Qualys Cloud Platform (VM, PC) 10.x

Release Notes

Version 10.19

June 7, 2022 (Updated June 15, 2022)

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

Qualys Cloud Platform

Updated Text in Password Retrieval Email

Qualys Policy Compliance (PC/SCAP/SCA)

Detailed Activity Logs for Policy Updates
Evaluated Timeframe Filter Added To Dashboard and Policy Summary
New Technology Support: Oracle WebLogic Server 14c (Scanner and Agent)
New Technology Support: Apache Tomcat 10.x (Scanner and Agent)
Support for New OCA Technologies

Qualys Vulnerability Management (VM)

New option of OT Device Scan (safe ICS active scan) for ICS
VM Scans Launched on FQDNs Shared as DNS Scan with PCI

API Changes

Refer to the Cloud Platform 10.19 API Release Notes for API changes in this release.

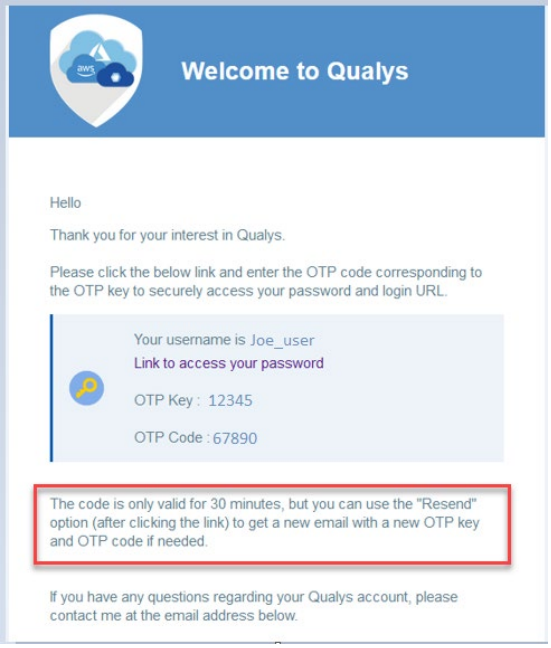
Qualys 10.19 brings you many more improvements and updates! Learn more

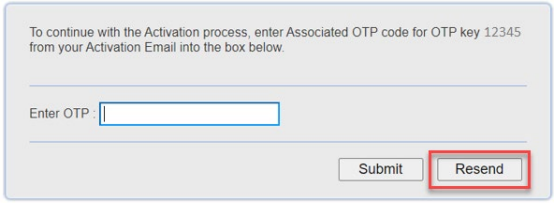
Qualys Cloud Platform

Updated Text in Password Retrieval Email

To obtain a password for a new account or a new password for an existing account, you get an email from Qualys with a link that offers secure access to your login information, an OTP key & OTP code. We updated the text in this email as highlighted below to make it clear that you can use the “Resend” option to get a new email with a new OTP key & OTP code when needed.

The OTP code is valid only for 30 minutes, but you can get a new OTP code by clicking the link in the email, then clicking the “Resend” button as shown below.





Qualys Policy Compliance (PC/SCAP/SCA)

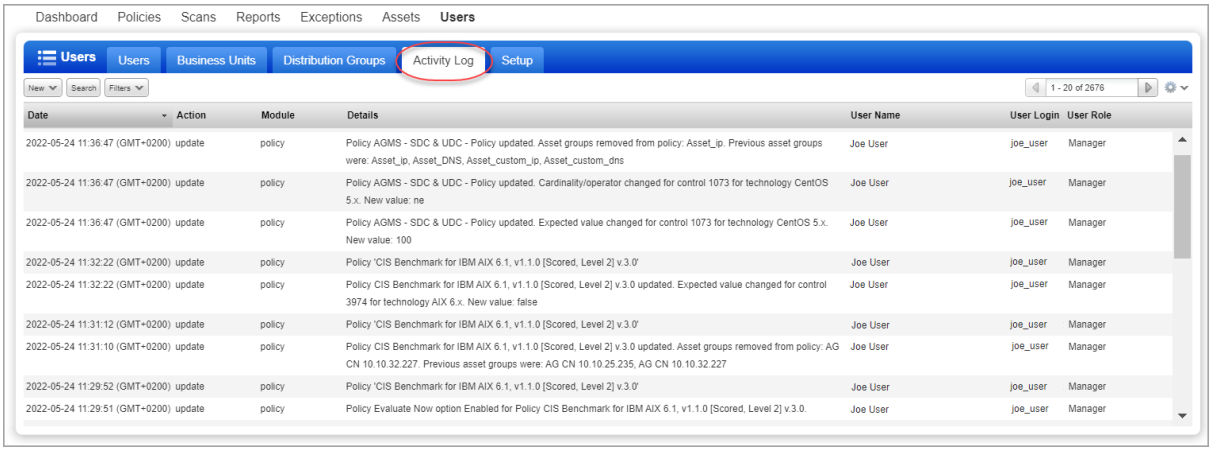
Detailed Activity Logs for Policy Updates

With this release, we have added more detailed activity logs for certain user actions performed while editing a policy in the Policy Editor. This allows for better monitoring and tracking of policy changes.

These policy changes will now be logged in detail:

- Control is added or removed
- Control technology is added or removed
- Expected value for a control is changed
- Policy technology is added or removed
- Policy asset group is added or removed
- Policy Evaluate Now option is enabled or disabled

To see activity logs for policy updates, go to **Users** > **Activity Log**. Logs for policy updates have **Action** "update" and **Module** "policy". In the **Details** column, you'll see the policy title and a description of the change that was made. The **User Name** and **User Login** columns let you know which user performed the action.



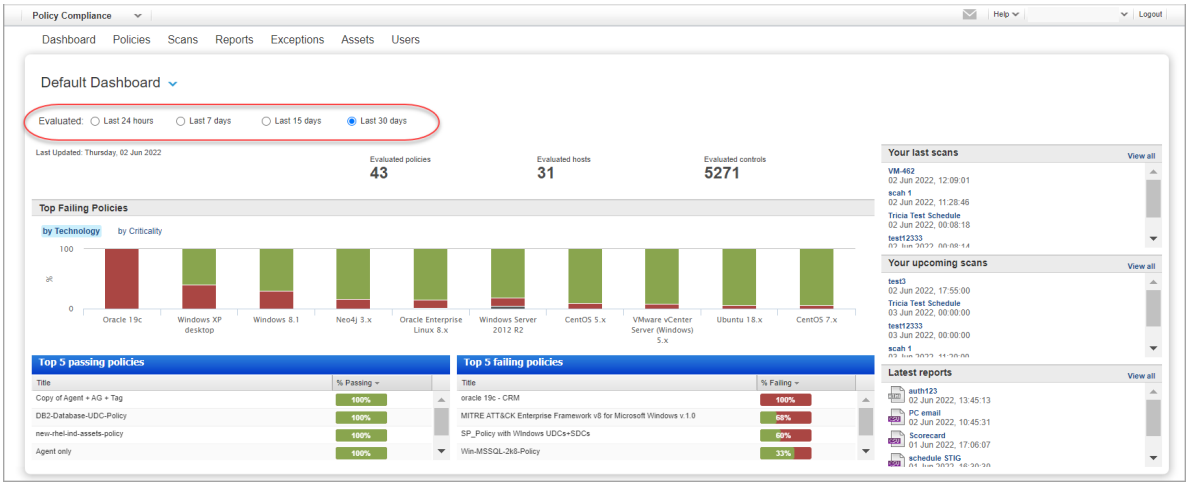
Evaluated Timeframe Filter Added To Dashboard and Policy Summary

When viewing a **Classic UI Dashboard** or the **Policy Summary** tab under **Reports**, you'll see the new **Evaluated** timeframe filter. This filters host control data by the last evaluated date. The Dashboard and Policy Summary will only include data for controls that were last evaluated in the timeframe that you select. This change is primarily for the benefit of SCA customers and customers with SCA+PC that want to see a combined dashboard. PC customers that have already been migrated to the Enhanced Policy Compliance UI will not be affected unless you choose the option to return to the Classic UI Dashboard.

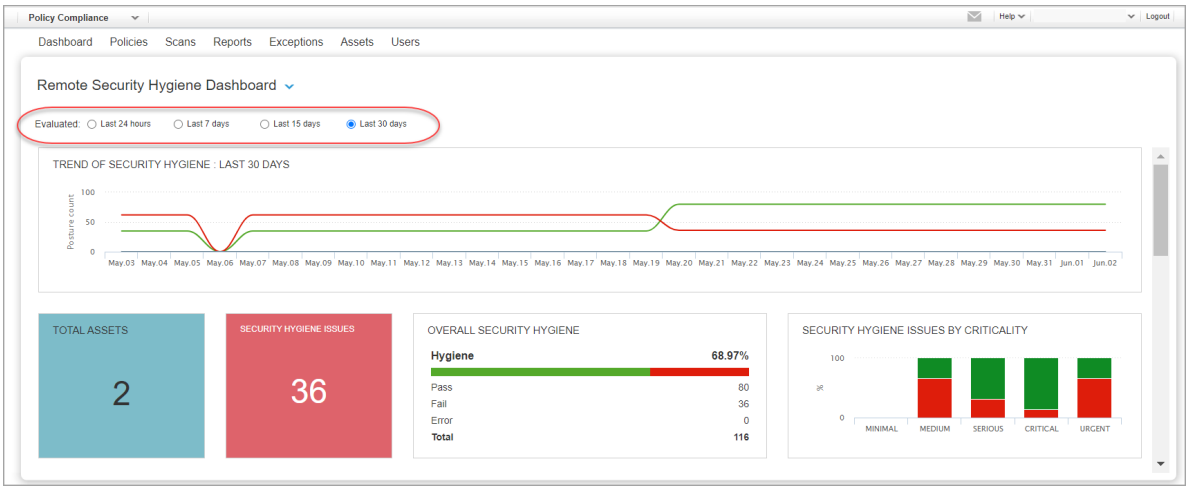
For the **Evaluated** timeframe filter, you can choose to include controls evaluated in the last 24 hours, last 7 days, last 15 days or last 30 days (the default).

Classic UI Dashboards

The **Default Dashboard** has been updated to include the new **Evaluated** timeframe filter. Note that this filter applies to all sections of the dashboard except for the following: Your last scans, Your upcoming scans and Latest reports.

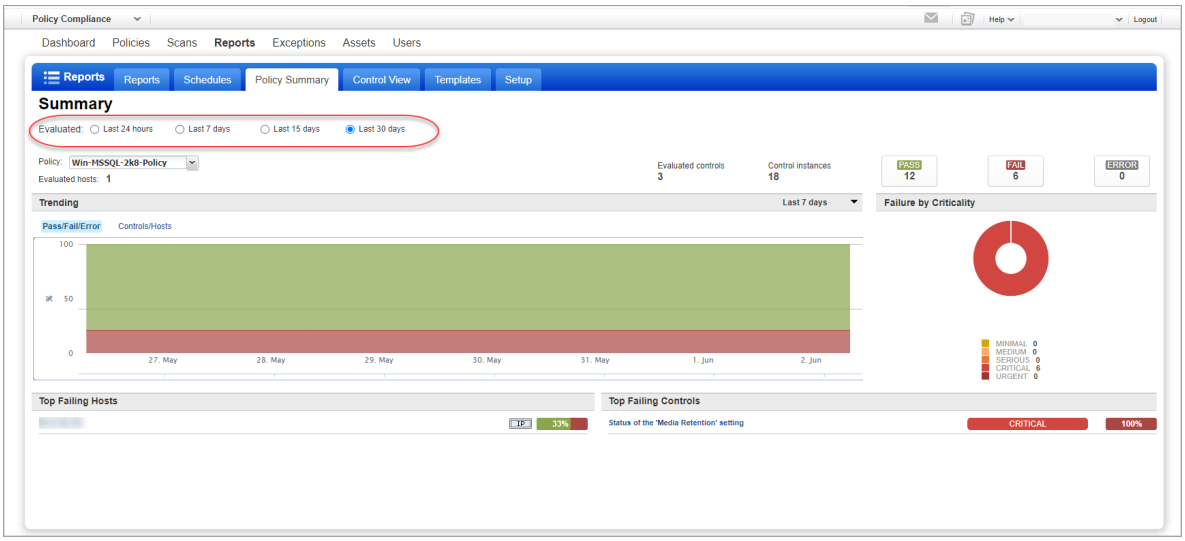


The **Remote Security Hygiene Dashboard** has also been updated to include the new **Evaluated** timeframe filter.



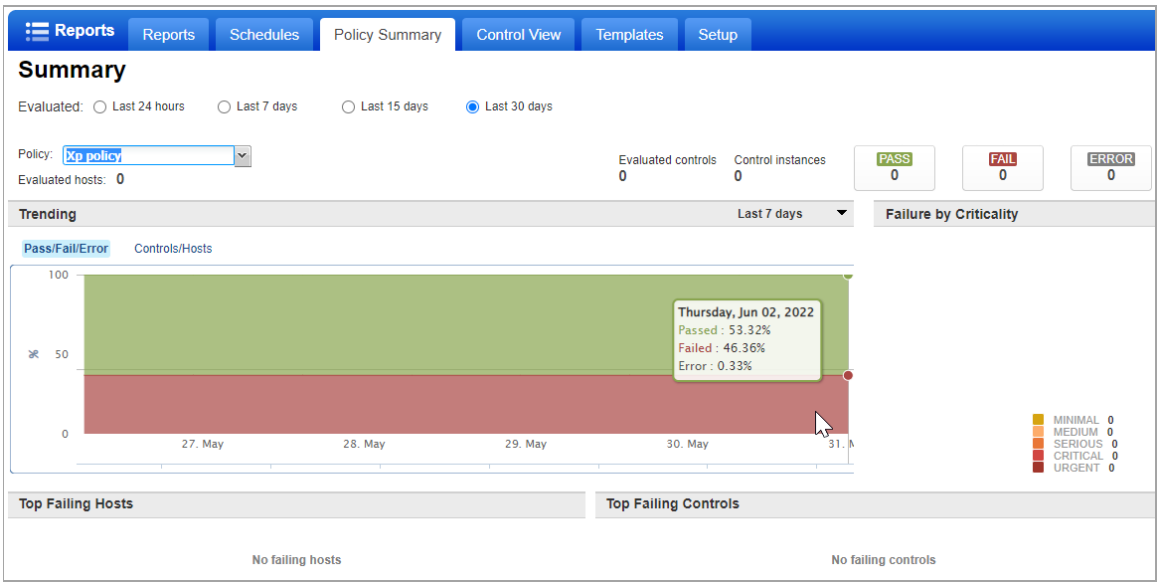
Policy Summary

The **Reports** > **Policy Summary** tab shows a dashboard view of your compliance status for a single policy. With the new **Evaluated** filter, only controls evaluated in the timeframe selected will be included in this view. The filter is applied to all sections, except the **Trending** graph.



If you have not evaluated any controls for the selected policy in the timeframe selected, then the **Policy Summary** will show 0 counts for the number of evaluated hosts, evaluated controls, control instances, number of controls with Pass/Fail/Error, and there won't be any top failing hosts or top failing controls listed. See the example below.

As mentioned, the **Evaluated** timeframe filter is not applied to the **Trending** graph. This graph will show data as long as controls were evaluated at some point and may include data from more than 30 days ago. Note that the **Trending** graph has its own timeframe selection (from last 7 days to last 90 days).

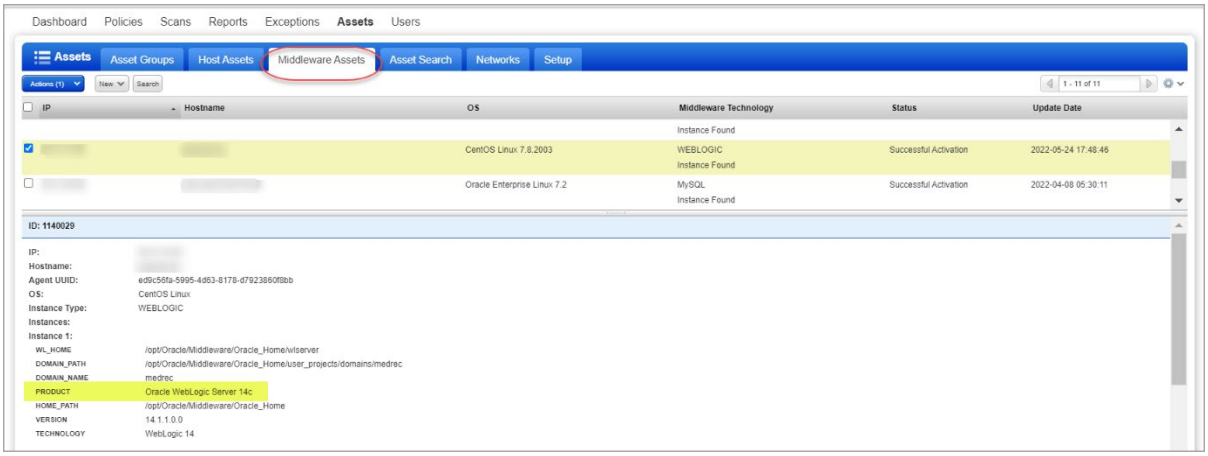


New Technology Support: Oracle WebLogic Server 14c (Scanner and Agent)

We've extended our support for Oracle Weblogic Server to include Oracle WebLogic Server 14c. This technology is supported for authenticated scans using a scanner and for agent scans.

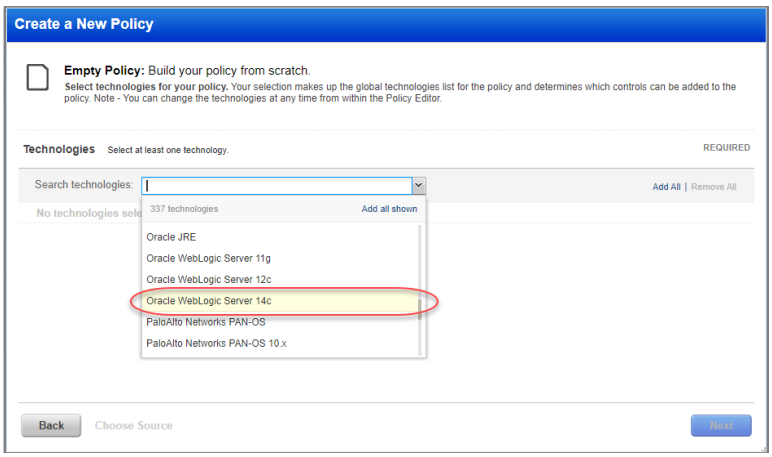
If you're using a scanner, you'll need to create an Oracle WebLogic Server authentication record in order to authenticate to the web server running on a Unix host. Unix authentication is also required so you'll also need a Unix record for the host running the web server. Go to **Scans** > **Authentication** > **New** to create authentication records for Unix and Oracle WebLogic Server.

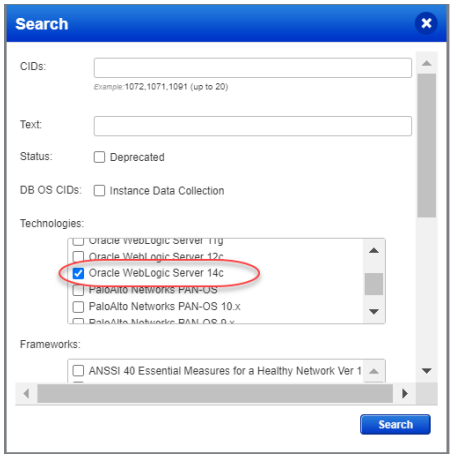
If you're using Cloud Agent for Policy Compliance (PC), Oracle WebLogic Server 14c instances will be auto-discovered by the Cloud Agent. When an Oracle WebLogic Server 14c instance is detected on a host by an agent scan, it will appear on the **PC** > **Assets** > **Middleware Assets** tab.



Policies and Controls

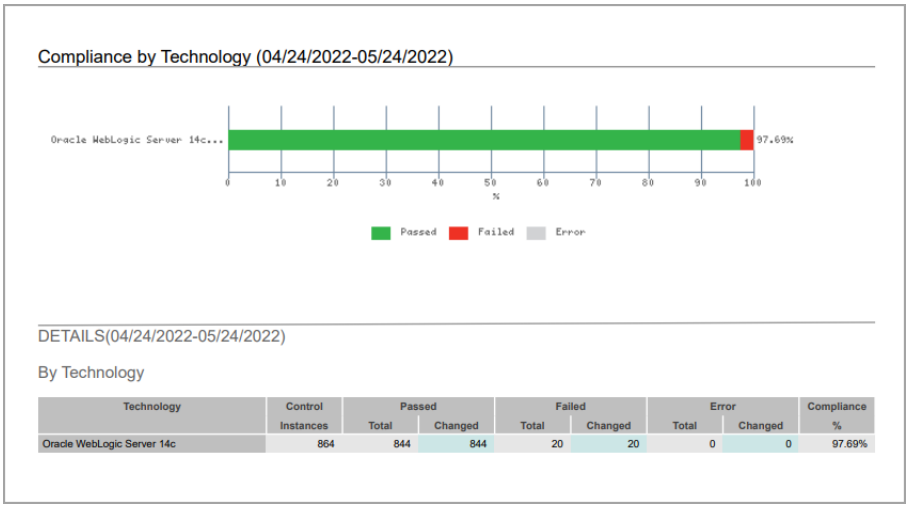
You'll see Oracle WebLogic Server 14c in the **Technologies** list when creating new policies and when searching controls by technology.





Sample Report

You'll see the Oracle WebLogic Server 14c technology for scanned hosts in Scan Results and Compliance Reports. Here's a sample Scorecard Report where the new technology appears.

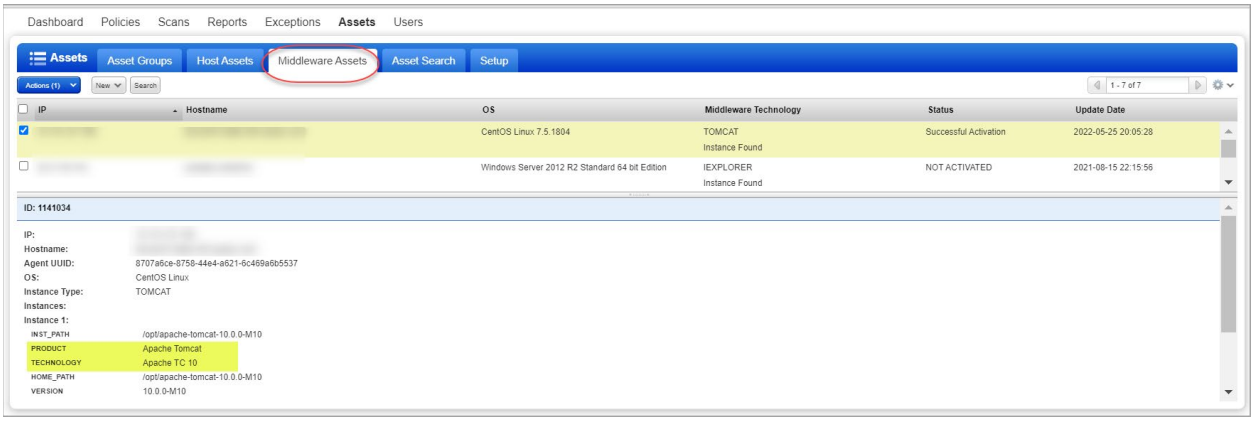


New Technology Support: Apache Tomcat 10.x (Scanner and Agent)

We've extended our support for Apache Tomcat Server to include Apache Tomcat 10.x on Unix hosts. This technology is supported for authenticated scans using a scanner and for agent scans. Note that Apache Tomcat 10.x is not supported for Windows hosts.

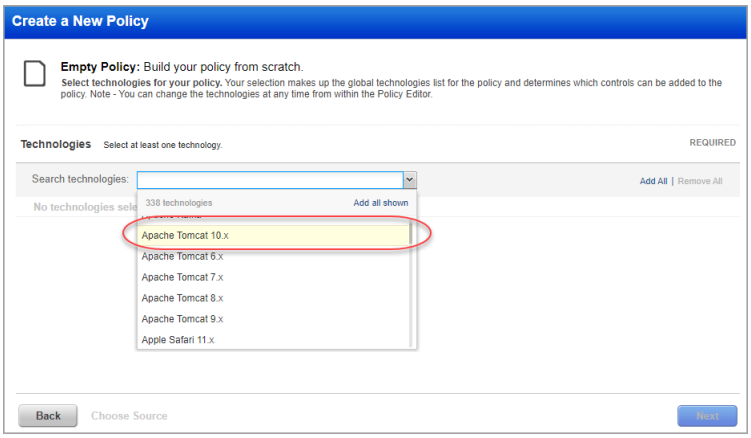
If you're using a scanner, you'll need to create a Tomcat Server authentication record in order to authenticate to the server running on a Unix host. You'll also need a Unix record defined for the host running the server. Go to **Scans** > **Authentication** > **New** to create new authentication records for Unix and Tomcat Server.

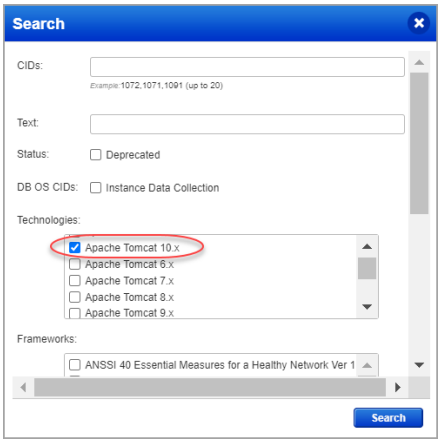
If you're using Cloud Agent for Policy Compliance (PC), Apache Tomcat 10.x instances will be auto-discovered by the Linux Cloud Agent. When a Tomcat Server 10.x instance is detected on a host by an agent scan, it will appear on the **PC** > **Assets** > **Middleware Assets** tab.



Policies and Controls

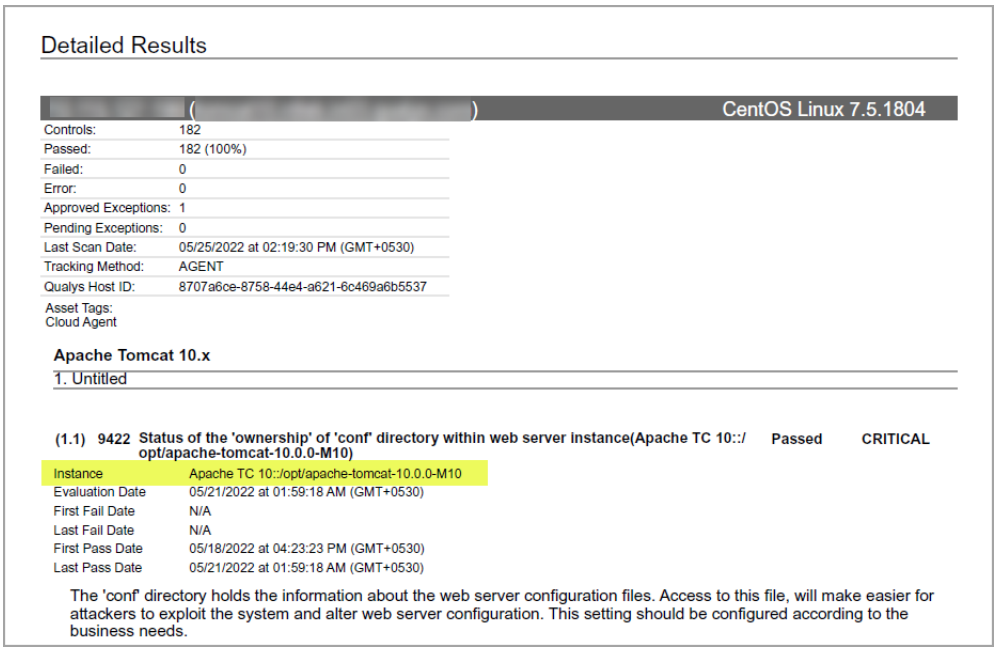
You'll see Apache Tomcat 10.x in the **Technologies** list when creating new policies and when searching controls by technology.





Sample Report

You'll see the Apache TC 10 instance technology for scanned hosts in Scan Results and Compliance Reports. Here's a sample report with an Apache Tomcat 10 instance.



Detailed Results

( ) CentOS Linux 7.5.1804

Controls:	182
Passed:	182 (100%)
Failed:	0
Error:	0
Approved Exceptions:	1
Pending Exceptions:	0
Last Scan Date:	05/25/2022 at 02:19:30 PM (GMT+0530)
Tracking Method:	AGENT
Qualys Host ID:	8707a6ce-8758-44e4-a621-6c469a6b5537

Asset Tags:
Cloud Agent

Apache Tomcat 10.x

1. Untitled

(1.1) 9422 Status of the 'ownership' of 'conf' directory within web server instance(Apache TC 10::/opt/apache-tomcat-10.0.0-M10) Passed CRITICAL

Instance	Apache TC 10::/opt/apache-tomcat-10.0.0-M10
Evaluation Date	05/21/2022 at 01:59:18 AM (GMT+0530)
First Fail Date	N/A
Last Fail Date	N/A
First Pass Date	05/18/2022 at 04:23:23 PM (GMT+0530)
Last Pass Date	05/21/2022 at 01:59:18 AM (GMT+0530)

The 'conf' directory holds the information about the web server configuration files. Access to this file, will make easier for attackers to exploit the system and alter web server configuration. This setting should be configured according to the business needs.

Support for New OCA Technologies

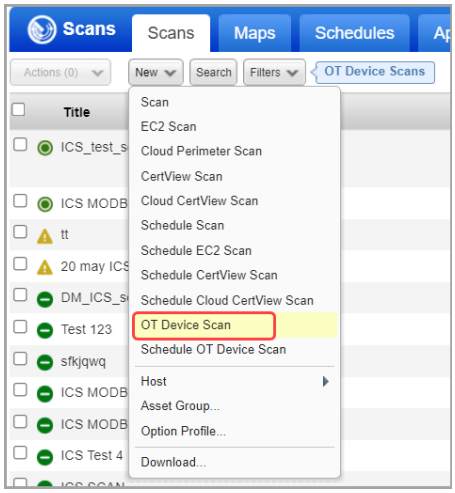
We now support the following new technologies on assets for which data is collected using Out-of-Band Configuration Assessment (OCA) tracking.

- CheckPoint Gaia SP (R80, R81)
- Alcatel Devices (OmniSwitch AOS 6.x)
- Arista MOS

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.

Qualys Vulnerability Management (VM)

New option of OT Device Scan (safe ICS active scan) for ICS



Qualys extends the VMDR capabilities to perform safe ICS active scan for Industrial Control Systems (ICS). This new limited scan (OT Device Scan) is designed to be safe for industrial devices, communicating with the target devices over industrial network protocols, querying the sensitive ICS devices in the language they understand. It eliminates the risk of destabilizing device operations during scans. In this release of VMDR, safe ICS active scan supports devices speaking Siemens S7Comm, Ethernet/IP, BACnet, DNP3 and Modbus protocols.

Note: The OT Device scan option is visible only if ICS is turned on in your subscription.

OT Device Scan option is provided for the safe ICS active scan. It is a protocol-oriented scan that fetches identity-related attributes. ICS collects the data from VM/VMDR, extracts the information and detects the vulnerability. There are many options to suit your needs. The following Option Profiles are supported for OT Device Scan.

- Bacnet with UDP
- DNP3 with TCP
- Ethernet IP with TCP
- Ethernet IP with UDP
- Modbus with TCP
- S7COMM with TCP
- SMB with TCP
- SSH with TCP

SMB with TCP and SSH with TCP protocols are added to scan the engineering stations like HMI, Windows or Linux machines used to configure the PLC. These devices are called OT Endpoints.

VM Scans Launched on FQDNs Shared as DNS Scan with PCI

Now when you share the results from a PCI external scan launched in the VM/VMDR application with the PCI service and the scan target included only FQDNs, the scan result is saved with scan type “DNS” in PCI where previously it was saved as scan type “IP”. In the PCI module, you can view the scan results shared from VM/VMDR by going to **Network** > **Scan Results**. The **Scan Type** column indicates whether the scan was a DNS or IP scan.

Note that if the scan target includes a mix of FQDNs and IP addresses, then the shared scan result is saved in PCI with “IP” scan type. Since the PCI module supports a single scan with a single host type, we recommend you scan FQDNs and IP addresses in separate scan jobs.

Notes:

- This functionality is available to VM/VMDR users that have set up PCI account links.
- You can only scan FQDNs when the DNS Tracking feature is enabled for your subscription.

Issues Addressed

- We fixed an issue where special characters entered in User Defined Controls (UDCs) were being converted to underscores (_) when the control was saved. Now special characters will not be converted to underscores.
- We fixed an issue where policy reports could not be successfully generated in some cases when the policy had more than 2000 hosts and the report template had host statistics and cloud metadata selected.
- In the Sybase Authentication Record, the Enable Password Encryption option will now be hidden when Authentication Vault is selected in the record since this option only applies when Basic Authentication is selected in the record.
- We increased the number of characters allowed for the "password" input parameter for several authentication record types when creating authentication records using the API, making it consistent with the number of characters allowed when creating records from the UI.
- We fixed an issue where the Authentication Details page was not being properly updated in cases where "Tag Support for Authentication Records" is enabled and the authentication records map to EC2 hosts.
- We fixed an issue where the scanned IP addresses in the Detailed Results section of Scan Results were not listed in ascending order. Now they will be shown in ascending order.
- Only one saved scan can be included in Scan Reports with Scan Based Findings when XML or CSV format is selected. We fixed an issue where we allowed users to pick more than one saved scan for these formats even though only one is allowed. Now an error will appear in the UI when the user selects multiple saved scans for reports in these formats.
- We fixed an issue where a vulnerability was not being properly marked as Fixed when the "Close Vulnerabilities on Dead Hosts" option was enabled in the option profile used at scan time.
- We improved performance for scans launched using the Scan Launch API.
- We fixed a performance issue where in some cases the PC > Reports > Policy Summary tab was not loading properly.