



Qualys Cloud Platform (VM, PC) v10.x

Release Notes

Version 10.4

October 12, 2020 (Updated November 4, 2020)

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

Qualys Cloud Platform

[Modules Displayed in Module Picker and Permissions](#)

[LDAP Authentication Support for MongoDB Record](#)

Qualys Vulnerability Management (VM)

[Target Type A10 Now Supported in Unix Authentication Record](#)

Qualys Policy Compliance (PC/SCAP/SCA)

[New Authentication Record for Kubernetes Now Available](#)

[Support for Editing a User-Defined Control](#)

[New Option to Auto Discover IBM WebSphere App Server instances from Server Directory](#)

[Launch/Schedule Compliance Scans on FQDNs](#)

[Policy Evaluation and Compliance Reporting on DNS Assets](#)

[Support for New OCA Technologies](#)

[User-Defined Control Support for CentOS 8.x](#)

[User-Defined Control Support for Oracle Enterprise Linux 8.x](#)

[User-Defined Control Support for Ubuntu 19.x and Ubuntu 20.x](#)

[User-Defined Control Support for Debian GNU/Linux 7.x, 8.x, 9.x, and 10.x](#)

[Support for OS Authentication-Based Technology Microsoft Edge Chromium \(Windows\)](#)

Qualys 10.4 brings you more improvements and updates! [Learn more](#)

Qualys Cloud Platform

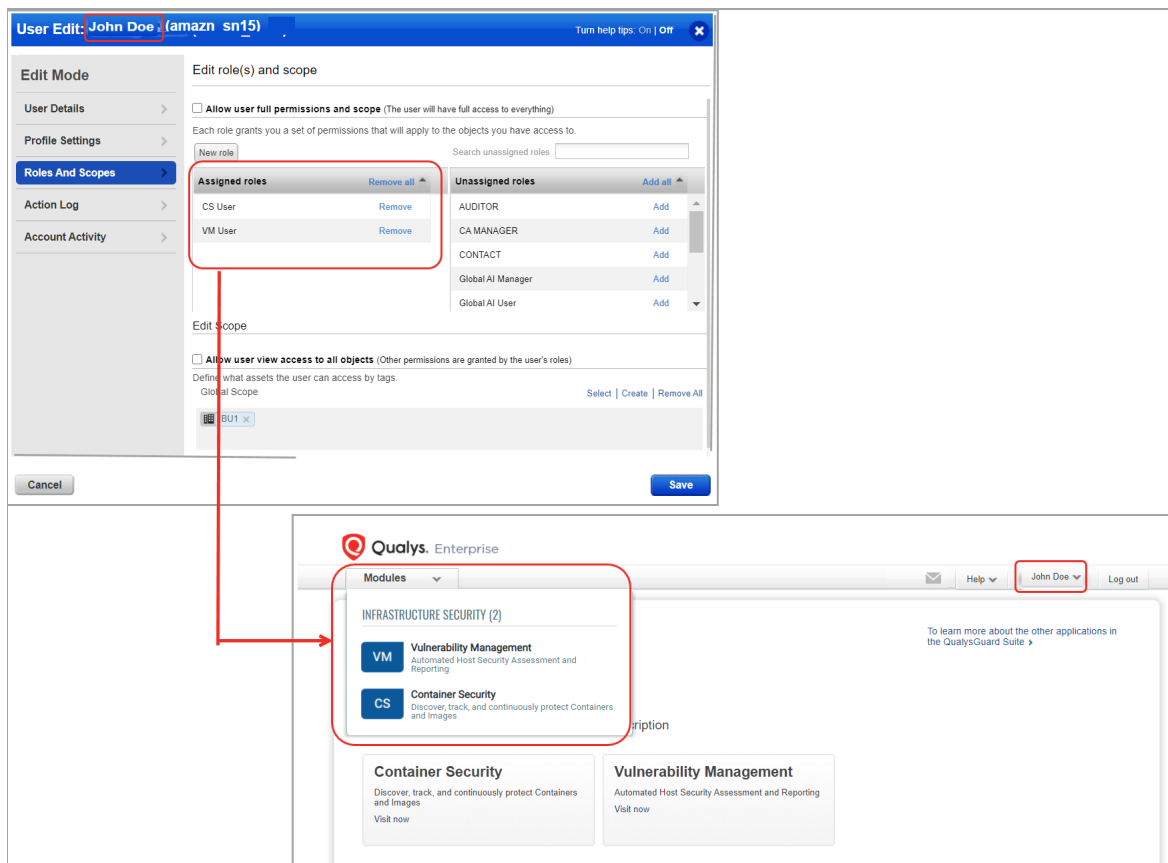
Modules Displayed in Module Picker and Permissions

For better customer experience, the module picker will now only display modules based on the permissions given to the user.

By default, the Manager user has permission for all the modules in the subscription.

The Manager user or user with Edit User permission then assigns roles and permissions to all the other users in the subscription.

For example, user John Doe is assigned **VM User** and **CS User** roles. These roles give him access to **Vulnerability Management (VM)** and **Container Security (CS)** modules. So, when John logs in to his Qualys account, the module picker will only display **VM** and **CS** modules based on his access permissions.



Using the **Administration** module, the Manager user or user with Edit User permission can now also assign UI access permission for **VM**, **PC**, and **SCA** modules. We have added two new default roles **VM User** and **PC User** to the **Administration** module.

Note: For SCA module permission, you must assign **PC User** role.

Account Type	User Assigned	Module displayed in Module Picker
PC	PC user	PC
PC and SCA	PC user	PC and SCA
SCA user	PC user	SCA

LDAP Authentication Support for MongoDB Record

With this release, you'll be able to create and update MongoDB records for LDAP authentication. For this, we have introduced a new field **Credential Type** with options - **Local authentication** and **External LDAP authentication**. Local authentication was already supported.

What are the steps?

- 1) Navigate to **Scans > Authentication > New > Databases... > MongoDB** and then click **Login Credentials**.
- 2) Select **Credential Type** as **Local authentication** to use this option. Local authentication was already supported. Select **Credential Type** as **External LDAP authentication** to create MongoDB records for LDAP authentication.

New MongoDB Record Launch Help

Record Title >

Login Credentials >

Target Configuration >

Unix Configuration >

IPs >

Comments >

Login Credentials

Use the local authentication or choose to use external LDAP authentication for credential type.

Credential Type: ☐ Local authentication ☒ External LDAP authentication

☒ Use clear text password

Authentication

Provide login credentials to use for authenticated scanning. Use the basic login credential or choose to use authentication vault for authenticated scanning.

Authentication Type: Basic

Username*: jdoe

Password*:

Confirm Password*:

For external LDAP authentication, we have introduced **Use clear text password** check-box which enables to send cleartext password over unencrypted channel. To authenticate a MongoDB server using an LDAP account, the password must be sent in the cleartext over the unencrypted channel. This cleartext password is then used by the MongoDB server to send a separate authentication request to the configured LDAP server.

For External LDAP authentication, only basic and vault based authentication type is supported.

Qualys Vulnerability Management (VM)

Target Type A10 Now Supported in Unix Authentication Record

You may have noticed that **A10** now appears in the **Target Type** menu in Unix authentication records. Selecting this option allows you to authenticate to A10 devices for vulnerability scanning, using Unix authentication. The A10 target type is supported in the UI and API. For help setting up authentication, please refer to [A10 Device Authentication](#).

New Unix Record Turn help tips: On | Off Launch Help

Record Title > **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 ☐ NO

☐ Skip Password

Password:

☐ Clear Text Password

Confirm Password*:

Target Type*:

Auto (default)

A10

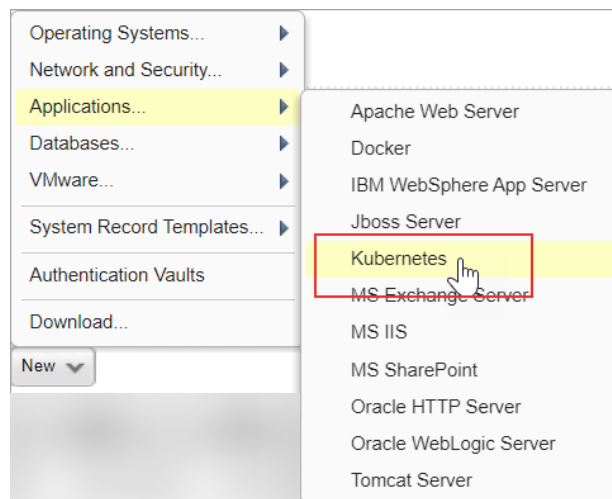
Auto (default)

Qualys Policy Compliance (PC/SCAP/SCA)

New Authentication Record for Kubernetes Now Available

With this release, you can assess the compliance posture of Kubernetes application installed on a Unix computer. All you need to do is create an authentication record for a Kubernetes instance running on a Unix host, add the Kubernetes 1.x technology in your policy, and scan it for middleware compliance assessment.

We'll use the credentials provided in your Unix authentication records to authenticate a Unix host first, and then scan the Kubernetes 1.x instance by using the Kubernetes authentication record.



How do I get started?

Go to **Scans > Authentication**.

Check that you have a Unix record already defined for the host on which Kubernetes is installed.

Create a Kubernetes record for the same host. Go to **New > Applications > Kubernetes**.

Kubernetes Record

While creating a Kubernetes authentication record, go to the **Unix Configuration** tab to provide details about configurations present on your Unix host. In the **Bin Path** field, specify the absolute path of the `kubectl` command. In the **Conf Path** field, specify the absolute path of the Kubernetes configuration file. These are optional fields.

Sample Reports

You'll see the Kubernetes technology in authentication reports and in compliance scan results.

Check out these samples:

The screenshot displays two side-by-side reports from Qualys. The left report, titled 'Summary', includes an 'IPs Summary' table showing 4 of 4 successful scans for IP 10.20.32.136-10.20.32.137. Below this is a 'Results' section with a table for 'Unix/Cisco/Checkpoint Firewall' and a highlighted table for 'Kubernetes'. The 'Kubernetes' table lists the host 10.20.32.136 with network details and instance information. The right report, titled 'Compliance Scan Results', shows an 'Appendix' section with a table of 'Target hosts found alive (IP)' and a table of 'Target distribution across scanner appliances'. A red box highlights the text 'Kubernetes authentication was successful for these hosts' in the 'Kubernetes 1.x' section. Below this, a 'Compliance Profile' section shows 'Kubernetes OP' settings, including 'Scan Settings' and 'Policy'. At the bottom, a table shows the status of the scan, with 'Passed' and 'CentOS Linux 7.5.1804' listed.

HOST	NETWORK	HOST TECHNOLOGY	INSTANCE
10.20.32.136 (-, -)	Global Default Network	CentOS 7.x	
10.20.32.137 (-, -)	Global Default Network	CentOS 7.x	
10.20.32.136 (-, -)	Global Default Network	Kubernetes 1.x	k8s 1.x, Bin Path=, Conf Path=

HOST	NETWORK	HOST TECHNOLOGY	INSTANCE
10.20.32.136 (-, -)	Global Default Network	CentOS 7.x	
10.20.32.137 (-, -)	Global Default Network	CentOS 7.x	
10.20.32.136 (-, -)	Global Default Network	Kubernetes 1.x	k8s 1.x, Bin Path=, Conf Path=

STATUS	CAUSE	OS	LAST AUTH	LAST SUCCESS
Passed	-	CentOS Linux 7.5.1804	09/08/2020	09/08/2020

Policies and Controls

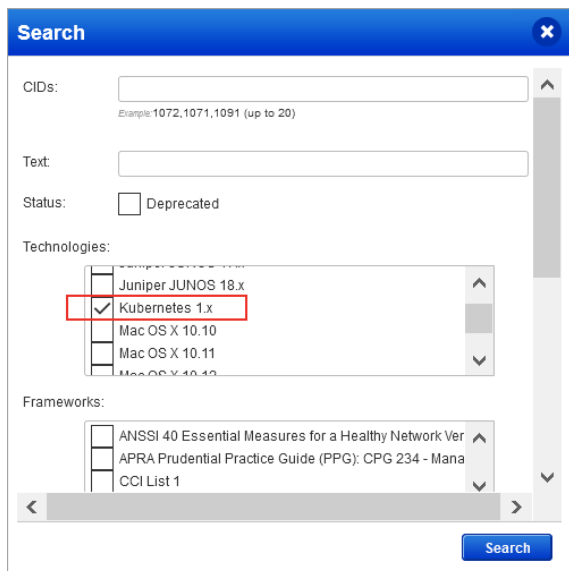
You'll see **Kubernetes 1.x** in the **Technologies** list when creating a new policy.

The screenshot shows the 'Create a New Policy' dialog in Qualys. It features a section titled 'Empty Policy: Build your policy from scratch.' with instructions to select technologies for the policy. Below this is a 'Technologies' section with a search bar and a list of technologies. A red box highlights 'Kubernetes 1.x' in the list. Other technologies listed include MS IIS 10.x, MS IIS 6.0, MS IIS 7.x, MS IIS 8.x, and Mac OS X 10.10. At the bottom, there are 'Back' and 'Next' buttons, and a 'Choose Source' button.

Search technologies:
No technologies selected
254 technologies
Kubernetes 1.x
MS IIS 10.x
MS IIS 6.0
MS IIS 7.x
MS IIS 8.x
Mac OS X 10.10

Search Controls

You'll see **Kubernetes 1.x** when searching controls by **Technologies**.



The screenshot shows a 'Search' dialog box with the following fields and options:

- CIDs:** A text input field with a placeholder example: '1072,1071,1091 (up to 20)'.
- Text:** A text input field.
- Status:** A checkbox labeled 'Deprecated'.
- Technologies:** A list box containing:
 - Juniper JUNOS 18.x
 - ☒ Kubernetes 1.x (highlighted with a red box)
 - Mac OS X 10.10
 - Mac OS X 10.11
 - Mac OS X 10.12
- Frameworks:** A list box containing:
 - ANSSI 40 Essential Measures for a Healthy Network Ver
 - APRA Prudential Practice Guide (PPG): CPG 234 - Mana
 - CCI List 1

A 'Search' button is located at the bottom right of the dialog.

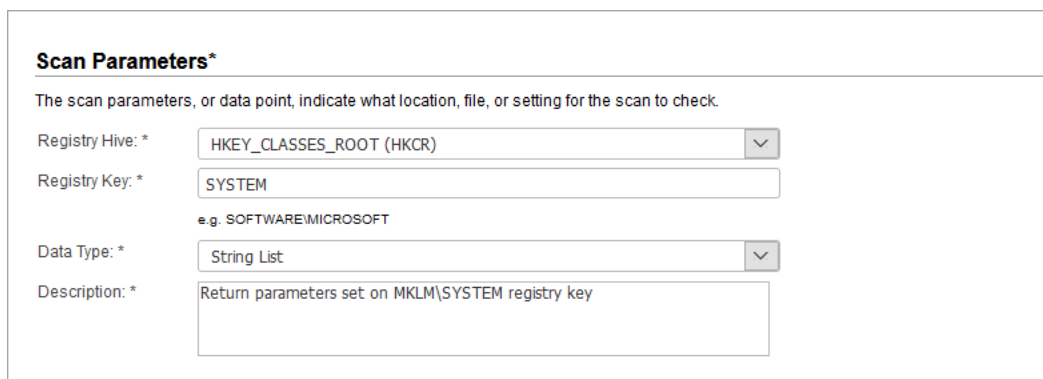
You can also evaluate the compliance posture of your Kubernetes assets by using your PC agents. All you need to do is set up Cloud Agent on your Kubernetes assets and activate them for middleware assessment.

Support for Editing a User-Defined Control

From now on, you can also edit scan parameters and the description of any type of a User-Defined Control (UDC). Earlier, you could not modify UDC settings after you created and saved it. You had to create another UDC instead. With this change now, we save you an overhead of maintaining redundant UDCs.

Managers and Auditors can edit a UDC. Unit Managers may be granted permission to edit a UDC.

Go to **PC > Policies > Controls**, select a user-defined control, and choose **Edit** from the Quick Actions menu. Then make your changes and save the control.



The screenshot shows the 'Scan Parameters*' form with the following fields:

- Registry Hive:** A dropdown menu showing 'HKEY_CLASSES_ROOT (HKCR)'.
- Registry Key:** A text input field containing 'SYSTEM'.
- Data Type:** A dropdown menu showing 'String List'.
- Description:** A text input field containing 'Return parameters set on MKLM\SYSTEM registry key'.

Below the Registry Key field, there is a small example text: 'e.g. SOFTWARE\MICROSOFT'.

Important - After you edit a UDC, to use the modified values in data collection and evaluation, you must run a fresh scan and generate a new report.

New Option to Auto Discover IBM WebSphere App Server instances from Server Directory

Now when you enable instance discovery and system record creation for IBM WebSphere App Server in a compliance option profile, you can choose to discover instances from the Installation Directory (the default and current behavior) or from the Server Directory. Previous releases always discovered instances at the Installation Directory level but now you can choose to have instances discovered at the Server Directory level, and have the system authentication records created based on this instance information.

What are the steps?

Go to **PC > Scans > Option Profiles**. Create a new profile or edit an existing profile. Then go to the **System Authentication** tab. Choose **Allow instance discovery and system record creation** and **IBM WebSphere App Server** (along with any other technologies you're interested in). Then pick **IBM WAS Installation Directory** or **IBM WAS Server Directory**.

The screenshot shows the 'New Compliance Profile' window with the 'System Authentication Records' tab selected. The left sidebar has a 'System Authentication' button highlighted. The main content area is titled 'System Authentication Records' and contains the following sections:

- 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. 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
 - ☐ IBM WAS Server Directory
 - ☒ Jboss Server
 - ☒ Tomcat Server
 - ☒ Oracle (system record template required)
- Login credentials for system created records are saved in Oracle system record templates. Choose the template you want to use from the list below.
Oracle system record template:
- 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

Tip – We recommend you use the same discovery mode consistently for each scan target to prevent too many system records being created. If you switch between Server Directory and Installation Directory discovery modes, then you'll get different instances discovered with each scan and that will affect your system records.

For example, let's say you first launch a scan using an option profile with instance discovery at the "Server Directory" level resulting in 4 instances discovered and 4 system authentication records created. Then let's say you launch a second scan on the same target but this time you use an option profile with instance discovery at the "Installation Directory" level. This time only 1 instance is discovered. As a result, the IP address will be removed from the 4 previous authentication records and 1 new system authentication record will be created with the new instance information.

Sample Reports

When you drill-down into the Detailed Results of your Policy Report you'll see the IBM WebSphere App Server (WAS) instance details, including whether the instance was discovered from the Server Directory or Installation Directory.

Instance from Installation Directory

The screenshot displays the 'Detailed Results' for IP 10.11.71.33 on a Red Hat Enterprise Linux Server 5.7. The overall status is 99.45% (182 controls passed, 1 failed, 0 errors, 0 exceptions). Under the 'IBM WebSphere Application Server 7.x' section, the '1. Access Control Requirements' are shown as 'PASS' (32 controls passed, 0 failed, 0 errors, 0 exceptions). A specific finding (1.1) 15723, titled 'Ownership and Permissions set for 'audit-authz.xml' file for each cell', is highlighted with a red circle. The instance details for this finding are: Instance: IBM WAS 7 (Installation Directory: /opt/IBM/WebSphere/AppServer), Previous Status: Passed, Evaluation Date: 09/30/2020 at 22:44:39 (GMT), First Fail Date: N/A, Last Fail Date: N/A, First Pass Date: 09/30/2020 at 22:44:41 (GMT), and Last Pass Date: 09/30/2020 at 22:44:41 (GMT). The finding is categorized as 'SERIOUS' and has a 'PASS' status.

Tracking Method:	IP address	Controls:	183
Last Scan Date:	09/30/2020 at 22:34:03 (GMT)	Passed:	182 (99.45%)
Qualys Host ID:		Failed:	1 (0.55%)
Asset Tags:	IBMWAS_AutoAuthDiscovery	Error:	0
		Approved Exceptions:	0
		Pending Exceptions:	0

1. Access Control Requirements	PASS	32	0	0
(1.1) 15723 Ownership and Permissions set for 'audit-authz.xml' file for each cell	SERIOUS	Status: PASS		
Instance:	IBM WAS 7 (Installation Directory: /opt/IBM/WebSphere/AppServer)			
Previous Status:	Passed			
Evaluation Date:	09/30/2020 at 22:44:39 (GMT)			
First Fail Date:	N/A			
Last Fail Date:	N/A			
First Pass Date:	09/30/2020 at 22:44:41 (GMT)			
Last Pass Date:	09/30/2020 at 22:44:41 (GMT)			

Instance from Server Directory

The screenshot displays the 'Detailed Results' for IP 10.11.71.33 on a Red Hat Enterprise Linux Server 5.7. The overall status is 'PASS' (183 controls passed, 0 failed, 0 errors, 0 exceptions). Under the 'IBM WebSphere Application Server 7.x' section, the '1. Access Control Requirements' are shown as 'PASS' (32 controls passed, 0 failed, 0 errors, 0 exceptions). A specific finding (1.1) 15723, titled 'Ownership and Permissions set for 'audit-authz.xml' file for each cell', is highlighted with a red circle. The instance details for this finding are: Instance: IBM WAS 7 (Server Directory: /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/config/cells/comwsphere7uNode01/servers/server1), Previous Status: Passed, Evaluation Date: 09/30/2020 at 11:10:39 (GMT), First Fail Date: N/A, Last Fail Date: N/A, First Pass Date: 09/28/2020 at 21:13:51 (GMT), and Last Pass Date: 09/30/2020 at 11:10:40 (GMT). The finding is categorized as 'SERIOUS' and has a 'PASS' status.

Tracking Method:	IP address	Controls:	183
Last Scan Date:	09/30/2020 at 10:59:48 (GMT)	Passed:	183 (100%)
Qualys Host ID:		Failed:	0
Asset Tags:	IBMWAS_AutoAuthDiscovery	Error:	0
		Approved Exceptions:	0
		Pending Exceptions:	0

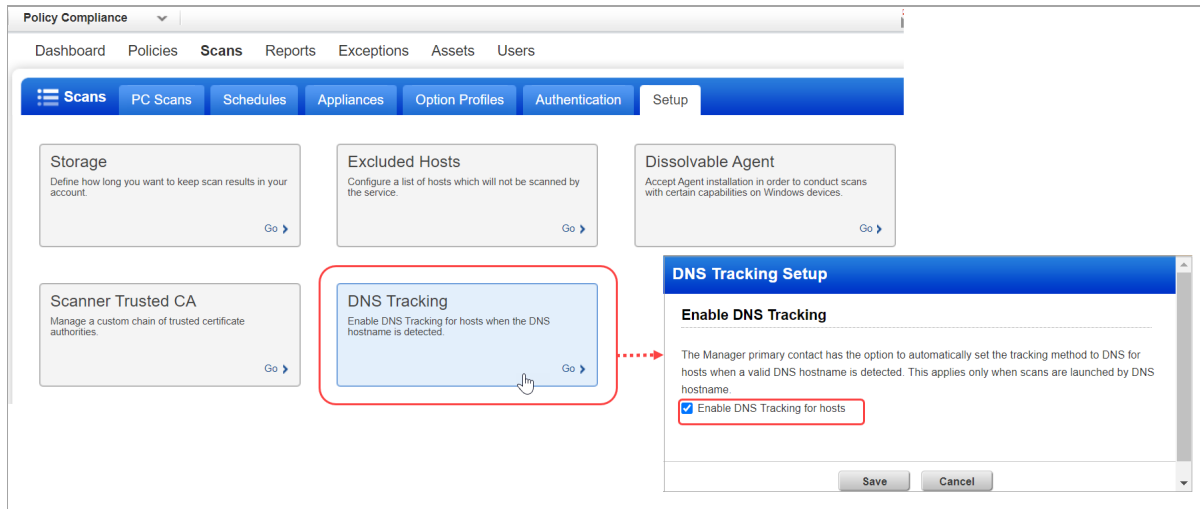
1. Access Control Requirements	PASS	32	0	0
(1.1) 15723 Ownership and Permissions set for 'audit-authz.xml' file for each cell	SERIOUS	Status: PASS		
Instance:	IBM WAS 7 (Server Directory: /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/config/cells/comwsphere7uNode01/servers/server1)			
Previous Status:	Passed			
Evaluation Date:	09/30/2020 at 11:10:39 (GMT)			
First Fail Date:	N/A			
Last Fail Date:	N/A			
First Pass Date:	09/28/2020 at 21:13:51 (GMT)			
Last Pass Date:	09/30/2020 at 11:10:40 (GMT)			

Launch/Schedule Compliance Scans on FQDNs

With this release you can launch and schedule compliance scans on Fully Qualified Domain Names (FQDNs). When defining the scan target, you'll enter FQDNs in the new FQDN input field. This is already supported for vulnerability scans.

DNS Tracking must be enabled

A Manager user can enable this feature by going to **Scans > Setup > DNS Tracking** and checking the **Enable DNS Tracking for hosts** option.



Enter the FQDNs you want to scan

When launching and scheduling compliance scans enter one or more FQDNs when defining the target hosts, as shown below. FQDNs can be entered in combination with asset groups and IPs/ranges but not with asset tags. If the scanned FQDN resolves to an IP address that is not in your account then it will be added to the PC/SCA license container. The newly added IP will be tracked by DNS. Not seeing the FQDN option? Make sure DNS Tracking is enabled as stated above.

Note: Currently, vulnerability and compliance scans are not visible to the sub-user when scans launched on FQDN by sub-user itself or by the Manager.

Launch Compliance Scan

Go to **Scans > PC Scans > New > Scan** to launch the compliance scan.

Launch Compliance Scan

Turn help tips: On | Off Launch Help

General Information

Give your scan a name, select a scan profile (a default is selected for you with recommended settings), and choose a scanner from the Scanner Appliance menu for internal scans, if visible.

Title:

Compliance Profile: [View](#)

Network:

Scanner Appliance: [View](#)

Choose Target Hosts from

Tell us which hosts (IP addresses) you want to scan.

☒ Assets ☐ Tags

Asset Groups [Select](#)

IPs/Ranges [Select](#)

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

Exclude IPs/Ranges [Select](#)

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

FQDN(s): [Select](#)

Example: Separate entries using commas. www.abc.com, www.xyz.com

☐ Temporarily add agent addresses
Select this option to add the IP addresses of any agents in your target when those IPs are not already in your subscription. They'll be added for this scan only.

Notification

☐ Send notification when this scan is finished

Launch

Cancel

Schedule Compliance Scan

Go to **Scans > PC Scans > New > Schedule Scan** to schedule the compliance scan.

New Scheduled Compliance Scan

Turn help tips: On | Off Launch Help

Task Title

Target Hosts

Scheduling

Notifications

Schedule Status

Target Hosts

☒ Assets ☐ Tags

Asset Groups [Select](#)

IPs/Ranges [Select](#)

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

Exclude IPs/Ranges [Select](#)

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

FQDN(s): [Select](#)

Example: Separate entries using commas. www.abc.com, www.xyz.com

☐ Temporarily add agent addresses

Cancel

Save

Policy Evaluation and Compliance Reporting on DNS Assets

Now we'll perform policy evaluation and compliance reporting on DNS assets included in policy asset groups. In previous releases, you were able to scan DNS assets for compliance but policy evaluation was skipped because we only performed policy evaluation on the IP addresses that were associated with asset groups in your policies. Now we'll also perform policy evaluation on the DNS hostnames associated with asset groups in your policies.

Policy evaluation

When the Scan by Hostname feature is enabled, you can add DNS hostnames to your asset groups in addition to IP addresses. These asset groups can then be added to the policies you want to evaluate for compliance. After running compliance scans on your assets, we'll look at the IP address and the DNS hostname for each scanned asset, and if the IP or the DNS name matches an asset group in your policy, then we'll perform the policy evaluation.

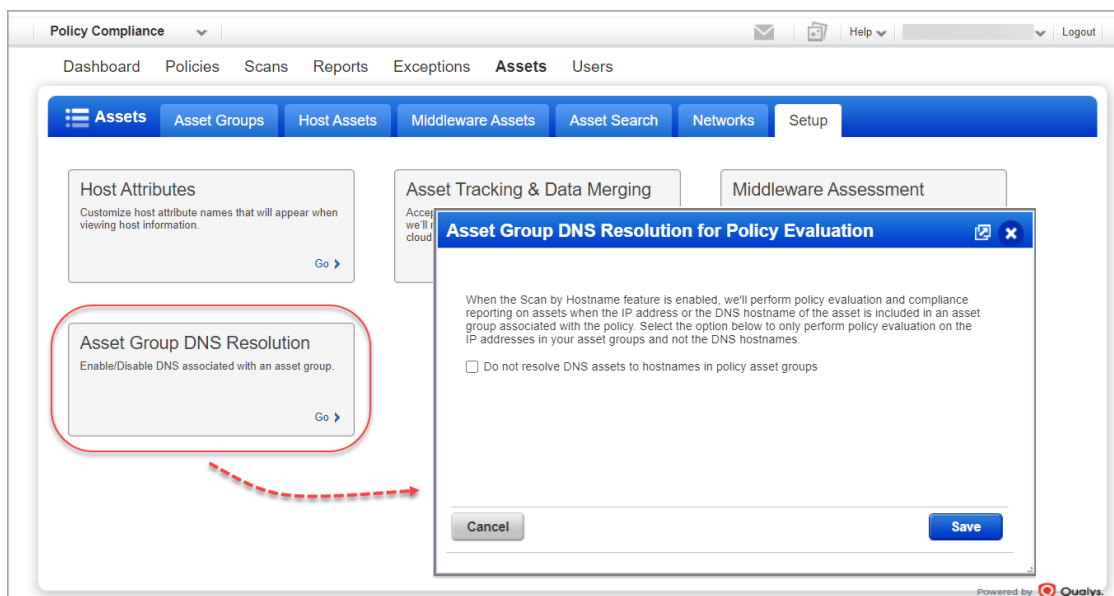
Compliance reporting

Policy Compliance reports can be now launched on any of the assets in your policy asset groups, including DNS assets and IP assets. Other compliance reports (scorecard reports, mandate based reports, interactive reports, etc) will continue to only include IP assets.

Prefer the way it worked before?

If you only want to perform policy evaluation on the IP addresses in your asset groups and not on the DNS hostnames, then you can choose to go back to the way it worked before.

Go to **Assets > Setup > Asset Group DNS Resolution**, and check the option **Do not resolve DNS assets to hostnames in policy asset groups**.



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.

- **FortiOS 5.x**
- **FortiOS 6.x**
- **Gigamon GigaVUE-OS 5.x**
- **Pulse Connect Secure 9.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.

User-Defined Control Support for CentOS 8.x

We have extended the User Defined Control (UDC) support for CentOS 8.x for scanner and agent.

Want to create a UDC for CentOS 8.x? Go to **Policies > Controls > New > Control > Unix Control Types** and select the required control types from the list. Scroll to the **Control Technologies** section to provide a rationale statement and expected value for each technology.

New Control: File/Directory Existence - Google Chrome

Control Technologies*

- ☐ AIX 5.x
Use this section to create a AIX 5.x instance of this control
- ☐ AIX 6.x
Use this section to create a AIX 6.x instance of this control
- ☐ AIX 7.x
Use this section to create a AIX 7.x instance of this control
- ☐ CentOS 4.x
Use this section to create a CentOS 4.x instance of this control
- ☐ CentOS 5.x
Use this section to create a CentOS 5.x instance of this control
- ☐ CentOS 6.x
Use this section to create a CentOS 6.x instance of this control
- ☐ CentOS 7.x
Use this section to create a CentOS 7.x instance of this control
- ☐ CentOS 8.x
Use this section to create a CentOS 8.x instance of this control
- ☐ Debian GNU/Linux 10.x
Use this section to create a Debian GNU/Linux 10.x instance of this control

While creating a new policy, you can select **CentOS 8.x** from the **Technologies** list.

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

251 technologies Add all shown

- CentOS 5.x
- CentOS 6.x
- CentOS 7.x
- CentOS 8.x**
- Checkpoint Firewall
- Cisco ASA 8.x

Back Choose Source Next

User-Defined Control Support for Oracle Enterprise Linux 8.x

We have extended the User Defined Control (UDC) support for Oracle Enterprise Linux 8.x for scanner and agent.

Want to create a UDC for Oracle Enterprise Linux 8.x? Go to **Policies > Controls > New > Control > Unix Control Types** and select the required control types from the list. Scroll to the **Control Technologies** section to provide a rationale statement and expected value for each technology.

New Control: File/Directory Existence - Google Chrome

Control Technologies*

- ☐ openSUSE 11.x
Use this section to create a openSUSE 11.x instance of this control
- ☐ openSUSE 13.x
Use this section to create a openSUSE 13.x instance of this control
- ☐ openSUSE 15.x
Use this section to create a openSUSE 15.x instance of this control
- ☐ Oracle Enterprise Linux 4.x
Use this section to create a Oracle Enterprise Linux 4.x instance of this control
- ☐ Oracle Enterprise Linux 5.x
Use this section to create a Oracle Enterprise Linux 5.x instance of this control
- ☐ Oracle Enterprise Linux 6.x
Use this section to create a Oracle Enterprise Linux 6.x instance of this control
- ☐ Oracle Enterprise Linux 7.x
Use this section to create a Oracle Enterprise Linux 7.x instance of this control
- ☐ Oracle Enterprise Linux 8.x
Use this section to create a Oracle Enterprise Linux 8.x instance of this control
- ☐ Red Hat Enterprise Linux 3/4
Use this section to create a Red Hat Enterprise Linux 3/4 instance of this control

While creating a new policy, select **Oracle Enterprise Linux 8.x** from the **Technologies** list.

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 251 technologies Add all shown

- Oracle Enterprise Linux 4.x
- Oracle Enterprise Linux 6.x
- Oracle Enterprise Linux 7.x
- Oracle Enterprise Linux 8.x**
- Oracle HTTP Server 11g
- Oracle HTTP Server 12c
- Oracle WebLogic Server 11g

Back Choose Source Next

User-Defined Control Support for Ubuntu 19.x and Ubuntu 20.x

We have extended the User Defined Control (UDC) support for Ubuntu 19.x and Ubuntu 20.x for scanner and agent.

Want to create a UDC for Ubuntu 19.x and Ubuntu 20.x? Go to **Policies > Controls > New > Control > Unix Control Types** and select the required control types from the list. Scroll to the **Control Technologies** section to provide a rationale statement and expected value for each technology.

New Control: File/Directory Existence - Google Chrome

Control Technologies*

- ☐ Ubuntu 10.x
Use this section to create a Ubuntu 10.x instance of this control
- ☐ Ubuntu 11.x
Use this section to create a Ubuntu 11.x instance of this control
- ☐ Ubuntu 12.x
Use this section to create a Ubuntu 12.x instance of this control
- ☐ Ubuntu 14.x
Use this section to create a Ubuntu 14.x instance of this control
- ☐ Ubuntu 16.x
Use this section to create a Ubuntu 16.x instance of this control
- ☐ Ubuntu 18.x
Use this section to create a Ubuntu 18.x instance of this control
- ☒ Ubuntu 19.x
Use this section to create a Ubuntu 19.x instance of this control
- ☒ Ubuntu 20.x
Use this section to create a Ubuntu 20.x instance of this control
- ☐ Ubuntu 8.x
Use this section to create a Ubuntu 8.x instance of this control
- ☐ Ubuntu 9.x
Use this section to create a Ubuntu 9.x instance of this control
- ☐ VMWare ESX Server 3.x
Use this section to create a VMWare ESX Server 3.x instance of this control

While creating a new policy, select **Ubuntu 19.x** and **Ubuntu 20.x** from the **Technologies** list.

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

251 technologies Add all shown

- Ubuntu 14.x
- Ubuntu 16.x
- Ubuntu 18.x
- ☒ Ubuntu 19.x
- ☒ Ubuntu 20.x
- Ubuntu 8.x
- Ubuntu 9.x

Back Choose Source Next

User-Defined Control Support for Debian GNU/Linux 7.x, 8.x, 9.x, and 10.x

We have extended the User Defined Control (UDC) support for Debian GNU/Linux 7.x, 8.x, 9.x, and 10.x.

Note: Debian GNU/Linux 7.x, 8.x, 9.x is supported for agent, and Debian GNU/Linux 10.x is supported for agent and scanner.

Want to create a UDC for Debian GNU/Linux 7.x, 8.x, 9.x, and 10.x? Go to **Policies > Controls > New > Control > Unix Control Types** and select the required control types from the list. Scroll to the **Control Technologies** section to provide a rationale statement and expected value for each technology.

New Control: File/Directory Existence - Google Chrome

Control Technologies*

- ☐ CentOS 7.x
Use this section to create a CentOS 7.x instance of this control
- ☐ CentOS 8.x
Use this section to create a CentOS 8.x instance of this control
- ☐ Debian GNU/Linux 10.x
Use this section to create a Debian GNU/Linux 10.x instance of this control
- ☐ Debian GNU/Linux 5.x
Use this section to create a Debian GNU/Linux 5.x instance of this control
- ☐ Debian GNU/Linux 7.x
Use this section to create a Debian GNU/Linux 7.x instance of this control
- ☐ Debian GNU/Linux 8.x
Use this section to create a Debian GNU/Linux 8.x instance of this control
- ☐ Debian GNU/Linux 9.x
Use this section to create a Debian GNU/Linux 9.x instance of this control
- ☐ HPUX 11.1v1
Use this section to create a HPUX 11.1v1 instance of this control
- ☐ HPUX 11.1v2
Use this section to create a HPUX 11.1v2 instance of this control

While creating a new policy, select **Debian GNU/Linux 7.x, 8.x, 9.x, and 10.x** from the **Technologies** list.

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 254 technologies Add all shown

- Debian GNU/Linux 10.x
- Debian GNU/Linux 5.x
- Debian GNU/Linux 7.x
- Debian GNU/Linux 8.x
- Debian GNU/Linux 9.x
- Docker 1.x

Back Choose Source Next

Support for OS Authentication-Based Technology Microsoft Edge Chromium (Windows)

We've expanded our support of OS authentication-based technologies to include Microsoft Edge Chromium (Windows). For OS authentication-based technologies, you can collect technology data using the underlying OS technology (in this case Windows) without the need to create authentication records.

Note: We support Microsoft Edge Chromium version 79.x and above.

The Microsoft Edge Chromium (Windows) technology is now available for inclusion in your compliance policies and when searching controls. You'll also see Microsoft Edge Chromium (Windows) host instance information in policy compliance authentication reports, scan results, and policy reports.

Policy Editor

You can now select the **Microsoft Edge Chromium (Windows)** technology for your compliance policies.

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 254 technologies Add all shown

- Mac OS X 10.9
- Mac OS X 10.x
- MariaDB 10.x
- Microsoft Edge Chromium (Windows)**
- Microsoft Exchange Server 2010
- Microsoft Exchange Server 2013

Back Choose Source Next

Search Controls

You'll also see Microsoft Edge Chromium when searching controls. Go to **Policies > Controls > Search** and select **Microsoft Edge Chromium (Windows)** in the list of **Technologies**.

Search

CIDs:

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

Text:

Status:

☐

Deprecated

Technologies:

☐ Mac OS X 10.x
☐ MariaDB 10.x
☐ Microsoft Edge Chromium (Windows)
☐ Microsoft Exchange Server 2010
☐ Microsoft Exchange Server 2013

Frameworks:

☐ ANSSI 40 Essential Measures for a Healthy Network Ver 1.0
☐ APRA Prudential Practice Guide (PPG): CPG 234 - Manage
☐ CCI List 1
☐ CIS - Apache HTTP Server 2.2 Benchmark v3.4.0 (09-23-20)

Framework ID:

Search

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 **Appendix**.

New Authentication Report

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

Report Details

Title:

Authentication Report with OS based

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

10.1.1.1

Select

Network:

All

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)

Appendix

☒ OS Authentication-based Technology

Report Options

☐ Scheduling

Run

Cancel

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

Results

MS Edge Chromium 1 of 1 (100%)

Windows

HOST	NETWORK	HOST TECHNOLOGY	INSTANCE	STATUS	CAUSE
10.115. (win10-113, WIN10-113)	Global Default Network	Windows 10		Passed	-

Appendix

Targets with OS authentication-based technologies

10.115. (win10-113, WIN10-113)

Network: Global Default Network

OS: Windows 10 Pro 64 bit Edition

Last Auth: 09/15/2020 at 09:08:29 AM (GMT+0530)

Last Success: 09/15/2020 at 09:08:29 AM (GMT+0530)

S.N.	Host Technology	Instance
1	Microsoft Edge Chromium (Windows)	Microsoft Edge Chromium (Windows)

Scan Results

You'll see Microsoft Edge Chromium (Windows) listed in the **Appendix** section of Compliance Scan Results under **Application technologies found based on OS-level authentication**.

Compliance Scan Results	
Appendix	
Target hosts found alive (IP)	
10.115.	
Target distribution across scanner appliances	
VirtualIndiaScanner-1 : 10.115.	
Windows authentication was successful for these hosts	
10.115.	
Application technologies found based on OS-level authentication	
Google Chrome was found for these hosts	
Google Chrome (Windows)	
10.115.	
Microsoft Edge Chromium (Windows) was found for these hosts	
Microsoft Edge Chromium (Windows)	
10.115.	

Policy Reports

You'll also see Microsoft Edge Chromium (Windows) and host instance information in your Compliance Policy reports.

Detailed Results			
10.115.108.113 (win10-113, WIN10-113)		Windows 10 Pro 64 bit Edition	
Controls:	6		
Passed:	5 (83.33%)		
Failed:	1 (16.67%)		
Error:	0		
Approved Exceptions:	0		
Pending Exceptions:	1		
Last Scan Date:	09/15/2020 at 08:59:10 (GMT+0530)		
Network:	Global Default Network		
Tracking Method:	IP		
Qualys Host ID:	-		
Asset Tags:			
Microsoft Edge Chromium (Windows)			
1. Untitled			
(1.1) 17613 Status of 'Allow users to proceed from the HTTPS warning page' setting(Microsoft Edge Chromium (Windows))			
Instance	Microsoft Edge Chromium (Windows)	Passed	CRITICAL
Evaluation Date	09/15/2020 at 10:36:06 (GMT+0530)		

Issues Addressed

- We now do not allow adding IP addresses for DNS hostnames when creating an asset group with DNS hostnames. We show an error message that will prompt you to add a valid DNS hostname when saving the asset group with one or more IP addresses in the DNS tab.
- We now show an appropriate error message when "invalid asset group IDs" are provided in API input. In the message, we show the invalid asset Group IDs in the output.
- We fixed an issue where the user was not able to edit a remediation ticket to add a comment in the ticket using the "Edit ticket" API request sample provided in the API VM/PC User Guide. The issue was due to adding the query string outside the Post parameter in the API request. We have now added the query string to the "Post" parameter in the sample "Edit ticket" API request.
- We fixed an issue in the Policy Compliance module where when creating a new UDC control, we were showing the non-mandatory "Remediation" field as a required field. After the fix, the "Remediation" field is not a required field and you can save the control without providing any value in the Remediation field.
- For some customers, EC2 metadata information was not showing up in Host-based CSV scan reports. This is now fixed.
- The error message on the IPs tab while creating an Apache Web Server authentication record will now display the IPs that are not a part of the Windows or Unix authentication record.
- You can now add and edit up to 10 references while creating Windows, Unix, and Database user-defined controls.
- We have fixed the navigation issue for accounts that had only SCA agents installed.
- Fixed an issue where scheduled map scans were giving error for the domains / Netblocks with size more than 4000 bytes.
- Fixed an issue where Scanner Trusted CA was not showing all the information on the certificate.
- Updated the vCenter map screenshot in the Scan ESXi Hosts on vCenter User Guide to reflect the accurate column headings for the csv file.
- Fixed an issue where the expected value for data-point was not set correctly if the same DP occur multiple times.
- Fixed an issue where an error was occurring while creating MSSQL Authentication Record with only member domain value and not IP.
- Fixed an issue where Middleware Assets were displayed with the 'Hostname' column even if 'Hostname' was unchecked from Settings > Columns. We have removed 'Hostname' from the column checking filter.
- Updated a 'Note' on UI which was misleading and interpreting that the Unix Auth Record is mandatory while creating MongoDB Authentication record.
- Fixed an issue related to editing the default value of a selected control technology.
- We've added the missing comma in the asset_data_report.dtd file.
- We have now enhanced our Asset Group Search queries to support space between words. Earlier, the Asset Group search did not accept space character.
- We have now fixed an issue so that the selection of CyberArk PIM Suite for authentication vault now correctly populates only CyberArk PIM authentication records. Earlier, the authentication records also populated HashiCorp and Azure Vault records along with CyberArk PIM Suite.