



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

## Release Notes

Version 8.21.6

November 14, 2019

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

### Qualys Cloud Platform

[Download vCenter and ESXi Mapping Data](#)  
[Purge vCenter and ESXi Mapping Data](#)  
[Create User with no Gender-specific Prefix](#)  
[Platform and Asset tags Information Optional for Cloud Perimeter Scan](#)  
[EC2 Instances with Public IP Addresses are now Scannable](#)

### Qualys Policy Compliance (PC)

[Support for Oracle HTTP Server Authentication](#)  
[New File Content Check for Windows](#)  
[UDC support for Oracle 18c and 19c](#)  
[UDC support for openSUSE 15.x](#)  
[Support for Instance Based Reporting for IBM WAS](#)  
[Apple Safari 11.x/12.x Instances Supported in Compliance Scans for Unix Host](#)  
[New Technologies Supported for Red Hat Enterprise Linux UDCs](#)  
[Expanded Support for Instance Discovery & Auto Record Creation](#)

### Qualys Vulnerability Management (VM)

[View CVSS3 vector strings in Scan Reports](#)  
[HashiCorp Vaults now Supported in DB Auth Records](#)  
[Support for Sybase Authentication in VM](#)

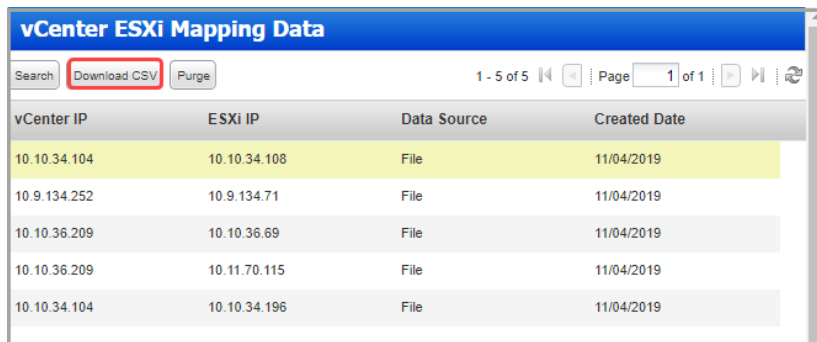
**Qualys 8.21.6 brings you many more improvements and updates! [Learn more](#)**

## Qualys Cloud Platform

### Download vCenter and ESXi Mapping Data

You can now download the vCenter and ESXi Mapping data in CSV format. This information will help you to validate if each ESXi server is connected from the correct vCenter.

Go to Scans > Authentication > New and select vCenter Mapping. Click on the Download CSV option.



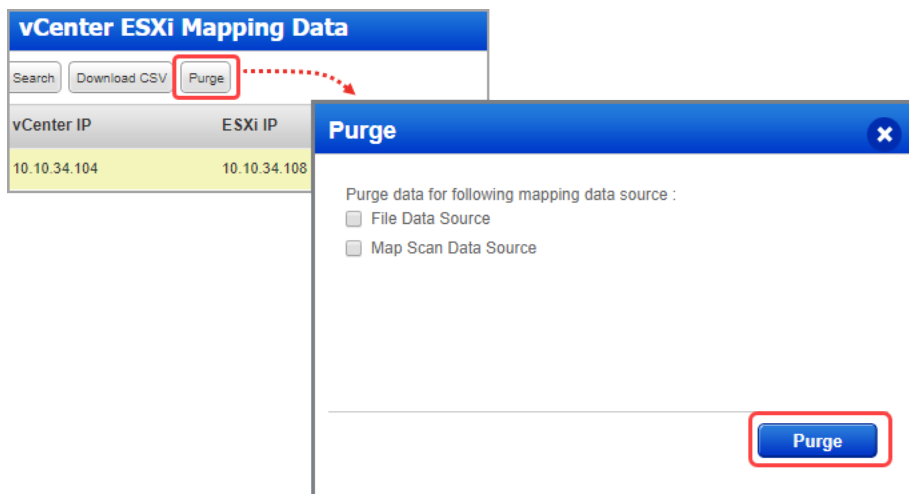
vCenter IP	ESXi IP	Data Source	Created Date
10.10.34.104	10.10.34.108	File	11/04/2019
10.9.134.252	10.9.134.71	File	11/04/2019
10.10.36.209	10.10.36.69	File	11/04/2019
10.10.36.209	10.11.70.115	File	11/04/2019
10.10.34.104	10.10.34.196	File	11/04/2019

If you have searched for certain IP (Scans > Authentication > New > vCenter Mapping>Search) and then clicked on Download CSV, then, all the records related to searched IP will be downloaded in CSV format.

### Purge vCenter and ESXi Mapping Data

With this release, you can delete the vCenter and ESXi Mapping Data.

Go to Scans > Authentication > New and select vCenter Mapping. Click on Purge, select one of the listed options, File Data Source or Map Scan Data Source. Click Purge.



**vCenter ESXi Mapping Data**

Search [Download CSV] [Purge]

vCenter IP	ESXi IP
10.10.34.104	10.10.34.108

**Purge**  
Purge data for following mapping data source :  
☐ File Data Source  
☐ Map Scan Data Source  
**Purge**

## Create User with no Gender-specific Prefix

From this release, you can create a Qualys user account without specifying a gender-specific prefix.

The Welcome screen, will now have “None” option under Prefix. If you set the prefix to None, further emails will not have a gender-specific prefix.

Hello John, Welcome to Qualys@

Verify the information below and carefully read the terms and conditions of Service Agreement.  
By clicking on the "I Agree" button, you are affirming that your company is bound by and is a party to this legal agreement.

**Personal Information**

Prefix:   
Mr   
Mrs   
Ms   
**None**

First Name: John Last Name: Doe

**Contact Information**

Email: jdoe123@gmail.com

Contact Number: \* 90909090 Fax:

I Agree I Decline

## Platform and Asset tags Information Optional for Cloud Perimeter Scan

It's now possible to launch a cloud perimeter scan job without specifying the platform, region code, vpc id or asset tags. Now you can create a new cloud perimeter scan job using only the connector.

If no assets are resolved from the connector and for the optional "platform" and "asset tags" selections, the scan is launched on the load balancer DNS names. If no load balancer DNS names are specified, then the scan will fail and get terminated.

New Cloud Perimeter (EC2) Scan Turn help tips: On | Off Launch Help

Cloud Information > **Target Hosts**

Scan Details >

Target Hosts >

Scanner >

Schedule & Notification >

Review >

Platform:   
EC2 Classic (Selected Region)   
EC2 VPC (All VPCs in Region)   
EC2 VPC (Selected VPC)

Select Asset Tags  
We'll include the instances that match your tags and your platform/region.

Include hosts that have Any of the tags below Add Tag  
(no tags selected)

Do not include hosts that have All of the tags below Add Tag  
(no tags selected)

Load Balancer DNS Names  
Tell us the DNS names for your Internet facing load balancers to include them in the scan.

Remove Selected Remove All Add

Cancel Continue

Note - You'll see these changes in your account only when available on your platform. Please reach out to Qualys Support if you need more information.

## EC2 Instances with Public IP Addresses are now Scannable

It's now possible to launch cloud perimeter scan on your EC2 instances that do not have public DNS hostnames but have public IP addresses. This means during launching a cloud perimeter scan we will include all the EC2 assets that have public IPs but do not have public DNS. If both public DNS and public IP address exist for your EC2 assets, then we will launch a scan using public DNS. We continue to support only DNS names for load balancers.

Note that of all the EC2 hosts that have public IPs and are included for scan, we will scan only those assets that are activated for PC and VM scan.

To create a cloud perimeter scan job, go to VM for a vulnerability scan (or PC for a compliance scan) and choose New > Cloud Perimeter Scan. Create an asset tag for your EC2 assets that have only public IPs and select this tag when creating a cloud perimeter scan job.

**New Cloud Perimeter (EC2) Scan** Turn help tips: On | Off Launch Help

**Cloud Information** > **Target Hosts**  
**Scan Details** >  
**Target Hosts** >  
Scanner >  
Schedule & Notification >  
Review >

**Target Hosts**

Platform: ☐ EC2-Classic (Selected Region) ☐ EC2-VPC (All VPCs in Region) ☒ EC2-VPC (Selected VPC)

**Select Asset Tags**  
We'll include the instances that match your tags and your platform/region.

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)

**Load Balancer DNS Names**  
Tell us the DNS names for your internet facing load balancers to include them in the scan.

Remove Selected Remove All Add

Cancel Continue

## Qualys Policy Compliance (PC)

### Support for Oracle HTTP Server Authentication

Introducing Oracle HTTP Server authentication. Create an Oracle HTTP Server record to authenticate to an Oracle HTTP Server running on a Unix or Windows host, and scan it for compliance.

This record type is only available with PC or SCA, and is only supported for compliance scans.

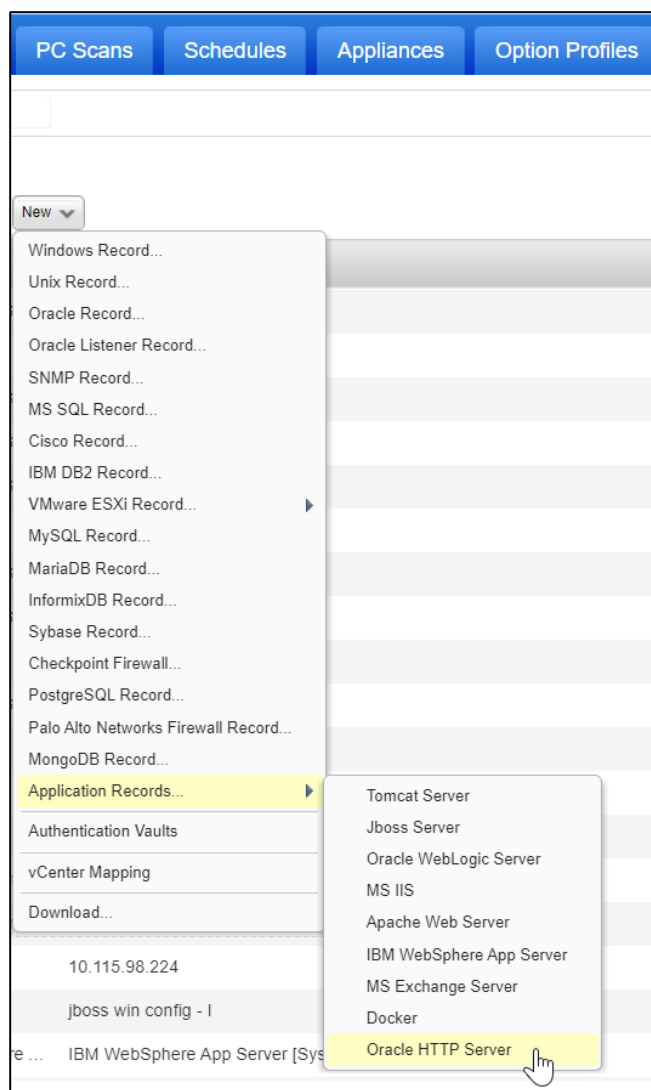
#### Supported Versions

- Oracle HTTP Server 11g
- Oracle HTTP Server 12c

#### How do I get started?

- Go to Scans > Authentication.
- Check that you already have a record defined for each host running an Oracle HTTP server. For Windows hosts, a Windows record is required. For Unix hosts, a Unix record is required.
- Create an Oracle HTTP Server record for the same host (IP). Go to New > Application Records > Oracle HTTP Server.

We'll use credentials from the Unix Record to authenticate to the Unix system and Windows record to authenticate to the Windows system where Oracle HTTP Server is installed.



#### Your record settings

You'll need to provide Windows and Unix configuration details. Enter the home path where the Oracle HTTP Server is installed. Then tell us where domains are configured (required for Oracle HTTP Server 12c and above), where instances are configured (required for Oracle HTTP Server 11g), and the name of the instance you want to authenticate to. Leave the instance name empty and we'll auto discover instances for you.

See examples on the screen for help.

New Oracle HTTP Server Record

Launch Help

Record Title

Windows Configuration

Windows Configuration

Unix Configuration

IPs

Comments

Windows Configuration

Home Path\*

Enter the home path where the Oracle HTTP Server is installed.

C:\Oracle\Middleware\Oracle\_Home

example: C:\Oracle\Middleware\Oracle\_Home

Domain Path

Enter the full directory path where domains are configured for Oracle HTTP Server. Required only for Oracle HTTP Server 12c and above (not required for 11g).

C:\Oracle\Middleware\Oracle\_Home\user\_projects\domains\base\_domain

example: C:\Oracle\Middleware\Oracle\_Home\user\_projects\domains\base\_domain

Instance Path

Enter the full path to where instances are configured for Oracle HTTP Server. Required only for Oracle HTTP Server 11g (not required for 12c and above).

C:\Oracle\Middleware\Oracle\_Home\instances\instance1

example: C:\Oracle\Middleware\Oracle\_Home\instances\instance1

Instance Name

Tell us the instance name you want to authenticate to, or leave this field blank and we'll auto discover the instances for you.

ohs1

example: ohs1

Cancel

Create

## Sample Reports

You'll see Oracle HTTP Server instances in compliance scan results and reports.

Compliance Scan Results

File Help

Appendix

Target hosts found alive (IP)

10.11.70.24, 10.11.70.68, 10.11.70.84, 10.11.70.193

Target distribution across scanner appliances

vs\_seenu\_ak-2 : 10.11.70.24,10.11.70.68,10.11.70.84,10.11.70.193

Windows authentication was successful for these hosts

10.11.70.84, 10.11.70.193

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

10.11.70.24, 10.11.70.68

Oracle HTTP Server authentication was successful for these hosts

OHS 11 (Home Path: C:\Oracle\Middleware\Oracle\_WT1, Instance Path: -, Instance Name: /opt/Oracle\Middleware\Oracle\_WT1/instances/instance1/config/OHS/ohs1, Instance File: ohs1, /opt/Oracle\Middleware\Oracle\_WT1/instances/instance1/config/OHS/ohs1/httpd.conf)

10.11.70.68

OHS 12 (Home Path: C:\Oracle\Middleware\Oracle\_Home, Instance Path: -, Instance Name: C:\Oracle\Middleware\Oracle\_Home\user\_projects\domains\base\_domain\config\fmwco Instance File: ohs1, C:\Oracle\Middleware\Oracle\_Home\user\_projects\domains\base\_domain\config\fmwco 10.11.70.84


Report Summary

Policy:	OHS_11g
Policy Locking:	Unlocked
Template:	Policy Report Template
Asset Groups:	
Ips:	10.11.70.68
Asset Tags:	N/A
Active Hosts:	1
Controls:	2
Technologies:	2 (Oracle HTTP Server 11g, Oracle HTTP Server 12c)
Total Control Instances:	4
Total Passed:	4 (100%)
Total Failed:	0
Total Error:	0
Approved Exceptions:	0
Pending Exceptions:	0
Policy Modified:	10/04/2019 at 05:15:22 (GMT+0530)
Policy Last Evaluated:	10/04/2019 at 16:18:45 (GMT+0530)

## Policies and Controls

You'll also see Oracle HTTP Server in the technologies list while 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:

No technologies selected

201 technologies

Add all shown

Oracle Enterprise Linux 6.x

Oracle Enterprise Linux 7.x

Oracle HTTP Server 11g

Oracle HTTP Server 12c

Oracle WebLogic Server 11g

Oracle WebLogic Server 12c

PaloAlto Networks PAN-OS

Add All |

Remove All

Back

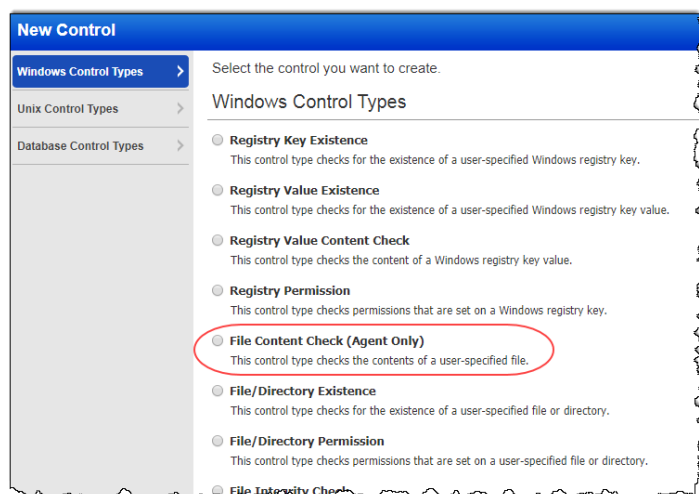
Choose Source

Next

## New File Content Check for Windows

Configure a File Content Check control to check the content of a Windows file. Tell us which file you want to evaluate and what you're looking for. We'll return all lines in the file that match. This control is only supported for Cloud Agents, which means that this control will only be evaluated using agent scan data.

Simply navigate to Policies > Controls > New > Control and from Windows Control Types choose File Content Check.

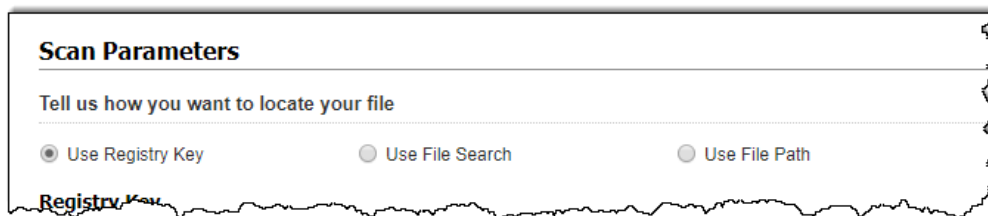


Provide required information like Scan Parameters, Control Technologies, etc. to create the check. Click the launch help link for help with scan parameter settings.

A screenshot of the 'New Control: File Content Check' configuration page. The page has a blue header bar with the text 'New Control: File Content Check' and a link 'Turn help tips: On'. On the left, there is a sidebar with four expandable sections: 'General Information', 'Scan Parameters', 'Control Technologies', and 'References'. The 'General Information' section is expanded, showing the following fields: 'Statement:\*' with a text input field containing 'DVA MSSQL 05.54 FortiDB Policy Version (ACTIVE)-CITI\_MSSQL', 'Category:\*' with a dropdown menu set to 'Database Settings', 'Sub-Category:\*' with a dropdown menu set to 'DB Specific Settings', 'Criticality:' with a radio button selected for 'No criticality level' and five buttons for 'MINIMAL', 'MEDIUM', 'SERIOUS', 'CRITICAL', and 'URGENT', and 'Comments:' with a text area. A blue information banner at the top of the main content area states: 'Windows File Content Check is only supported for Cloud Agents. Therefore, this control will only be evaluated using agent scan data.'



In the Scan Parameters, you can specify your file location using any of the path types: Registry Key, File Search, File Path



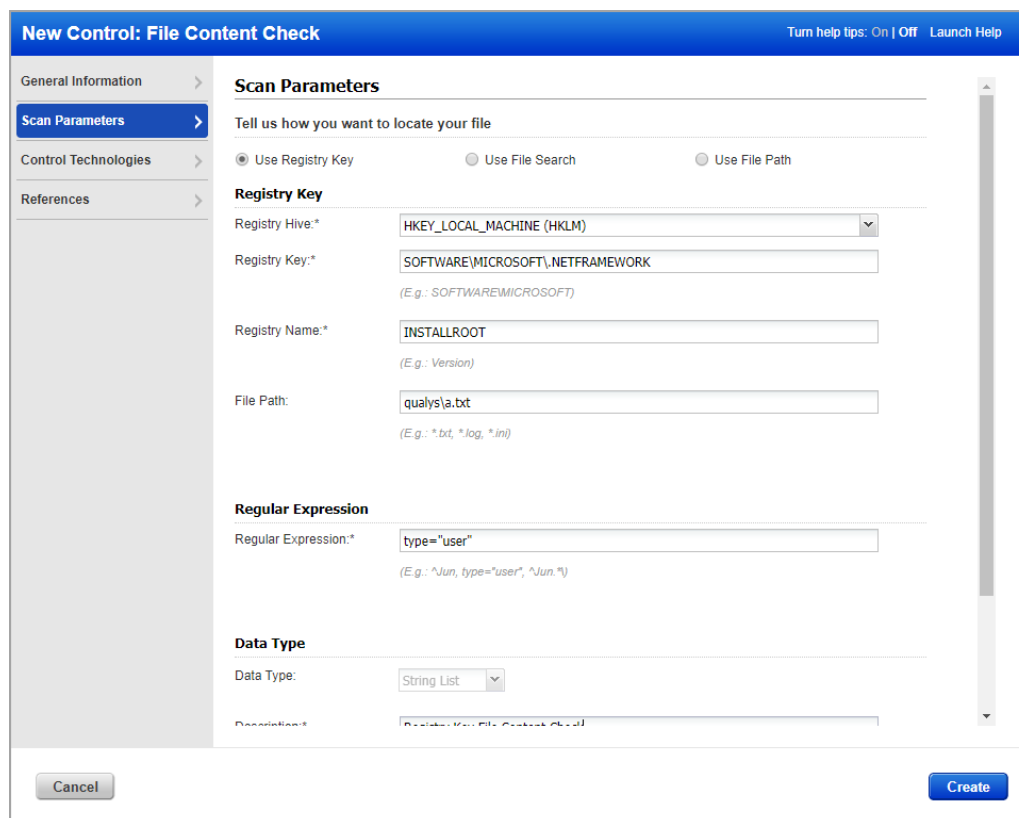
**Scan Parameters**

Tell us how you want to locate your file

☒ Use Registry Key      ☐ Use File Search      ☐ Use File Path

**Registry Key**

See examples on the screen for help.



**New Control: File Content Check** Turn help tips: On | Off Launch Help

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

**Scan Parameters**

Tell us how you want to locate your file

☒ Use Registry Key      ☐ Use File Search      ☐ Use File Path

**Registry Key**

Registry Hive:\* HKEY\_LOCAL\_MACHINE (HKLM) ▼

Registry Key:\* SOFTWARE\MICROSOFT\NETFRAMEWORK  
(E.g.: SOFTWARE\MICROSOFT)

Registry Name:\* INSTALLROOT  
(E.g.: Version)

File Path: qualys\\*.txt  
(E.g.: \*.txt, \*.log, \*.ini)

**Regular Expression**

Regular Expression:\* type=user  
(E.g.: ^Jun, type=user\*, ^Jun.\*)

**Data Type**

Data Type: String List ▼

Description:\* New Control: File Content Check

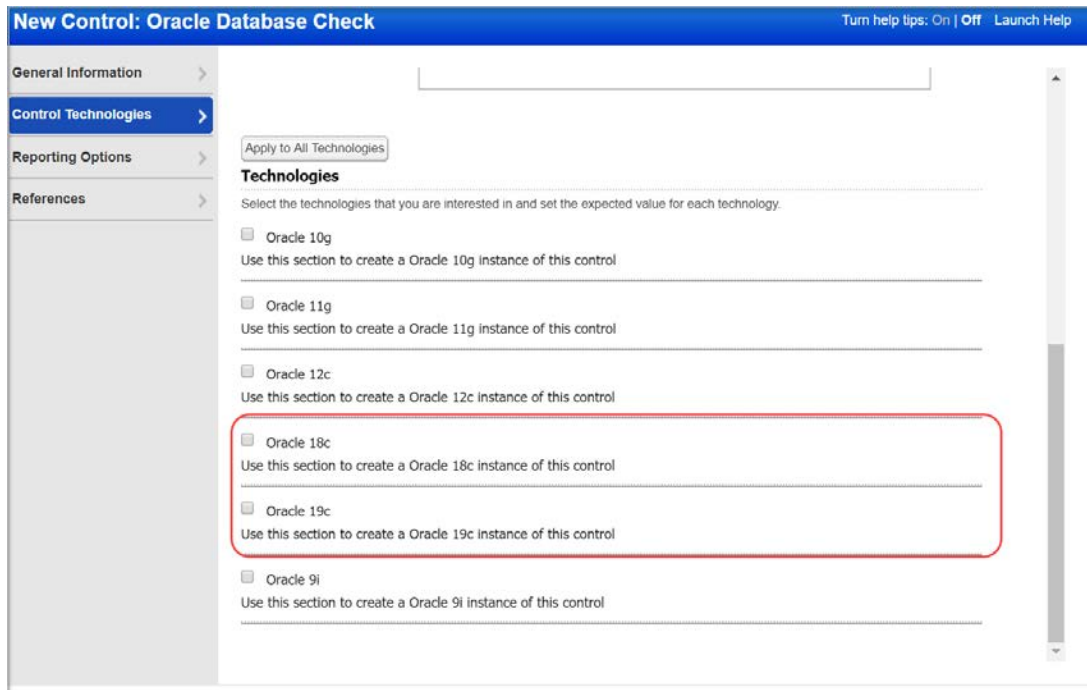
Cancel Create

That's it! Your check is ready to be added to a policy.

## UDC support for Oracle 18c and Oracle 19c

We added User Defined Control (UDC) support for Oracle 18c and Oracle 19c in this release.

Want to create a UDC for Oracle 18c and Oracle 19c? Go to Policies > Controls > New > Control>Database Control Types and select Oracle Database Check. Click on the Control Technologies section to provide a rationale statement and expected value for each technology.



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

**General Information** >

**Control Technologies** >

**Reporting Options** >

**References** >

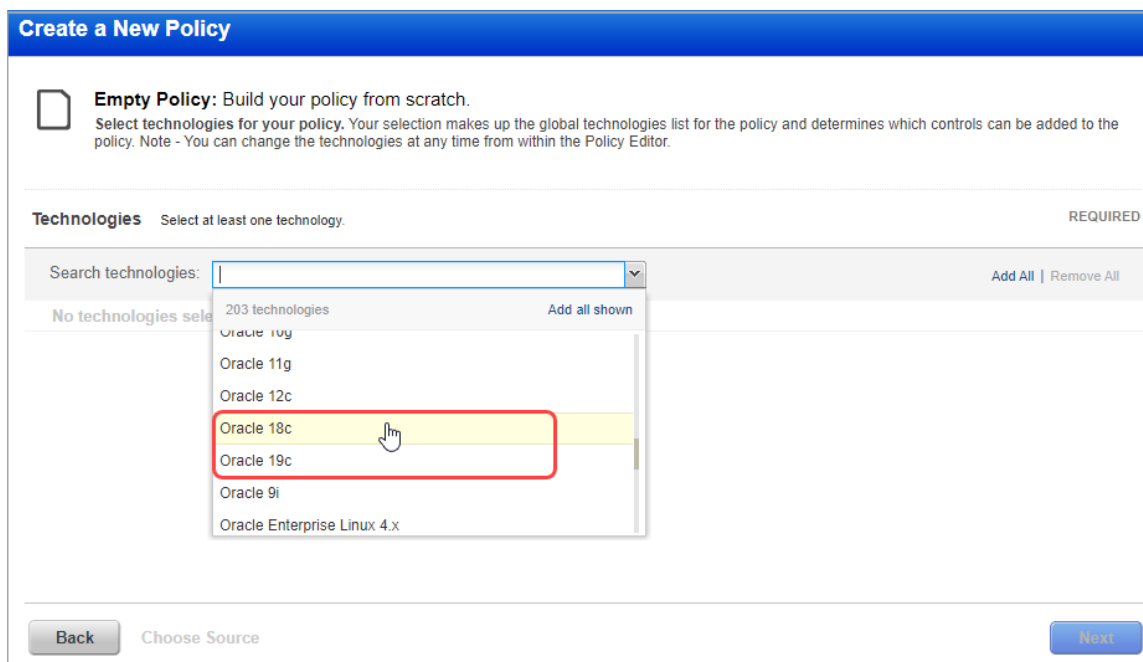
Apply to All Technologies

**Technologies**

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

- ☐ Oracle 10g  
Use this section to create a Oracle 10g instance of this control
- ☐ Oracle 11g  
Use this section to create a Oracle 11g instance of this control
- ☐ Oracle 12c  
Use this section to create a Oracle 12c instance of this control
- ☐ Oracle 18c  
Use this section to create a Oracle 18c instance of this control
- ☐ Oracle 19c  
Use this section to create a Oracle 19c instance of this control
- ☐ Oracle 9i  
Use this section to create a Oracle 9i instance of this control

While creating a new policy, you can select Oracle 18c and Oracle 19c from the technologies list.



**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

203 technologies Add all shown

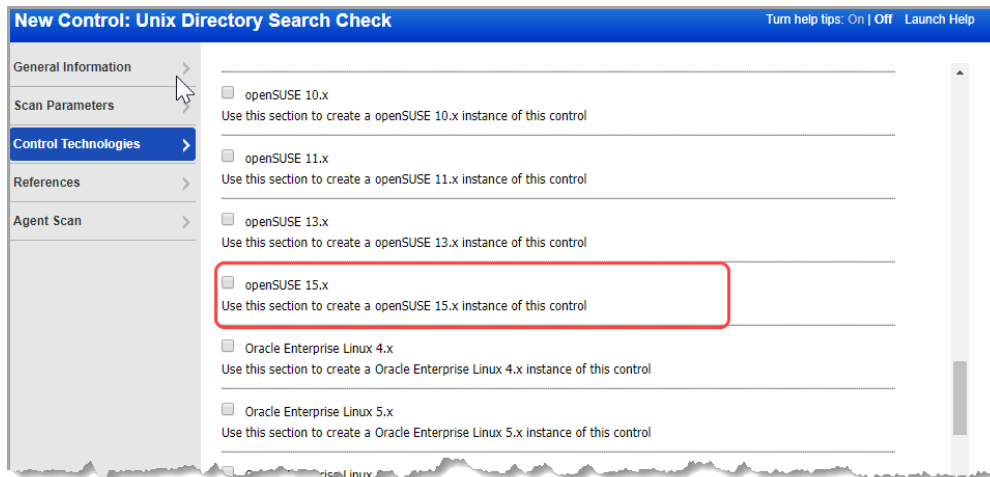
- Oracle 10g
- Oracle 11g
- Oracle 12c
- Oracle 18c
- Oracle 19c
- Oracle 9i
- Oracle Enterprise Linux 4.x

Back Choose Source Next

## UDC support for openSUSE 15.x

We have added User Defined Control (UDC) support for openSUSE 15.x for scanner and agent.

Want to create a UDC for openSUSE 15.x? Go to Policies > Controls > New > Control>Unix Control Types and select the required control types from the list. Click on the Control Technologies section to provide a rationale statement and expected value for each technology.

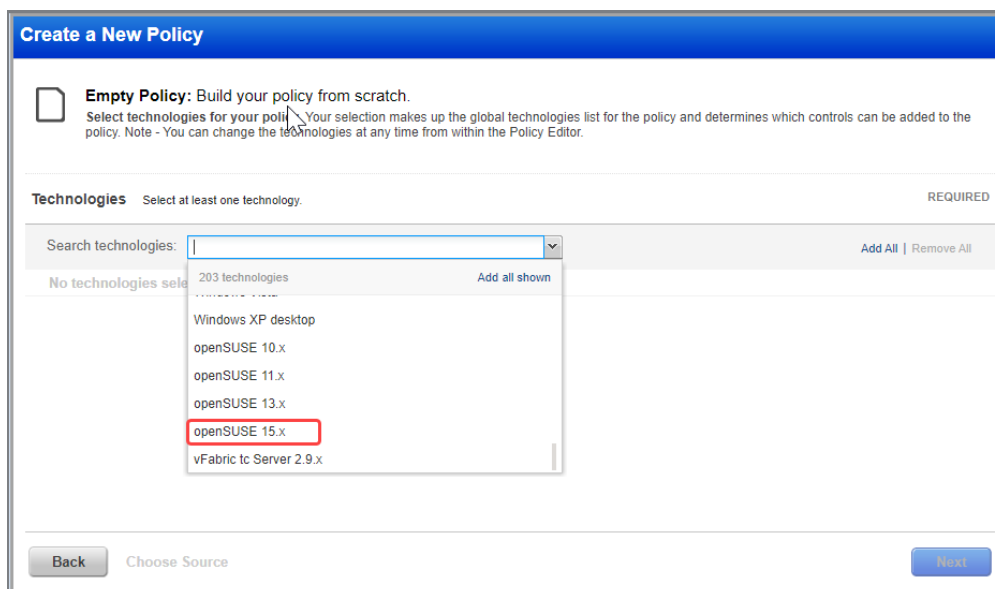


**New Control: Unix Directory Search Check** Turn help tips: On | Off Launch Help

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

- ☐ openSUSE 10.x  
Use this section to create a openSUSE 10.x instance of this control
- ☐ openSUSE 11.x  
Use this section to create a openSUSE 11.x instance of this control
- ☐ openSUSE 13.x  
Use this section to create a openSUSE 13.x instance of this control
- ☐ openSUSE 15.x  
Use this section to create a openSUSE 15.x instance of this control
- ☐ Oracle Enterprise Linux 4.x  
Use this section to create a Oracle Enterprise Linux 4.x instance of this control
- ☐ Oracle Enterprise Linux 5.x  
Use this section to create a Oracle Enterprise Linux 5.x instance of this control

While creating a new policy, you can select openSUSE 15.x from the Search technologies list.



**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 203 technologies Add all shown

- Windows XP desktop
- openSUSE 10.x
- openSUSE 11.x
- openSUSE 13.x
- openSUSE 15.x**
- vFabric tc Server 2.9.x

Back Choose Source Next

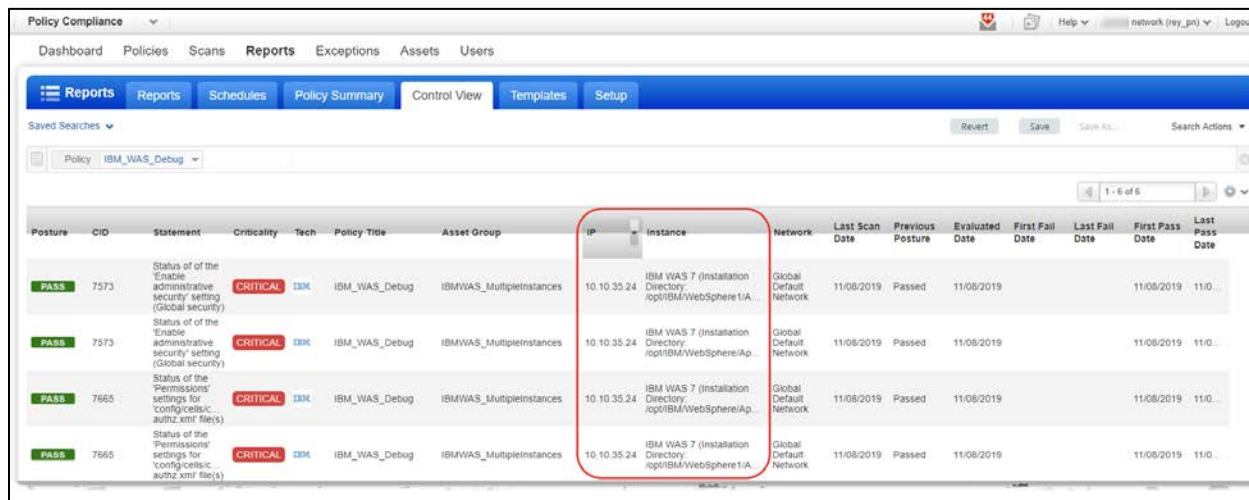
## Support for Instance Based Reporting for IBM WAS

Before this release, WebSphere scanning was only supported for a single instance per target and instance report was without WebSphere installation path.

Now, you will be able to do authenticated scanning for multiple auth records and multiple instances of IBM WAS on single host. Installation directory path is now shown with instance.

### Control View

Multiple IBM WAS instances on single host with Installation Directory is shown in the Control View.

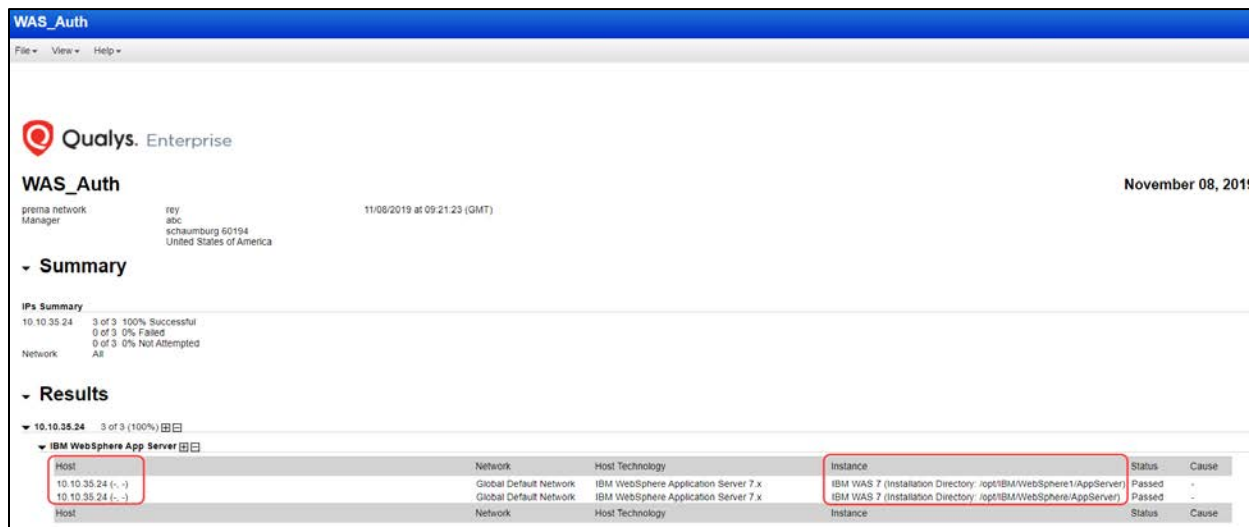


The screenshot shows the 'Control View' in the Qualys Policy Compliance interface. A table lists four rows of scan results for the policy 'IBM\_WAS\_Debug'. Each row represents a different instance of IBM WAS 7 on the host 10.10.35.24. The 'Instance' column is highlighted with a red box, showing the installation directory path for each instance. The 'Status' column shows 'PASS' for all instances.

Posture	CID	Statement	Criticality	Tech	Policy Title	Asset Group	IP	Instance	Network	Last Scan Date	Previous Posture	Evaluated Date	First Fail Date	Last Fail Date	First Pass Date	Last Pass Date
PASS	7573	Status of the 'Enable administrative security' setting (Global security)	CRITICAL	IBM	IBM_WAS_Debug	IBMVAS_MultiInstances	10.10.35.24	IBM WAS 7 (Installation Directory: /opt/IBM/WebSphere1/A...	Global Default Network	11/08/2019	Passed	11/08/2019			11/08/2019	11/0...
PASS	7573	Status of the 'Enable administrative security' setting (Global security)	CRITICAL	IBM	IBM_WAS_Debug	IBMVAS_MultiInstances	10.10.35.24	IBM WAS 7 (Installation Directory: /opt/IBM/WebSphere1/Ap...	Global Default Network	11/08/2019	Passed	11/08/2019			11/08/2019	11/0...
PASS	7665	Status of the 'Permissions' settings for 'config/cells/c... authz.xml' file(s)	CRITICAL	IBM	IBM_WAS_Debug	IBMVAS_MultiInstances	10.10.35.24	IBM WAS 7 (Installation Directory: /opt/IBM/WebSphere1/Ap...	Global Default Network	11/08/2019	Passed	11/08/2019			11/08/2019	11/0...
PASS	7665	Status of the 'Permissions' settings for 'config/cells/c... authz.xml' file(s)	CRITICAL	IBM	IBM_WAS_Debug	IBMVAS_MultiInstances	10.10.35.24	IBM WAS 7 (Installation Directory: /opt/IBM/WebSphere1/A...	Global Default Network	11/08/2019	Passed	11/08/2019			11/08/2019	11/0...

### Sample Authentication Report

In the following report, scanning is performed for a single host (IP – 10.10.35.24) with multiple IBM WAS instances. Installation Directory path is mentioned along with instance name.



The screenshot shows a 'WAS\_Auth' report from Qualys Enterprise. It includes a summary of the scan and a detailed results section. The 'Results' section is expanded for the host 10.10.35.24, showing three instances of IBM WebSphere App Server. The 'Instance' column is highlighted with a red box, showing the installation directory path for each instance. The 'Status' column shows 'Passed' for all instances.

Host	Network	Host Technology	Instance	Status	Cause
10.10.35.24 (-.-)	Global Default Network	IBM WebSphere Application Server 7.x	IBM WAS 7 (Installation Directory: /opt/IBM/WebSphere1/AppServer)	Passed	-
10.10.35.24 (-.-)	Global Default Network	IBM WebSphere Application Server 7.x	IBM WAS 7 (Installation Directory: /opt/IBM/WebSphere1/AppServer)	Passed	-
Host	Network	Host Technology	Instance	Status	Cause

## Apple Safari 11.x/12.x Instances Supported in Compliance Scans for Unix Host

We now support compliance scans for Apple Safari 11.x and Safari 12.x instances for host running on Unix platform. Scan reports show information for Safari 11.x /12.x instances only if they are found on the Unix host during the compliance scan.

You'll need a Unix authentication record with sudo as root delegation for the hosts running Safari 11.x/12.x instances. Then scan those hosts using authentication.

### Sample Reports

You'll see Apple Safari 11.x/12.x instances in compliance scan results and reports for Unix host.

Compliance Scan Results	
File ▾ Help ▾	
Asset Groups:	-
IPs:	10.11.75.101
Excluded IPs:	-
Compliance Profile:	<a href="#">safari</a>
<b>Appendix</b>	
<b>Target hosts found alive (IP)</b>	
10.11.75.101	
<b>Target distribution across scanner appliances</b>	
cy2_vsn04 : 10.11.75.101	
<b>Unix/Cisco/Checkpoint Firewall authentication was successful for these hosts</b>	
10.11.75.101	
<b>Application technologies found based on OS-level authentication</b>	
<b>Apple Safari was found for these hosts</b>	
Apple Safari 12.x (Installation Path: /Applications/Safari.app)	
10.11.75.101	

Compliance Scan Results	
File ▾ Help ▾	
Asset Groups:	-
IPs:	10.10.10.202
Excluded IPs:	-
Compliance Profile:	<a href="#">safari</a>
<b>Appendix</b>	
<b>Target hosts found alive (IP)</b>	
10.10.10.202	
<b>Target distribution across scanner appliances</b>	
vsn03 : 10.10.10.202	
<b>Unix/Cisco/Checkpoint Firewall authentication was successful for these hosts</b>	
10.10.10.202	
<b>Application technologies found based on OS-level authentication</b>	
<b>Apple Safari was found for these hosts</b>	
Apple Safari 11.x (Installation Path: /Applications/Safari.app)	
10.10.10.202	

## Policies and Controls

You'll also see Apple Safari 11.x/12.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 203 technologies Add all shown

- Apache Tomcat 8.x
- Apache Tomcat 9.x
- Apple Safari 11.x
- Apple Safari 12.x
- ArubaOS 6.x
- Brocade Fabric 7.x

Back Choose Source Next

## Search Controls

You'll see Apple Safari 11.x/12.x when searching controls by technologies.

**Search**

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

Text:

Status: ☐ Deprecated

Technologies:

- Apache Tomcat 8.x
- Apache Tomcat 9.x
- Apple Safari 11.x
- Apple Safari 12.x
- ArubaOS 6.x
- Brocade Fabric 7.x

Frameworks:

- CIS - HP-UX 1.4.2 [iv1-3] (09/2008) .iv1, .iv2, .iv3
- CIS - HP-UX 1.5.0 [iv2-3] (09/2009) .iv2-3
- CIS - HP-UX 1.3.1 [iv1] (10/2005) 1.3.1
- CIS - HP-UX 1.4.1 [iv1-3] (11/2007) v. 1.4.1: 2007
- CIS - IRIX 6.5.1 (10/2005) 1.0 1.1 2005

Framework ID:

Search

**Find controls for this technology**

CID	Statement	Severity
11030	'Configuration of wireless settings	CRITICAL
11031	'Configuration of wireless settings	CRITICAL
4756	'Ownership' set for the '/etc/secur	CRITICAL
4568	'Ownership' set for the '/var/coref	CRITICAL
5081	'Ownership' settings for the '/etc/g	CRITICAL
4755	'Permissions' set for the '/etc/secu	CRITICAL
2190	'Permissions' settings for the '/etc	CRITICAL
8785	'Umask' setting in '/etc/proftpd.conf	CRITICAL
8933	'User: Group: File's Owner: File's	CRITICAL
8935	'User: Group: File's Owner: File's	CRITICAL
8932	'User: Group: File's Owner: File's	CRITICAL
100000	1	CRITICAL
9282	ACL setting for the Idapsslkeyf file	CRITICAL
9724	Accept Remote rsyslog Messages	CRITICAL
9725	Accept Remote rsyslog Messages	CRITICAL
1133	Access to 'system privileges' by PUBLIC	CRITICAL

## New Technologies Supported for Red Hat Enterprise Linux UDCs

Want to create a UDC for Red Hat Enterprise Linux 8.x? Go to Policies > Controls > New > Control and select any of the Unix control types. Scroll down to the Control Technologies section to provide a rationale statement and expected value for each technology.

New Control: File/Directory Existence - Google Chrome

**Control Technologies\***

- ☐ AIX 5.x  
Use this section to create a AIX 5.x instance of this control
- ☐ AIX 6.x  
Use this section to create a AIX 6.x instance of this control
- ☐ AIX 7.x  
Use this section to create a AIX 7.x instance of this control
- ☐ Amazon Linux 2 AMI  
Use this section to create a Amazon Linux 2 AMI instance of this control
- ☐ Red Hat Enterprise Linux 7.x  
Use this section to create a Red Hat Enterprise Linux 7.x instance of this control
- ☐ Red Hat Enterprise Linux 8.x  
Use this section to create a Red Hat Enterprise Linux 8.x instance of this control
- ☐ Solaris 10.x  
Use this section to create a Solaris 10.x instance of this control
- ☐ Solaris 11.x  
Use this section to create a Solaris 11.x instance of this control
- ☐ Solaris 8.x  
Use this section to create a Solaris 8.x instance of this control
- ☐ Solaris 9.x  
Use this section to create a Solaris 9.x instance of this control
- ☐ SUSE Linux Enterprise 11.x  
Use this section to create a SUSE Linux Enterprise 11.x instance of this control
- ☐ SUSE Linux Enterprise 12.x  
Use this section to create a SUSE Linux Enterprise 12.x instance of this control
- ☐ SUSE Linux Enterprise 9/10  
Use this section to create a SUSE Linux Enterprise 9/10 instance of this control

←..... New technology supported

## Expanded Support for Instance Discovery & Auto Record Creation

Instance discovery and auto record creation is now supported for Apache Tomcat Server. You can learn more about this feature and how it works in the "System Authenticated Records" help file.

### Summary

These capabilities now are available for Tomcat Server.

- Support for scanning multiple instances running on the same host, and when hosts have varying configurations
- Two phased scanning process. First, a discovery scan finds Tomcat Server instances, consolidates instance data, and creates/updates auth records in the user's account. Then an assessment scan uses the records saved in the user's account for control evaluations.
- New option profile settings allow you to 1) enable instance discovery and auto record creation, 2) include system-created records for scans, and 3) determine whether to send system records or user records when there are 2 records for the same instance configuration.
- Compliance scan results show a list of instances discovered by the scan when the instance discovery and auto record creation feature is enabled for the scan. Compliance assessment data is not collected during instance discovery scans.
- New System created auth records. Auto created authentication records have the owner "System". These records cannot be edited by users.
- You can enable Tomcat records for authenticated scanning, i.e. set as Active, or disable this, i.e. set as Inactive.

### Option Profiles

When configuring option profiles, you'll now see Tomcat Server listed under System Authentication Records.

Option Profile 1: Choose "Allow instance discovery and system record creation" and select one or more application.

Use this option profile for instance discovery scans. We'll discover running instances during the scan, and then use the information collected about your running instances to create auth records.

For Tomcat Server, Unix authentication is required. So be sure you have Unix authentication records in your account.

**System Authentication Records**

Allow the system to create authentication records automatically using the scan data discovered for running instances. In follow up scans, compliance assessments can be performed using those system created records. [Learn more about instance discovery and system authentication records](#)

**Create System Authentication Records**

By choosing this option we'll restrict scans to instance discovery and record creation for the selected technology. Unix authentication is required. Compliance assessments will not be performed for any technology.

☒ Allow instance discovery and system record creation

For the following technology

- ☐ Apache Web Server
- ☐ IBM WebSphere App Server
- ☐ Jboss Server
- ☒ Tomcat Server

**Use System Authentication Records**

When selected, compliance assessments will be performed using all active authentication records (system and user created). Instance discovery and record creation will not be performed.

☐ Include system created authentication records in scans

Only 1 record is used for scanning each instance. If there are 2 records (system and user created) with the same instance configuration, tell us which record to use

- ☒ User created record
- ☐ System created record



Option Profile 2: Choose “Include system created authentication records in scans” in the option profile you’ll use for compliance assessments.

System created records will be used along with user created records. If you have a user created record and a system created record for the same instance configuration, we’ll use the user record by default. You can change this if you prefer to use the system record.

**System Authentication Records**

Allow the system to create authentication records automatically using the scan data discovered for running instances. In follow up scans, compliance assessments can be performed using those system created records. [Learn more about instance discovery and system authentication records](#)

Create System Authentication Records

By choosing this option we'll restrict scans to instance discovery and record creation for the selected technology. Unix authentication is required. Compliance assessments will not be performed for any technology.

☐ Allow instance discovery and system record creation

For the following technology

☐ Apache Web Server

☐ IBM WebSphere App Server

☐ Jboss Server

☐ Tomcat Server

**Use System Authentication Records**

When selected, compliance assessments will be performed using all active authentication records (system and user created). Instance discovery and record creation will not be performed.

☒ Include system created authentication records in scans

Only 1 record is used for scanning each instance. If there are 2 records (system and user created) with the same instance configuration, tell us which record to use

☒ User created record


☐ System created record

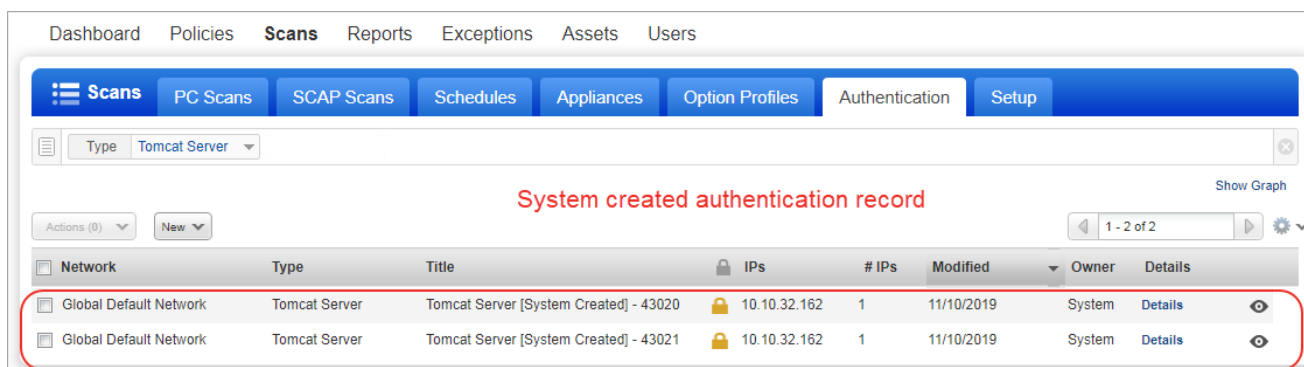
## Compliance Scan Results

For a compliance scan with the option "Allow instance discovery and system record creation", you can go to the Appendix section of your compliance scan results to see the auto discovered instances.

Compliance Scan Results	
File ▾	Help ▾
Unix/Cisco/Checkpoint Firewall authentication was successful for these hosts	
10.10.32.162	
Auto Discovered Instances	
Apache Web Server instances were not found for these hosts	
10.10.32.162	
IBM WebSphere App Server instances were not found for these hosts	
10.10.32.162	
Tomcat Server (Installation Directory: /root/apache-tomcat-9.0.1, Instance Directory: /root/apache-tomcat-9.0.1)	
10.10.32.162	
Tomcat Server (Installation Directory: /root/apache-tomcat-9.0.1-inst2, Instance Directory: /root/apache-tomcat-9.0.1-inst2)	
10.10.32.162	

## System Created Records

You'll see a gold lock  and Owner "System" for system-created authentication records for Tomcat Server.



Dashboard Policies **Scans** Reports Exceptions Assets Users



Scans PC Scans SCAP Scans Schedules Appliances Option Profiles Authentication Setup

Type Tomcat Server

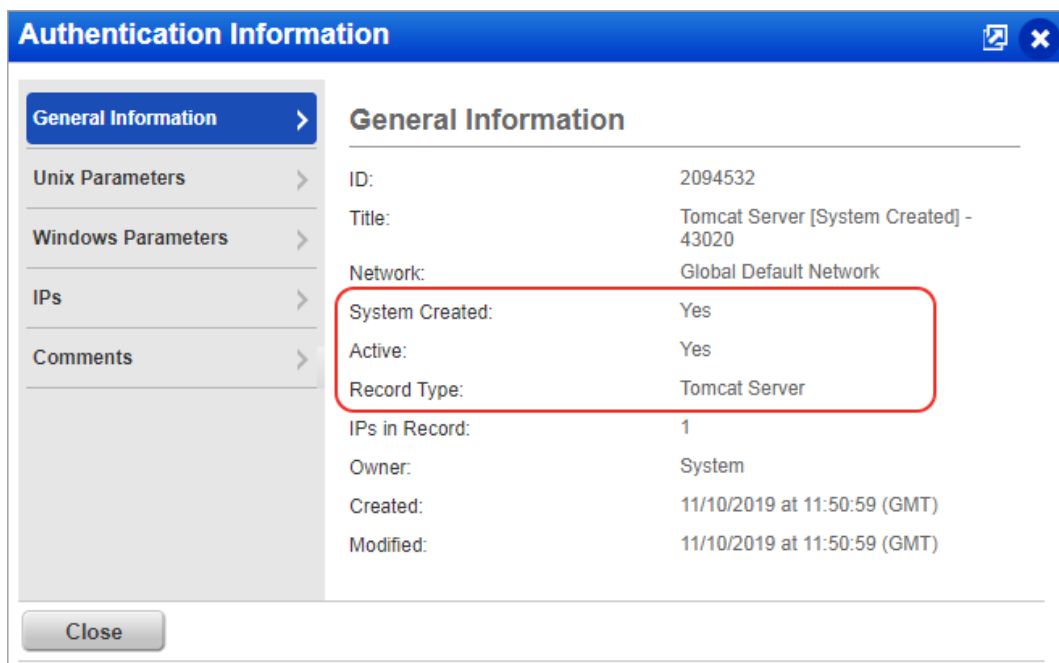
System created authentication record

Actions (0) New

1 - 2 of 2

Network	Type	Title	IPs	# IPs	Modified	Owner	Details
Global Default Network	Tomcat Server	Tomcat Server [System Created] - 43020	 10.10.32.162	1	11/10/2019	System	Details
Global Default Network	Tomcat Server	Tomcat Server [System Created] - 43021	 10.10.32.162	1	11/10/2019	System	Details

You will see the system created and active status when you view a Tomcat authentication record from the Quick Actions menu.



Authentication Information

General Information

Unix Parameters

Windows Parameters

IPs

Comments

Close

General Information

ID: 2094532

Title: Tomcat Server [System Created] - 43020

Network: Global Default Network

System Created: Yes

Active: Yes

Record Type: Tomcat Server

IPs in Record: 1

Owner: System

Created: 11/10/2019 at 11:50:59 (GMT)

Modified: 11/10/2019 at 11:50:59 (GMT)

Also, when you download the authentication records list to CSV format (New > Download) you'll see the column "Is System Created" with a value of Yes or No for each record.

	Network	Type	Title	Is System Created	IPs	IPs	Modified	Owner	Status
4	Global Default Network	Jboss Server	Jboss Server [System Created] - 43019	Yes	10.10.36.1	1	11/10/201	System	Active
5	Global Default Network	Tomcat Server	Tomcat Server [System Created] - 43020	Yes	10.10.32.1	1	11/10/201	System	Active
6	Global Default Network	Tomcat Server	Tomcat Server [System Created] - 43021	Yes	10.10.32.1	1	11/10/201	System	Active
7	Global Default Network	Unix	Unix	No	10.10.26.1	4	11/08/201	prerna ne	Active
8	Global Default Network	IBM WebSphere	IBM WebSphere App Server [System Created]	Yes	10.10.35.2	1	11/07/201	System	Active

## Make Records Inactive

You can make any Tomcat Server authentication record inactive. Inactive records are not included in scans (even if the "Include system created authentication records in scans" option is selected in the option profile). Simply choose the records you want to make Inactive and pick Deactivate from the Actions menu above the data list. To activate records choose Activate.



## Want to know more?

Search the help for "System Authentication Records". For details on API changes, please see the Qualys API Release Notes.

# Qualys Vulnerability Management (VM)

## View CVSS3 Vector Strings in Scan Reports

The scan reports will now display the CVSS3 base and temporal vector strings along with the CVSS2 base and temporal vector strings. Vector strings helps to process CVSS metrics for the various compliance programs.

You'll only see CVSS scores and vector strings in the subscription when CVSS Scoring is enabled by a Manager user.

Asset Group	IPs	Total Vuln	Avg Security Risk	Total Vulnerabilities
NONE	10.10.23.84,10.10.36.22-10.10.36.23,10.11.65.152,10.11.65.185-10.11.65.186,10.113.196.80	809	3.5	
P				
10.10.36.2				13
10.11.65.1				8
10.11.65.1				1
10.10.23.8				234
10.11.65.1				295
10.11.65.1				20
10.113.196				238

QID	Title	Vuln St	Type	Severity	Port	CVSS Base	CVSS Temporal	CVSS Et	CVSS3	CVSS3 Base	CVSS3 Temporal
370375	Mozilla Fii Active	Vuln		5		7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)	5.9 (E:POC/RL:OF/RC:C)	Asset Groi	8.4	9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	8.8 (E:P/RL:O/RC:C)
370371	Oracle Jav Active	Vuln		5		5.1 (AV:N/AC:H/Au:N/C:P/I:P/A:P)	3.8 (E:U/RL:OF/RC:C)	Asset Groi	7.2	8.3 (AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H)	7.2 (E:U/RL:O/RC:C)
370341	Mozilla Fii Active	Vuln		5		7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)	5.5 (E:U/RL:OF/RC:C)	Asset Groi	8.4	9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	8.5 (E:U/RL:O/RC:C)
370325	Mozilla Fii Active	Vuln		5		10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)	7.8 (E:POC/RL:OF/RC:C)	Asset Groi	8.4	9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	8.8 (E:P/RL:O/RC:C)
370297	Microsoft Active	Vuln		5		9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)	7.3 (E:POC/RL:OF/RC:C)	Asset Groi	7.4	8.1 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)	7.3 (E:P/RL:O/RC:C)
370289	Mozilla Fii Active	Vuln		5		7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)	5.9 (E:POC/RL:OF/RC:C)	Asset Groi	8.4	9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	8.8 (E:P/RL:O/RC:C)
370280	Oracle Jav Active	Vuln		5		6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)	5.9 (E:POC/RL:OF/RC:C)	Asset Groi	8.4	9.6 (AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H)	8.6 (E:P/RL:O/RC:C)
370264	Mozilla Fii Active	Vuln		5		7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)	5.9 (E:POC/RL:OF/RC:C)	Asset Groi	8.4	9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	8.8 (E:P/RL:O/RC:C)
370245	Mozilla Fii Active	Vuln		5		5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)	4.4 (E:H/RL:OF/RC:C)	Asset Groi	7.2	7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)	7.2 (E:H/RL:O/RC:C)
370225	Mozilla Fii Active	Vuln		5		7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)	5.5 (E:U/RL:OF/RC:C)	Asset Groi	8.4	9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	8.5 (E:U/RL:O/RC:C)
370161	Oracle Jav Active	Vuln		5		9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)	6.9 (E:U/RL:OF/RC:C)	Asset Groi	8.4	9.6 (AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H)	8.3 (E:U/RL:O/RC:C)
370141	Mozilla Fii Active	Vuln		5		7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)	5.5 (E:U/RL:OF/RC:C)	Asset Groi	8.4	9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	8.5 (E:U/RL:O/RC:C)
124192	Mozilla Fii Active	Vuln		5		7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)	5.5 (E:U/RL:OF/RC:C)	Asset Groi	8.5	9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	8.5 (E:U/RL:O/RC:C)

You can see the CVSS3 base and temporal vector string on the Info/ Edit Vulnerability window for all QIDs that have a CVSS3 score.

Vulnerability Information - QID 38623

Launch Help

General Information

Details

Software

Threat

Impact

Solution

Exploitability

Associated Malware

Search Lists

Compliance

Change Log

Details

QID: 38623

Category: General remote services

CVE ID: [CVE-2016-3115](#)

Vendor Reference: [OpenSSH 7.2p2](#)

Bugtraq ID: [84314](#)

Patch Available: Yes

Virtual Patch Available: No

Detection Information

PCI Reasons: Reasons for failing PCI compliance are below.

[The QID adheres to the PCI requirements based on the CVSS base score.](#)

Supported Modules: VM, CA-Linux Agent, CA-Mac Agent

CVSS Base: 5.5 AV:N/AC:L/Au:S/C:P/I:P/A:N

CVSS Temporal: 4.3 E:POC/RL:OF/RC:C

CVSS Access Vector: Network

CVSS3 Base: 6.4 AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:I/A:N

CVSS3 Temporal: 5.8 E:P/RL:O/RC:C

Close

Edit

## HashiCorp Vaults now Supported in DB Auth Records

We've now extended the support for HashiCorp vaults to all database auth records. You can now configure authentication records for Oracle, MS SQL, MySQL, MariaDB, Sybase, PostgreSQL, MongoDB and DB2 to use HashiCorp vaults.

Authentication records for Windows, Unix and Cisco are already supported.

### Configure authentication records

The HashiCorp vault is now supported in Oracle, MS SQL, MySQL, MariaDB, Sybase, PostgreSQL, MongoDB and DB2 along with Cisco, Windows and Unix authentication records. Here's a sample MS SQL Server record with the vault selected.

The screenshot shows the 'New MS SQL Server Record' configuration form. The 'Login Credentials' tab is selected. Under 'Authentication Type', 'Database' is chosen. In the 'Database Information' section, 'Vault Type' is set to 'HashiCorp' (highlighted with a red box). Other fields include 'Instance' (MSSQLSERVER), 'Database' (master), 'Port' (1311), 'Vault Title' (Test-Hashi), 'Path' (secret), 'Name' (hashi\_1), and 'Key' (hashi\_1\_key).

Provide these settings:

#### **Vault Type**

HashiCorp

#### **Vault Title**

Your vault record.

#### **Path**

The path of the secret engine.  
The default is "secret".

#### **Name**

The secret name which stores the key-value pairs.

#### **Key**

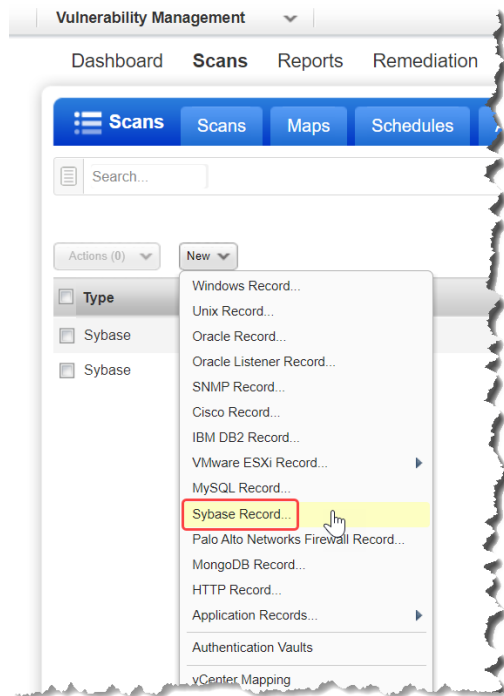
The key name for identifying a specific key-value pair.

## Sybase Authentication is Now Supported in VM

Sybase authentication was already supported for PC and now it's also supported in VM for vulnerability scanning.

### How do I get started?

Go to Scans > Authentication and choose Sybase Record. We'll authenticate to each target host using the credentials provided in the Sybase record.



### VM Scan Option Profile

You'll be able to select Sybase under Authentication while creating an option profile. You can launch a VM scan using an option profile with Sybase authentication selected along with Unix and/or Windows.

**Authentication**

Authentication enables the scanner to log into hosts at scan time to extend detection capabilities. See the online help to learn how to configure this option.

- ☒ Windows
- ☒ Unix/Cisco
- ☐ Oracle
- ☐ Oracle Listener
- ☐ SNMP
- ☐ VMware
- ☐ DB2
- ☐ HTTP
- ☐ MySQL
- ☐ Tomcat Server
- ☐ MongoDB
- ☐ Palo Alto Networks Firewall
- ☐ Oracle WebLogic Server
- ☐ Jboss Server
- ☒ Sybase

## Issues Addressed

- The LAN IP column on the Scans > Appliances data list will now be sorted in numerical order.
- We fixed an issue where VM was not sending details about closed ports to AssetView after a custom scan, causing a discrepancy in the open ports reported between VM and AssetView.
- We fixed an issue in Compliance Report. When the host OS changed in a successive scan, the user saw old host OS details in the Compliance Report host statistics section. Now, after this fix, the user will see the new OS details in the report.
- Fixed an issue where the IP 128.0.0.0 appeared in XML Scan Report under the NO\_VULNS IP list when this IP was not included in the scan.
- We removed trailing spaces between columns in the headers for the Authentication Report and Compliance Scorecard Report in CSV format.
- Now customer will not see the discrepancy in diff types of Detection Method. Now if detection method is "Authenticated only" it will not show the "Remote discovery" in the Quick link.
- We fixed an issue where the wrong page name appeared on the browser tab when on the PC > Reports > Policy Summary page. Now Policy Summary will appear on the browser tab.
- We fixed an issue where QIDs with the Half-Yellow and Half-Red severity icon had vulnerability type "Potential Vulnerability" when you viewed vulnerability information in the UI when this should be type "Vulnerability or Potential Vulnerability". The API showed the correct type.
- Fixed an issue where controls set to "Undefined" in a policy by a user reverted to the system-defined criticality in the Policy Report.
- Fixed a validation issue in Tomcat authentication records where the same Home Path could not be used in multiple Tomcat authentication records. This is needed to support multiple instances.
- Fixed an issue where control criticality was not showing up in Policy Reports in PDF format when the report was grouped by control.
- Fixed an issue in Policy Report in CSV format where an extra comma was removed after "Qualys Host ID" on the RESULTS header.
- We made performance improvements to the VM > Remediation > Tickets data list.
- Updated the Qualys VM-PC API User Guide to include a Best Practices section to help reduce the amount of data being retrieved by the compliance posture API.
- We have updated the online help to rectify the EC2 connector sync cycle value to 4 hours.