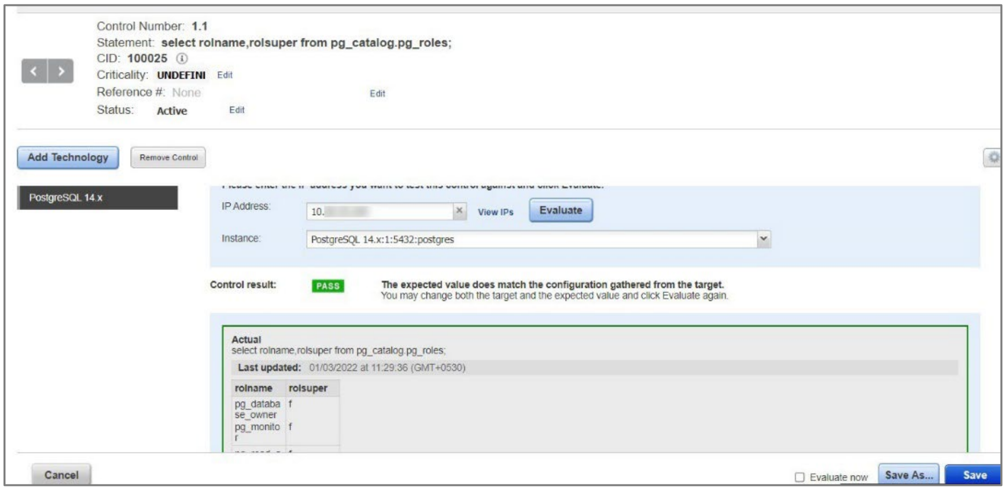
Status: □ Deprecated

DB OS CIDs: □ Instance Data Collection

Technologies:
□ PostgreSQL 11.x
□ PostgreSQL 12.x
□ PostgreSQL 13.x
□ PostgreSQL 14.x
□ PostgreSQL 9.x

Frameworks:
□ ANSSI 40 Essential Measures for a Healthy Network Ver 1

UDC Control



Control Number: **1.1**
Statement: **select rolname,rolsuper from pg_catalog.pg_roles;**
CID: **100025**
Criticality: **UNDEFINI**
Reference #: None
Status: **Active**

PostgreSQL 14.x

IP Address: 10.[redacted]

Instance: PostgreSQL 14.x:1:5432:postgres

Control result: PASS **The expected value does match the configuration gathered from the target.**
You may change both the target and the expected value and click Evaluate again.

Actual
select rolname,rolsuper from pg_catalog.pg_roles;
Last updated: 01/03/2022 at 11:29:36 (GMT+0530)

rolname	rolsuper
pg_database_owner	f
pg_monitor	f

□ Evaluate now

Qualys Vulnerability Management (VM)

Add Custom Header, Footer and Logo to Host Based Scan Reports in PDF

Now you can have a custom header, footer and logo appear on every page of your Host Based Scan Reports in PDF format. This is a subscription level setting that applies to all Host Based Scan Reports in PDF format, regardless of which user created the report or which scan report template was used. For example, you might want to include an important confidentiality notice in the footer of every report page to ensure it's not missed.

How to customize your reports

Please reach out to your Technical Account Manager or Qualys Support to add a custom header, footer and logo to your Host Based Scan Reports in PDF format. They'll add your custom text to your subscription settings.

Logo

The logo appears at the top of every page on the right side. The logo area has a fixed size of 100 pixels by 50 pixels.

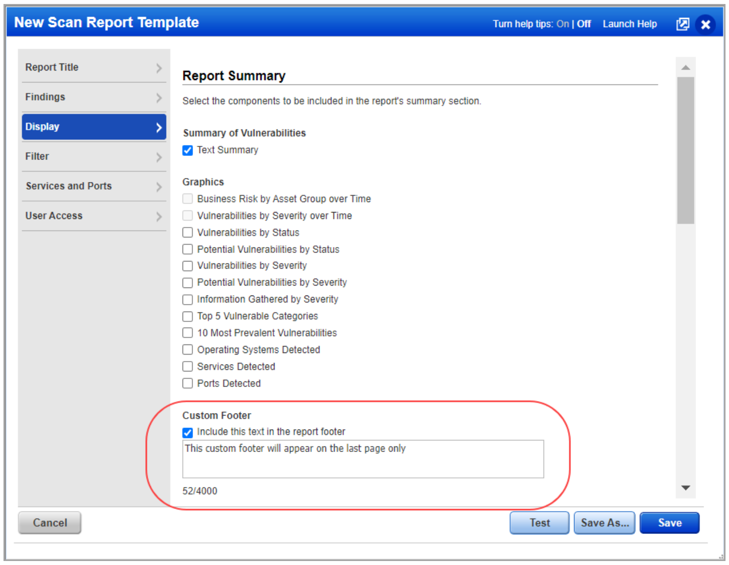
Header

The header appears at the top of every page in the center. You can include up to 50 characters for the header text. The header text is red and 26px in size.

Footer

The footer appears at the bottom of every page. You can include up to 4000 characters for the footer text. The footer text is black and 6px in size.

Note: The scan report template has an existing option that allows users to display a custom footer on the last page of their reports. This footer applies to all report formats except XML and CSV. You can still include this custom footer on the last page along with the subscription level footer which will appear on every page, including the last page.



Report Summary

Select the components to be included in the report's summary section.

Summary of Vulnerabilities

☑ Text Summary

Graphics

□ Business Risk by Asset Group over Time
□ Vulnerabilities by Severity over Time
□ Vulnerabilities by Status
□ Potential Vulnerabilities by Status
□ Vulnerabilities by Severity
□ Potential Vulnerabilities by Severity
□ Information Gathered by Severity
□ Top 5 Vulnerable Categories
□ 10 Most Prevalent Vulnerabilities
□ Operating Systems Detected
□ Services Detected
□ Ports Detected

Custom Footer

☑ Include this text in the report footer

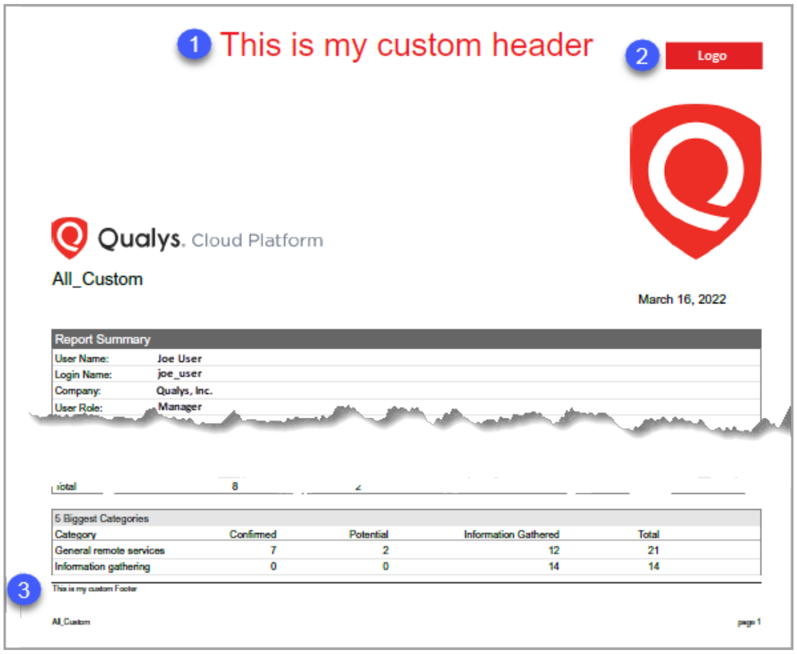
This custom footer will appear on the last page only

52/4000

Sample Host Based Scan Report

This sample Host Based Scan Report in PDF format illustrates how the (1) header, (2) logo, and (3) footer will appear in your report.

First page of the PDF report



This is my custom header

Logo

Qualys. Cloud Platform

All_Custom

March 16, 2022

Report Summary	
User Name:	Joe User
Login Name:	joe_user
Company:	Qualys, Inc.
User Role:	Manager

Total 8 2

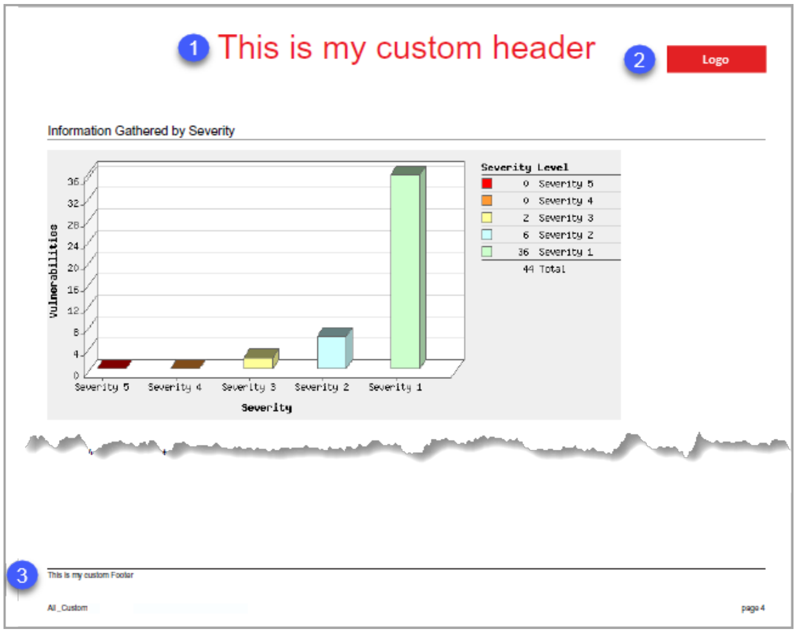
5 Biggest Categories				
Category	Confirmed	Potential	Information Gathered	Total
General remote services	7	2	12	21
Information gathering	0	0	14	14

This is my custom Footer

All_Custom

page 1

Subsequent pages of the PDF report



This is my custom header

Logo

Information Gathered by Severity

Severity Level		
🟥	0	Severity 5
🟧	0	Severity 4
🟨	2	Severity 3
🟦	6	Severity 2
🟩	36	Severity 1
	44	Total

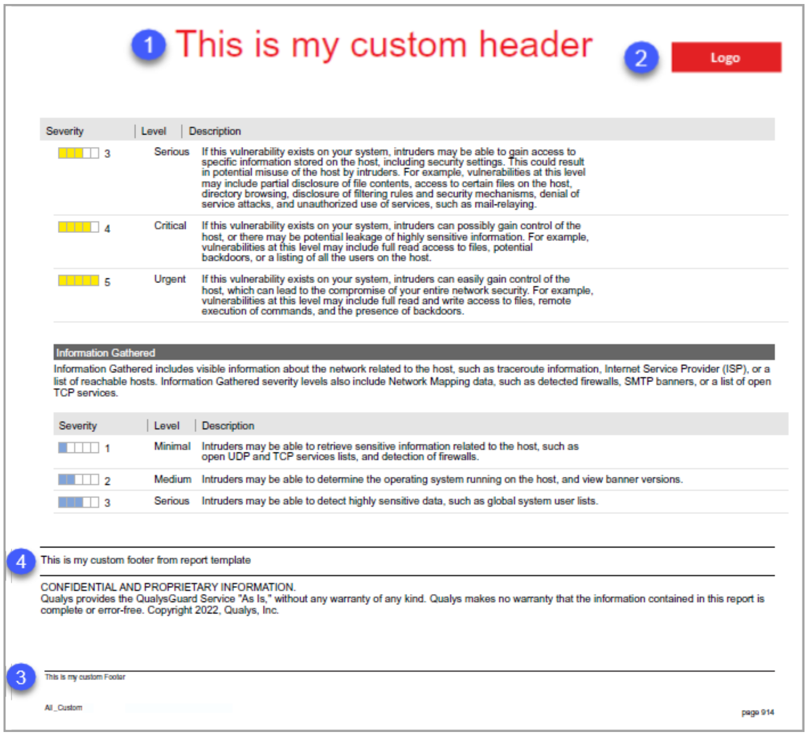
This is my custom Footer

All_Custom

page 4

Last page of the PDF report

In this example, the user has defined a custom footer in the report template along with the subscription level footer. On the last page of the report, you'll see the (3) footer defined at subscription level and the (4) footer defined in the report template.



This is my custom header

Severity	Level	Description
3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
1	Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
2	Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
3	Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.

This is my custom footer from report template

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 2022, Qualys, Inc.

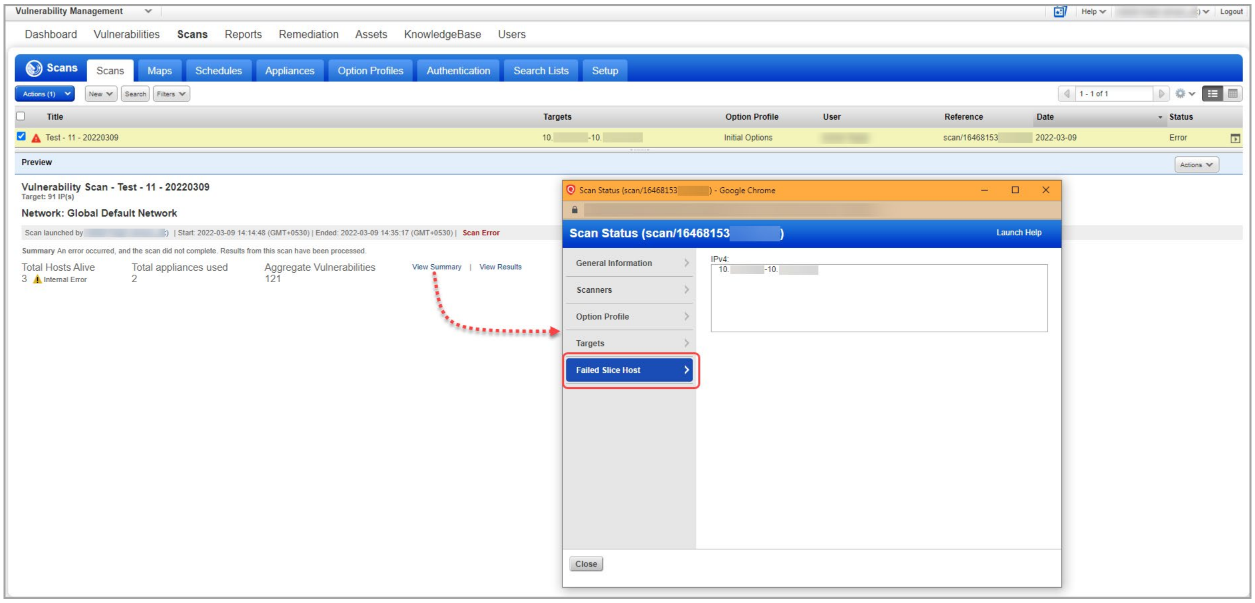
This is my custom Footer

All_Custom [redacted]

page 914

Failed Slice Host in Scan Summary

With this release, you can see a list of failed targets (IPv4, IPv6, DNS, and NETBIOS) in the Failed Slice Host section of the vulnerability scan summary.



Title	Targets	Option Profile	User	Reference	Date	Status
☑ Test - 11 - 20220309	10.[redacted]-10.[redacted]	Initial Options	[redacted]	scan/16468153[redacted]	2022-03-09	Error

Vulnerability Scan - Test - 11 - 20220309
Target: 91 IP(s)

Network: Global Default Network

Scan launched by [redacted]) | Start: 2022-03-09 14:14:48 (GMT+0530) | Ended: 2022-03-09 14:35:17 (GMT+0530) | Scan Error

Summary An error occurred, and the scan did not complete. Results from this scan have been processed.

Total Hosts Alive	Total appliances used	Aggregate Vulnerabilities
3 ⚠ Internal Error	2	121

Scan Status (scan/16468153[redacted]) - Google Chrome

Scan Status (scan/16468153[redacted])

IPv4:
10.[redacted]-10.[redacted]

Issues Addressed

- Now the Conflict Report that appears when deleting asset groups will display the correct number of Scheduled Reports with conflicts.
- Fixed an issue where the user could not build a scanner appliance list when configuring an EC2 scan because the option appeared disabled. This is now fixed.
- Now when launching or scheduling a scan, if you pick the "All Scanners in TagSet" Scanner Appliance option, then we will automatically enable the "Use IP Network Range Tags for Include" option under Target Hosts > Tags, and this option cannot be disabled.
- We fixed an issue for AGMS-enabled subscriptions where when the user launched a map on an asset group with a domain/netblock specified, the scan was launched on the entire netblock defined for the domain instead of only the netblock specified in the asset group.
- We fixed an issue where offline scanners were not listed for Unit Manager users on the Appliances list even when the Unit Manager was granted the "Manage offline scanner appliances" permission. Now offline scanners will be listed.
- We fixed an issue where compliance reports included report data for agent middleware instances which no longer existed on the target.
- We fixed an issue so that anytime the Compliance Policy Report Template has "Cloud Metadata" selected, the CSV report will include the Cloud Metadata headers even if no EC2 instance is found in the policy.
- We made a fix to the Missing Values list under Cause of Failure in Compliance Reports so this section only shows unmatched expected values.
- We fixed an issue where some incorrect values appeared in the Unexpected Values section under Cause of Failure in Compliance Reports. Now you can view the correct values in the report.
- We fixed an issue in Compliance Scan Reports where report data for deleted database instances on targets was being reported.
- We fixed an issue to improve the loading of the User Accounts (Users > Users) page.
- We fixed a performance issue where in some cases the PC > Reports > Policy Summary tab was not loading properly.
- We fixed an issue in Consultant accounts where the Client information was not being populated on the vulnerability scans data list for scans that used an option profile with the "Select at run time" vulnerability detection option enabled.
- We fixed an issue where "Host Alive" count in scan summary was shown incorrectly when the host was successfully scanned and vulnerabilities were detected.
- We fixed an issue in subscriptions with Korean language enabled where the Results section in Scan Reports did not correctly display Korean software names. Now the Korean software names will be shown correctly.
- We fixed an issue where a period (.) appended to the end of a DNS hostname caused duplicate asset entries on the Host Assets list. Now the period will be trimmed.
- We fixed an issue with Payment Card Industry (PCI) Executive and Technical reports generated from the VM/VMDR module where the list of IPs were not shown in the Overall PCI Status section. Also, we fixed an issue with the Overall PCI Status was showing the incorrect status during the report generation.

- We fixed an issue in Patch Report where no data appeared in the report (CSV and XML) for an asset group included in the report target.
- We have now fixed an issue where the sub-user was unable to create a virtual host when the Network Support feature was disabled in the subscription.
- We have enhanced our backend functionality to reduce the space issue to the Disk Usage for Reports were not being properly calculated for the subscription leading to new reports not being allowed.
- Now non-Manager users will see the correct count of authentication records they have access to on the Authentication Records list and the Overview Credential Breakdown.
- Now the Default Value input field is marked as a Required field when editing User Defined Controls (UDCs) in the UI.
- We fixed an issue with schedule scans that failed with “Invalid network for scanner appliance error.”
- Now a scan will not result in an error as long as there’s at least one valid scanner in the scanner list for the scan job.
- We fixed an issue for AGMS-enabled subscriptions so users will now get the correct assigned asset group list returned from the User List API (/msp/user_list.php).
- Now you’ll get an appropriate error message when updating a host in a custom network using the API and the host_id specified does not belong to the network_id specified or the network_id was not specified.
- We fixed an issue where the Update Schedule Scan API incorrectly returned an error message in the API response stating that a virtual or physical scanner is needed to scan private IPs. Now users can scan private and non-internal IPs in same scan job with virtual/physical scanner.
- We fixed an issue where the user could not create a Windows authentication record with the same IP present in a different network via API. Now users can create a Windows record if the IP is in a different network. An error for the duplicate network is displayed if a user tries to create a Windows record in the same network with the same IP.
- When the customer was using asset tags-related parameters in the Posture API call, the posture data was not getting filtered properly.
- Improved UI and API validation error messages and documentation to explain that if the Network Support feature is enabled for your subscription, then authentication records for application technologies must have the same network selection as the corresponding Unix/Windows authentication record for the host running the application.