Qualys Cloud Platform (VM, PC) v10.x

Release Notes

Version 10.11

June 2, 2021

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

Qualys Cloud Platform

New Authentication Support for Network SSH

UI Change: IP Addresses/Ranges changed to IPv4 Addresses/Ranges

Linux PowerPC Support for Agent Scans

Qualys Vulnerability Management (VM)

Agent Correlation Identifier is now GA!

Qualys Policy Compliance (PC/SCAP/SCA)

New Authentication Support for Neo4j

Enhanced Support for Database Technology Data Collection Using Host OS Authentication Records in Compliance Option Profile

Control Remediation Information Included in More Workflows

Qualys 10.11 brings you more improvements and updates! **Learn more**

Qualys Cloud Platform

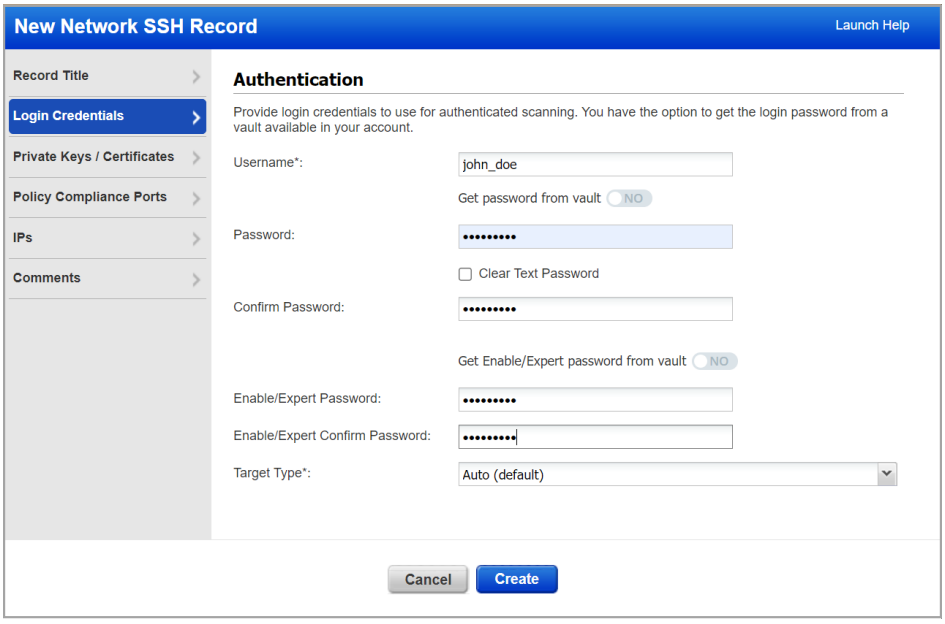
New Authentication Support for Network SSH

Network SSH authentication is supported for vulnerability and compliance scans. With this release, we've has extended functionality to authenticate network devices (such as Cisco and Checkpoint Firewall) using SSH2 authentication format. Previously only Unix devices were supported to use SSH2 authentication format.

Network SSH authentication record can be used in place of the Cisco and Checkpoint Firewall authentication records. This new authentication record has all the same functionality as the previous Cisco and Checkpoint Firewall records along with newly added support for Target Type field similar to Unix authentication record.

What are the steps?

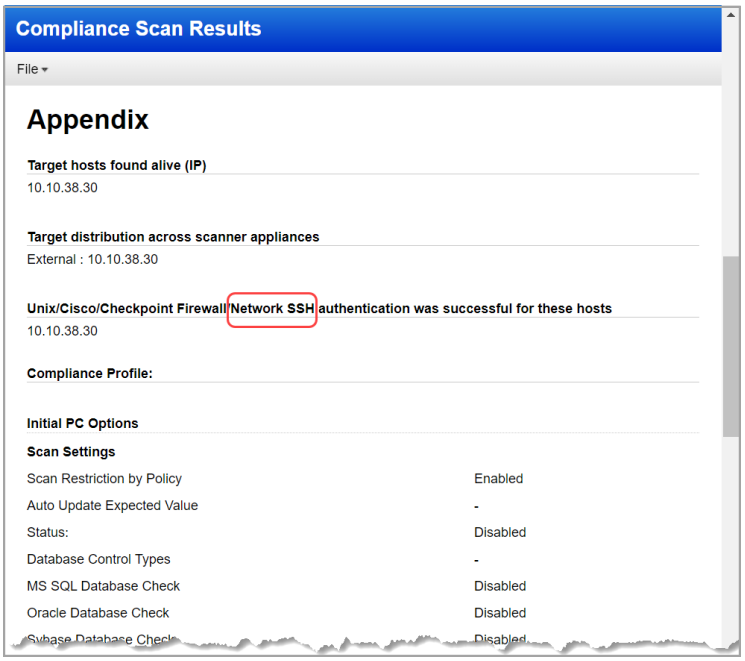
Go to **Scans** > **Authentication** > **New** > **Network Security...** > **Network SSH**.



Good to know

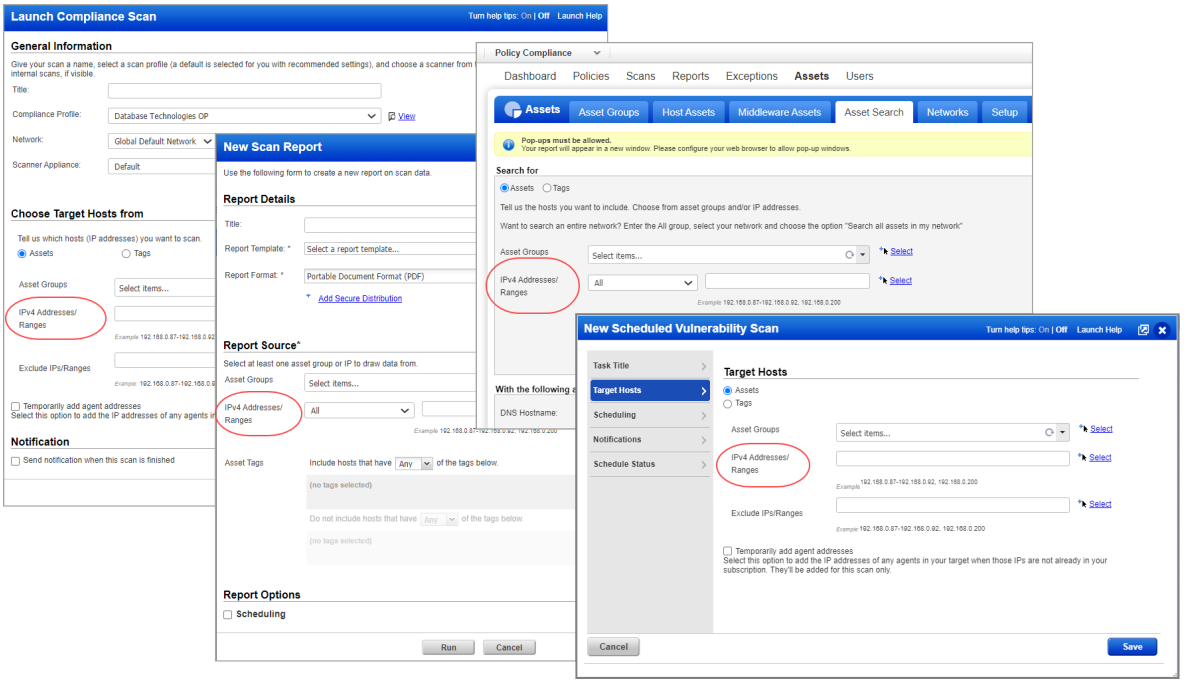
- You have the option to get the login password and enable/expert password from a vault.
- Provide a target type while creating or updating the Network SSH (SSH2) authentication record. With this field, you can define the non-shell based target types in the SSH2 authentication record. The target type is set to "Auto (default)" in this case. Newly supported target types will be added to the Target Type menu.
- You can use multiple private keys and/or certificates for authentication. Any combination of private keys (RSA, DSA, ECDSA, ED25519) and certificates (OpenSSH, X.509). Private key authentication is supported for SSH2 only. All of the private keys can either be unencrypted or encrypted with a passphrase.
- An IP added to the Network SSH authentication record cannot added in Unix, Cisco or Checkpoint authentication records.

Sample Compliance Scan Results



UI Change: IP Addresses/Ranges changed to IPv4 Addresses/Ranges

Throughout the Qualys UI (for VM, PC, SCA) you'll notice that we changed the field label "IP Addresses/Ranges" to "IPv4 Addresses/Ranges". You'll see this change in workflows where you need to select target IP addresses like when launching or scheduling scans, running reports, and more. This label change was made to provide better clarity on the IP address format, and make it easier to represent IPv6 addresses at a later date. Here are some examples:



Linux PowerPC Support for Agent Scans

We have supported vulnerability and compliance scans using Qualys Cloud Agent deployed on Linux platform with PowerPC architecture.

For supported platforms and agent versions, refer Qualys Cloud Agent Getting Started Guide.

Qualys Vulnerability Management (VM)

Agent Correlation Identifier is now GA!

With this release, the Agent Correlation Identifier feature is generally available (GA). We have removed 'beta' text from the UI. Refer to the Cloud Platform 10.7 UI Release Notes for feature details.

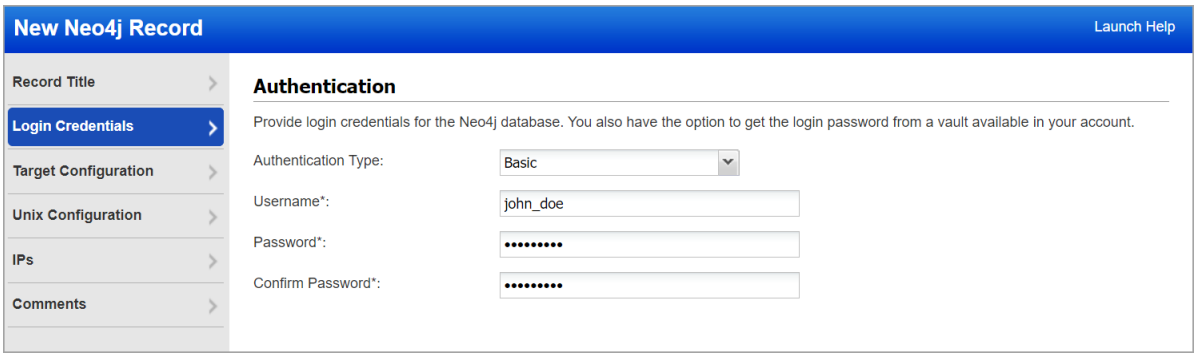
Qualys Policy Compliance (PC/SCAP/SCA)

New Authentication Support for Neo4j

We now support Neo4j authentication for compliance scans using Qualys apps PC, SCA. Simply create a Neo4j authentication record with details about your credentials to authenticate to a Neo4j database instance running on a host, and scan it for compliance. Currently, version supported is Neo4j 3.x.

What are the steps?

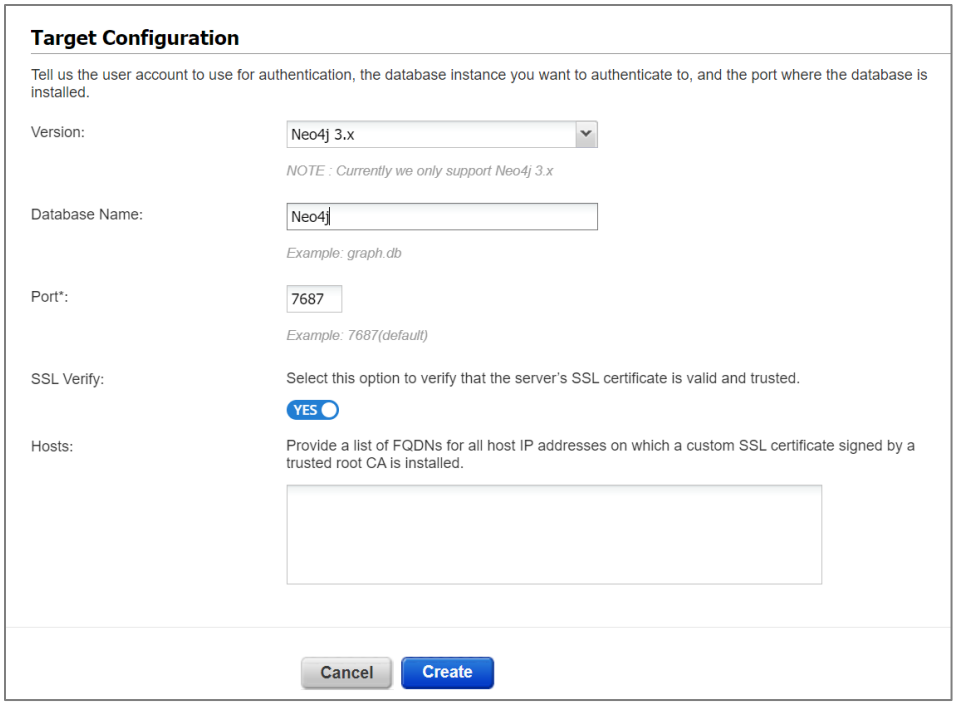
Go to **Scans** > **Authentication** > **New** > **Databases** > **Neo4j**.



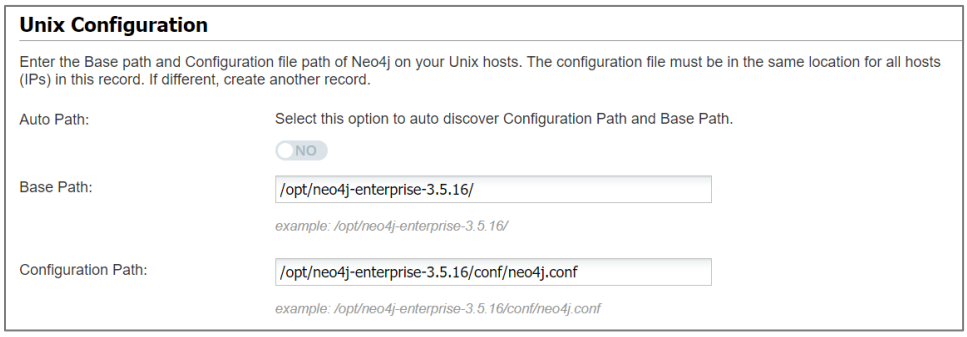
Your Neo4j authentication record

Each Neo4j 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 password vault. Supported vaults are: ARCON PAM Vault, Azure Key, BeyondTrust PBPS, CyberArk AIM, CyberArk PIM Suite, HashiCorp, Thycotic Secret Server.

Tell us the user account to use for authentication, the database instance you want to authenticate to, and the port where the database is installed.



Enter the Base path and Configuration file path of Neo4j on your Unix hosts. The configuration file must be in the same location for all hosts (IPs) in this record. If different, you must create another record.



Enhanced Support for Database Technology Data Collection Using Host OS Authentication Records in Compliance Option Profile

In Policy Compliance, on the Instance Data Collection tab of a compliance option profile, you have an option to enable database instance data collection by using the underlying OS authentication records without creating an authentication record for the database technology. You can enable this setting while creating or editing an option profile. In this release, we have extended this support. We now support the OS authentication record-based data collection for the following database technologies as well:

Database	Supported Versions	Which OS Record to Use?
IBM DB2	IBM DB2 9.x IBM DB2 10.x IBM DB2 11.x	UNIX (with Sudo as root delegation) OR Windows

IBM Informix	IBM Informix 11.x IBM Informix 12.x	UNIX (with Sudo as root delegation)
Pivotal Greenplum	Pivotal Greenplum 5.x Pivotal Greenplum 6.x	UNIX (with Sudo as root delegation)
PostgreSQL	PostgreSQL 9.x PostgreSQL 10.x PostgreSQL11.x PostgreSQL 12.x	UNIX (with Sudo as root delegation)
Sybase/SAP ASE	Sybase ASE 15.x SAP Adaptive Server Enterprise 16.x	UNIX (with Sudo as root delegation)

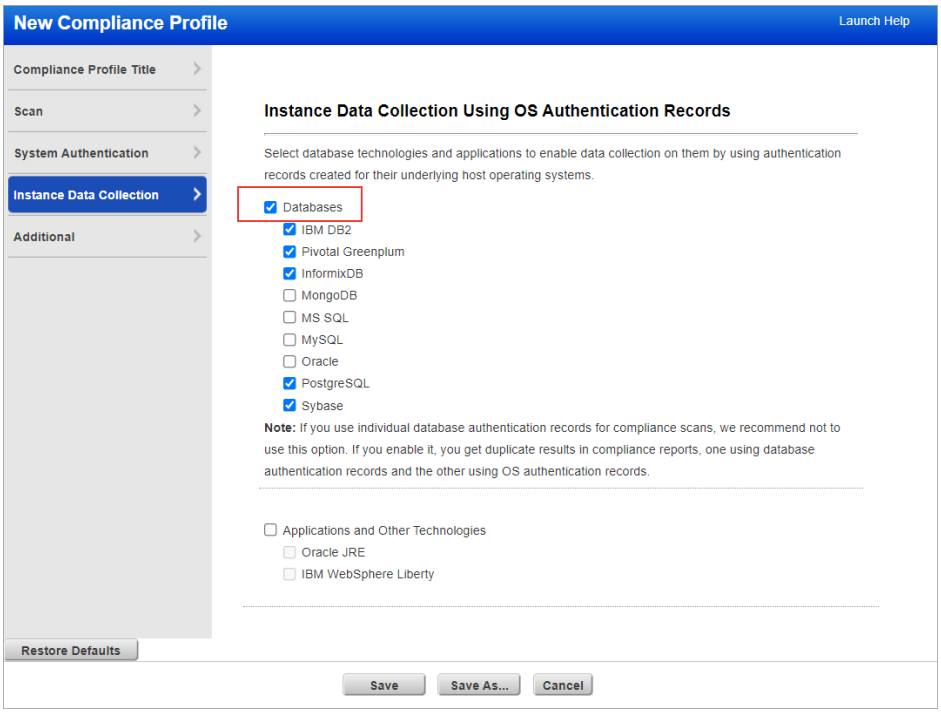
For data collection on IBM DB2 instances, you can use your UNIX (with Sudo as root delegation) or Windows authentication record depending on the host operating system.

For data collection on all other technologies listed earlier, you need a UNIX authentication record with Sudo as root delegation.

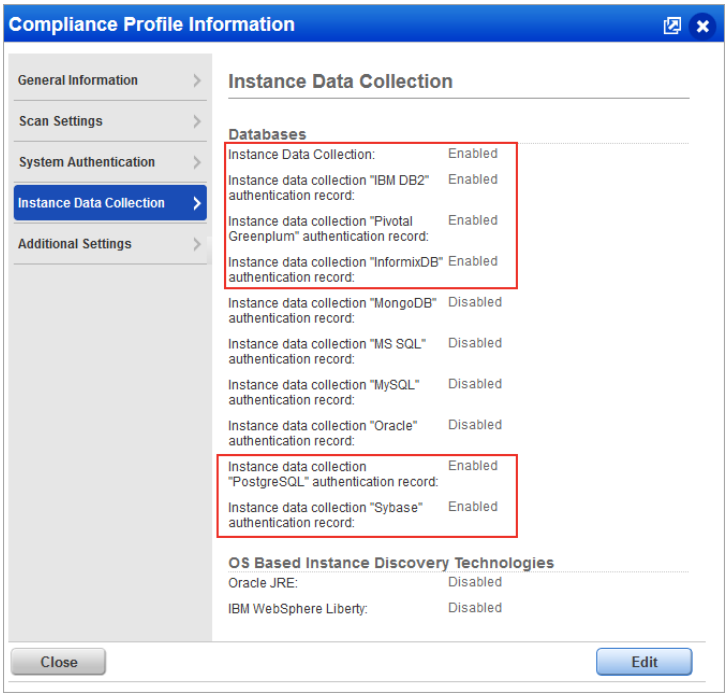
Enabling OS-Auth-based Data Collection for Database Instances

To enable database instance data collection by using underlying OS authentication record, you must select the **Databases** checkbox on the **Instance Data Collection** tab. Only then can you select the database technologies from the available options.

Note: The **Additional** tab now appears below the **Instance Data Collection** tab.

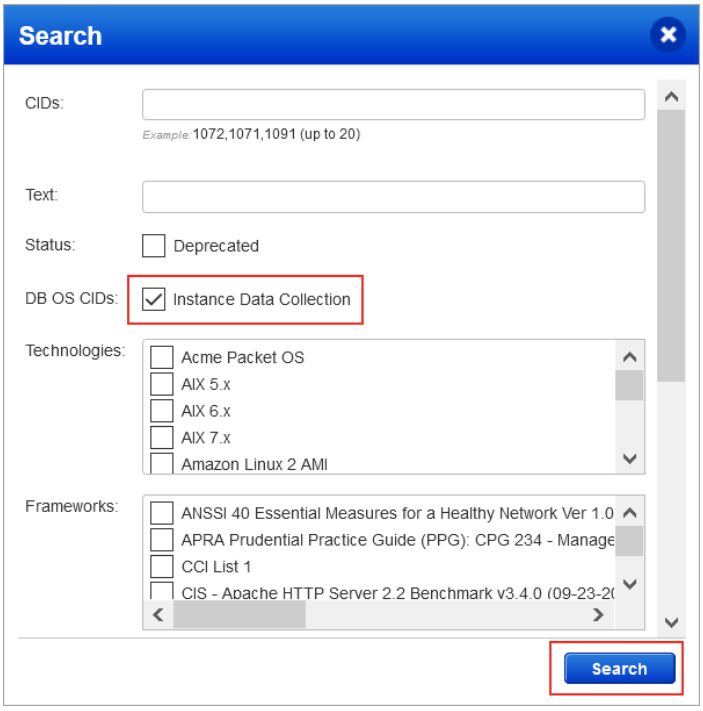


After you save your changes, the settings in the option profile are used in the next compliance scan. You can always go back and review your compliance profile information and edit it if required.



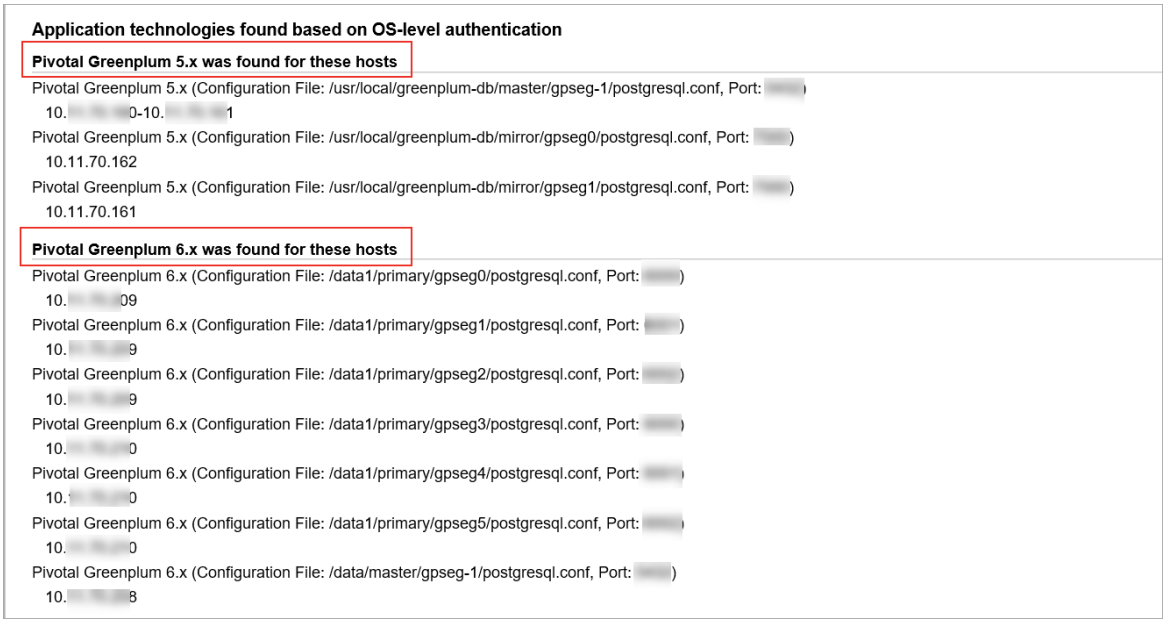
Searching for OS-Dependent Database Controls

Only system-defined OS-dependent database controls are used in data collection and evaluation of database technology instances. To see the list of OS-dependent database controls (SDCs only), go to **Policies** > **Controls** > **Search**, in the Search dialog box, select the **Instance Data Collection** box for DB OS CIDs, and click **Search**.



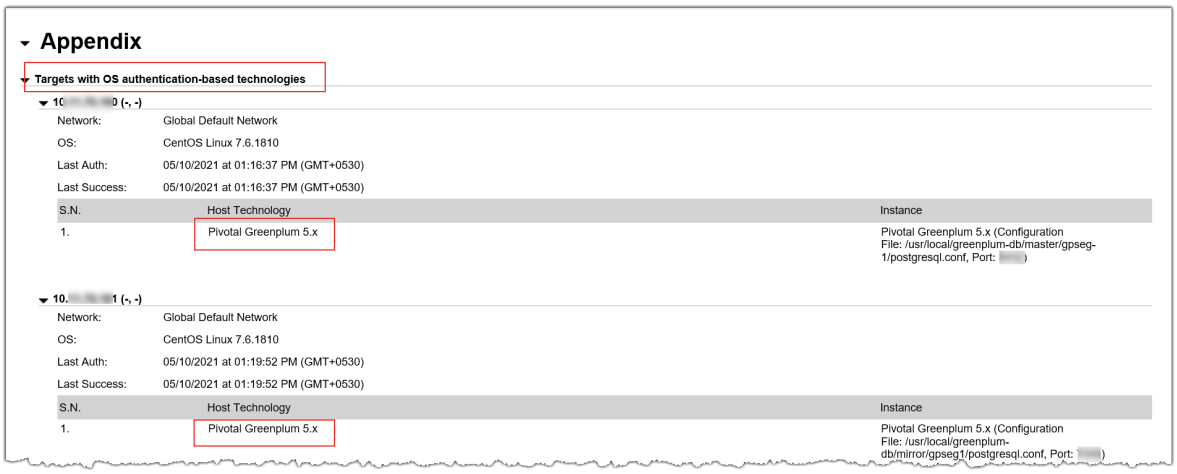
Sample Compliance Scan Result

Here's a sample compliance scan result where, in the **Application technologies found based on OS-level authentication** section, you can see the hosts on which database instances are identified.



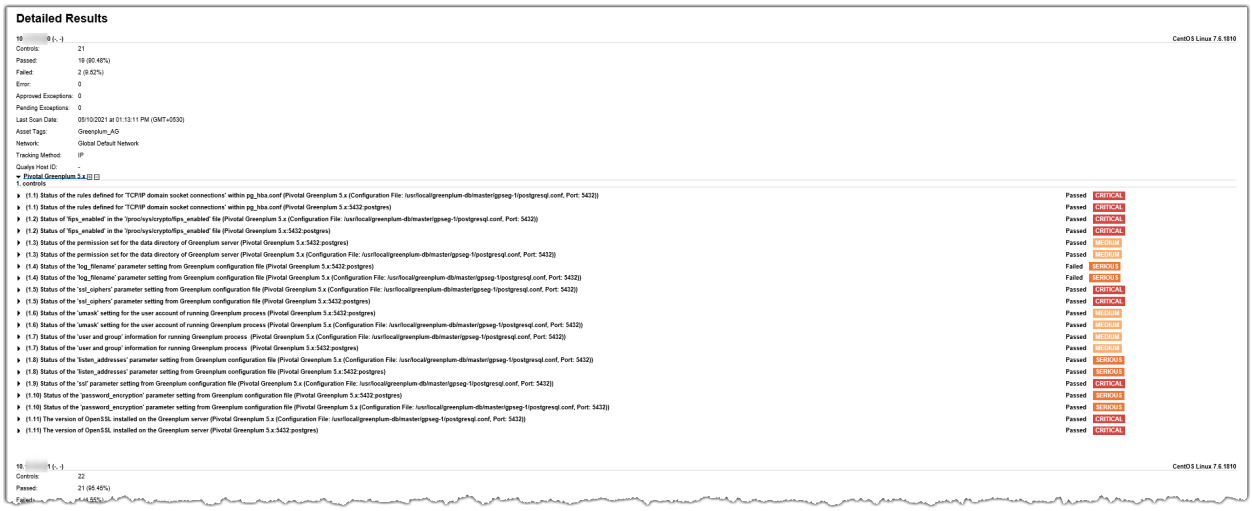
Sample Authentication Report

Here's a sample authentication report where you can check the authentication status of the database instances that are scanned by using the underlying OS authentication records.



Sample Policy Report

And here's a sample policy report where you can check the detailed results for each database instance that is scanned against a policy.



Control Remediation Information Included in More Workflows

In the Qualys 10.10 release we introduced the ability to customize remediation information for controls/technologies from the Policy Editor UI and we included remediation values in XML output for Policy Export. We're expanding on this feature in the current release to include the remediation value in more workflows. Now when you copy controls from another policy or copy control settings when adding a new technology to your policy, we'll include the remediation information for each control/technology. Also, when you view a policy or export a policy to CSV format, we'll show the remediation information.

Remediation Included When You Copy Control Settings

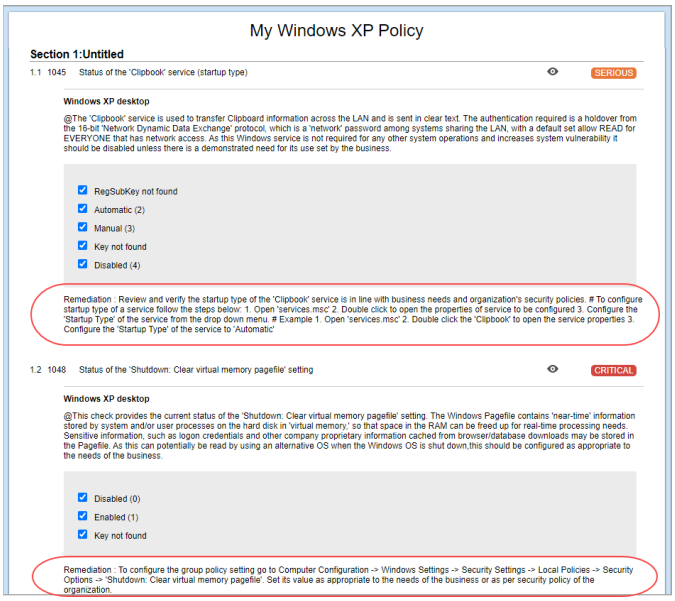
When you use the following existing workflows to copy controls to your policy or copy control settings for new technologies, remediation values will now be included.

- Copy controls from another policy in your account or from a policy in the Policy Library. In the Policy Editor, click the **Copy Controls** link on the Overview page or click the **Copy Controls** button from within a section. Choose the policy you're copying controls from, and select the controls you're interested in. We'll add the controls and copy the control settings, including remediation.

- Add one or more technologies to your policy and copy control settings from another technology in the policy, from another policy in your account or from a policy in the Policy Library. In the Policy Editor, click the **Edit** link under Assigned Technologies on the Overview page, or click **Add Technology** from within Control Details. Select the technologies you want to add and then click **Copy Control Settings**. Choose the technology or policy you're copying from. We'll add the selected technologies to your policy and copy the control settings, including remediation.

Policy View Shows Remediation

You'll now see the remediation value for each control/technology when you view a policy. Go to **Policies** > **Policies** and choose **View** from the Quick Actions menu.



Policy Export To CSV Shows Remediation

When you export policies to CSV format from the UI, the CSV output will now include a **Remediation** column under Control Information with remediation values. Go to **Policies** > **Policies** and choose **Export** from the Quick Actions menu. Service-Defined Controls are always included in the policy export. Check the option "Include UDCs and QCCs" to also include User-Defined Controls and Qualys Custom Controls. Then click **Export** again.

In the CSV output:

For Service-Defined Controls (SDCs), if the remediation value for the control/technology was customized in the policy, then you'll see the custom value in the Remediation column. If the remediation value for the control/technology was not customized in the policy, meaning the default value is used, then the field appears blank.

For User-Defined Controls (UDCs), you'll see the custom remediation value defined for each control/technology. The remediation value for a UDC can be defined in the control or in the policy. If no remediation value is defined for the control, then the field appears blank.

In this sample, you'll see the new **Remediation** column with sample values for SDCs and UDCs.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Policy Information														
2	Title	Cover Page													
3	My Policy														
4															
5	Technologies (3)														
6	ID	Name													
7	43	CentOS 6.x													
8	53	Windows 2012 Server													
9	80	CentOS 7.x													
10															
11	Control Information														
12	Section Nc	Section He	Reference	CID	UDC_ID	Statement	Descriptio	Technolog	Technology Name	Criticality Lal	Criticality '	Evaluatior	Is Control	Remediation	
13	1	Untitled		1072	N/A	Status of t	Among th	43	CentOS 6.x	URGENT	5	The	0	user's custom value in policy	
14	1	Untitled		1072	N/A	Status of t	Among th	53	Windows 2012 Server	URGENT	5	The	0		
15	1	Untitled		101569	298f36d5-	File/Direct	.*	43	CentOS 6.x	MINIMUM	1	des	0	user's custom value in policy	
16	1	Untitled		101554	b7849397	My-UDC	rd	80	CentOS 7.x	UNDEFINED	0	my value	0	user's custom value in control	
17															

My_Policy_20210511

Issues Addressed

- Fixed an issue where you could not add more than 2048 characters when adding custom ports to the Blocked resources list of the option profile.
- Fixed an issue where new IPs were skipped when trying to add a list of IPs that contained previously scanned IPs. Now, when you add a list of IPs, the already existing IPs are skipped and the new IPs get added. This has been fixed for adding IPs through both, UI and API.
- We fixed an issue where assets that did not have a host OS instance were not being listed in asset search while creating a policy from previously scanned hosts. Now, such assets are populated in the search.
- We fixed an issue where an error is shown when the user tries to launch a scheduled Mandate Based Report using the “Launch Now” option from the Quick Actions menu.
- Fixed an issue where the root delegation password did not accept the '<' and '>' characters under Unix record. These characters are now accepted in the root delegation password.
- 3rd-party vulnerabilities provided by iDefense Threat Intelligence were exposed to some users who had not opted for this service in their subscription leading to a discrepancy. We have now fixed the issue so that these vulnerabilities are displayed only to users who have opted for it in their subscription.
- We fixed an issue where the tags selection was disabled for users after editing the existing Windows authentication record and adding tags to it.
- We fixed an issue where due to a recent change in the scan processing, a condition was not mapped correctly. This issue caused the cancel scan operation to fail.
- Fixed an issue where the value for DNS Hostname was populated as the EC2 Instance ID for EC2 hosts. With the fix, DNS Hostname is getting updated correctly.
- Fixed an issue where IPs were not getting displayed on the Select IP Addresses pop-up when creating SAP HANA or SAP IQ auth records.
- Fixed an issue where Cisco and Checkpoint Firewall authentication records were getting created even when the IP was present in another Unix auth record. We have now added a validation to check if the IP already has a Cisco/Unix/Checkpoint/Network SSH authentication record created before creating new records.
- Fixed an issue where the scheduled report notification email contained an unwanted email ID that was not part of the Distribution group nor was manually configured.
- We fixed an issue where incomplete technology instance names were displayed in an Authentication Report. Now, the complete strings are displayed in the report.
- We updated the Asset Search Report help to explain that when a Manager launches the report on the “ALL” asset group then all hosts are included, including hosts with cloud agents even if those hosts are not added to the VM/PC license.
- We made a fix in the compliance option profile help where it said users can set a default profile. Only VM option profiles can have a default set.