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

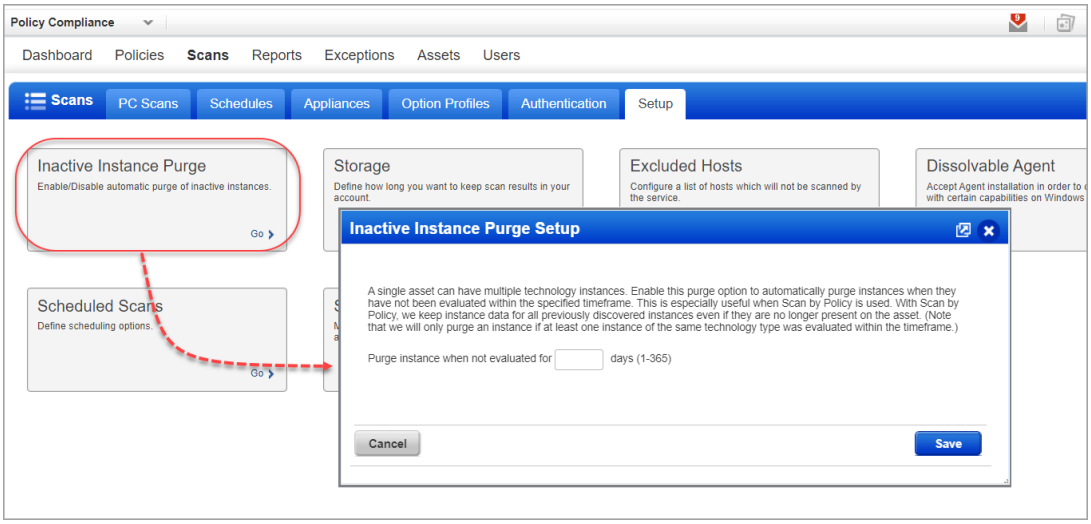
Qualys 10.6 brings you more improvements and updates! **Learn more**

Qualys Policy Compliance (PC/SCAP/SCA)

Purge Compliance Data for Inactive Instances

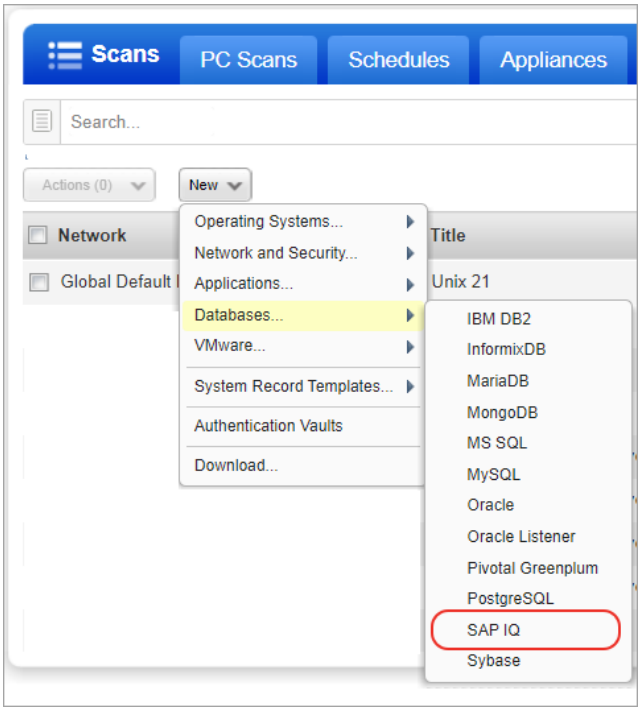
With this release, we've added a new setup option that will allow you to purge compliance data for only the instances on an asset that are no longer active, and keep compliance data for the active instances. This is especially useful for customers that use Scan by Policy because with Scan by Policy we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

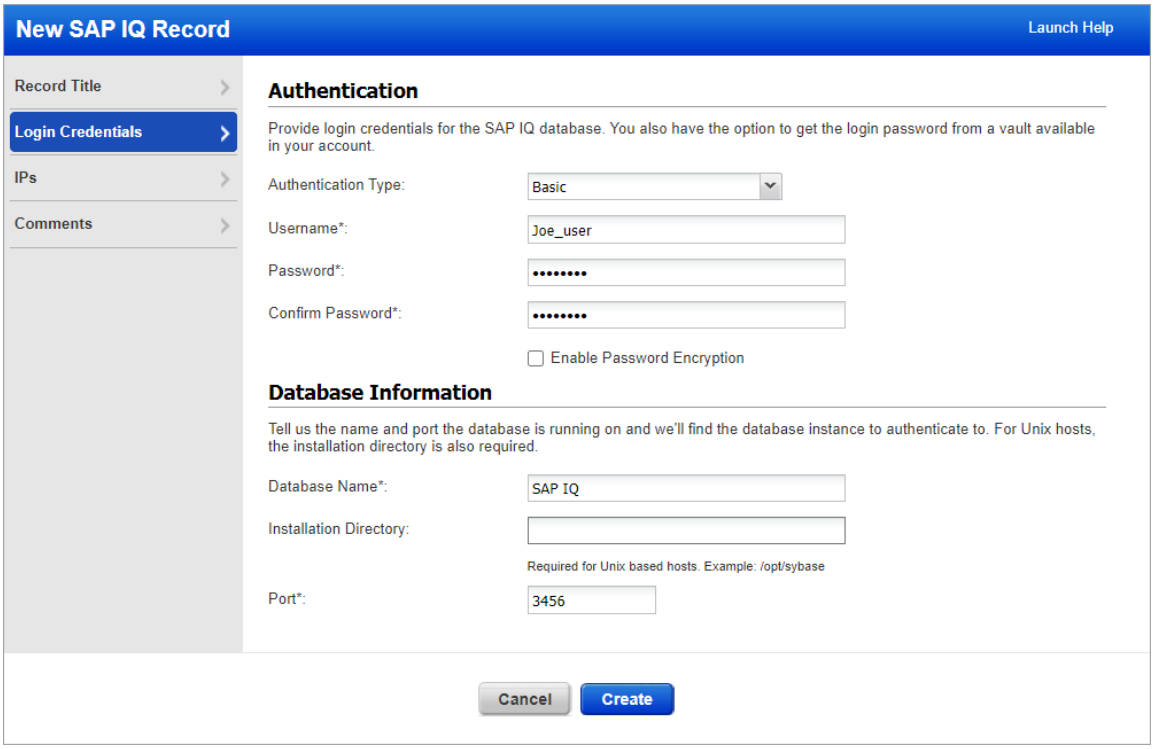


How do I get started?

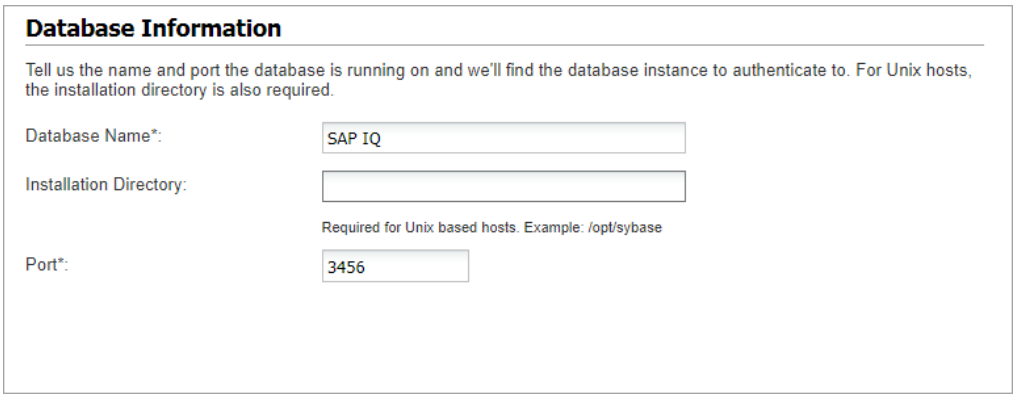
Go to **Scans** > **Authentication**, and choose **New** > **Databases** > **SAP IQ** Record (as shown on the right).

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)

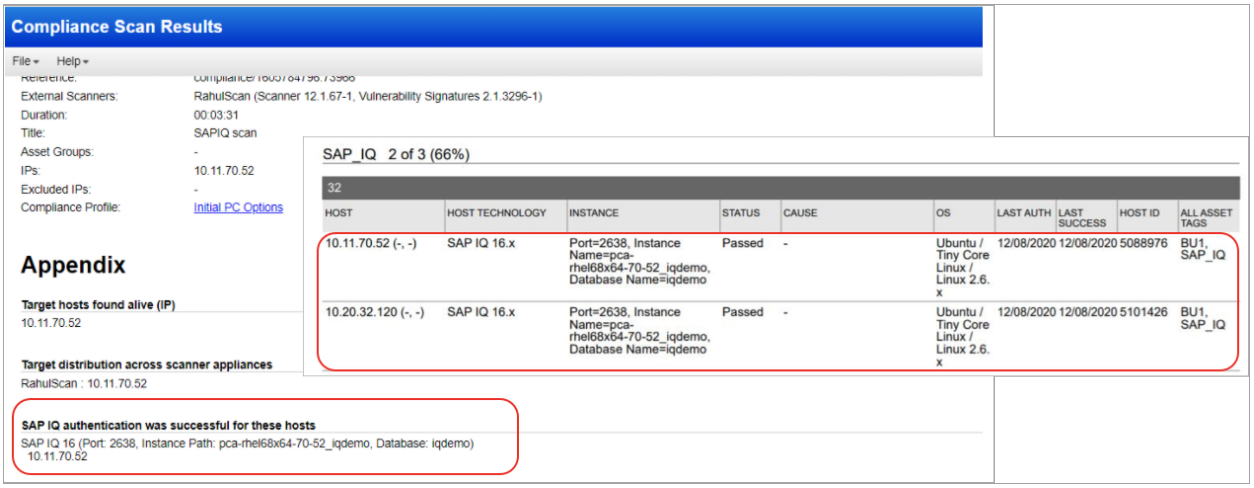


Tell us the database name to authenticate to and the port the database is running on. The installation directory name is required only for Unix based hosts.



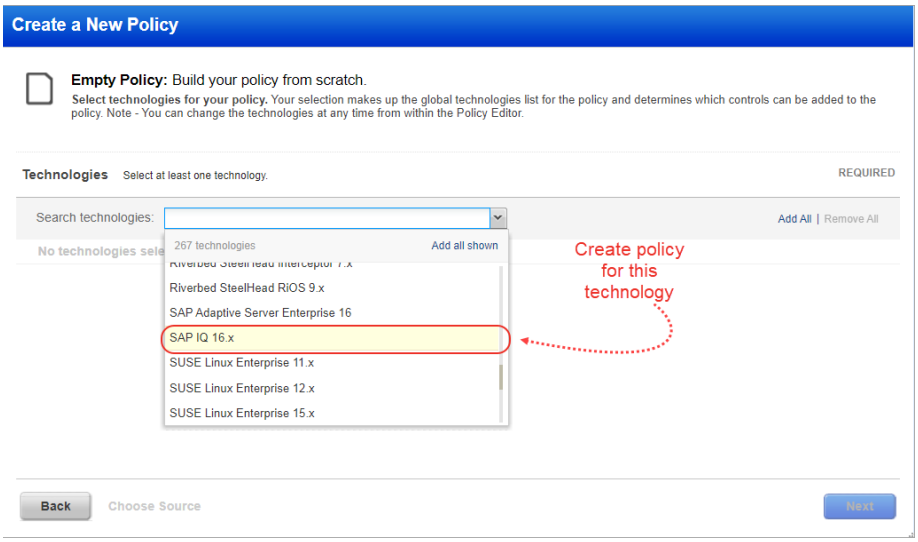
Sample Reports

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



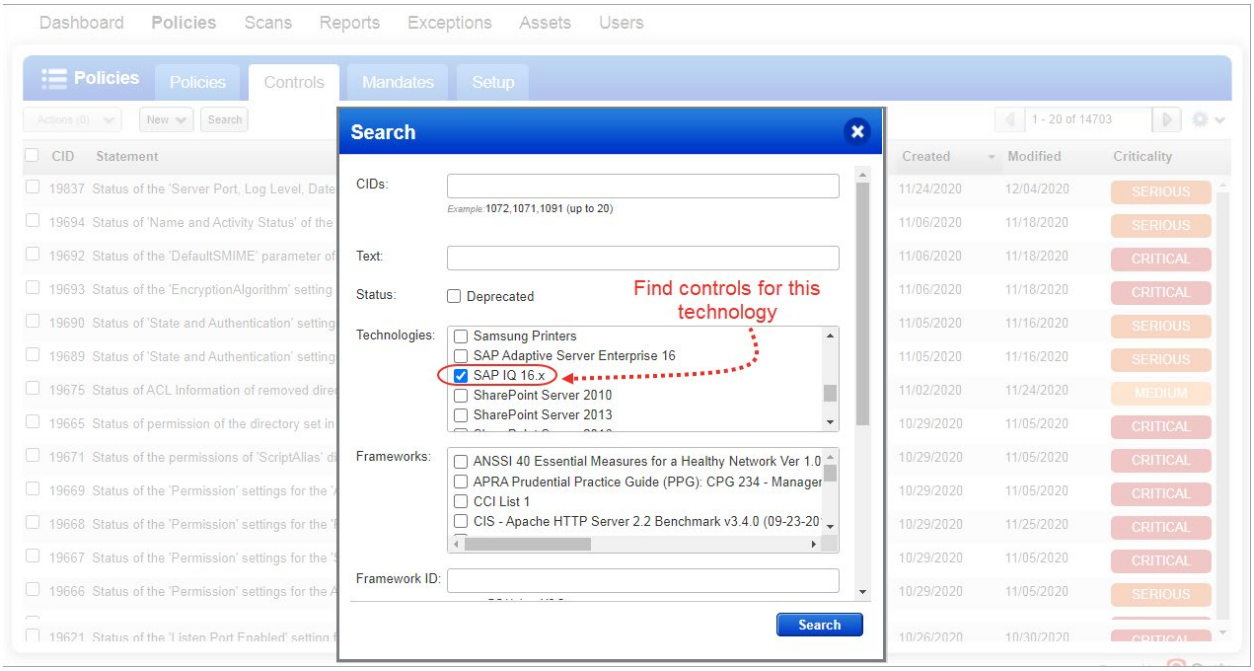
Policies and Controls

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



Search Controls

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



SAP IQ Database User-Defined Control Support

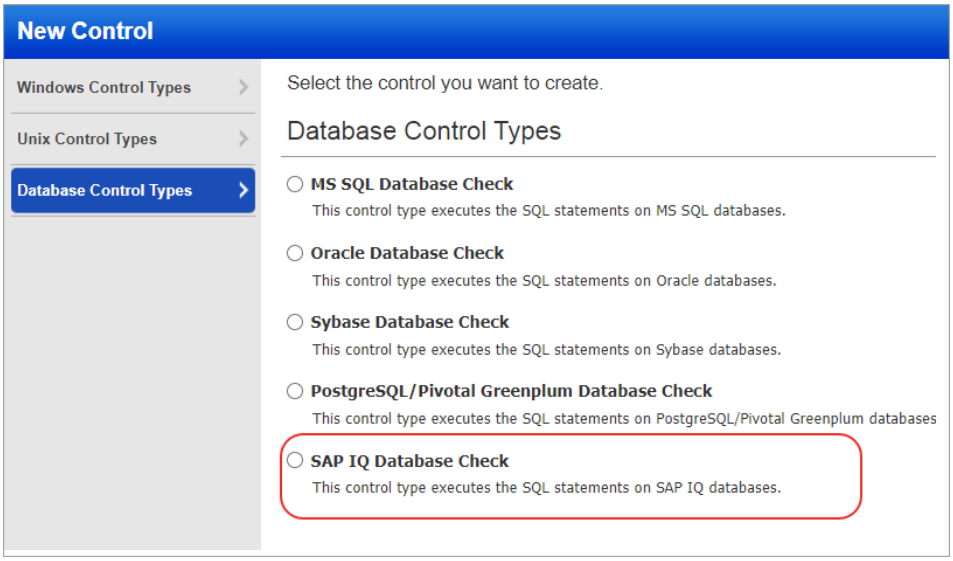
You can now use SAP IQ database user-defined controls to create custom checks by executing SQL statements on databases. These controls can then be used to generate policy reports on your databases. We're already supporting MS SQL, Oracle databases, Sybase and PostgreSQL/Pivotal Greenplum.

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

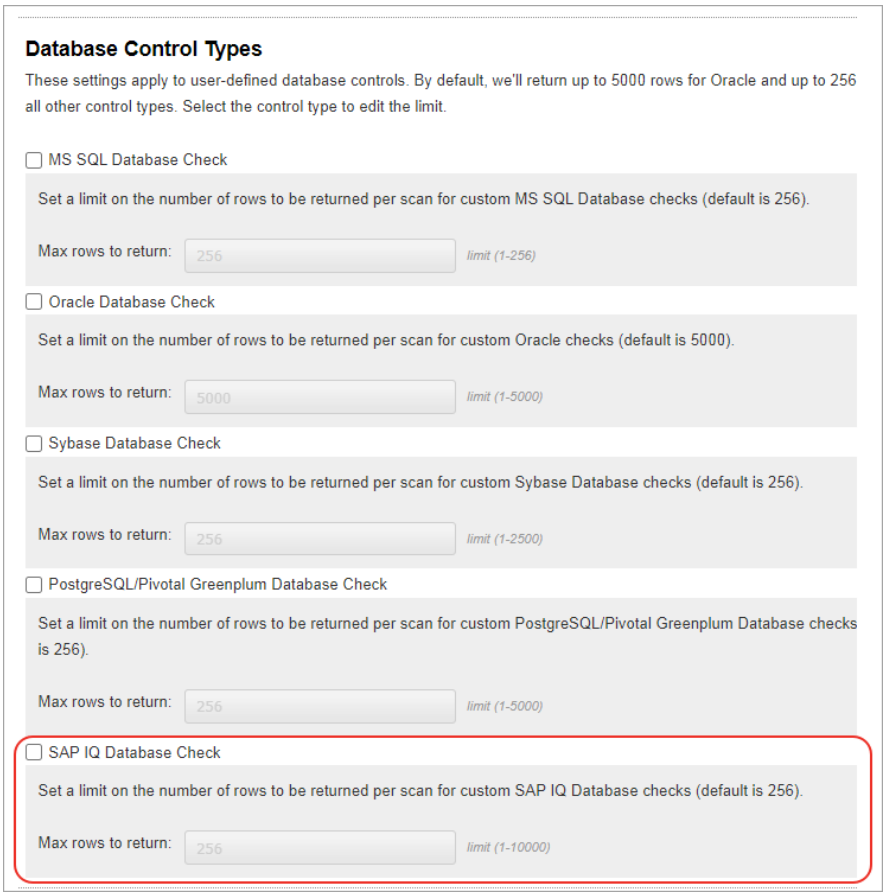
Create a new compliance policy or edit an existing policy, and add your database controls to the policy.
Tip - Make sure your policy has the database technologies selected in the control.

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.

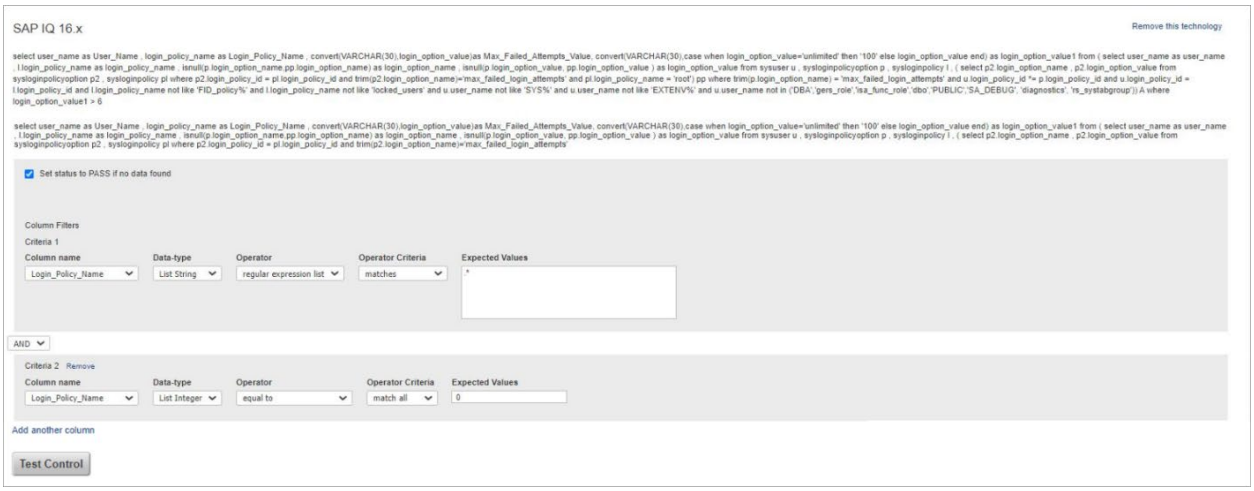


Step 4 - Return to your policy to set control criteria

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.

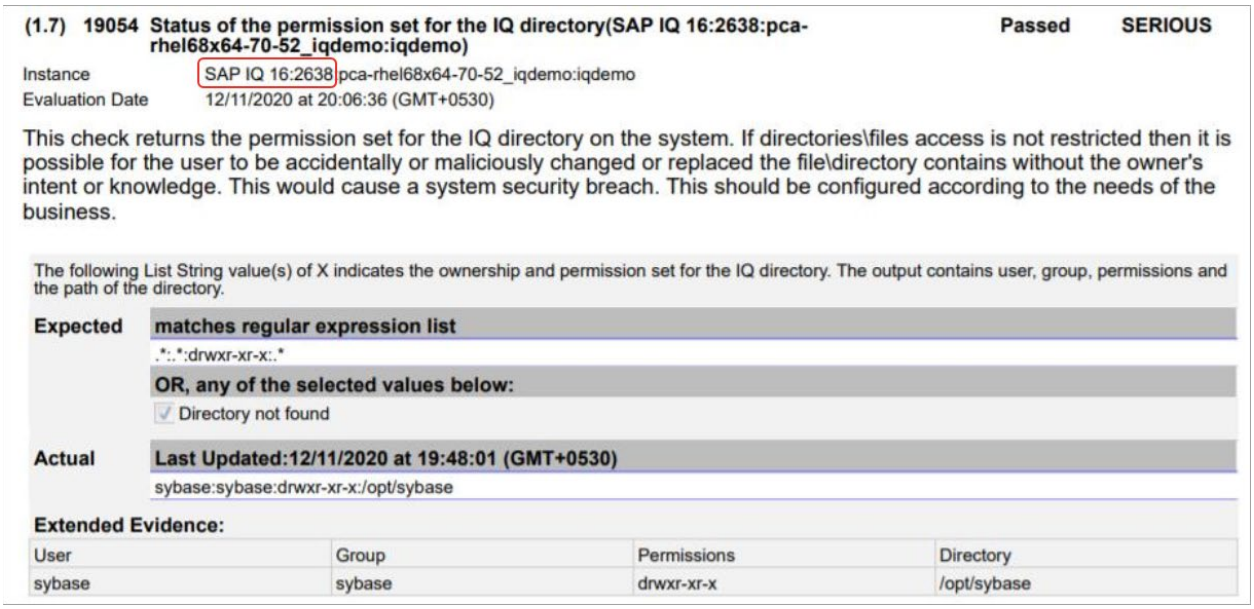
You can choose AND or OR between each criteria. If you choose AND then both criteria must match to Pass. If you choose OR then at least one criteria must match to Pass. Click **Test Control** to verify the criteria you set. Then save your policy.



Step 5 - Run a report

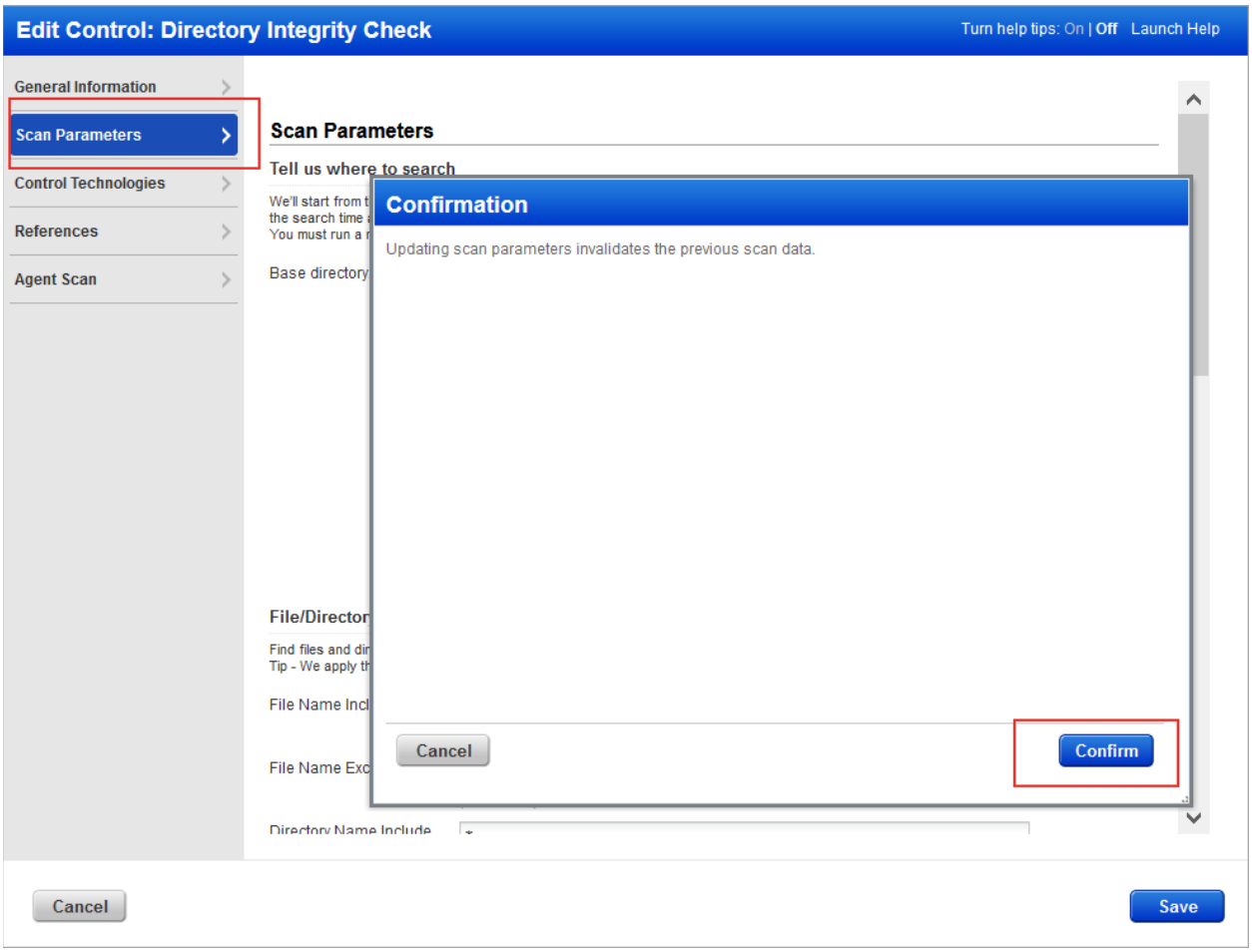
You'll see PASS or FAIL status in your report like you do with any control. If the columns returned by the most recent scan are different than previous scans then you'll want to edit your policy to modify the criteria selected for the control.

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

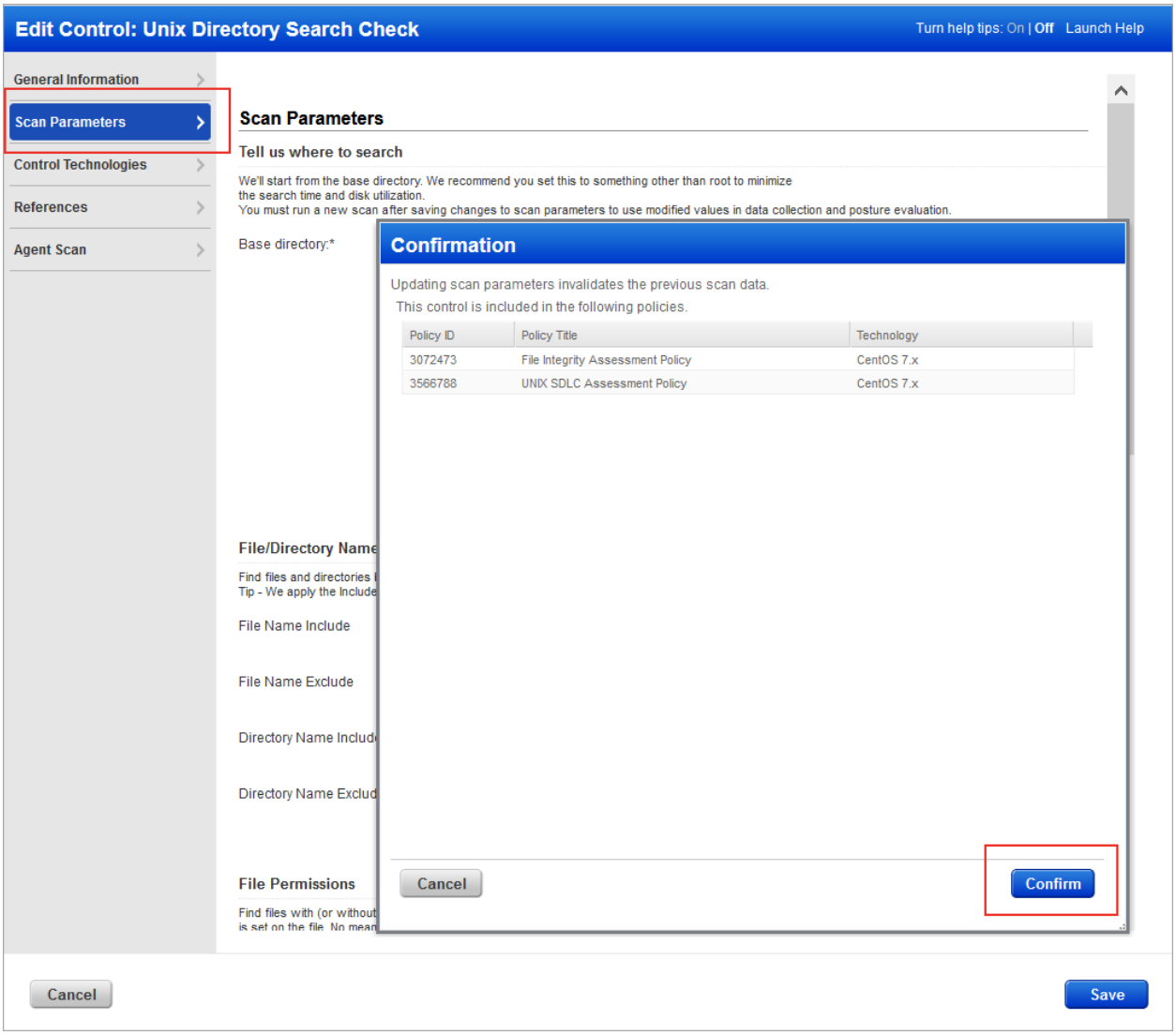


Confirmation Page When You Edit Scan Parameters in UDCs

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.

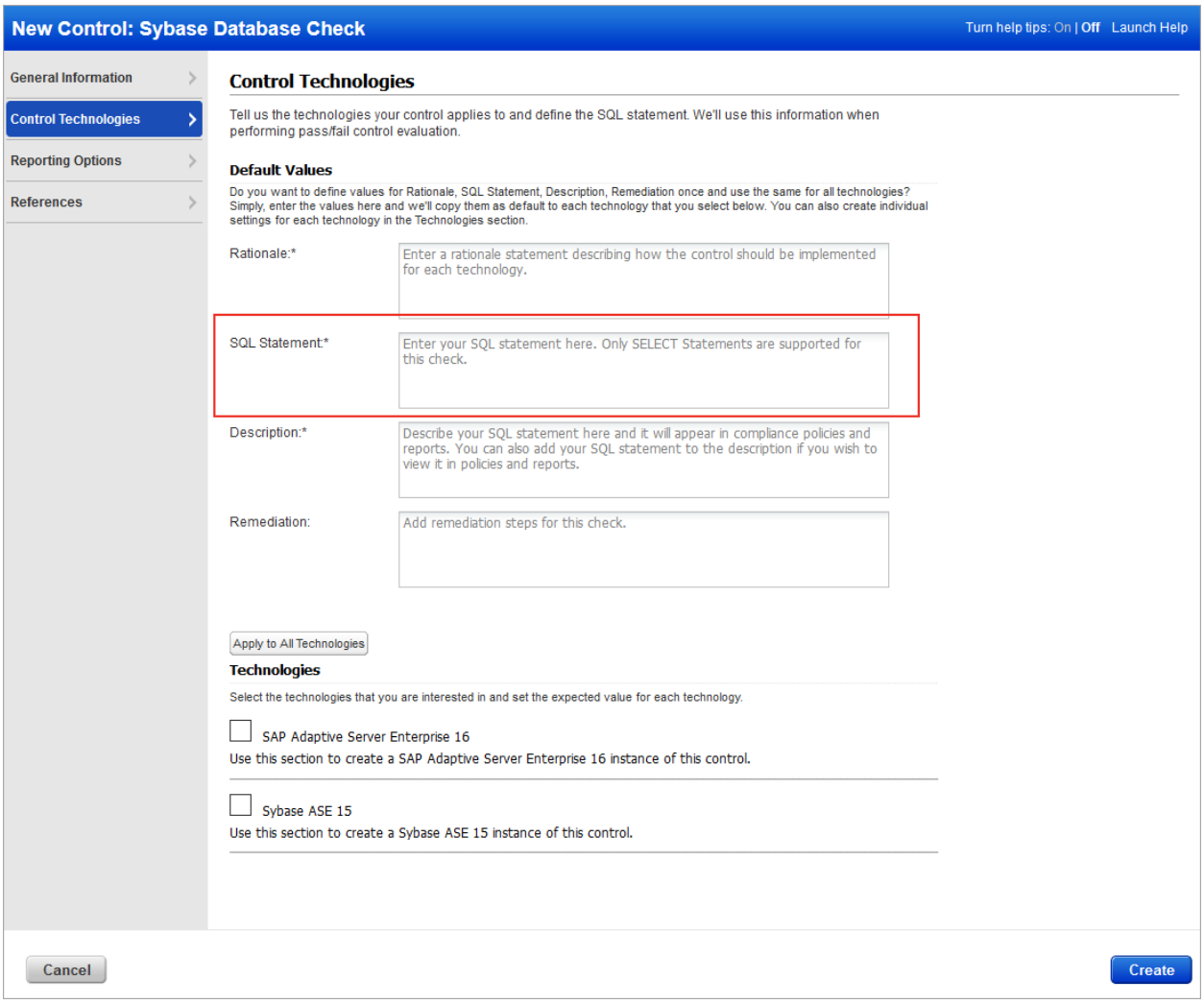


Suppose you change the expected value of a particular UDC from any of its parent policies. After you save the policy, if you go to the Controls tab and edit the scan parameters of the same UDC, which you edited earlier, on the confirmation page, you see the details of all the parent policies that contain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


Edit Control: Unix Directory Search Check
Turn help tips: On | Off Launch Help
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:*
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
File/Directory Name
File Name Include
File Name Exclude
Directory Name Includ
Directory Name Exclud
File Permissions
Cancel
Confirm
Cancel
Save

Character Limit for SQL Statement in UDCs Increased to 32000

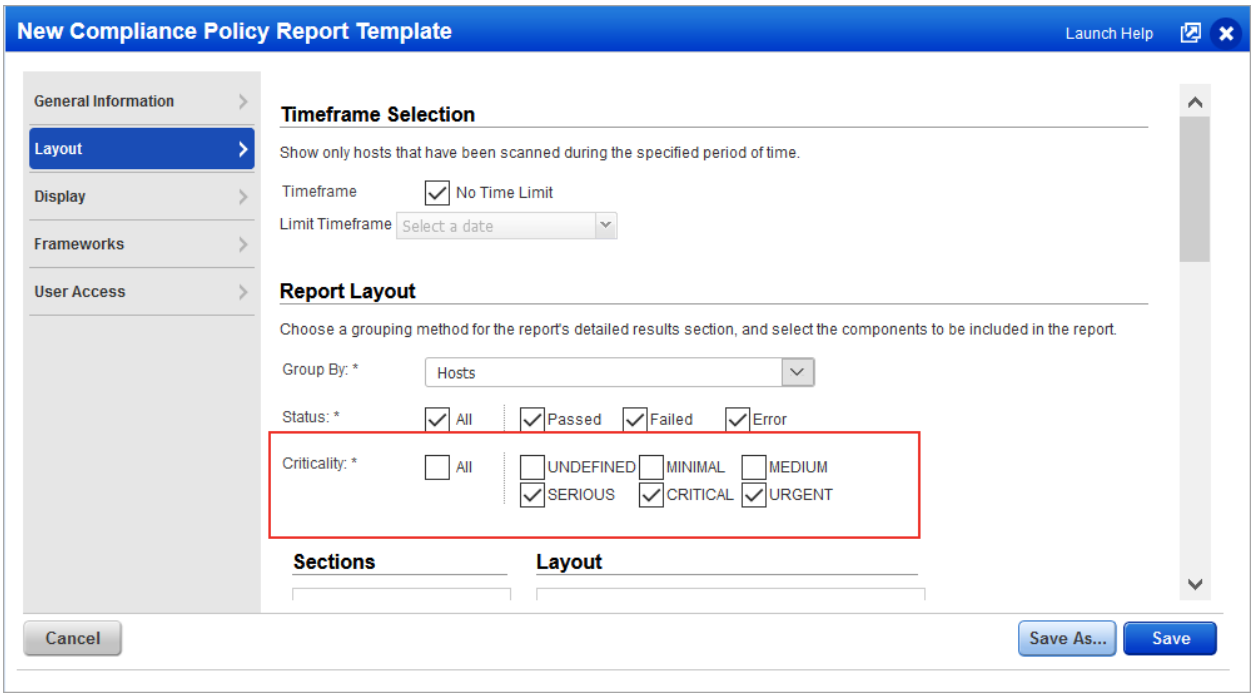
Now you can create a more complex query in the SQL Statement field on the **Control Technologies** tab as you define a database User Defined Control (UDC). Earlier, the maximum permissible limit for a SQL statement query was 4000 characters. Now, we have increased this limit to 32000 characters.



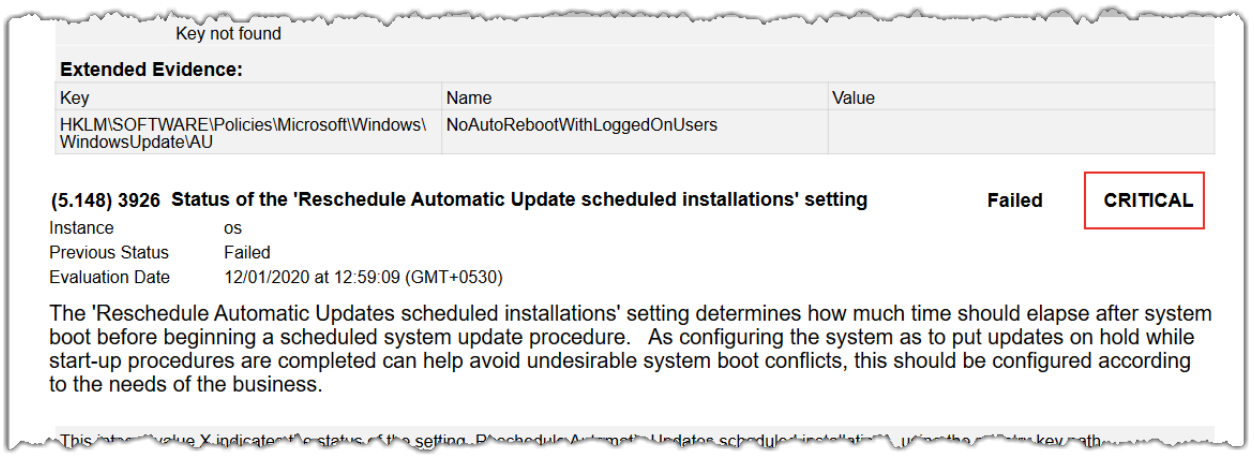
You can also edit the SQL statements in your existing UDCs to optimize your query definition.

Control Criticality Option in SCA Report Templates

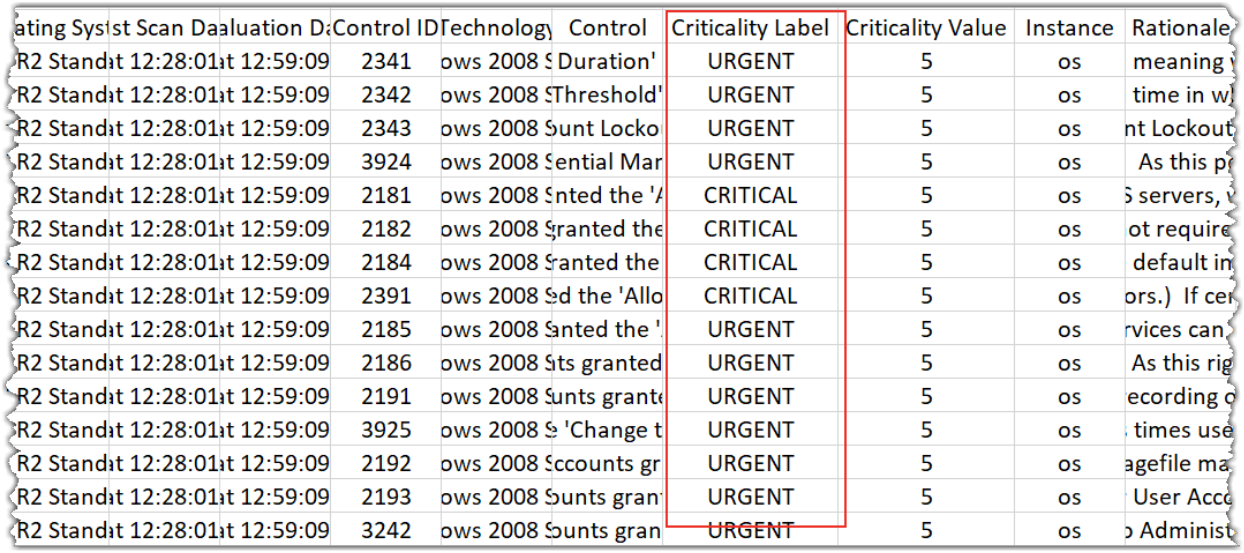
While creating an SCA Policy Report template, on the **Layout** tab of the New Compliance Policy Report Template screen, in the Report Layout section, now you have the **Criticality** option. With this change, now your SCA reports also show the criticality ratings of your controls. You can select the 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.



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.



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



ating Sys	st Scan Da	aluation D	Control ID	Technology	Control	Criticality Label	Criticality Value	Instance	Rationale
R2 Stand	t 12:28:01	t 12:59:09	2341	ows 2008 S	Duration'	URGENT	5	os	meaning
R2 Stand	t 12:28:01	t 12:59:09	2342	ows 2008 S	Threshold'	URGENT	5	os	time in w
R2 Stand	t 12:28:01	t 12:59:09	2343	ows 2008 S	unt Locko	URGENT	5	os	nt Lockout
R2 Stand	t 12:28:01	t 12:59:09	3924	ows 2008 S	ential Mar	URGENT	5	os	As this p
R2 Stand	t 12:28:01	t 12:59:09	2181	ows 2008 S	nted the 'A	CRITICAL	5	os	S servers,
R2 Stand	t 12:28:01	t 12:59:09	2182	ows 2008 S	ranted the	CRITICAL	5	os	ot require
R2 Stand	t 12:28:01	t 12:59:09	2184	ows 2008 S	anted the	CRITICAL	5	os	default in
R2 Stand	t 12:28:01	t 12:59:09	2391	ows 2008 S	d the 'Allo	CRITICAL	5	os	ors.) If ce
R2 Stand	t 12:28:01	t 12:59:09	2185	ows 2008 S	anted the '	URGENT	5	os	rvices can
R2 Stand	t 12:28:01	t 12:59:09	2186	ows 2008 S	ts granted	URGENT	5	os	As this rig
R2 Stand	t 12:28:01	t 12:59:09	2191	ows 2008 S	unts grante	URGENT	5	os	ecording c
R2 Stand	t 12:28:01	t 12:59:09	3925	ows 2008 S	'Change t	URGENT	5	os	times use
R2 Stand	t 12:28:01	t 12:59:09	2192	ows 2008 S	ccounts gr	URGENT	5	os	agefile ma
R2 Stand	t 12:28:01	t 12:59:09	2193	ows 2008 S	unts gran	URGENT	5	os	User Acc
R2 Stand	t 12:28:01	t 12:59:09	3242	ows 2008 S	unts gran	URGENT	5	os	Administ

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.

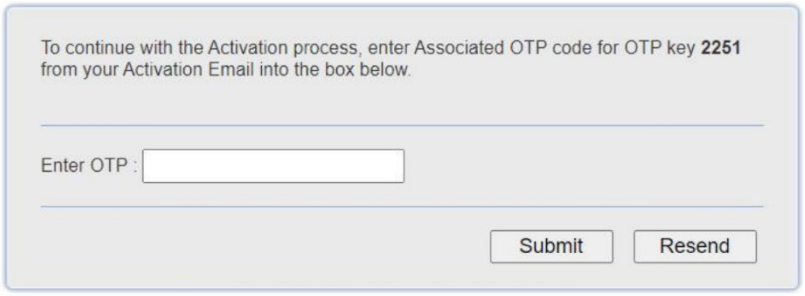
A Manager can change the password for any user in the subscription. A Unit Manager can do this for users in their business unit.

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:



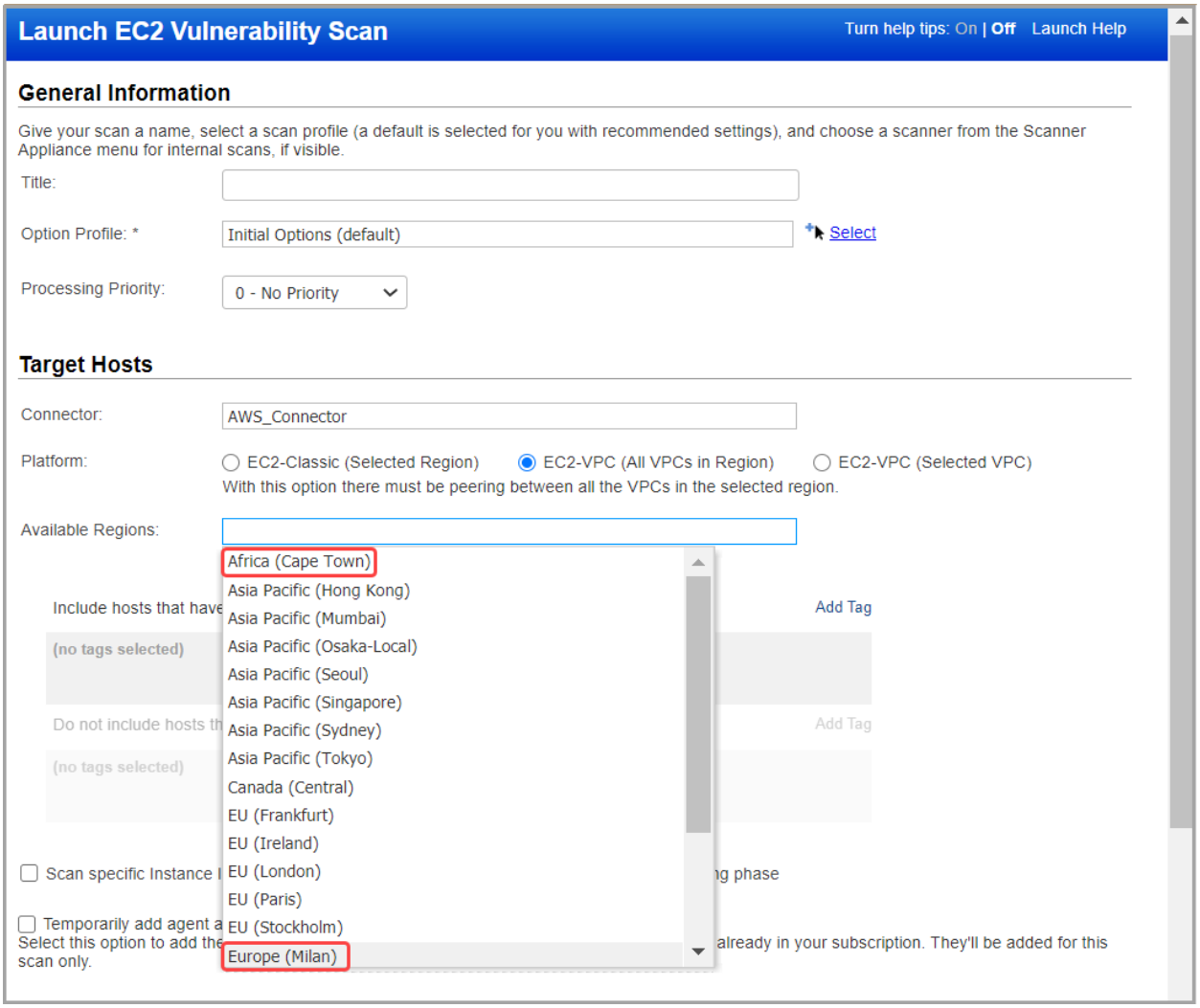
Provide OTP code corresponding to the OTP key in the **Enter OTP** textbox and click **Submit**. This shows **Welcome to Qualys** screen with login information.

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).

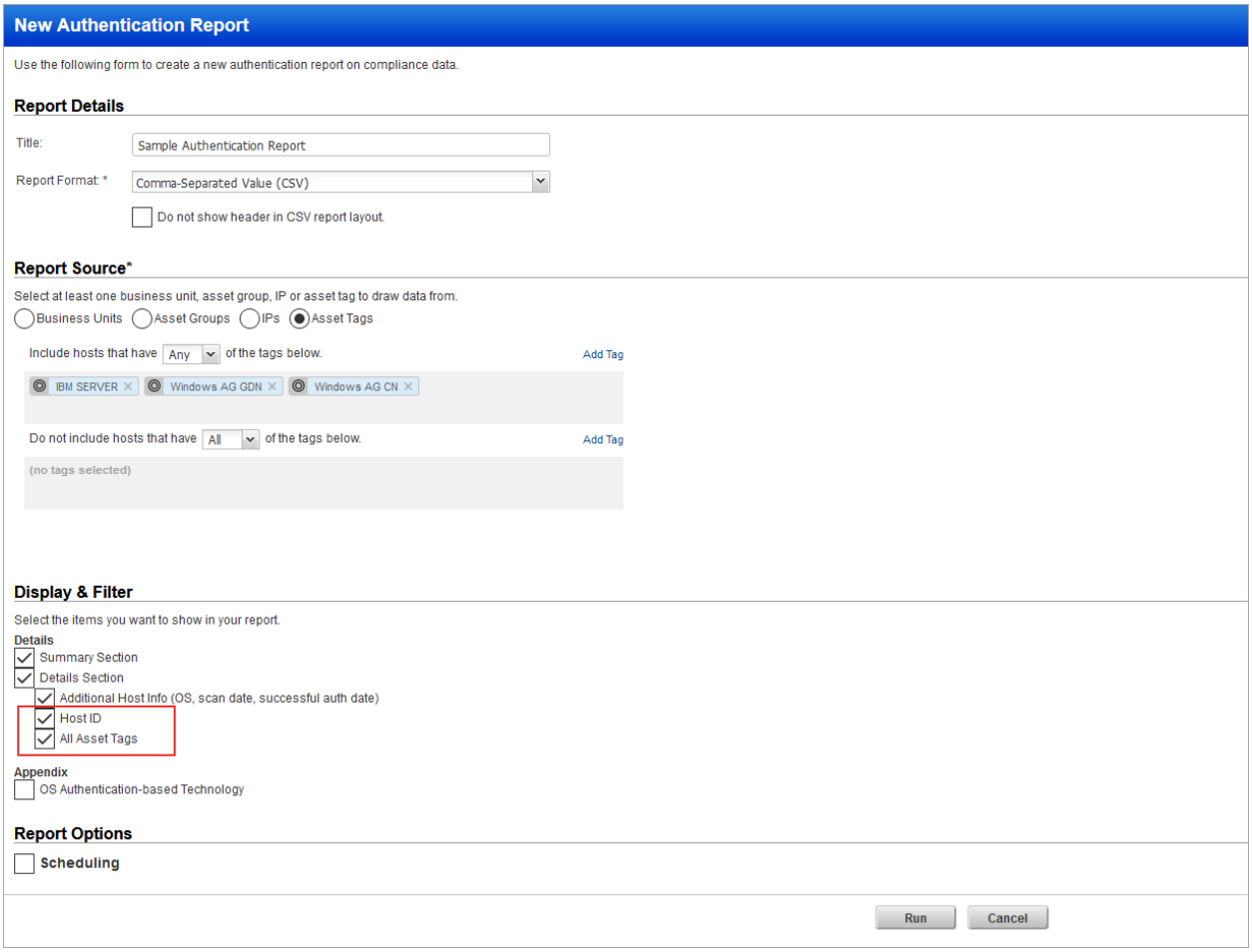
Sample – Launch EC2 Vulnerability Scan

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



More Details in Authentication Reports: Host ID and Asset Tags

Now you have the option to include additional details in authentication reports. When you generate an authentication report from the Vulnerability Management or the Policy Compliance UI, now you see new options for including Host IDs and All Asset Tags in the Display & Filter section in the Report Details form. These are optional details that are not included by default. The details you pick will appear in all the supported report formats, including XML and CSV.



Here's the sample CSV report generated based on the options selected in the previous screenshot. The enhancements in the report format are highlighted for your reference:

1	Sample Authenti	12/14/2020 at 16:18:04 (GMT-08)																
2	RMTEC	Pimple		California	None	California	123456											
3	Joe Spencer	Manager																
4	SUMMARY																	
5	Asset Tags	Passed Au	Insufficier	Failed Aut	Not Attempted Aut	Not Instal	Total Autl	Passed Pe	Failed Per	Not Attempted Percentage								
6	Included(any):	87	1	6	1	0	94	92	6	1								
7	RESULTS																	
8	Asset Tags	Technolo	Host Tech	Instance	Host IP	DNS Host	NetBIOS H	Tracking	Network	Status	Failure	OS	Last Auth	Last Suc	Host Id	All Asset Tags		
9	Windows AG GD	Windows	Windows	Server 201	10.20.32.154	mlw2012r	MLW2012	IP	Global De	Passed	'-	Windows	12/8/2020	########	4427600	Internet Facing Assets, OCA, Windows AG GDN		
10	Windows AG CN	Windows	Windows	Server 201	10.20.32.154	mlw2012r	MLW2012	IP	Custom N	Passed	'-	Windows	10/9/2020	########	3931914	Internet Facing Assets, OCACOMW, Windows AG CN		
11	IBM SERVER	Windows	Windows	2016 Serve	10.115.120.70	win-fmei8	WIN-FMEI	IP	Global De	Passed	'-	Windows	8/7/2020	########	3917494	IBM SERVER		
12	IBM SERVER	Apache W	'-	Apache W	10.115.120.70	win-fmei8	WIN-FMEI	IP	Global De	Passed*	Apach	Windows	8/7/2020	'-	3917494	IBM SERVER		
13	IBM SERVER	Apache W	IBM HTTP	IHS 8:1:C:\	10.115.120.70	win-fmei8	WIN-FMEI	IP	Global De	Passed	'-	Windows	8/7/2020	########	3917494	IBM SERVER		
14	Internet Facing A	IBM/zOS	IBM/zOS	Security S	33.99.99.33	ibm/zos	NB	OCA	Global De	Passed	'-	Windows	8/7/2020	########	3917497	Internet Facing Assets		

What has changed?

- 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.