



Qualys Cloud Platform (VM, PC) v10.x

Release Notes

Version 10.6

December 18, 2020 (Updated December 22, 2020)

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

Qualys Policy Compliance (PC/SCAP/SCA)

[Purge Compliance Data for Inactive Instances](#)

[New Support for SAP IQ 16.x Authentication](#)

[SAP IQ Database User-Defined Control Support](#)

[Confirmation Page When You Edit Scan Parameters in UDCs](#)

[Character Limit for SQL Statement in UDCs Increased to 32000](#)

[Control Criticality Option in SCA Report Templates](#)

Qualys Cloud Platform

[New Workflow to Generate Passwords](#)

[More Regions Supported for EC2 and Cloud Perimeter Scans](#)

[More Details in Authentication Reports: Host ID and Asset Tags](#)

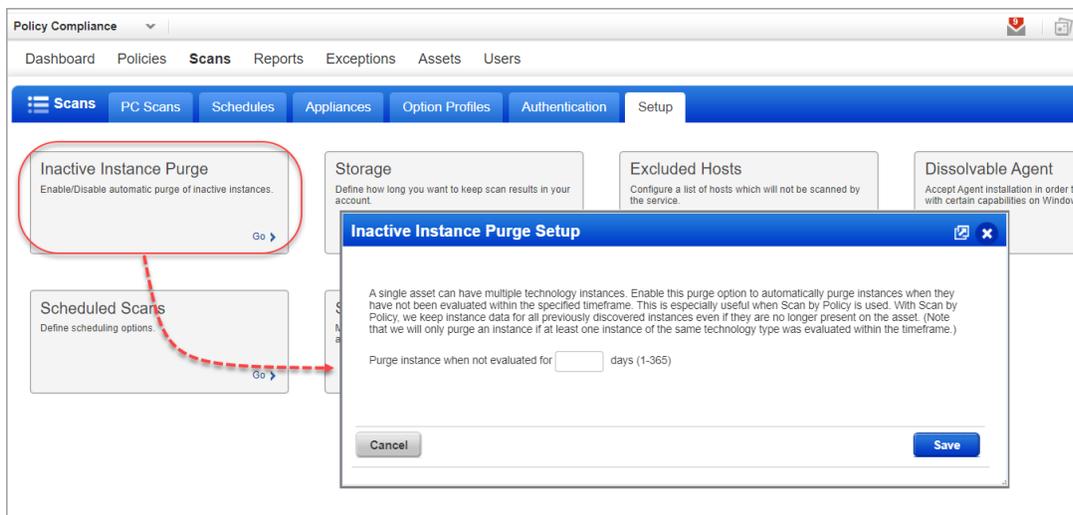
Qualys 10.6 brings you more improvements and updates! [Learn more](#)

Qualys Policy Compliance (PC/SCAP/SCA)

Purge Compliance Data for Inactive Instances

With this release, we've added a new setup option that will allow you to purge compliance data for only the instances on an asset that are no longer active, and keep compliance data for the active instances. This is especially useful for customers that use Scan by Policy because with Scan by Policy we keep instance data for all previously discovered instances even if they are no longer present on the asset.

A Manager can enable this option by going to **PC > Scans > Setup > Inactive Instance Purge**. Then set a timeframe from 1 to 365 days. Once enabled, instances that have not been evaluated within the set timeframe will be purged automatically. Compliance data for purged instances will no longer appear in your reports. (Note that we will only purge an instance if at least one instance of the same technology type has been evaluated within the timeframe.)



New Support for SAP IQ 16.x Authentication

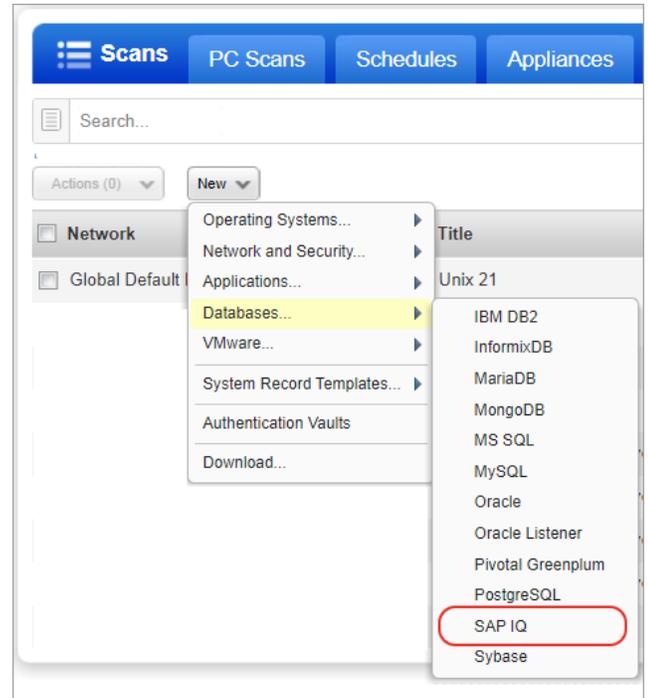
We now support SAP IQ authentication for compliance scans using Qualys apps PC, SCA. Simply create an SAP IQ authentication record with details about your credentials to authenticate to an SAP IQ database instance running on a host, and scan it for compliance.

How do I get started?

Go to **Scans > Authentication**, and choose **New > Databases > SAP IQ Record** (as shown on the right).

Your SAP IQ authentication record

Each SAP IQ record identifies account login credentials, database information and target hosts (IPs). Provide basic login credentials (username and password) to be used for authentication or get the password from a supported password vault. Supported vaults are: Arcon PAM, Azure Key, BeyondTrust PBPS, CA Access Control, CA PAM, CyberArk AIM, CyberArk PIM Suite, HashiCorp, Hitachi ID PAM, Liberman ERPM, Quest Vault, Thycotic Secret Server, Wallix AdminBastion (WAB)

A screenshot of the 'New SAP IQ Record' form in the Qualys interface. The form has a blue header with the title 'New SAP IQ Record' and a 'Launch Help' link. On the left, there is a sidebar with navigation options: 'Record Title', 'Login Credentials' (selected), 'IPs', and 'Comments'. The main content area is titled 'Authentication' and contains the following fields:

- Authentication Type:** A dropdown menu set to 'Basic'.
- Username*:** A text input field containing 'Joe_user'.
- Password*:** A password input field with masked characters.
- Confirm Password*:** A password input field with masked characters.
- Enable Password Encryption

Below the authentication section is the 'Database Information' section, which includes:

- Database Name*:** A text input field containing 'SAP IQ'.
- Installation Directory:** An empty text input field.
- Required for Unix based hosts. Example: /opt/sybase
- Port*:** A text input field containing '3456'.

At the bottom of the form are two buttons: 'Cancel' and 'Create'.

Tell us the database name to authenticate to and the port the database is running on. The installation directory name is required only for Unix based hosts.

Database Information

Tell us the name and port the database is running on and we'll find the database instance to authenticate to. For Unix hosts, the installation directory is also required.

Database Name*:

Installation Directory:

Required for Unix based hosts. Example: /opt/sybase

Port*:

Sample Reports

You'll see SAP IQ 16.x instances in compliance scan results and reports.

Compliance Scan Results

File ▾ Help ▾

Reference: C:\Programmer\1000\04\30\73300

External Scanners: RahulScan (Scanner 12.1.67-1, Vulnerability Signatures 2.1.3296-1)

Duration: 00:03:31

Title: SAPIQ scan

Asset Groups: -

IPs: 10.11.70.52

Excluded IPs: -

Compliance Profile: [Initial PC Options](#)

SAP_IQ 2 of 3 (66%)

32

HOST	HOST TECHNOLOGY	INSTANCE	STATUS	CAUSE	OS	LAST AUTH	LAST SUCCESS	HOST ID	ALL ASSET TAGS
10.11.70.52 (-, -)	SAP IQ 16.x	Port=2638, Instance Name=pca-rhel68x64-70-52_iqdemo, Database Name=iqdemo	Passed	-	Ubuntu / Tiny Core Linux / Linux 2.6.x	12/08/2020	12/08/2020	5088976	BU1, SAP_IQ
10.20.32.120 (-, -)	SAP IQ 16.x	Port=2638, Instance Name=pca-rhel68x64-70-52_iqdemo, Database Name=iqdemo	Passed	-	Ubuntu / Tiny Core Linux / Linux 2.6.x	12/08/2020	12/08/2020	5101426	BU1, SAP_IQ

SAP IQ authentication was successful for these hosts

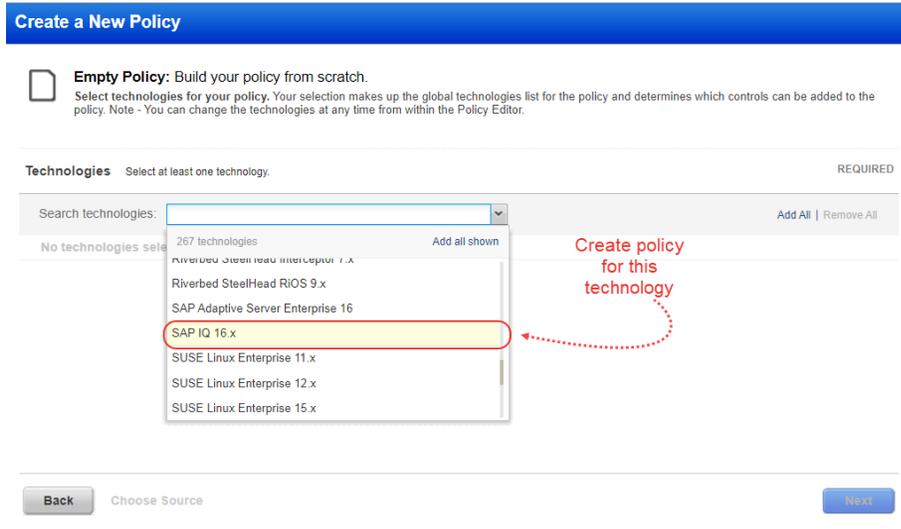
SAP IQ 16 (Port: 2638, Instance Path: pca-rhel68x64-70-52_iqdemo, Database: iqdemo)
10.11.70.52

Qualys Release Notes

4

Policies and Controls

You'll see SAP IQ 16.x when creating new policies and searching controls



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: 267 technologies Add all shown Add All | Remove All

No technologies selected

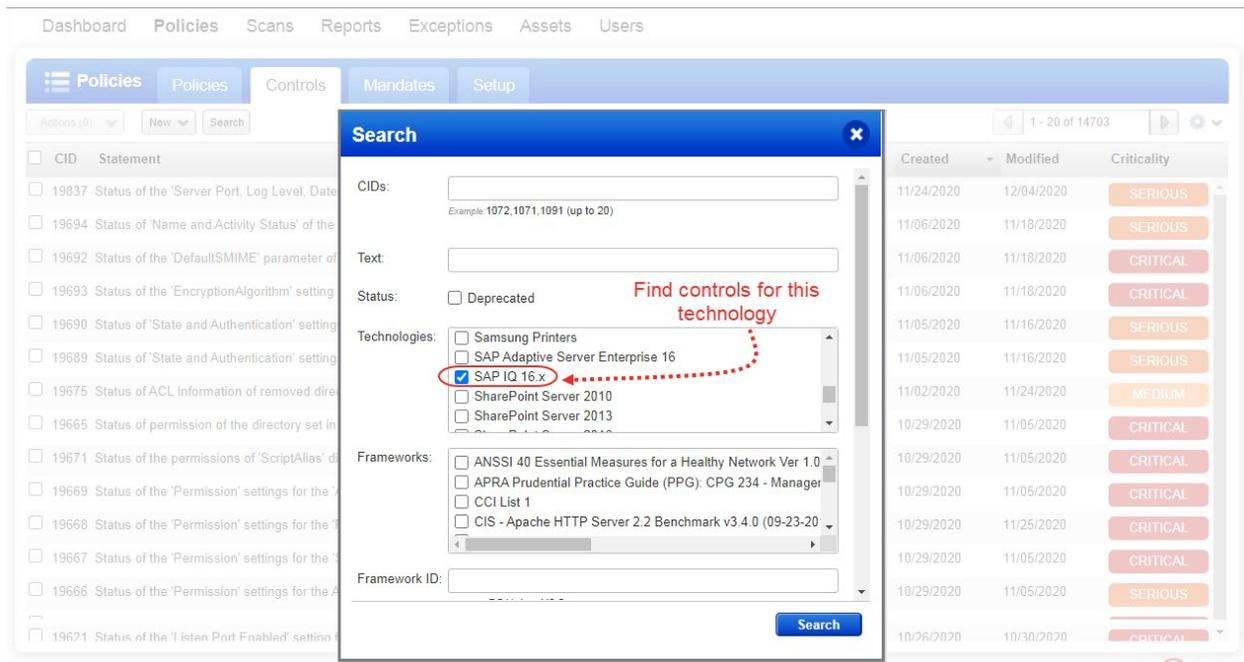
- Riverbed SteelHead Interceptor 7.x
- Riverbed SteelHead RIOS 9.x
- SAP Adaptive Server Enterprise 16
- SAP IQ 16.x**
- SUSE Linux Enterprise 11.x
- SUSE Linux Enterprise 12.x
- SUSE Linux Enterprise 15.x

Back Choose Source **Next**

Create policy for this technology

Search Controls

You'll see SAP IQ 16.x when searching controls by technologies.



Dashboard Policies Scans Reports Exceptions Assets Users

Search

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

Text:

Status: Deprecated

Technologies:

- Samsung Printers
- SAP Adaptive Server Enterprise 16
- SAP IQ 16.x**
- SharePoint Server 2010
- SharePoint Server 2013

Frameworks:

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

Framework ID:

Search

Find controls for this technology

Created	Modified	Criticality
11/24/2020	12/04/2020	SERIOUS
11/06/2020	11/18/2020	SERIOUS
11/06/2020	11/18/2020	CRITICAL
11/06/2020	11/18/2020	CRITICAL
11/05/2020	11/16/2020	SERIOUS
11/05/2020	11/16/2020	SERIOUS
11/02/2020	11/24/2020	MEDIUM
10/29/2020	11/05/2020	CRITICAL
10/29/2020	11/05/2020	CRITICAL
10/29/2020	11/05/2020	CRITICAL
10/29/2020	11/25/2020	CRITICAL
10/29/2020	11/05/2020	CRITICAL
10/29/2020	11/05/2020	CRITICAL
10/29/2020	11/05/2020	SERIOUS
10/26/2020	10/30/2020	CRITICAL

SAP IQ Database User-Defined Control Support

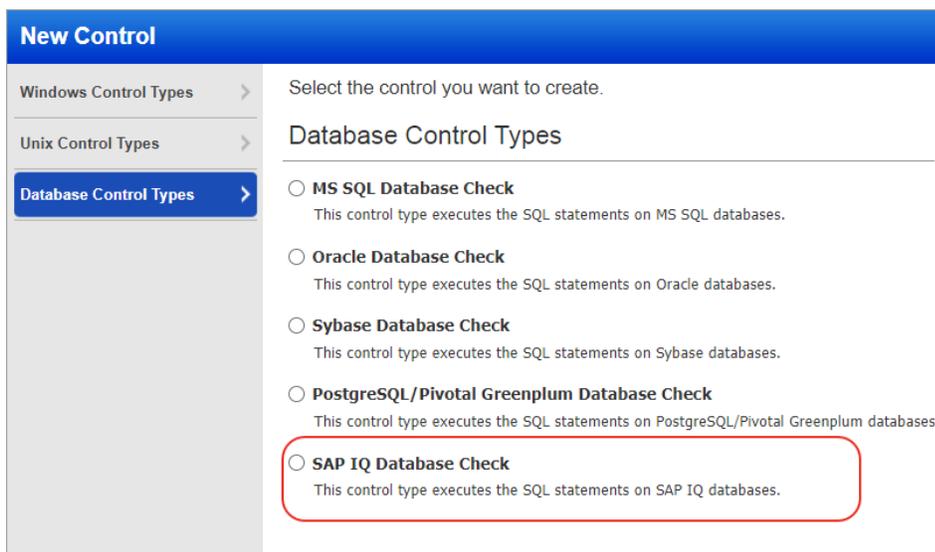
You can now use SAP IQ database user-defined controls to create custom checks by executing SQL statements on databases. These controls can then be used to generate policy reports on your databases. We're already supporting MS SQL, Oracle databases, Sybase and PostgreSQL/Pivotal Greenplum.

Follow these steps to create SAP IQ 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 **SAP IQ Database Check** control type.



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 SAP IQ 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 an Sap IQ Database

Check is 256 rows. To lower this limit, select the Database Control Types in the compliance option profile and pick a new value. Maximum allowed limit for SAP IQ is 10000 rows.

Database Control Types

These settings apply to user-defined database controls. By default, we'll return up to 5000 rows for Oracle and up to 256 all other control types. Select the control type to edit the limit.

MS SQL Database Check

Set a limit on the number of rows to be returned per scan for custom MS SQL Database checks (default is 256).

Max rows to return: limit (1-256)

Oracle Database Check

Set a limit on the number of rows to be returned per scan for custom Oracle checks (default is 5000).

Max rows to return: limit (1-5000)

Sybase Database Check

Set a limit on the number of rows to be returned per scan for custom Sybase Database checks (default is 256).

Max rows to return: limit (1-2500)

PostgreSQL/Pivotal Greenplum Database Check

Set a limit on the number of rows to be returned per scan for custom PostgreSQL/Pivotal Greenplum Database checks (default is 256).

Max rows to return: limit (1-5000)

SAP IQ Database Check

Set a limit on the number of rows to be returned per scan for custom SAP IQ Database checks (default is 256).

Max rows to return: limit (1-10000)

Step 4 - Return to your policy to set control criteria

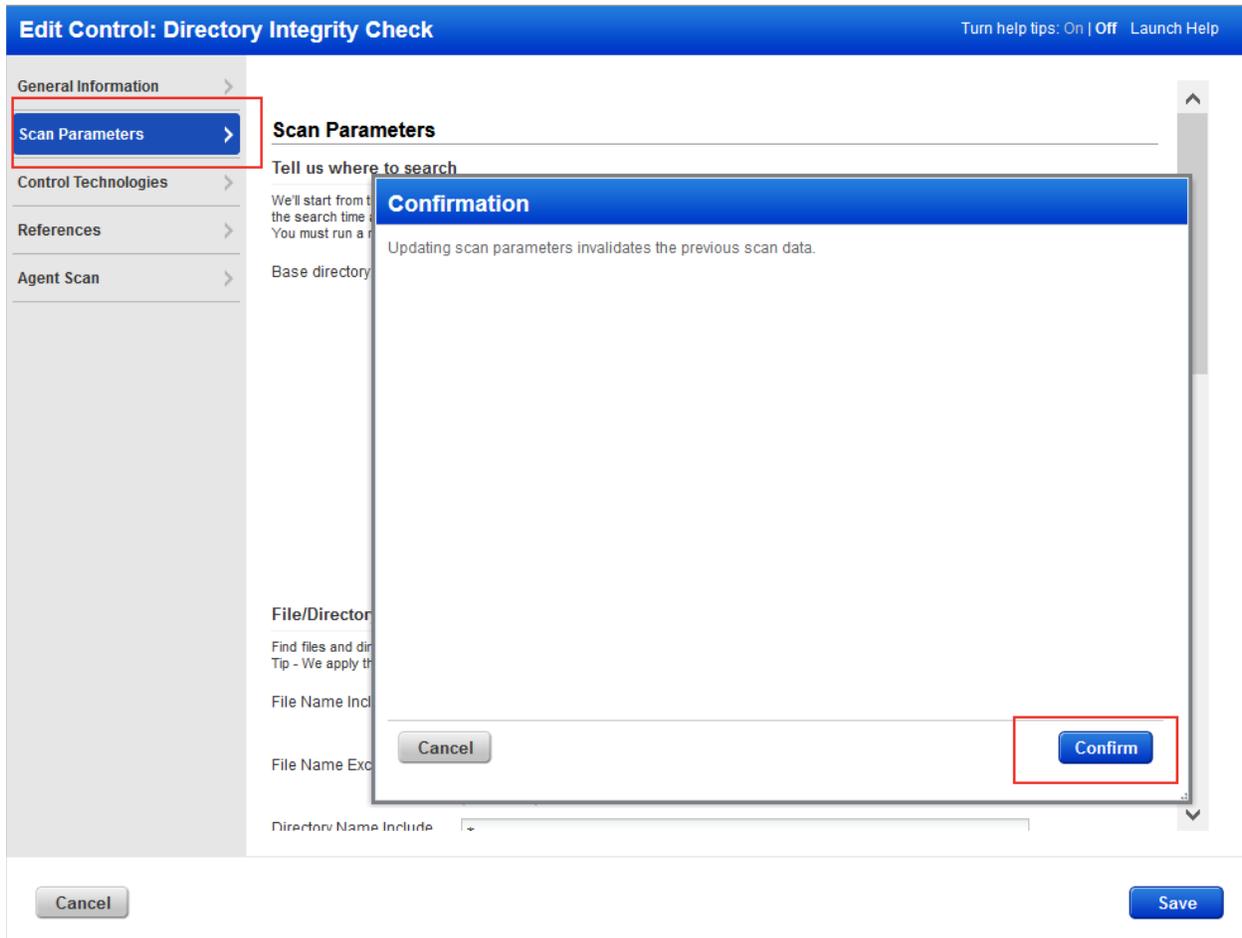
Edit your compliance policy using the policy editor to see the actual data returned by your scan. Select a column and define the expected value. This is how you set the criteria that will determine pass/fail status for the control.

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.

Confirmation Page When You Edit Scan Parameters in UDCs

When you edit scan parameters in a User Defined Control (UDC), now you see a confirmation page after you choose to save your changes. We've added the confirmation page to inform you that any modification in scan parameters of a UDC invalidates the data captured in a previous scan for that UDC. At this stage, you can click Confirm and proceed, or cancel your edits.



Suppose you change the expected value of a particular UDC from any of its parent policies. After you save the policy, if you go to the Controls tab and edit the scan parameters of the same UDC, which you edited earlier, on the confirmation page, you see the details of all the parent policies that contain the edited UDC. This means you must run a fresh scan to collect and evaluate data for those policies.

- General Information >
- Scan Parameters >**
- Control Technologies >
- References >
- Agent Scan >

Scan Parameters

Tell us where to search

We'll start from the base directory. We recommend you set this to something other than root to minimize the search time and disk utilization.
You must run a new scan after saving changes to scan parameters to use modified values in data collection and posture evaluation.

Base directory:*

File/Directory Name

Find files and directories
Tip - We apply the include

File Name Include

File Name Exclude

Directory Name Include

Directory Name Exclude

File Permissions

Find files with (or without)
is set on the file. No mean

Confirmation

Updating scan parameters invalidates the previous scan data.
This control is included in the following policies.

Policy ID	Policy Title	Technology
3072473	File Integrity Assessment Policy	CentOS 7.x
3566788	UNIX SDLC Assessment Policy	CentOS 7.x

Cancel Confirm

Cancel

Save

Character Limit for SQL Statement in UDCs Increased to 32000

Now you can create a more complex query in the SQL Statement field on the **Control Technologies** tab as you define a database User Defined Control (UDC). Earlier, the maximum permissible limit for a SQL statement query was 4000 characters. Now, we have increased this limit to 32000 characters.

New Control: Sybase Database Check Turn help tips: On | Off Launch Help

General Information > **Control Technologies**

Control Technologies > Tell us the technologies your control applies to and define the SQL statement. We'll use this information when performing pass/fail control evaluation.

Reporting Options >

References >

Default Values
Do you want to define values for Rationale, SQL Statement, Description, Remediation once and use the same for all technologies? Simply, enter the values here and we'll copy them as default to each technology that you select below. You can also create individual settings for each technology in the Technologies section.

Rationale:*

SQL Statement*

Description:*

Remediation:

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

SAP Adaptive Server Enterprise 16
Use this section to create a SAP Adaptive Server Enterprise 16 instance of this control.

Sybase ASE 15
Use this section to create a Sybase ASE 15 instance of this control.

You can also edit the SQL statements in your existing UDCs to optimize your query definition.

Control Criticality Option in SCA Report Templates

While creating an SCA Policy Report template, on the **Layout** tab of the New Compliance Policy Report Template screen, in the Report Layout section, now you have the **Criticality** option. With this change, now your SCA reports also show the criticality ratings of your controls. You can select the control criticality ratings that you want to view in your SCA policy report. By default, all the criticality ratings are selected. This is a mandatory field, and hence, you must select at least one criticality level.

The screenshot shows the 'New Compliance Policy Report Template' window. The 'Layout' tab is selected in the left sidebar. The 'Report Layout' section is highlighted with a red box. It contains the following options:

- Group By:** Hosts (dropdown)
- Status:** All, Passed, Failed, Error (checkboxes)
- Criticality:** All, UNDEFINED, MINIMAL, MEDIUM, SERIOUS, CRITICAL, URGENT (checkboxes)

Criticality ratings of controls are displayed in all the supported report formats. For example, here is a sample report in PDF format, where you can see the criticality rating next the Failed status of the control (5.148) 3936.

Key	Name	Value
HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU	NoAutoRebootWithLoggedOnUsers	
(5.148) 3926 Status of the 'Reschedule Automatic Update scheduled installations' setting		Failed CRITICAL
Instance	os	
Previous Status	Failed	
Evaluation Date	12/01/2020 at 12:59:09 (GMT+0530)	
<p>The 'Reschedule Automatic Updates scheduled installations' setting determines how much time should elapse after system boot before beginning a scheduled system update procedure. As configuring the system as to put updates on hold while start-up procedures are completed can help avoid undesirable system boot conflicts, this should be configured according to the needs of the business.</p>		

Here's another example of a report in CSV format. You can see the Criticality Label column highlighted in the screenshot:

ating Syst	st Scan Da	evaluation D:	Control ID	Technology	Control	Criticality Label	Criticality Value	Instance	Rationale
R2 Stand	at 12:28:01	t 12:59:09	2341	ows 2008	'Duration'	URGENT	5	os	meaning
R2 Stand	at 12:28:01	t 12:59:09	2342	ows 2008	'Threshold'	URGENT	5	os	time in w
R2 Stand	at 12:28:01	t 12:59:09	2343	ows 2008	'Sunt Locko	URGENT	5	os	nt Lockout
R2 Stand	at 12:28:01	t 12:59:09	3924	ows 2008	'Sential Mar	URGENT	5	os	As this p
R2 Stand	at 12:28:01	t 12:59:09	2181	ows 2008	'Snted the 'A	CRITICAL	5	os	S servers, v
R2 Stand	at 12:28:01	t 12:59:09	2182	ows 2008	'S granted the	CRITICAL	5	os	ot require
R2 Stand	at 12:28:01	t 12:59:09	2184	ows 2008	'S granted the	CRITICAL	5	os	default in
R2 Stand	at 12:28:01	t 12:59:09	2391	ows 2008	'Sd the 'Allo	CRITICAL	5	os	ors.) If cer
R2 Stand	at 12:28:01	t 12:59:09	2185	ows 2008	'Snted the '	URGENT	5	os	r vices can
R2 Stand	at 12:28:01	t 12:59:09	2186	ows 2008	'S granted	URGENT	5	os	As this rig
R2 Stand	at 12:28:01	t 12:59:09	2191	ows 2008	'Snts grante	URGENT	5	os	ecording o
R2 Stand	at 12:28:01	t 12:59:09	3925	ows 2008	'S 'Change t	URGENT	5	os	. times use
R2 Stand	at 12:28:01	t 12:59:09	2192	ows 2008	'Sccounts gr	URGENT	5	os	agefile ma
R2 Stand	at 12:28:01	t 12:59:09	2193	ows 2008	'Snts gran	URGENT	5	os	User Acco
R2 Stand	at 12:28:01	t 12:59:09	3242	ows 2008	'Snts gran	URGENT	5	os	o Administr

Qualys Cloud Platform

New Workflow to Generate Passwords

With this release, we have introduced a new workflow to generate passwords for new and existing users. In the new workflow, users will receive an email containing activation URL, OTP code, and OTP key. When users click the activation URL, they need to provide the OTP code corresponding to the OTP key to view login information, including their username and password.

This new workflow helps to overcome constraints occurring due to network security protocols.

A Manager can change the password for any user in the subscription. A Unit Manager can do this for users in their business unit.

Note:

- If the subscription has only one Manager user, and that user's password is lost, contact Support.
- When entering the OTP code, ensure that code corresponds to the OTP Key. OTP code is valid for 30 minutes and it expires after 3 unsuccessful attempts.

What are the steps to see the login information?

Once user receives an email containing activation URL, OTP code, and OTP key, click the activation URL which shows following popup:



To continue with the Activation process, enter Associated OTP code for OTP key **2251** from your Activation Email into the box below.

Enter OTP :

Provide OTP code corresponding to the OTP key in the **Enter OTP** textbox and click **Submit**. This shows **Welcome to Qualys** screen with login information.



 **Welcome to Qualys**

Hello [redacted],

Login information for your new Qualys account is shown below. Please login now to complete your registration.

URL: [https://\[redacted\].qualys.com/](https://[redacted].qualys.com/)
Username: [redacted]
Password: [redacted]

 This letter was auto-generated by the Qualys cloud Platform. Your secure link to this letter ensures that no one else can access your login information. It is recommended that you print this letter and store it safely for future references.

More Regions Supported for EC2 and Cloud Perimeter Scans

With this release, we have added a support to the new regions when launching vulnerability and compliance scans on EC2 instances, and when launching cloud perimeter scans: Europe (Milan) and Africa (Cape Town).

Sample – Launch EC2 Vulnerability Scan

Go to **Scans > Scans > New > EC2 Scan**. You'll see two new regions in **Available Regions** dropdown list: **Africa (Cape Town)** and **Europe (Milan)**.

Launch EC2 Vulnerability 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:

Option Profile: * [Select](#)

Processing Priority: ▼

Target Hosts

Connector:

Platform: EC2-Classical (Selected Region) EC2-VPC (All VPCs in Region) EC2-VPC (Selected VPC)
With this option there must be peering between all the VPCs in the selected region.

Available Regions:

- Africa (Cape Town)
- Asia Pacific (Hong Kong)
- Asia Pacific (Mumbai)
- Asia Pacific (Osaka-Local)
- Asia Pacific (Seoul)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Canada (Central)
- EU (Frankfurt)
- EU (Ireland)
- EU (London)
- EU (Paris)
- EU (Stockholm)
- Europe (Milan)

Include hosts that have [Add Tag](#)

Do not include hosts that [Add Tag](#)

Scan specific Instance

Temporarily add agent a [Add Tag](#)

Select this option to add the already in your subscription. They'll be added for this

- When you run an authentication report by specifying asset tags as the report source, you see the Asset Tags column in the output. Earlier, in the Asset Tags column, only the text “Selected Tags” was displayed. Now you see the asset tags that you specify explicitly in the report source and which are associated with each asset listed in the report.
- We’ve added the Host Id column where you see the host Id for each host in the report. Only if you select the **Host ID** checkbox on the Report Details page, you see this column in the report.
- We’ve added the All Asset Tags column where you see a complete list of tags associated with the asset. Only if you select the **All Asset Tags** checkbox on the Report Details page, you see this column in the report.

Issues Addressed

- Fixed an issue where Asset Groups were not populating correctly under **Assets > Application**.
- We fixed an issue where notification options were not updated in the user's account when user preferences were imported from XML using the Subscription API.
- The Compliance Posture API (/api/2.0/fo/compliance/posture/info/) now returns an error when run with invalid tags.
- For Unix Directory Search UDC, now we'll evaluate values in scan data which include both values and error codes.
- Now we'll allow DNS names with an underscore (_) when entering DNS names in an asset group.
- When adding users to a distribution list, the Users list will now display active users only.
- Fixed an issue where error was occurring if the last label of the DNS name contains hyphen (-). As per RFC-1034, RFC-1123, and RFC-2181 standards, hyphen (-) is not allowed in the last label of the DNS name. With this fix, we are now following these 3 RFC standards for DNS name and the last label of DNS name will not allow hyphen (-).
- Now all Manager users (not just the Manager primary contact) can view and edit the "Asset Tracking & Data Merging" setup options under **Assets > Setup**.
- We've provided more elaborate error message for a scenario where you try to import a policy or a UDC in an XML file, and the import fails due to erroneous tagging in the XML. Now, you can see the line number where we identify erroneous tagging and the tags that are causing problems.
- In the HashiCorp Vault help, we updated the description for the Path value. The default path is secret/data.
- We updated the Online Help for JBoss and MS IIS to clearly state that the Windows record must have domain type "NetBIOS, User-Selected IPs" with the IP address assigned or the domain type "NetBIOS, Service-Selected IPs".
- We updated the Online Help and docs for CyberArk AIM vaults to include support for variables in folder/file names.