



Qualys Cloud Platform (VM, PC) v8.x

Release Notes

Version 8.18

March 11, 2019

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

Qualys Vulnerability Management (VM)

[Launch Cloud CertView Vulnerability Scan for EC2 Assets](#)
[Support for New Authentication Types to Filter Vulnerabilities](#)

Qualys Policy Compliance (PC/SCA)

[Support for InformixDB Authentication](#)
[IBM WebSphere Application Server 9.x Support](#)
[PostgreSQL 10.x Support](#)

Qualys 8.18 brings you many more improvements and updates! [Learn more](#)

Qualys Vulnerability Management (VM)

Launch Cloud CertView Vulnerability Scan for EC2 Assets

You can now launch Cloud CertView scans and start getting up to date view on your certificates and security posture for your AWS EC2 hosts using Qualys Certificate View!

Before you launch Cloud CertView scans you must activate EC2 Assets for CertView Scanning. Once you create an EC2 connector in AssetView, EC2 assets will be activated automatically to scan CertView Scanning application.

Simply got to VM and navigate to Scans > Scans > New > Cloud CertView Scan and provide setup the scan options and launch the scan.

Launch Cloud CertView Vulnerability Scan

Turn help tips: On | Off [Launch Help](#)

Service

Provider: AWS
Service: EC2

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-Classic (Selected Region) EC2-VPC (All VPCs in Region) EC2-VPC (Selected VPC)

Available Regions:

Include hosts that have of the tags below. [Add Tag](#)

(no tags selected)

Do not include hosts that have of the tags below. [Add Tag](#)

(no tags selected)

Scan specific Instance IDs, applicable typically for scanning instances in build or AMI testing phase

Scan agent hosts in my target

Scanner Appliances

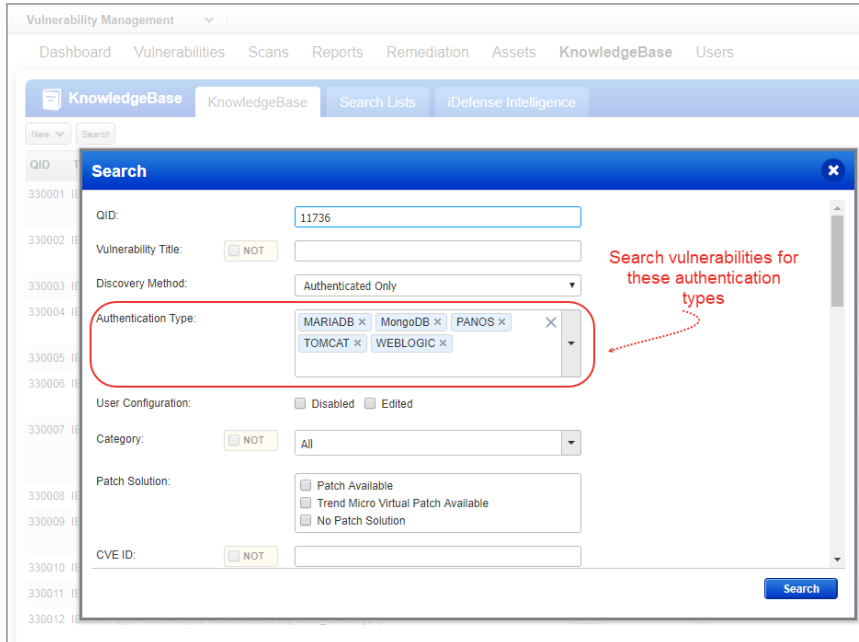
Be sure the scanner appliances you pick can reach the target EC2 instances, i.e. within the region on the EC2 Classic or in the same VPC, or a connected VPC. You must select appliances with the same EC2 proxy settings. Don't see the Scanner in the list. Click the Show All link next to the Scanner Appliance drop-down.

Scanner Appliance: * [View](#) [Show All](#)

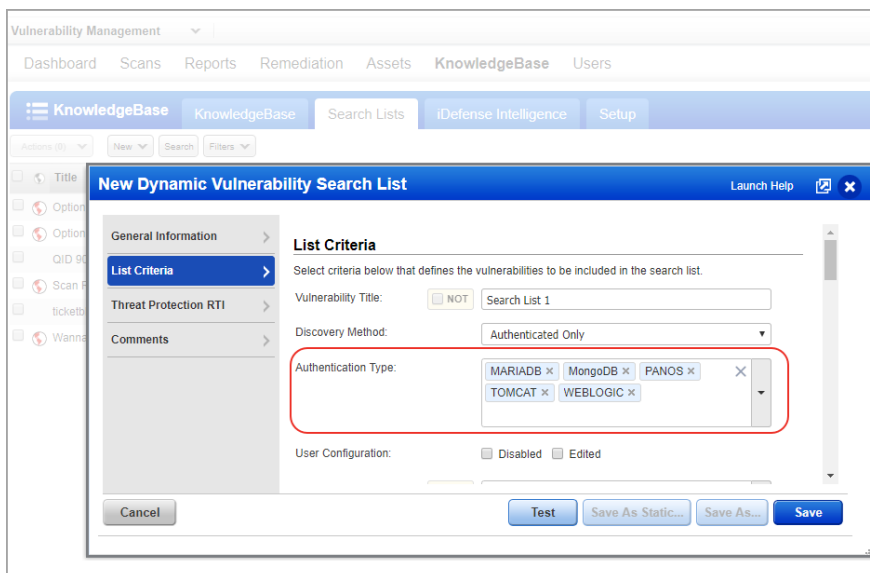
Support for New Authentication Types to Filter Vulnerabilities

Now you can also search in our KnowledgeBase for vulnerabilities that are under authenticated only/remote and authenticated categories with authentication types set as TOMCAT, MARIADB, MongoDB, WebLogic and PANOS. To filter such vulnerabilities we have added the following new authentication types: TOMCAT, MARIADB, MongoDB, WebLogic, PANOS for “Remote and Authenticated” and “Authenticated Only” discovery methods. These authentication types are also available when creating dynamic search lists.

Search for vulnerabilities in KnowledgeBase using the new authentication types.



Create dynamic search lists using the new authentication types.



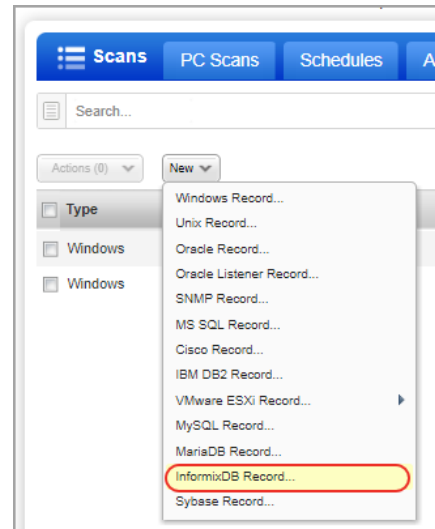
Qualys Policy Compliance (PC/SCA)

Support for InformixDB Authentication

We now support InformixDB authentication for compliance scans using Qualys app PC and SCA. Simply create a InformixDB authentication record with details about your credentials to authenticate to a InformixDB database instance running on a host, and scan it for compliance. We are supporting authentication record creation only for InformixDB installed on Unix.

How do I get started?

Go to Scans > Authentication, and choose New > InformixDB Record (as shown on the right).



Your InformixDB authentication record

A screenshot of the 'New InformixDB Record' form in the Qualys interface. The form has a blue header with the title 'New InformixDB Record' and a 'Launch Help' link. On the left, there is a sidebar with tabs: 'Record Title', 'Login Credentials', 'Target Configuration', 'Unix Configuration', 'IPs', and 'Comments'. The 'Authentication' tab is selected. The main content area shows the following fields: 'Authentication Type:' with a dropdown menu set to 'Basic'; 'Username*:' with a text input field containing 'joe_user'; 'Password*:' with a password input field containing six dots; and 'Confirm Password*:' with a password input field containing six dots. At the bottom of the form are 'Cancel' and 'Create' buttons.

Each InformixDB record identifies account login credentials, database information and target hosts (IPs). Provide basic login credentials (username and password) to be used for authentication.

Note that you must have an Unix record containing the IPs assigned to this record.

A screenshot of the 'New InformixDB Record' form in the Qualys interface. The form has a blue header with the title 'New InformixDB Record' and a 'Launch Help' link. On the left, there is a sidebar with tabs: 'Record Title', 'Login Credentials', 'Target Configuration', 'Unix Configuration', 'IPs', and 'Comments'. The 'Target Configuration' tab is selected. The main content area shows the following fields: 'Database Name*:' with a text input field containing 'informixdb' and a small example text 'Example: admin(default)'; 'Server Name:' with a text input field and a small example text 'Example: demo_on'; 'Port*:' with a text input field containing '1526' and a small example text 'Example: 1526(default)'; and 'SSL Verify:' with a radio button set to 'NO' and a label 'Select this option to verify that the server's SSL certificate is valid and trusted.' At the bottom of the form are 'Cancel' and 'Create' buttons.

Tell us the database name to authenticate to and the port the database is running on. We provide default settings for both, but these may be customized. Use SSL Verify option to specify FQDNs of server hosts that use SSL for authentication.

Enter the full path to the InformixDB configuration files on your Unix hosts. These files are accessed to run certain checks. Ensure that files are in the same location for all the hosts that you want scan.

New InformixDB Record Launch Help

Record Title > **Unix Configuration**

Login Credentials > Enter the full path to the InformixDB configuration file on your Unix hosts. The file must be in the same location for all hosts (IPs) in this record. If different, create another record.

Target Configuration > Configuration File:
example: /opt/Informix/

Unix Configuration > On Configuration File:
example: /opt/Informix/etc/onconfig.demo

IPs > Sql Hosts Configuration File:
example: /opt/Informix/etc/sqlhosts.demo

Comments >

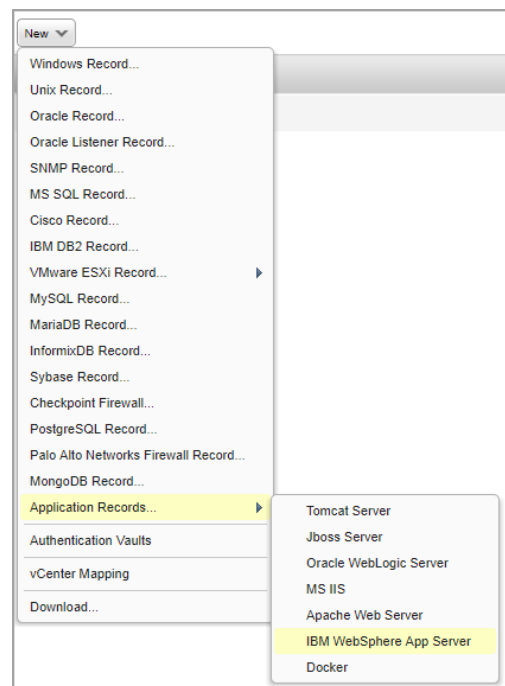
IBM WebSphere Application Server 9.x Support

We've extended our support for IBM WebSphere App Server authentication to include WebSphere Application Server 9.x for Unix. (See the help for other supported technologies.)

You'll need a IBM WebSphere App Server authentication record to authenticate to your web server, and scan it for compliance. You'll also need a Unix record for the host running the web server.

How do I get started?

- Go to Scans > Authentication.
- Check that you already have a Unix record defined for each host running the web server.
- Create a WebSphere App Server record for the same host. Go to New > Application Records > IBM WebSphere App Server.



Sample Reports

You'll see IBM WebSphere App Server 9.x instances in compliance scan results and reports.

The screenshot displays a 'Compliance Scan Results' report. On the left, under 'Appendix', it lists 'Target hosts found alive (IP)' as 10.11.70.54 and 'Target distribution across scanner appliances' as SV_VScanner2: 10.11.70.54. It also notes 'Unix/Cisco/Checkpoint Firewall authentication was successful for 10.11.70.54' and 'IBM WebSphere authentication was successful for these hosts Instance Name: IBM WAS 9 10.11.70.54'. On the right, a 'Summary' section shows 'Asset Groups Summary' for IBM WAS 9.x: 2 of 2 100% Successful, 0 of 2 0% Failed, 0 of 2 0% Not Attempted. Below this is a 'Results' section for 'IBM WAS 9.x 2 of 2 (100%)'. It contains two tables: one for 'Unix/Cisco/Checkpoint Firewall' and one for 'IBM WebSphere App Server'. Both tables show a 'Passed' status for host 10.11.70.54. A red box highlights the IBM WebSphere App Server table.

HOST	HOST TECHNOLOGY	INSTANCE	STATUS	CAUSE	OS	LAST AUTH	LAST SUCCESS
10.11.70.54 (-, -)	CentOS 7.x		Passed	-	CentOS Linux 7.2.1511	02/21/2019	02/21/2019

HOST	HOST TECHNOLOGY	INSTANCE	STATUS	CAUSE	OS	LAST AUTH	LAST SUCCESS
10.11.70.54 (-, -)	IBM WebSphere Application Server 9.x	IBM WebSphere	Passed	-	CentOS Linux 7.2.1511	02/21/2019	02/21/2019

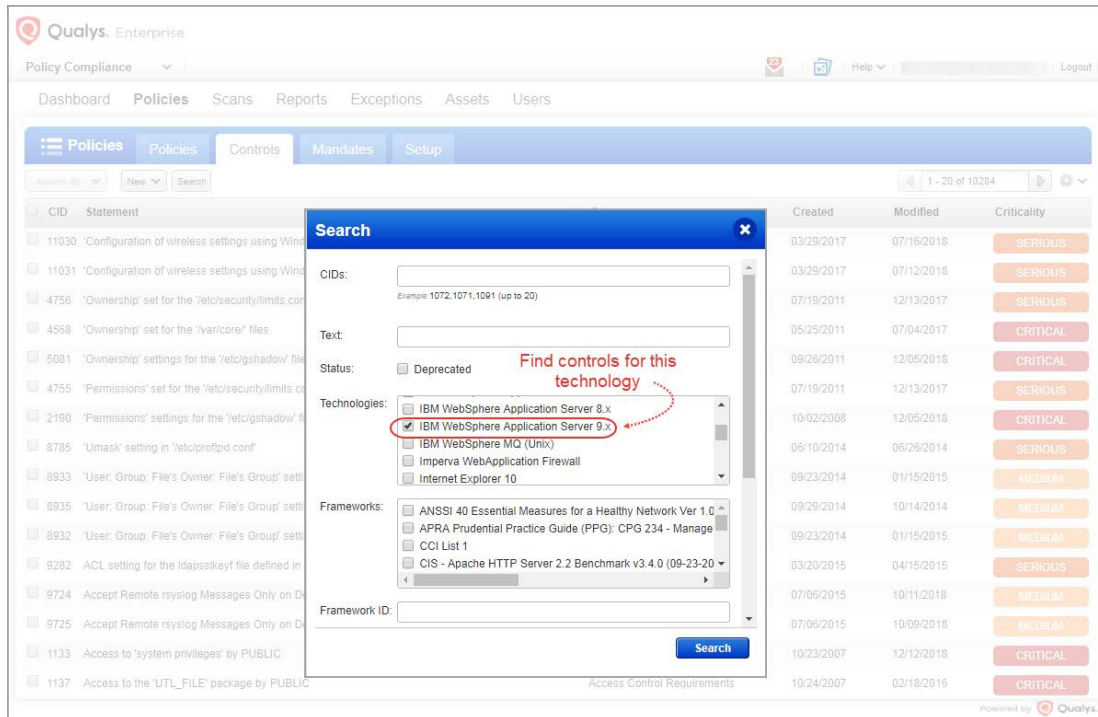
Policies and Controls

You'll also see IBM WebSphere Application Server 9.x in the technologies list when creating a new policy.

The screenshot shows the 'Create a New Policy' interface. It features an 'Empty Policy' section with instructions to 'Build your policy from scratch' and 'Select technologies for your policy'. Below this, a 'Technologies' section is labeled 'REQUIRED' and contains a search box. A dropdown menu is open, showing a list of 174 technologies. The technology 'IBM WebSphere Application Server 9.x' is highlighted with a red box and a red arrow pointing to it, with the text 'Create policy for this technology.' next to it. At the bottom, there are 'Back' and 'Next' buttons.

Search Controls

You'll see IBM WebSphere Application Server 9.x when searching controls by technologies.



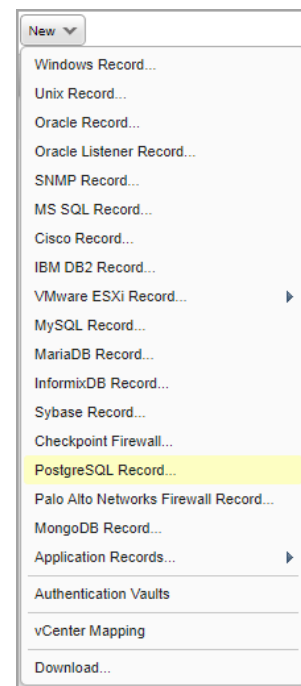
PostgreSQL 10.x Support

We've extended our support for PostgreSQL database authentication to include PostgreSQL 10.x for Unix. (See the help for other supported technologies.)

You'll need a PostgreSQL authentication record to authenticate to your web server, and scan it for compliance. You'll also need a Unix record for the host running the web server.

How do I get started?

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



Sample Reports

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

Summary							
IPs Summary							
10.11.70.116: 2 of 2 100% Successful 0 of 2 0% Failed 0 of 2 0% Not Attempted							
Results							
10.11.70.116 2 of 2 (100%)							
PostgreSQL							
HOST	HOST TECHNOLOGY	INSTANCE	STATUS	CAUSE	OS	LAST AUTH	LAST SUCCESS
10.11.70.116 (-, -)	PostgreSQL 10.x	Port=5432, Database Name=postgres	Passed	-	CentOS 6.9	02/21/2019	02/21/2019
Unix/Cisco/Checkpoint Firewall							
HOST	HOST TECHNOLOGY	INSTANCE	STATUS	CAUSE	OS	LAST AUTH	LAST SUCCESS
10.11.70.116 (-, -)	CentOS 6.x		Passed	-	CentOS 6.9	02/21/2019	02/21/2019

Policies and Controls

You'll also see PostgreSQL 10.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 174 technologies Add all shown

- Pivotal web Server 0.x
- Pivotal tc Server 3.x
- PostgreSQL 10.x**
- PostgreSQL 9.x
- Red Hat Enterprise Linux 3/4
- Red Hat Enterprise Linux 5.x
- Red Hat Enterprise Linux 6.x

Back Choose Source Next

Create policy for this technology

Search Controls

You'll see PostgreSQL 10.x when searching controls by technologies.

The screenshot shows the Qualys Express interface with a search modal open. The search criteria are as follows:

- CIDs:** (Empty)
- Text:** (Empty)
- Status:** Deprecated
- Technologies:**
 - Pivotal tc Server 3.x
 - Pivotal Web Server 6.x
 - PostgreSQL 10.x
 - PostgreSQL 9.x
 - Red Hat Enterprise Linux 3/4
 - Red Hat Enterprise Linux 5.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:** (Empty)

The search results table is partially visible, showing columns for CID, Statement, Created, Modified, and Criticality. The first row is highlighted in red and labeled 'CRITICAL'.

CID	Statement	Created	Modified	Criticality
14322	Status of the 'superuser-backend' context's runtime pa	12/25/2018	12/25/2018	CRITICAL
14320	QPC - Status of BIOS boot sequence in dynamic secu	12/21/2018	12/21/2018	
14305	QPC - Boot sequence - verify CD-ROM description in	12/20/2018	12/20/2018	
14314	QPC - Check existence of the file Application.evtx	12/20/2018	12/20/2018	
14317	QPC - Check existence of the file proagent.brc	12/20/2018	12/20/2018	
14315	QPC - Check existence of the file security.evtx	12/20/2018	12/20/2018	
14316	QPC - Check existence of the file system.evtx	12/20/2018	12/20/2018	
14318	QPC - Check existence of dynamic security suite logs	12/20/2018	12/20/2018	
14312	Dispenser Encryption Status - USB Currency D	12/20/2018	12/20/2018	
14313	Dispenser Encryption Status - USB Media Disp	12/20/2018	12/20/2018	
14308	QPC - PCE Terminal Security - USB Protection	12/20/2018	12/20/2018	
14304	QPC - Status of BIOS Password in dynamic security s	12/20/2018	12/20/2018	
14310	Status of the Hard Disk Encryption status via PCE Ter	12/20/2018	12/20/2018	
14311	Status of the Dynamic Security Suite software hde_inte	12/20/2018	12/20/2018	
14309	Status of the WinMagic SecureDoc Disk Encryption sta	12/20/2018	12/20/2018	
14307	Status of the WinMagic software SDLog.log file existe	12/20/2018	12/20/2018	SERIOUS
14306	Status of the WinMagic software SJob.log file existe	12/20/2018	12/20/2018	SERIOUS
	OS Security Settings	12/20/2018	12/20/2018	SERIOUS

Issues Addressed

- We have fixed an issue where the Scorecard Report was not showing scan results for Agent Tracked Assets even if the tag used in the scan has Agent Tracked Assets. Now Scorecard Report shows scan data for Agent Tracked Assets when a scan is run on a tag that also has Agent Tracked Assets.
- When uploading vCenter – ESXi mappings (under Scans > Authentication), the user can upload a CSV file with the column header as vCenter IP.
- The issue of run history data not available for the scheduled reports is fixed. Now the Run History tab on the Scheduled Task Information screen shows the run history data.
- The Service Now user when connecting to Qualys Cloud Platform was getting an error "The account does not have Service Now integration feature enabled". This issue is fixed and the user will be able to connect to the Qualys Cloud Platform.
- We have fixed an issue where the compliance report was showing control status as failed for inactive controls. This issue is fixed by showing only active controls data for policy summary and Policy Compliance dashboard.
- We have fixed an issue where the new customers were not navigated to the Vulnerability Management module when changing the module to VM. This issue was due to an error in calculating a condition which was returning an incorrect value that showed that the new customer account did not have permission to access VM.
- We have fixed an issue where multiple Tomcat instances were not detected on Windows 2012 during authenticated PC scan. Now if we have multiple Tomcat authentication records for instances running on the single node and different installation path/directory, these instances are now getting detected and come in compliance scan report.
- We now correctly display summary of Added/Removed/Modified files or directories in a Policy Editor.
- We now display correct information about the QIDs excluded for the scan in Host information of the Vulnerabilities Tab in AssetView.
- We have now fixed the issue so that the cancel and pause feature for Cloud Perimeter scan functions correctly. Previously, it was adding cancel and pause time to the next schedule date instead of current schedule date, making it pause and cancel at incorrect time.
- The Posture API request with tag_set_include filter now returns correct posture information on hosts for specified tag names/id.
- We have now fixed the issue to correctly display list of SCAP Enabled Scanners during Launch and/or Scheduling SCAP Scan.
- We have now fixed the asset tag palette so that on clicking any parent Asset tag the child tags are now displayed properly.
- We updated the screen text that appears below the support options on the Help > Contact Support page.
- We have updated the online help and added information about Certificates.
- We have fixed an issue in the API Quick Reference guide where the Scan API (/api/2.0/fo/scan) has a couple of options missing for the output_format parameter. We have added the missing parameters: csv_extended | json_extended in the guide.

- We have now updated the Qualys API User Guide (VM, PC) with correct example for API `/msp/report_template_list.php`.
- We have updated the Windows Authentication document to reflect registry related information on page 15 in “Agentless tracking”.