



# Qualys Cloud Platform (VM, PC) v8.x

## Release Notes

Version 8.22.2

March 16, 2020

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

### **Qualys Policy Compliance (PC)**

[Pivotal Greenplum Authentication Support](#)

[Microsoft SharePoint Authentication Support](#)

[PostgreSQL Support for Windows](#)

[PostgreSQL 12.x Support for Unix](#)

[Microsoft SQL Server 2019 Support](#)

**Qualys 8.22.2 brings you more improvements and updates! [Learn more](#)**

# Qualys Policy Compliance (PC)

## Pivotal Greenplum Authentication Support

We now support Pivotal Greenplum authentication for compliance scans on Unix hosts. Authentication is supported for Greenplum versions 5.x and 6.x.

You'll need a Pivotal Greenplum authentication record to authenticate to a Pivotal Greenplum database instance running on a Unix host, and scan it for compliance.

### How do I get started?

Go to Scans > Authentication, then New > Pivotal Greenplum Record.

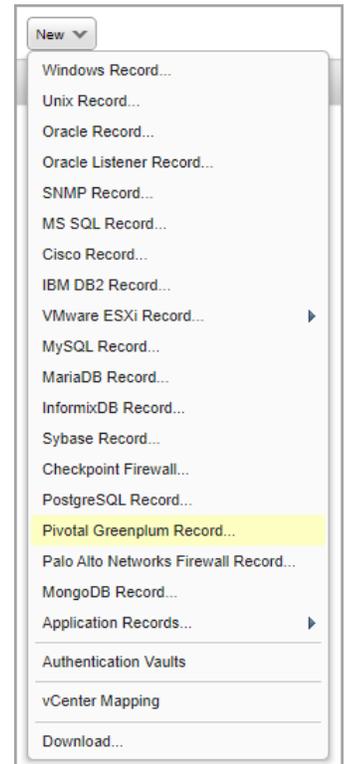
### Pivotal Greenplum Record

In the record, you'll need to tell us the user account to be used for authentication, the database instance to authenticate to, and the port where the database is installed.

The type of authentication method you use depends on your server settings and how you've configured client authentication.

You can use:

- a password (enter it on the Login Credentials tab or get it from a password vault),
- a client certificate (enter it on the Private Key / Certificate tab),
- a password AND client certificate (enter values on both tabs).

A screenshot of the 'New Pivotal Greenplum Record' form. The form has a blue header with the title 'New Pivotal Greenplum Record' and a 'Launch Help' link. On the left, there is a sidebar with tabs: 'Record Title', 'Login Credentials', 'Private Key / Certificate', 'Unix', 'IPs', and 'Comments'. The 'Authentication' tab is selected. The main content area contains the following fields and options:

- Authentication**: 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.
- Username\***: Input field with 'qualys\_scan' entered.
- Database Name\***: Input field with 'my-greenplum-db' entered.
- Port**: Input field with '5432' entered. A note says '(Default is 5432)'.
- Hosts**: Text area with 'host.domain, host.domain,...' entered.
- SSL verification is skipped by default. Select this option to verify that the server's SSL certificate is valid and trusted.**
- SSL Verify**: A checkbox labeled '(server must support SSL)' is currently unchecked.
- For authentication, you can use a password, a client certificate, or both (depending on your server settings). To use a client certificate, enter it on the Private Key/Certificate tab.**
- Get password from vault**: A toggle switch set to 'NO'.
- Password\***: Input field with masked characters '\*\*\*\*\*'.
- Confirm Password\***: Input field with masked characters '\*\*\*\*\*'.

At the bottom of the form, there are 'Cancel' and 'Create' buttons.

## Unix installation

If you want to perform OS-dependent compliance checks, you'll need to tell us where the PostgreSQL configuration file is located on your Unix hosts. Unix authentication is required for these types of checks, so you'll need a Unix record for the same hosts in this record.

Note that the configuration file must be in the same location on all hosts (IPs) in the record. If the file is in a different location for some, then create additional Pivotal Greenplum records.

### New Pivotal Greenplum Record Launch Help

Record Title	>	<b>Unix</b>
Login Credentials	>	To perform OS-dependent compliance checks, enter the full path to the PostgreSQL configuration file on your Unix hosts. This file must be in the same location for all Unix hosts in this record. Unix authentication is required.
Private Key / Certificate	>	
<b>Unix</b>	>	Configuration File: <input type="text" value="/var/lib/greenplum/data/postgresql.conf"/> example: /var/lib/greenplum/data/postgresql.conf
IPs	>	
Comments	>	

## Sample Reports

You'll see the Pivotal Greenplum technology in authentication reports and in compliance scan results. Check out these samples.

The screenshot displays the Qualys Enterprise interface. On the left, a navigation pane shows a tree view with 'Summary' and 'Results'. Under 'Results', 'GreenPlum 5' is expanded to show 'Pivotal Greenplum' with a table of results. The table has columns for Host, Network, Host Technology, and Instance. One entry for host 10.11.70.160 shows 'Pivotal Greenplum 5.x' as the Host Technology and 'Instance' as the Instance. On the right, the 'Compliance Scan Results' panel is visible. It includes a 'Report Summary' section with details like Launch Date, Active Hosts, and Reference. Below that, an 'Appendix' section lists 'Target hosts found alive (IP)' and includes a red-bordered box stating 'Pivotal Greenplum authentication was successful for these hosts' followed by the IP 10.11.70.160.

## Policies and Controls

You'll see Pivotal Greenplum 5.x and 6.x in the technologies list when creating a new policy.

**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 218 technologies Add all shown

- Oracle WebLogic Server 11g
- Oracle WebLogic Server 12c
- PaloAlto Networks PAN-OS
- Pivotal Greenplum 5.x**
- Pivotal Greenplum 6.x**
- Pivotal Web Server 6.x
- Pivotal tc Server 3.x

Choose Source

You'll see Pivotal Greenplum 5.x and 6.x when searching controls by technologies.

**Search** ✕

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

Text:

Status:  Deprecated

Technologies:

- Oracle WebLogic Server 12c
- PaloAlto Networks PAN-OS
- Pivotal Greenplum 5.x**
- Pivotal Greenplum 6.x**
- Pivotal tc Server 3.x

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:

## Microsoft SharePoint Authentication Support

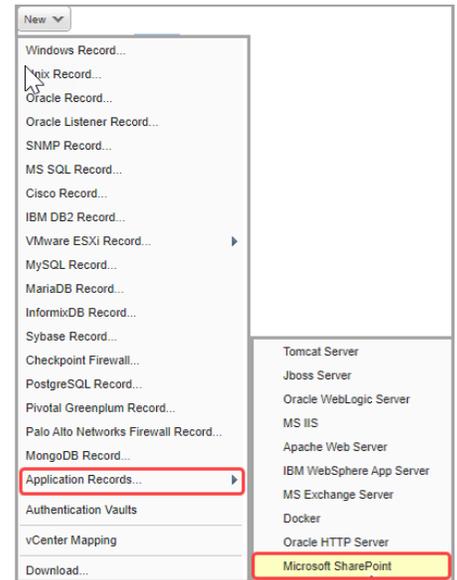
We now support Microsoft SharePoint authentication for compliance scans. Authentication is supported for SharePoint versions 2010, 2013, 2016, and 2019.

Windows authentication is required so you'll also need a Windows record for the host running Microsoft SharePoint. The Microsoft SharePoint record type is only available in accounts with PC or SCA and is only supported for compliance scans.

SharePoint instance will be auto discovered through the Windows Authentication Record. To connect to the MS SQL server, you'll need to provide information under MS SQL Login credentials in Microsoft SharePoint Record.

### Which technologies are supported?

We've added support for Microsoft SharePoint 2010, 2013, 2016, 2019 authentication for compliance scans.



### How do I get started?

- Go to Scans > Authentication.
- Check that you have a Windows record already defined for the host running SharePoint.
- Create a Microsoft SharePoint record for the same host. Go to New > Application Records > Microsoft SharePoint.

### Sample Reports

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

Check out these samples:

The screenshot shows a Qualys Enterprise report. On the left, a 'Results' table shows three SharePoint servers. On the right, a 'Compliance Scan Results' panel shows details for a scan on 03/11/2020. A red box highlights the 'Appendix' section, which states: 'Microsoft SharePoint authentication was successful for these hosts' followed by a list of IP addresses and server versions.

HOST	HOST TECHNOLOGY	INSTANCE
10.11.70.126 (csharepoint2016. qualys.com, CSHAREPOINT2016)	SharePoint Server 2016	SharePoint Server 2016
10.11.70.140 (csharepoint2013. qualys.com, CSHAREPOINT2013)	SharePoint Server 2013	SharePoint Server 2013
10.11.70.151 (csharepoint2019. qualys.com, CSHAREPOINT2019)	SharePoint Server 2019	SharePoint Server 2019

**Compliance Scan Results**

Report Summary

Launch Date: 03/11/2020 at 10:48:52 (GMT)  
Active Hosts: 4  
Total Hosts: 4  
Type: On demand  
Status: Finished  
Reference: compliance/1583945274.00821  
External Scanners: vs\_rey\_pt (Scanner 11.7.45-1, Vulnerability Signatures 2.1.2823-1)  
Duration: 00:05:12  
Title: SharePointAuth  
Asset Groups: -  
IPs: 10.11.70.126,10.11.70.140,10.11.70.151,  
Excluded IPs: -  
Compliance Profile: [Initial PC Options](#)

**Appendix**

Target hosts found alive (IP)

10.11.70.126, 10.11.70.140, 10.11.70.151

Microsoft SharePoint authentication was successful for these hosts

- SharePoint Server 2013  
10.11.70.140
- SharePoint Server 2016  
10.11.70.126
- SharePoint Server 2019  
10.11.70.151

## Policies and Controls

You'll see SharePoint Server in the technologies list when creating a new policy.

**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 Add all shown

- SUSE Linux Enterprise 10.x
- SUSE Linux Enterprise 9/10
- SharePoint Server 2010**
- SharePoint Server 2013**
- SharePoint Server 2016**
- SharePoint Server 2019**
- Solaris 10.x

Choose Source

You'll see SharePoint Server 2010, 2013, 2016, and 2019 when searching controls by technologies.

**Search**

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

Text:

Status:  Deprecated

Technologies:

- SharePoint Server 2010**
- SharePoint Server 2013**
- SharePoint Server 2016**
- SharePoint Server 2019**
- Solaris 10.x

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:

## PostgreSQL Support for Windows

We've extended our support for PostgreSQL authentication to include PostgreSQL Windows hosts. We already support PostgreSQL on Unix hosts.

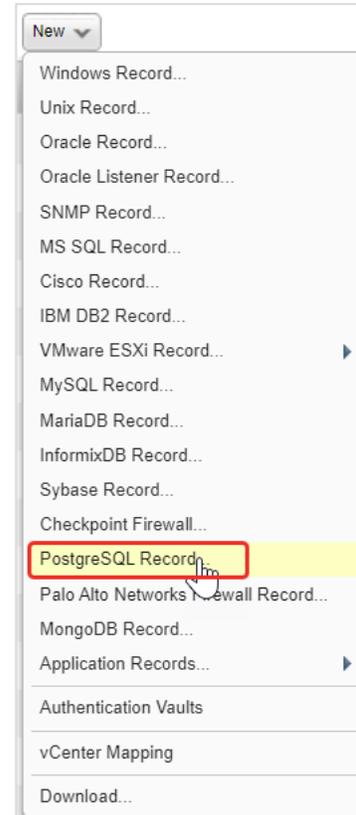
You'll need a PostgreSQL authentication record to authenticate to a PostgreSQL database instance running on a Windows host, and scan it for compliance. Windows authentication is required so you'll also need a Windows record for the host running the database. This record type is only available in accounts with PC or SCA and is only supported for compliance scans.

### Which technologies are supported?

We've added support for PostgreSQL 9.x, PostgreSQL 10.x, PostgreSQL 11.x and PostgreSQL 12.x authentication for compliance scans on Windows hosts.

### How do I get started?

- Go to Scans > Authentication.
- Check that you have a Windows record already defined for the host running the database.
- Create a PostgreSQL record for the same host. Go to New > PostgreSQL Record.



### Sample Reports

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

**Summary**

**Asset Groups Summary**

PostgreSQL 9/10/11/12	8 of 8	100% Successful (4 with insufficient privileges)
	0 of 8	0% Failed
	0 of 8	0% Not Attempted

**Results**

PostgreSQL 9/10/11/12 8 of 8 (100%)

Host	Network	Host Technology
10.11.70.95 (ctomcatw2012r2, CTOMCATW2012R2)	Global Default Network	PostgreSQL 10.x
10.11.70.131 (cdw2016sql2017, CDW2016SQL2017)	Global Default Network	PostgreSQL 11.x
10.11.70.149 (compsql9, COMPSQL9)	Global Default Network	PostgreSQL 9.x
10.11.70.206 (cw2019data, CW2019DATA)	Global Default Network	PostgreSQL 12.x

**Compliance Scan Results**

**Appendix**

**Target hosts found alive (IP)**

10.11.70.95, 10.11.70.131, 10.11.70.149, 10.11.70.206

**Target distribution across scanner appliances**

External : 10.11.70.95,10.11.70.131,10.11.70.149,10.11.70.206

**PostgreSQL authentication was successful for these hosts**

- PostgreSQL 10.x (Port: 5432, Database: postgres) 10.11.70.95
- PostgreSQL 11.x (Port: 5432, Database: postgres) 10.11.70.131
- PostgreSQL 9.x (Port: 5432, Database: postgres) 10.11.70.149
- PostgreSQL 12.x (Port: 5432, Database: postgres) 10.11.70.206

## Policies and Controls

You'll see PostgreSQL in the technologies list when creating a new policy.

**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 | 217 technologies | Add all shown

- PostgreSQL 10.x
- PostgreSQL 11.x
- PostgreSQL 12.x
- PostgreSQL 9.x
- Red Hat Enterprise Linux 3/4
- Red Hat Enterprise Linux 5.x

**Back** Choose Source **Next**

You'll see PostgreSQL when searching controls by technologies.

**Search**

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

Text:

Status:  Deprecated

Technologies:

- PostgreSQL 10.x
- PostgreSQL 11.x
- PostgreSQL 12.x
- PostgreSQL 9.x
- Red Hat Enterprise Linux 3/4

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**

## PostgreSQL 12.x Support for Unix

We've extended our support for PostgreSQL authentication to include PostgreSQL 12.x on Unix hosts. We already support PostgreSQL 9.x, 10.x and 11.x on Unix hosts.

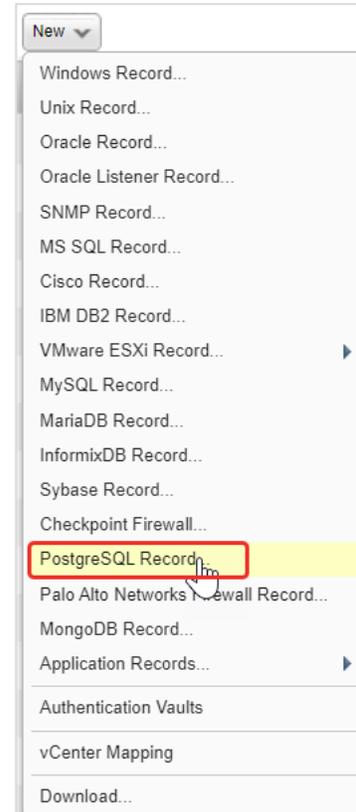
You'll need a PostgreSQL authentication record to authenticate to a PostgreSQL database instance running on a Unix host, and scan it for compliance. Unix authentication is required so you'll also need a Unix record for the host running the database. This record type is only available in accounts with PC or SCA and is only supported for compliance scans.

### How do I get started?

- Go to Scans > Authentication.
- Check that you have a Unix record already defined for the host running the database.
- Create a PostgreSQL record for the same host. Go to New > PostgreSQL Record.

### Sample Reports

You'll see the PostgreSQL 12.x technology in compliance reports and in compliance scan results.



#### Summary

IPs Summary  
10.11.70.179: 2 of 3 66% Successful  
1 of 3 33% Failed  
0 of 3 0% Not Attempted  
Network: All

#### Results

10.11.70.179 2 of 3 (66%)

HOST	NETWORK	HOST TECHNOLOGY	INSTANCE
10.11.70.179 (-, -)	Global Default Network	PostgreSQL 12.x	Port=5432, Database Name=postgres

#### Compliance Scan Results

Report Summary  
Launch Date: 01/24/2020 at 14:42:30 (GMT+0530)  
Active Hosts: 2  
Total Hosts: 2  
Type: On demand  
Status: Finished  
Reference: compliance/1579857052 66700  
External Scanners: new-nq-scanner (Scanner 11.8.27-1, Vulnerability Signatures 2.1.2707-1)  
Duration: 00:01:12  
Title: postgres 12.x - 20200124 - 20200124  
Network: Global Default Network  
Asset Groups: postgresql 12.x  
IPs: 10.11.70.179, 10.115.105.243  
Excluded IPs: -  
Compliance Profile: [postgresql\\_12.x](#)

#### Appendix

Target hosts found alive (IP)  
10.11.70.179, 10.115.105.243

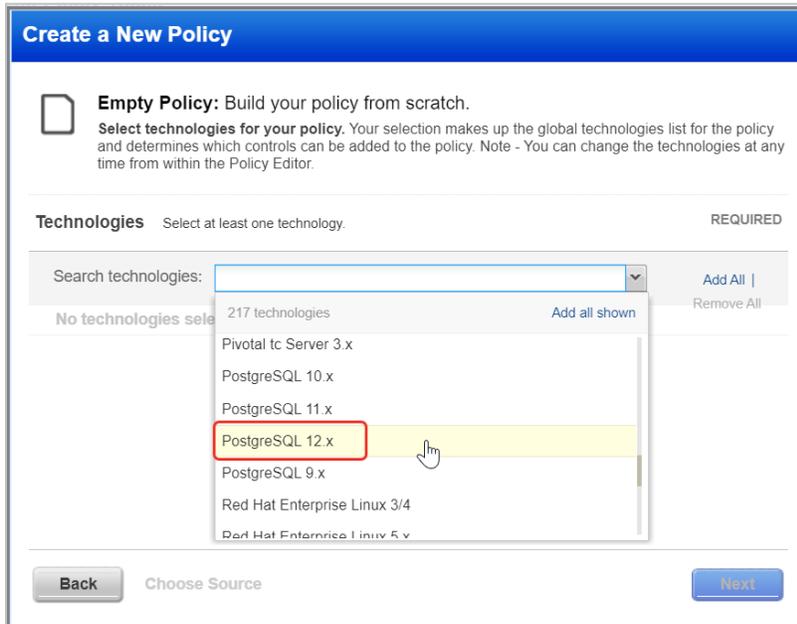
Target distribution across scanner appliances  
new-nq-scanner : 10.11.70.179, 10.115.105.243

Unix/Cisco/Checkpoint Firewall authentication was successful for these hosts  
10.11.70.179

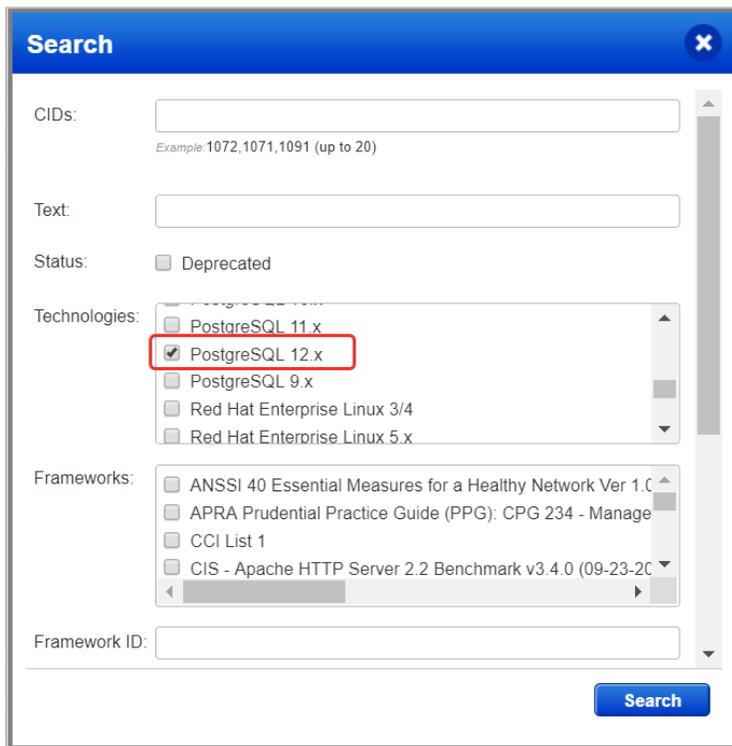
PostgreSQL authentication was successful for these hosts  
PostgreSQL 12.x (Port: 5432, Database: postgres)  
10.11.70.179

## Policies and Controls

You'll see PostgreSQL 12.x in the technologies list when creating a new policy.



You'll see PostgreSQL 12.x when searching controls by technologies.



## Microsoft SQL Server 2019 Support

We've extended our support for MS SQL Server authentication to include Microsoft SQL Server 2019. These technologies are already supported: Microsoft SQL Server 2000, 2005, 2008, 2012, 2014, 2016 and 2017.

You'll need a MS SQL Server record to authenticate to your Microsoft SQL Server 2019 database, and scan it for compliance.

### How do I get started?

Go to Scans > Authentication, and choose New > MS SQL Record. This authentication type is supported for compliance scans only.



## Issues Addressed

- Updated the online help for Search Lists to explain that vulnerabilities with the half red / half yellow severity icon match search lists for both confirmed and potential vulnerabilities. If you create a search list that includes all confirmed QIDs and excludes all potential QIDs, then the QIDs with half red / half yellow severity will be excluded.
- Updated the online help to explain that only the Manager user has privileges to edit storage settings to auto delete scan results.
- Updated the online help for CheckPoint Firewall Authentication to list supported technology versions as CheckPoint Gaia R75 and above, and CheckPoint SecurePlatform PRO R75 and above.
- Updated the System Requirements help to state that we do not support browsers on mobile devices at this time.
- Updated the online help for the VM Scan Summary Notification to clarify that this email includes vulnerability trend information based on the processed results including the total number of new, reopened, active and closed vulnerabilities. Please keep in mind that this email includes trend data, not the actual scan results.
- Updated the online help for OPatch Checks to explain that some Oracle detections use the OPatch method and others do not. In all cases database authentication is required in addition to host authentication for successful Oracle scanning.