Qualys Cloud Platform (VM, PC) v8.x

Release Notes

Version 8.20

June 20, 2019

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

Qualys Cloud Platform

Configure Password Expiration Notification
Configure Session Timeout Settings for User Roles
Character limit Increased for DNS and NetBIOS Hostnames fields

Qualys Policy Compliance (PC/SCA)

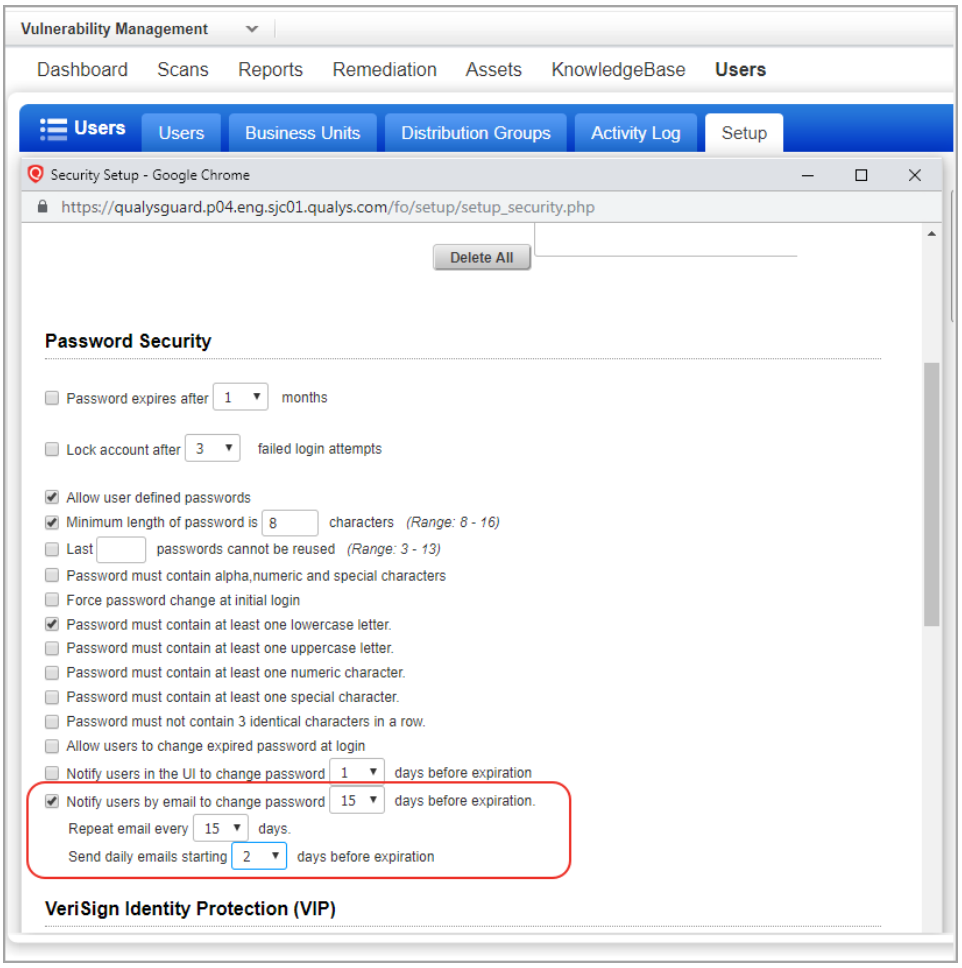
Docker CE/EE Application Support
MongoDB 4.x Support
Database User-Defined Controls Support

Qualys 8.20 brings you many more improvements and updates! Learn more

Qualys Cloud Platform

Configure Password Expiration Notification

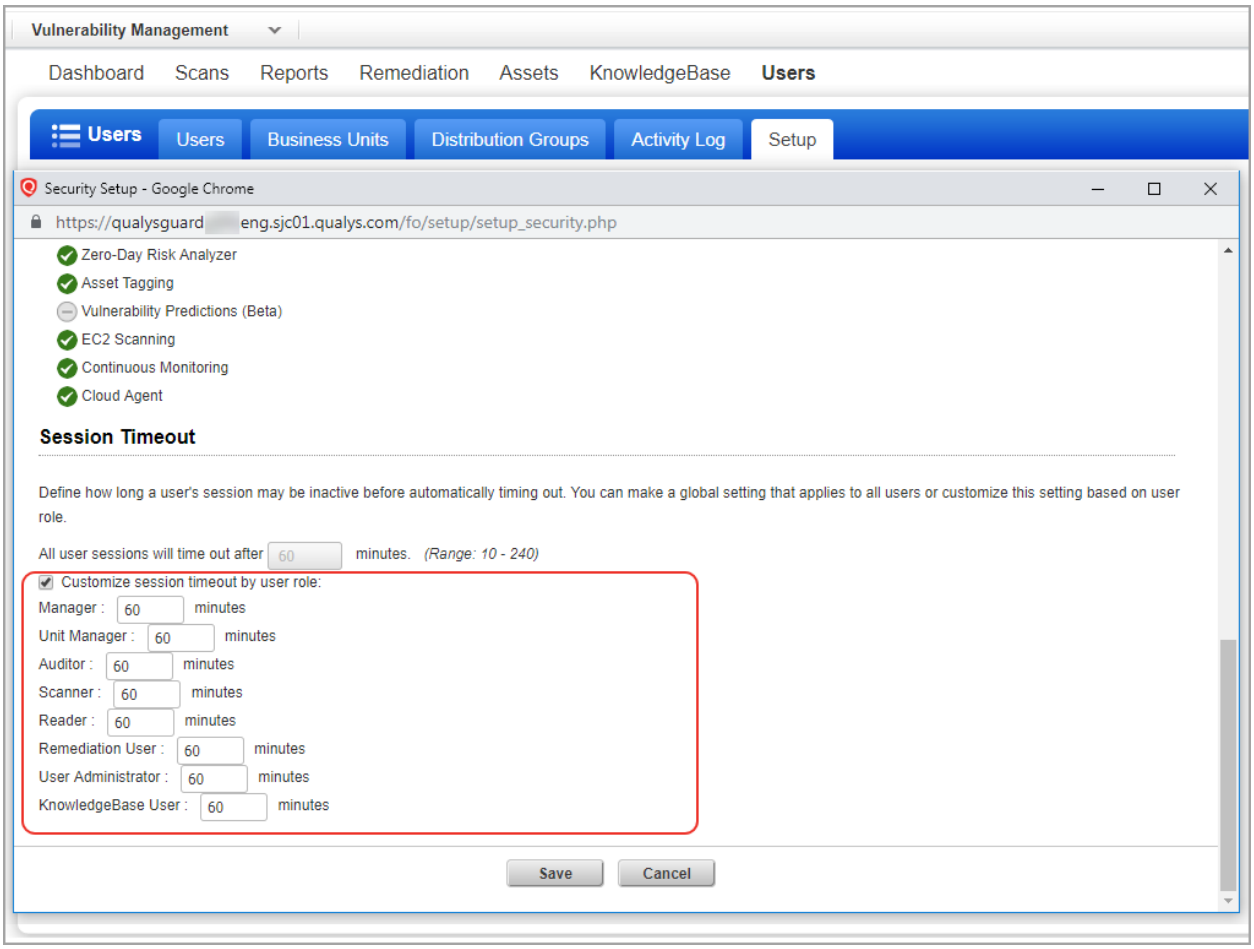
Now users can be notified by email when their password is set to expire. A Manager can enable this option by going to Users > Setup > Security. Select the option "Notify users by email to change password N days before expiration". Then choose the number of days before password expiration when the first email will be sent to the user, how often the email will be sent (every 3 days, every 2 days, etc) and when to switch to daily emails. Note - If there's an overlap between two notification periods, the system will only send one email.



Configure Session Timeout Settings for User Roles

Now you have the option to customize a different session timeout for each user role. This allows you to set shorter timeouts for more restricted users. For example, you can set a timeout of 15 minutes for most users and then define a longer session timeout for the users who need to be logged in for longer periods of time because of long running tasks.

A Manager can enable this option by going to Users > Setup > Security. Select the option "Customize session timeout by user role" and then choose between 10-240 minutes for each role. The default setting for each role is 60 minutes.



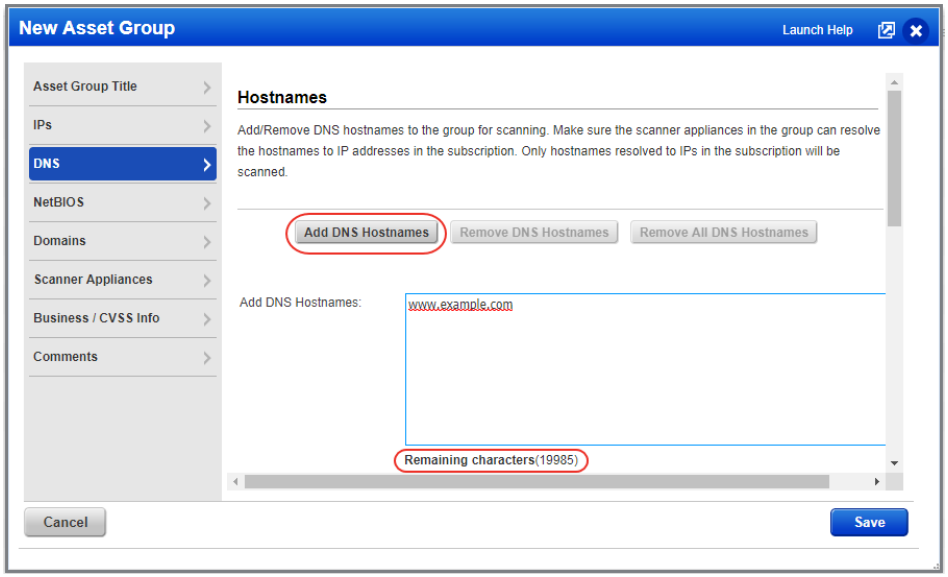
Character limit Increased for DNS and NetBIOS Hostnames fields

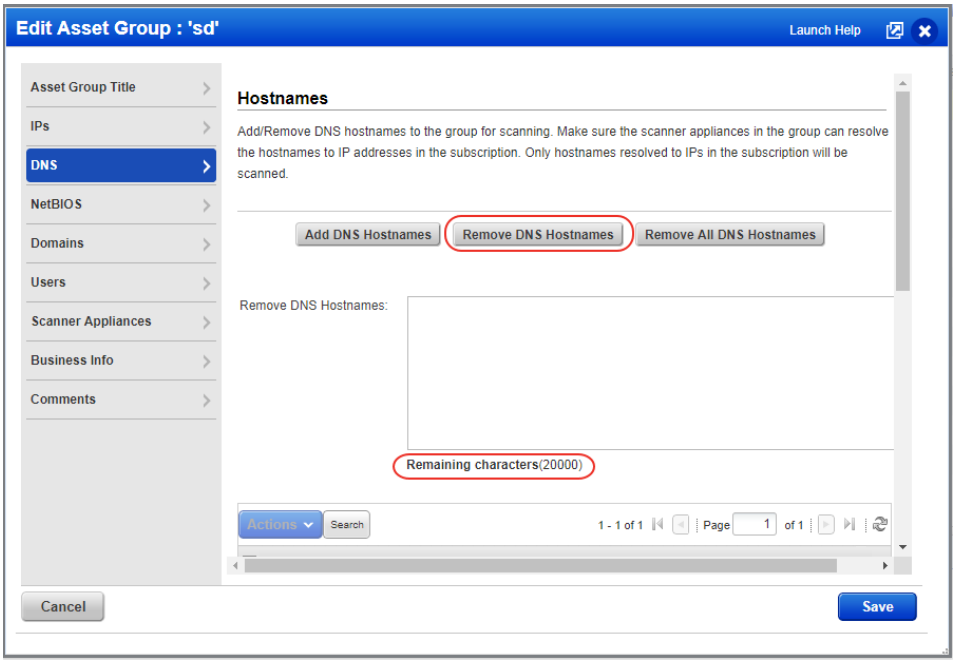
Applicable only to subscriptions with the Scan by Hostname feature enabled.

We have increased the maximum character limit for adding and removing DNS Hostnames and NetBIOS Hostnames fields in Asset Group to 20,000 characters.

At the bottom of the Add and Remove DNS and NetBIOS hostnames text boxes, the Remaining Characters label shows you how many more characters you can enter in the field.

To add DNS and NetBIOS hostnames to the asset group, Go to Assets > Asset Groups. Select New > Asset Group. Navigate to the DNS or NetBIOS tab.

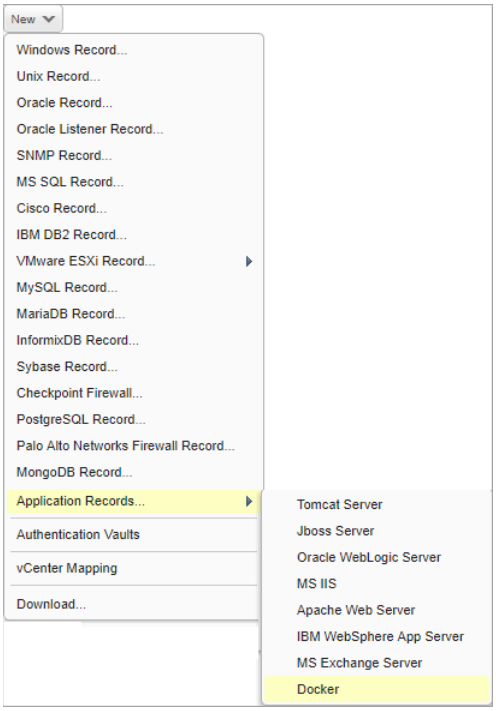




Qualys Policy Compliance (PC/SCA)

Docker CE/EE Support

We've extended our support for Docker authentication to include Docker CE/EE for Unix. (See the help for other supported technologies.) You'll need a Docker authentication record to authenticate to a Docker daemon running on a Linux host, and scan it for compliance. You'll also need a Unix record for the host running the docker.



Which docker versions are supported?

- Docker daemon versions 1.9 to 1.13

- Docker Community Edition (CE) version 17.x or later

- Docker Enterprise Edition (EE) version 17.x or later

How do I get started?

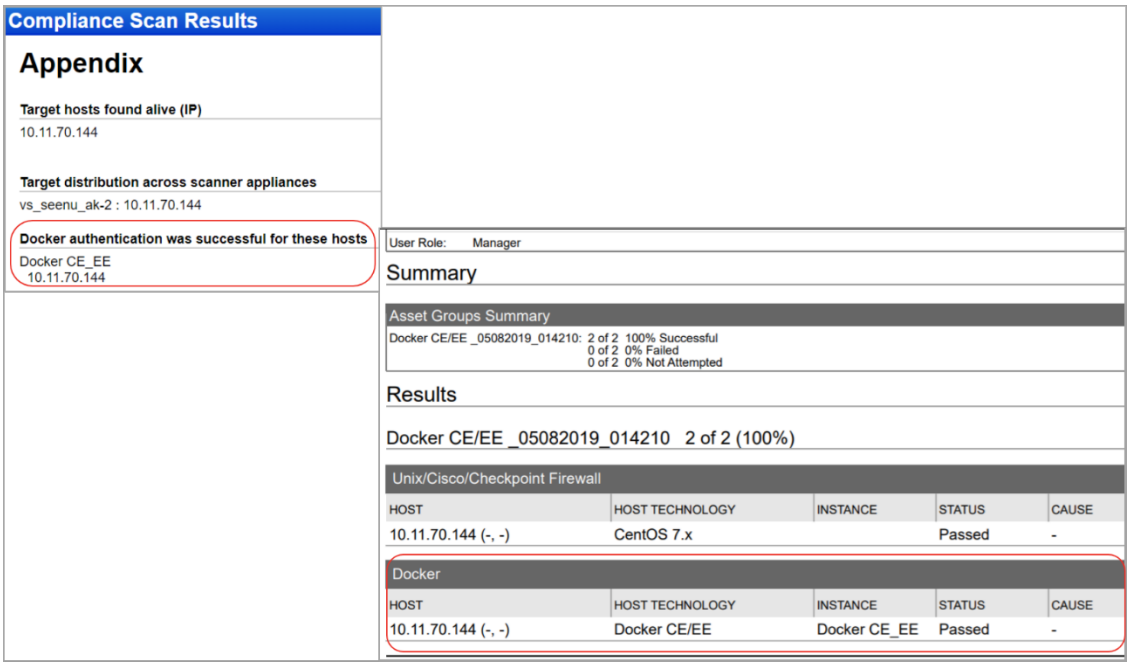
- Go to Scans > Authentication.

- Check that you already have a Unix record defined for each host running the docker.

- Create a docker record for the same host. Go to New > Application Records > Docker.

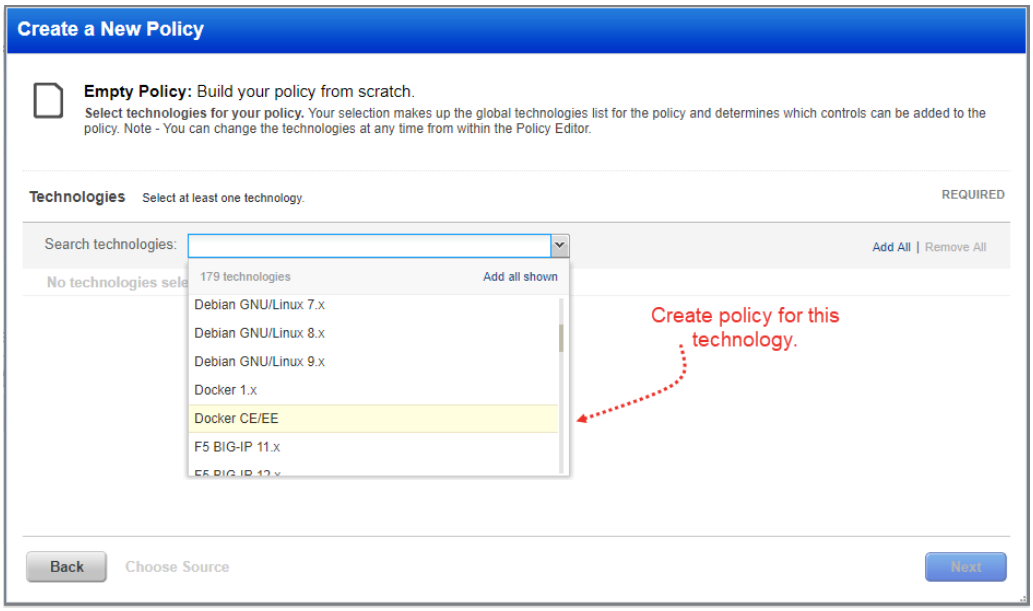
Sample Reports

You'll see Docker CE/EE instances in compliance scan results and reports.



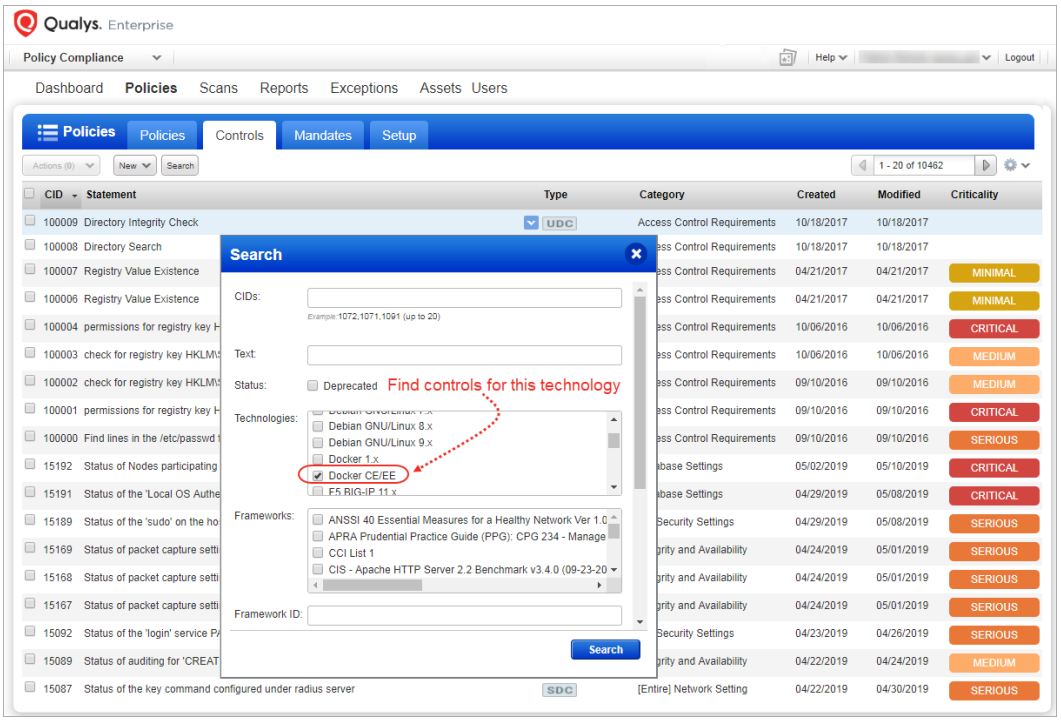
Policies and Controls

You'll also see Docker CE/EE instances in the technologies list when creating a new policy.



Search Controls

You'll see Docker CE/EE when searching controls by technologies.



MongoDB 4.x Support

We've extended our support for MongoDB database authentication to include MongoDB 4.x for Unix. (See the help for other supported technologies.)

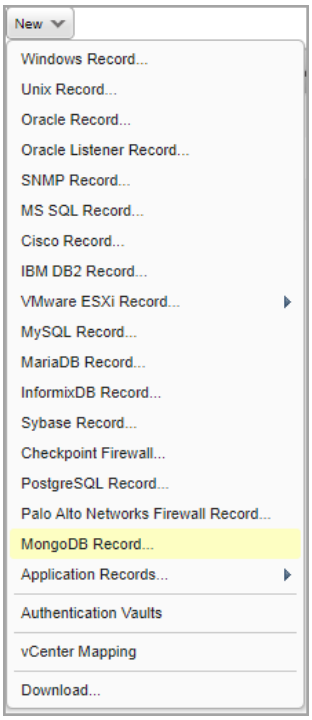
You'll need a MongoDB authentication record to authenticate to MongoDB database instance, and scan it for compliance. You'll also need a Unix record for the host running the database.

How do I get started?

- Go to Scans > Authentication.

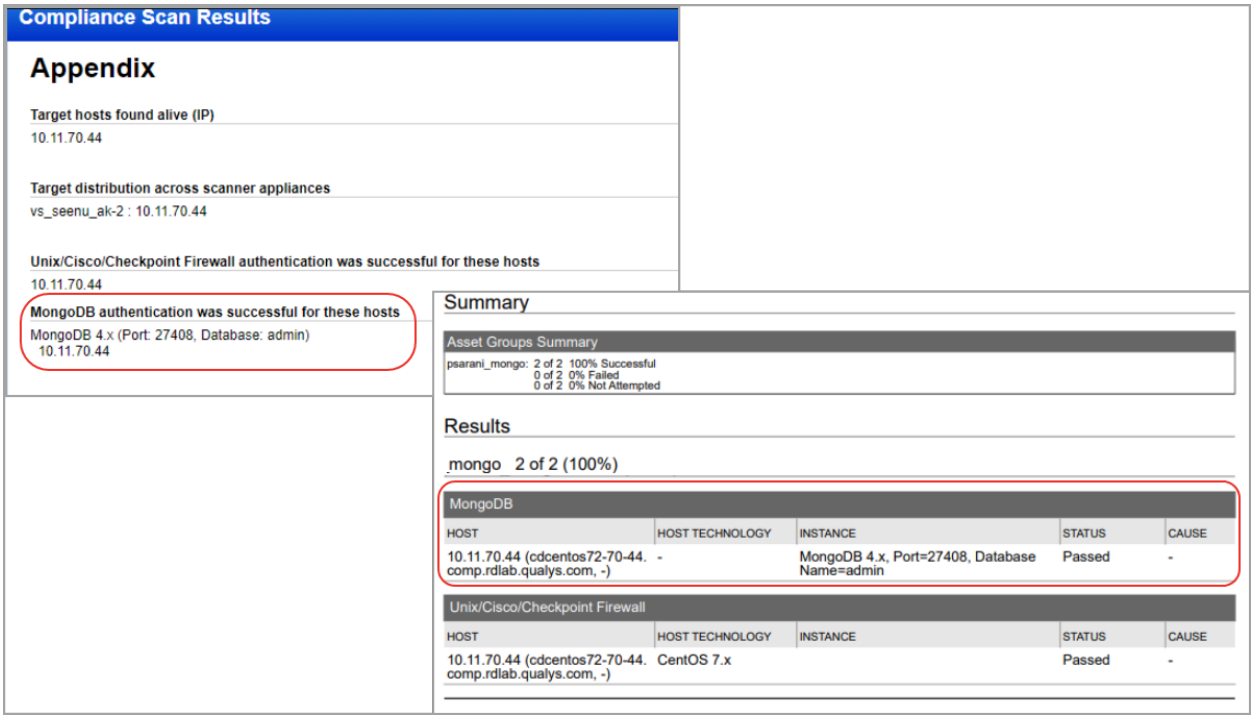
- Check that you already have a Unix record defined for each host running the database.

- Create a MongoDB authentication record for the same host. Go to New > Application Records > MongoDB Record.



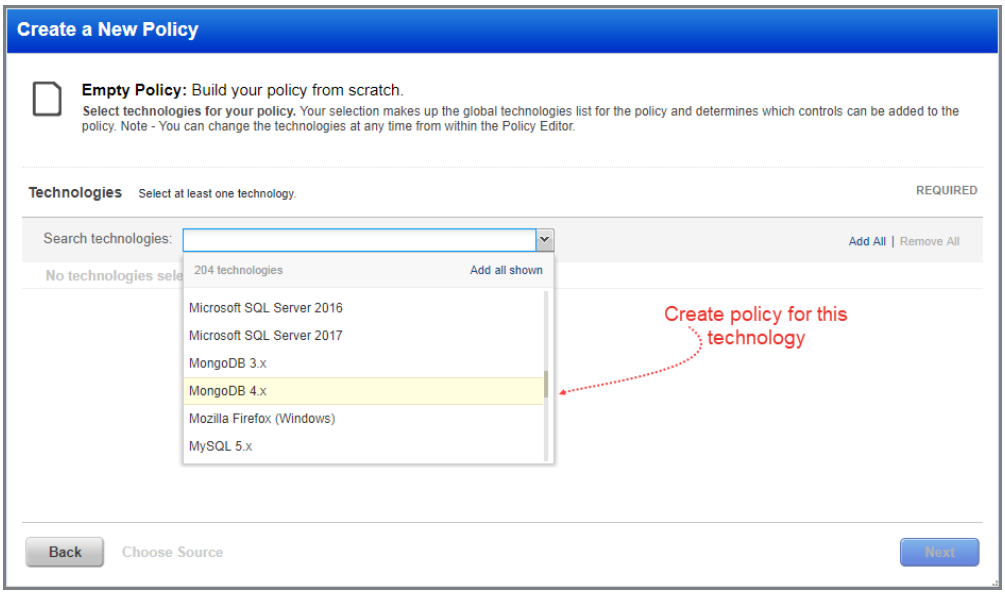
Sample Reports

You'll see MongoDB database instances in compliance scan results and reports.



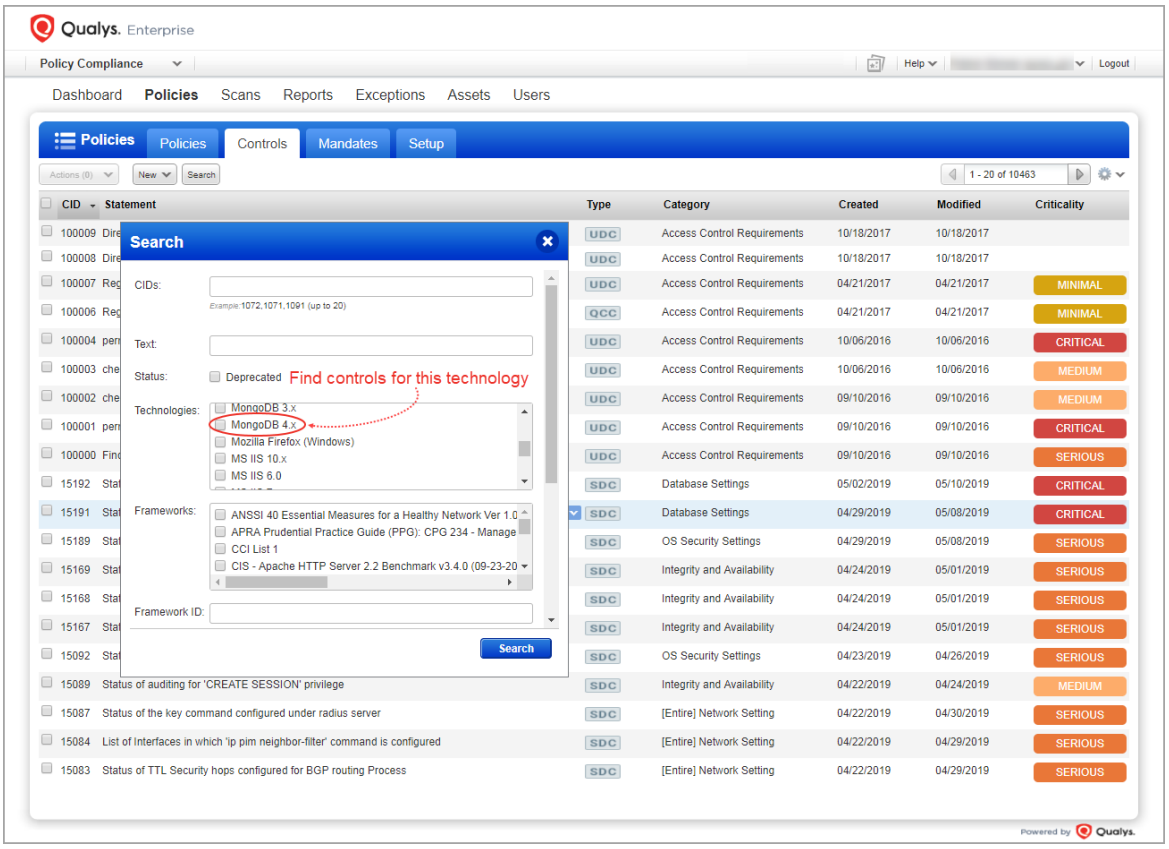
Policies and Controls

You'll also see MongoDB 4.x in the technologies list when creating a new policy.



Search Controls

You'll see MongoDB 4.x when searching controls by technologies.



Database User-Defined Controls Support

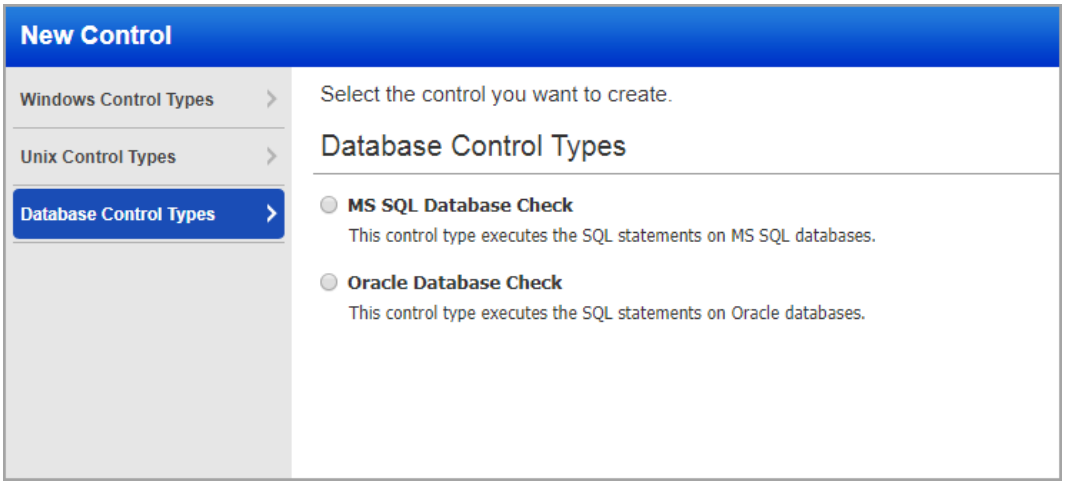
You can now use database user defined controls to create custom checks by executing SQL statements on databases. These controls can then be used to generate policy reports on your databases. Currently we support MS SQL and Oracle databases.

Follow these steps to create database controls and generate a report:

Step 1 - Add database controls

Go to PC > Policies > Controls > New > Control.

Select Database Control Types and then click the control type you want to create: MS SQL Database Check or Oracle Database Check.



In each control you'll define the SQL statement that you want to execute on your database. Note - Only SELECT statements are supported for the database controls. For example, you can use the following SQL statement to list all fields from "Customers" where country is "Germany" AND city is "Berlin":

SELECT * FROM Customers WHERE Country='Germany' AND City='Berlin'

See the online help for sample queries and results.

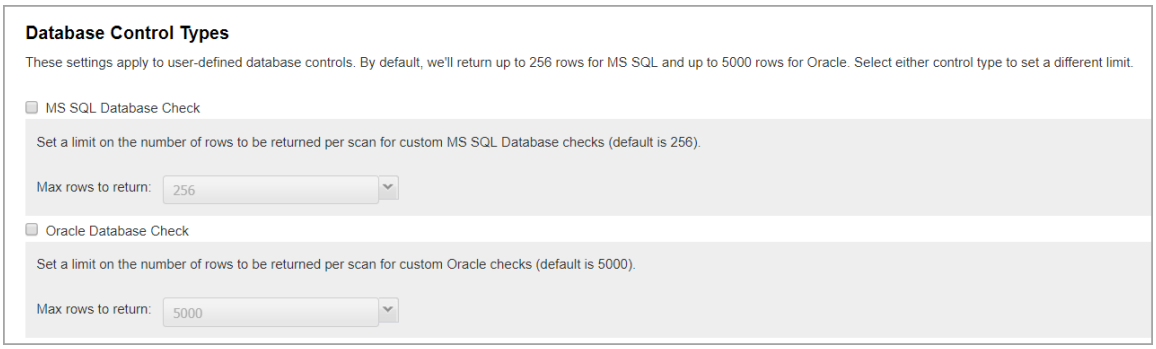
Step 2 - Add database controls to a policy

Create a new compliance policy or edit an existing policy, and add your database controls to the policy. Tip - Make sure your policy has the database technologies selected in the control.

Step 3 - Launch a compliance scan

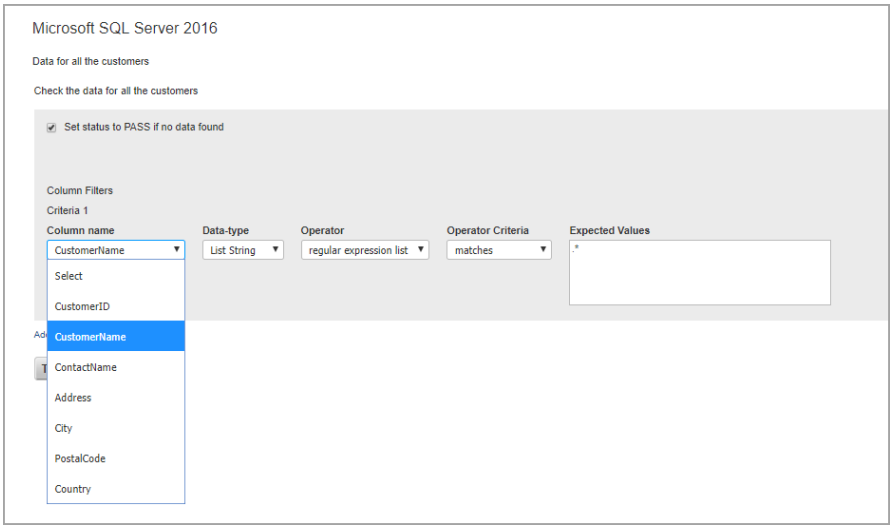
Launch a compliance scan on the host running the database.

You can edit the compliance option profile you'll use for the scan to set the max number of rows you want the check to return. By default, the max rows we'll return for a MS SQL Database Check is 256 rows and the max rows we'll return for an Oracle Database Check is 5000 rows. To lower this limit, select the database control type in the compliance option profile and pick a new value. (For Oracle Database Checks there is a limit on the number of columns we'll return – 30 columns max. This is not configurable.)



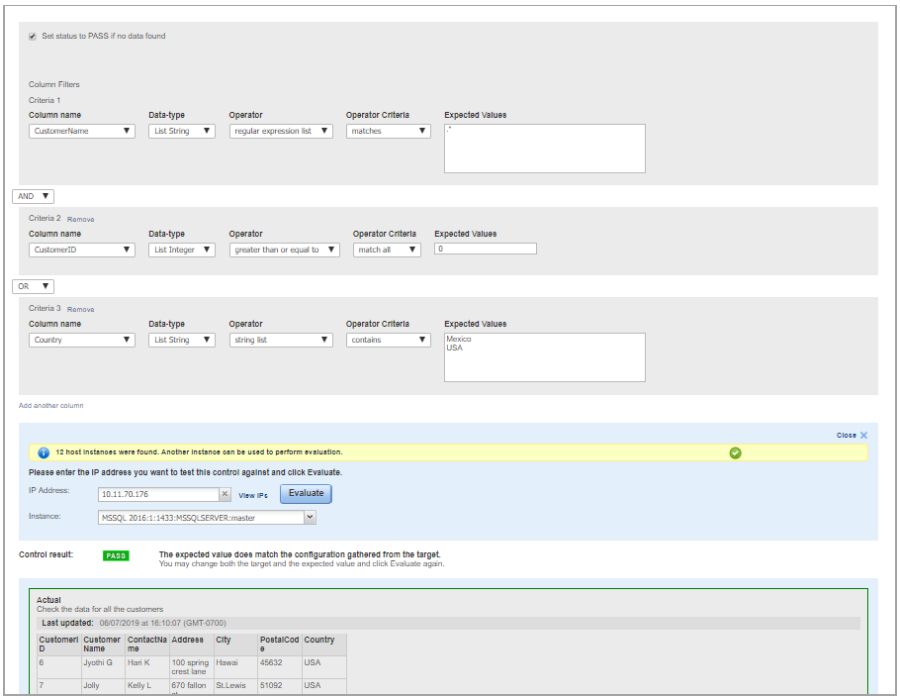
Step 4 - Return to your policy to set control criteria

Edit your compliance policy using the policy editor to see the actual data returned by your scan. Select a column and define the expected value. This is how you set the criteria that will determine pass/fail status for the control.



Click "Add another column" to add more criteria. You can add up to 5 criteria, i.e. Criteria 1, Criteria 2, Criteria 3 and so on.

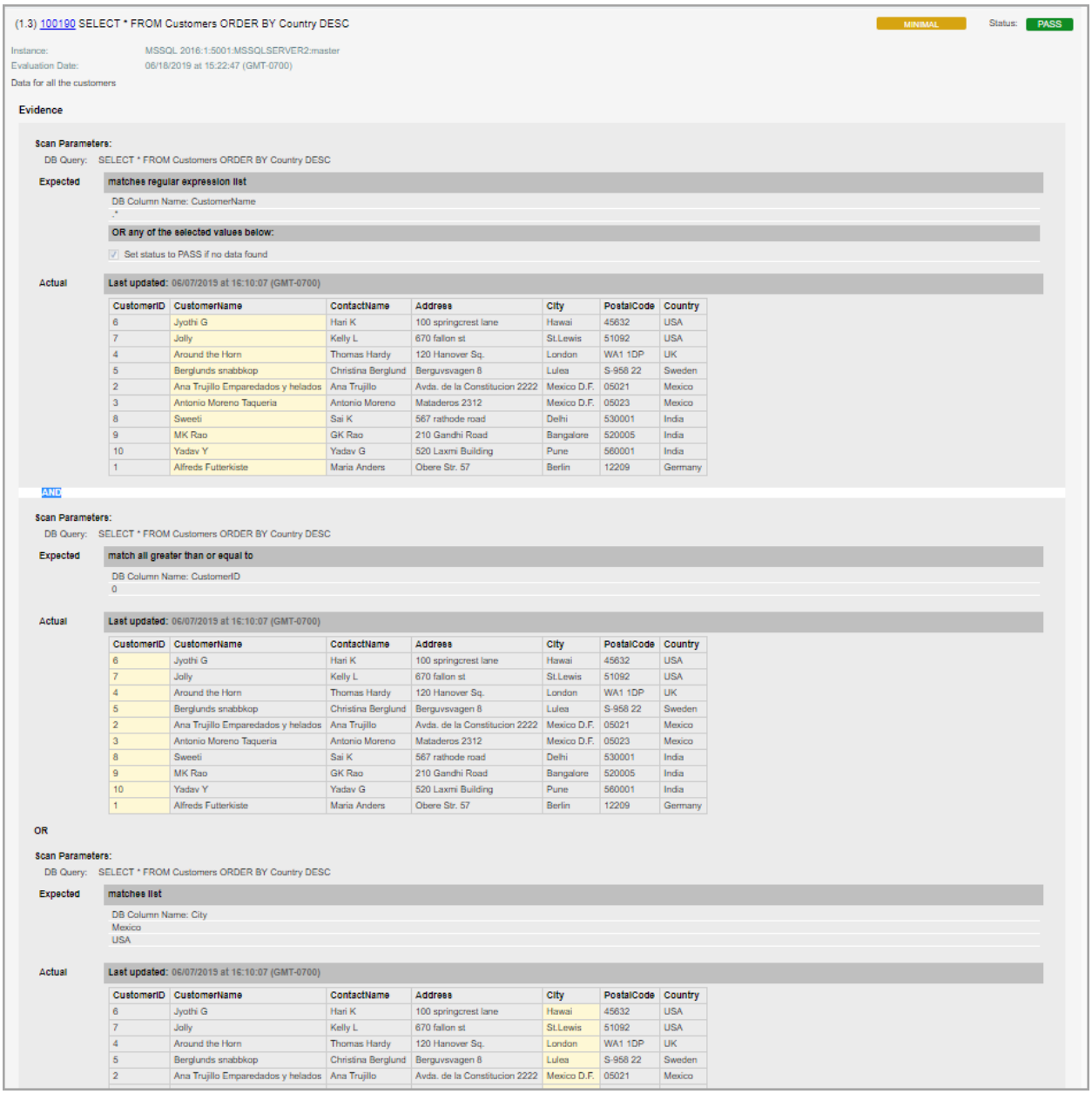
You can choose AND or OR between each criteria. If you choose AND then both criteria must match to Pass. If you choose OR then at least one criteria must match to Pass. Click Test Control to verify the criteria you set. Then save your policy.



Step 5 - Run a report

You'll see PASS or FAIL status in your report like you do with any control. If the columns returned by the most recent scan are different than previous scans then you'll want to edit your policy to modify the criteria selected for the control.

Here's a sample report where the expected value matches the actual value, resulting in status PASS.


(1.3) 100190 SELECT * FROM Customers ORDER BY Country DESC

MINIMAL Status: PASS

Instance: MSSQL 2016:1:5001:MSSQLSERVER2:master
Evaluation Date: 06/18/2019 at 15:22:47 (GMT-0700)
Data for all the customers

Evidence

Scan Parameters:
DB Query: SELECT * FROM Customers ORDER BY Country DESC

Expected **matches regular expression list**

DB Column Name: CustomerName
.*

OR any of the selected values below:

Set status to PASS if no data found

Actual **Last updated:** 06/07/2019 at 16:10:07 (GMT-0700)

CustomerID	CustomerName	ContactName	Address	City	PostalCode	Country
6	Jyothi G	Hari K	100 springcrest lane	Hawai	45632	USA
7	Jolly	Kelly L	670 fallon st	St.Lewis	51092	USA
4	Around the Horn	Thomas Hardy	120 Hanover Sq.	London	WA1 1DP	UK
5	Berglunds snabbkop	Christina Berglund	Berguvsvagen 8	Lulea	S-958 22	Sweden
2	Ana Trujillo Emparedados y helados	Ana Trujillo	Avda. de la Constitucion 2222	Mexico D.F.	05021	Mexico
3	Antonio Moreno Taqueria	Antonio Moreno	Mataderos 2312	Mexico D.F.	05023	Mexico
8	Sweeti	Sai K	567 rathode road	Delhi	530001	India
9	MK Rao	GK Rao	210 Gandhi Road	Bangalore	520005	India
10	Yadav Y	Yadav G	520 Laxmi Building	Pune	560001	India
1	Alfreds Futterkiste	Maria Anders	Obere Str. 57	Berlin	12209	Germany

AND

Scan Parameters:
DB Query: SELECT * FROM Customers ORDER BY Country DESC

Expected **match all greater than or equal to**

DB Column Name: CustomerID
0

Actual **Last updated:** 06/07/2019 at 16:10:07 (GMT-0700)

CustomerID	CustomerName	ContactName	Address	City	PostalCode	Country
6	Jyothi G	Hari K	100 springcrest lane	Hawai	45632	USA
7	Jolly	Kelly L	670 fallon st	St.Lewis	51092	USA
4	Around the Horn	Thomas Hardy	120 Hanover Sq.	London	WA1 1DP	UK
5	Berglunds snabbkop	Christina Berglund	Berguvsvagen 8	Lulea	S-958 22	Sweden
2	Ana Trujillo Emparedados y helados	Ana Trujillo	Avda. de la Constitucion 2222	Mexico D.F.	05021	Mexico
3	Antonio Moreno Taqueria	Antonio Moreno	Mataderos 2312	Mexico D.F.	05023	Mexico
8	Sweeti	Sai K	567 rathode road	Delhi	530001	India
9	MK Rao	GK Rao	210 Gandhi Road	Bangalore	520005	India
10	Yadav Y	Yadav G	520 Laxmi Building	Pune	560001	India
1	Alfreds Futterkiste	Maria Anders	Obere Str. 57	Berlin	12209	Germany

OR

Scan Parameters:
DB Query: SELECT * FROM Customers ORDER BY Country DESC

Expected **matches list**

DB Column Name: City
Mexico
USA

Actual **Last updated:** 06/07/2019 at 16:10:07 (GMT-0700)

CustomerID	CustomerName	ContactName	Address	City	PostalCode	Country
6	Jyothi G	Hari K	100 springcrest lane	Hawai	45632	USA
7	Jolly	Kelly L	670 fallon st	St.Lewis	51092	USA
4	Around the Horn	Thomas Hardy	120 Hanover Sq.	London	WA1 1DP	UK
5	Berglunds snabbkop	Christina Berglund	Berguvsvagen 8	Lulea	S-958 22	Sweden
2	Ana Trujillo Emparedados y helados	Ana Trujillo	Avda. de la Constitucion 2222	Mexico D.F.	05021	Mexico

Issues Addressed

- Fixed an issue where deleting an asset group from a scheduled report which is being run, throws an error and cancels the report. The report will now successfully run for the remaining asset groups in the scheduled report.
- Fixed an issue where activity logs were not getting generated on modification of approved host list under domain.
- Additional error messages will now be shown to help understand the probable cause of VM/PC scan failures.
- We'll now report cloud metadata for your EC2 assets collected directly from your EC2 connectors in the Host Detection API and UI.
- Fixed an issue in Edit Asset Groups wizard where the Add/Remove DNS/NETBIOS options were available for Unit Managers. These options are only available for Managers.
- Fixed an issue where PCI Scan Report Template > PCI Risk Rating displayed an older version of PCI DSS. It now shows the correct version.
- Fixed an issue where excluded IPs were not getting removed from the excluded hosts lists upon expiration.
- Fixed an issue where VM > Assets > Host Assets > View host information displayed duplicate authentication records for a single asset for Cisco.
- Now in VM/PC, when the user on the Assets > Host Assets tab views the host information for EC2 agent assets, the user will now see ec2 agent information in the EC2 Metadata tab and EC2 agent instance Id in the General Information tab.
- We have fixed an issue where the user when editing a Scheduled Map was shown a drop-down field "Client" in the Task Title tab, which was not available while creating a new Scheduled Map. Now the user will not see this field when editing a Scheduled Map.
- The customer was getting an error message "There are no scans remaining in your account...." when the user tried to launch the CertView scan with PPS. This issue was occurring because CertView was consuming VM licenses for CertView scans. We have fixed this issue by putting a check that will ensure that VM licenses are not used when CertView scan is launched.
- We have fixed an issue where when the user searched for CertView hosts using the CertView Host filter in the Assets > Host Assets tab, VM was showing Agent/DNS tracked hosts along with CertView hosts. Now we have fixed the issue to show only CertView hosts when the CertView Host filter is chosen.
- We have fixed an issue where the PC report was showing incorrect instance details in the extended evidence for the host that had multiple tomcat instances running. Now the PC report will display the correct instance name if the host has multiple instances of the same technology running.
- The 'HOST INSTANCE' field will appear in compliance csv report only when the single instance filter is applied.
- We have fixed an issue where the Compliance Scan report was not showing auto discovered Apache instances for subscriptions that had cron-based task launching enabled and the scan was launched by a non-POC Manager and option profile used for the scan is created by a POC Manager.
- We made additional improvements to the newly introduced back-end processing pipeline to further improve Agent snapshot processing rates.

- Fixed an issue where the number of physical scanners shown under Account Info > My Scanner Appliances was incorrect.
- Now appliances are no longer tied to regular user accounts. So, we removed the deprecated message from the reset password page. "Your account was used to install scanner appliances and there are appliances running software version 2.2, then you must reboot the appliances and re-login with your new password using the LCD interface."
- We have updated the Set Up JBoss Server Authentication topic in online help to specify that we support version 8.0 and above for WildFly and version 6.0 and above for JBoss EAP technologies both on Windows and Unix for JBoss Server Authentication.
- We have updated the User Roles Comparison (Vulnerability Management) and User Roles Comparison (Policy Compliance) topics in online help to add information that "Only Manager has permission to remove a Host Asset from the subscription".