Qualys 8.7 Release Notes

This new release of the Qualys Cloud Suite of Security and Compliance Applications includes improvements to Vulnerability Management and Policy Compliance.

Qualys Cloud Platform

Qualys Vulnerability Management (VM)

Qualys Policy Compliance (PC/SCAP)

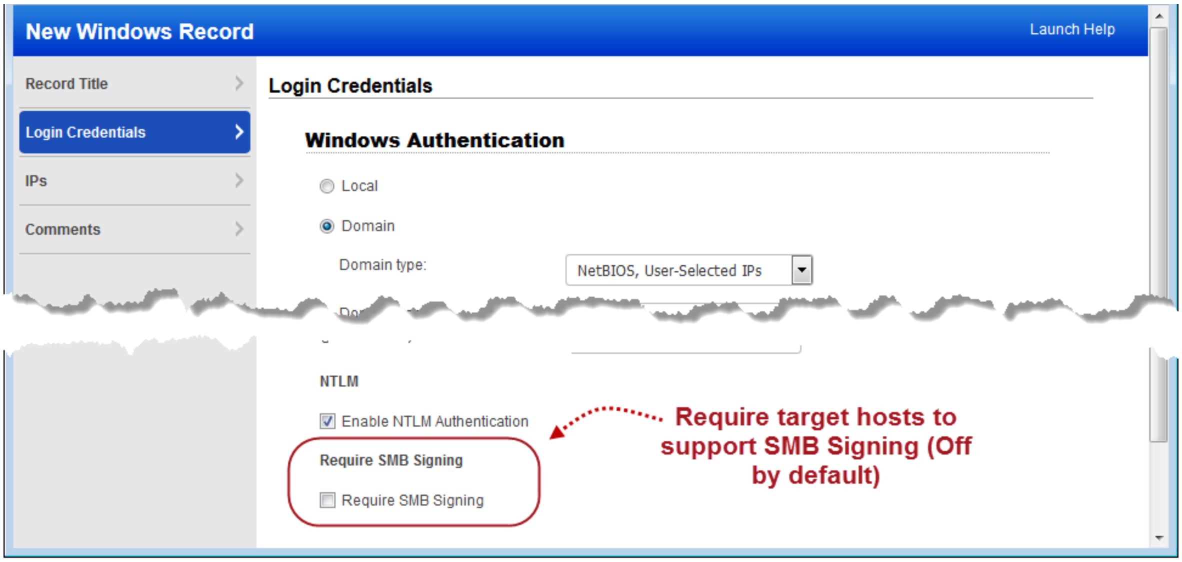
Qualys API Enhancements

Qualys Cloud Platform

Require SMB Signing for Windows Authentication

You’ll see the new “Require SMB Signing” option in your Windows authentication records. This option is unchecked by default, meaning SMB signing is not required. This is the recommended setting. When unchecked, we can authenticate to any Windows version regardless of how SMB signing is configured on the target. You are not protected, however, against man-in-the-middle (MITM) attacks.

If you select this option in your record, we will require each Windows target to support SMB signing, whether configured through Local Policy or Group Policy. If SMB signing is disabled on a target host, authentication will fail and the host will not be scanned. This option protects against MITM attacks but we won’t be able to authenticate to some hosts.



Login Credentials

Windows Authentication

○ Local

● Domain

Domain type: NetBIOS, User-Selected IPs

NTLM

☑ Enable NTLM Authentication

Require SMB Signing

□ Require SMB Signing

Require target hosts to support SMB Signing (Off by default)

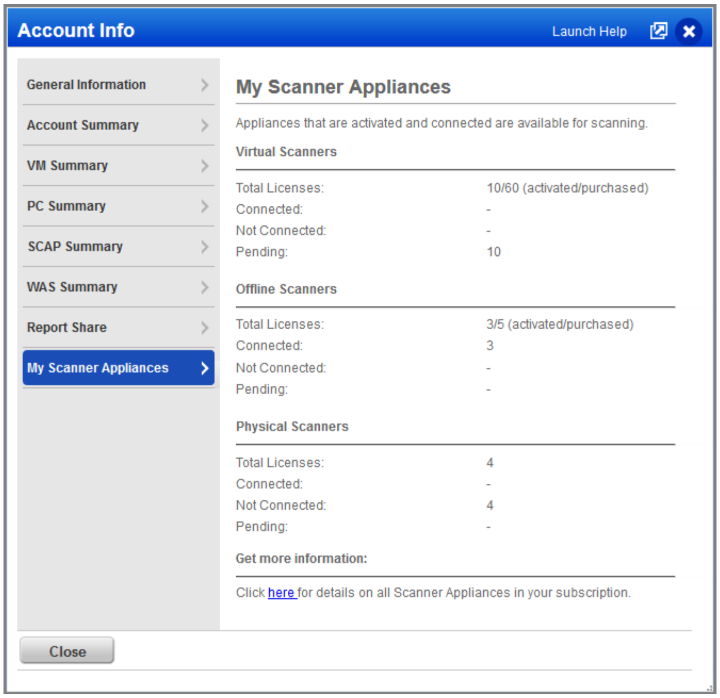
SAML Support for SHA256 Signature Algorithm

Using SAML SSO? You now have the option to use the SHA256 signature algorithm when connecting from the Qualys Cloud Platform to your IdP. We’ll continue to use SHA1. Contact your Technical Account Manager or Qualys Support to switch to SHA256.

View Scanner License Count

You can now easily track scanner licenses for your account.

Go to Help > Account Info and choose the My Scanner Appliances tab. We'll show you how many of your purchased licenses are activated for virtual, offline and physical scanner appliances.



My Scanner Appliances

Appliances that are activated and connected are available for scanning.

Virtual Scanners

Total Licenses:	10/60 (activated/purchased)
Connected:	-
Not Connected:	-
Pending:	10

Offline Scanners

Total Licenses:	3/5 (activated/purchased)
Connected:	3
Not Connected:	-
Pending:	-

Physical Scanners

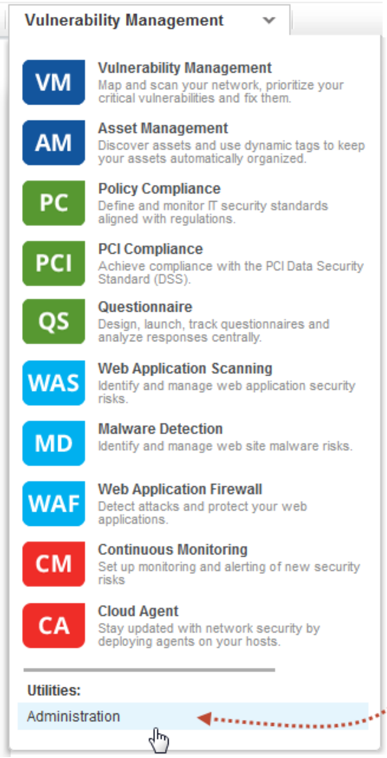
Total Licenses:	4
Connected:	-
Not Connected:	4
Pending:	-

Get more information:

Click here for details on all Scanner Appliances in your subscription.

Administration Utility in the Module Picker

Use the Administration utility to view and manage users with access to certain applications like AM, WAS, WAF, MD, CM, etc. This option was not visible from the VM and PC applications in previous releases.



Vulnerability Management: Map and scan your network, prioritize your critical vulnerabilities and fix them.

Asset Management: Discover assets and use dynamic tags to keep your assets automatically organized.

Policy Compliance: Define and monitor IT security standards aligned with regulations.

PCI Compliance: Achieve compliance with the PCI Data Security Standard (DSS).

Questionnaire: Design, launch, track questionnaires and analyze responses centrally.

Web Application Scanning: Identify and manage web application security risks.

Malware Detection: Identify and manage web site malware risks.

Web Application Firewall: Detect attacks and protect your web applications.

Continuous Monitoring: Set up monitoring and alerting of new security risks

Cloud Agent: Stay updated with network security by deploying agents on your hosts.

Click here to jump to the Admin utility

Qualys Vulnerability Management (VM)

Quickly Identify SHA1 Certificates

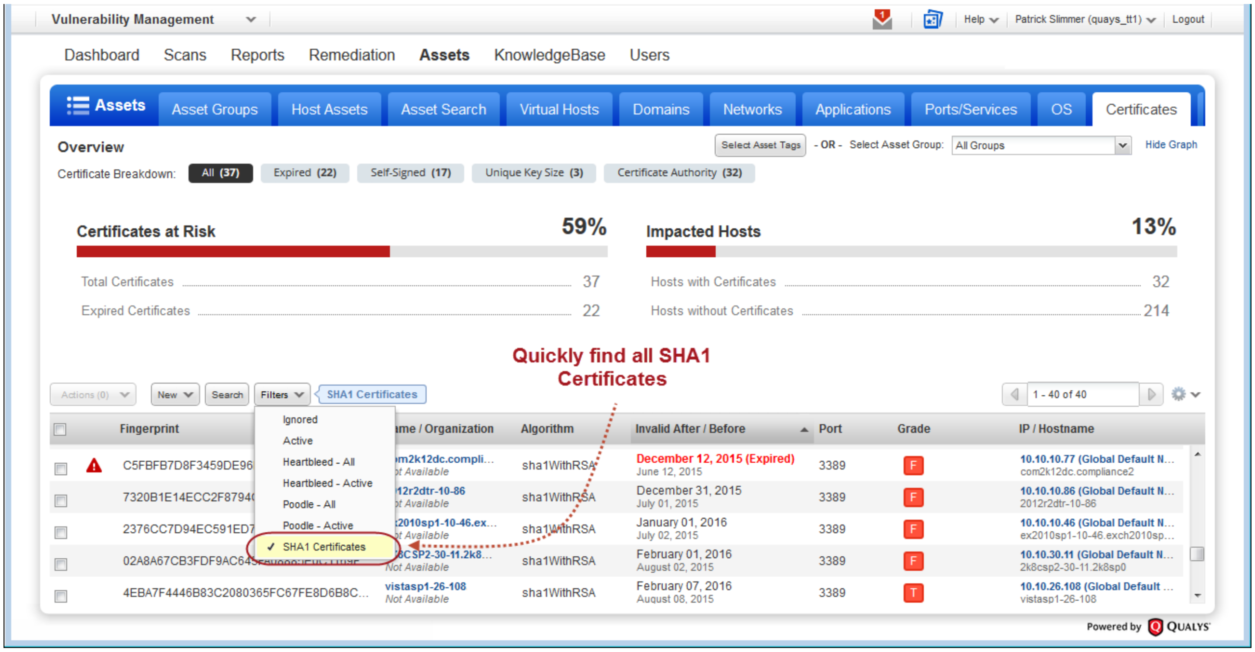
SHA1 is being deprecated so it's critical that any new certificates installed on the hosts in your environment use SHA256 and that existing SHA1 certificates are replaced. Our easy to search certificates inventory will help you with this task.

From the Community

SHA1 Deprecation: What You Need to Know

How do I find my SHA1 certificates?

We've made this easy for you. Go to VM > Assets > Certificates and choose the SHA1 Certificates filter. We'll list all hosts with SHA1 certificates installed.



Overview

Select Asset Group: All Groups

Certificate Breakdown: All (37) | Expired (22) | Self-Signed (17) | Unique Key Size (3) | Certificate Authority (32)

Certificates at Risk 59%

Total Certificates 37

Expired Certificates 22

Impacted Hosts 13%

Hosts with Certificates 32

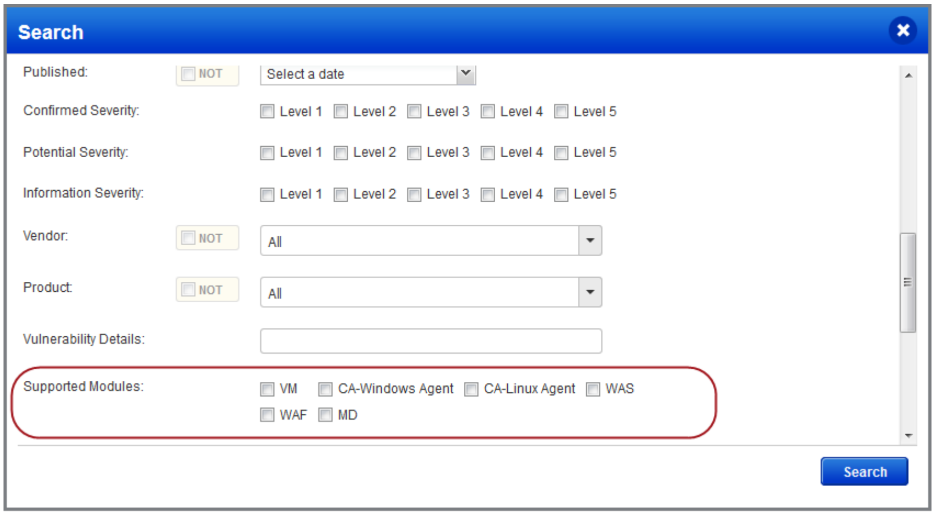
Hosts without Certificates 214

Quickly find all SHA1 Certificates

☐		Fingerprint	…ame / Organization	Algorithm	Invalid After / Before	Port	Grade	IP / Hostname
☐	⚠	C5FBFB7D8F3459DE96…	…m2k12dc.compli… …ot Available	sha1WithRSA	December 12, 2015 (Expired) June 12, 2015	3389	F	10.10.10.77 (Global Default N… com2k12dc.compliance2
☐		7320B1E14ECC2F8794…	…12r2dtr-10-86 …ot Available	sha1WithRSA	December 31, 2015 July 01, 2015	3389	F	10.10.10.86 (Global Default N… 2012r2dtr-10-86
☐		2376CC7D94EC591ED7…	…2010sp1-10-46.ex… …ot Available	sha1WithRSA	January 01, 2016 July 02, 2015	3389	F	10.10.10.46 (Global Default N… ex2010sp1-10-46.exch2010sp…
☐		02A8A67CB3FDF9AC64…	…8CSP2-30-11.2k8… Not Available	sha1WithRSA	February 01, 2016 August 02, 2015	3389	F	10.10.30.11 (Global Default N… 2k8csp2-30-11.2k8sp0
☐		4EBA7F4446B83C2080365FC67FE8D6B8C…	vistasp1-26-108 Not Available	sha1WithRSA	February 07, 2016 August 08, 2015	3389	T	10.10.26.108 (Global Default … vistasp1-26-108

Easily Identify Vulnerabilities Supported by Module

Find out what vulnerabilities in our KnowledgeBase are supported by different Qualys modules – VM, Cloud Agent, WAS, WAF and MD. Use the KnowledgeBase Search option to identify vulnerabilities that can be detected by VM scans, Windows Cloud Agent and Linux Cloud Agent plus more. Note – These same options appear when selecting list criteria for dynamic search lists.



Published: □ NOT Select a date

Confirmed Severity: □ Level 1 □ Level 2 □ Level 3 □ Level 4 □ Level 5

Potential Severity: □ Level 1 □ Level 2 □ Level 3 □ Level 4 □ Level 5

Information Severity: □ Level 1 □ Level 2 □ Level 3 □ Level 4 □ Level 5

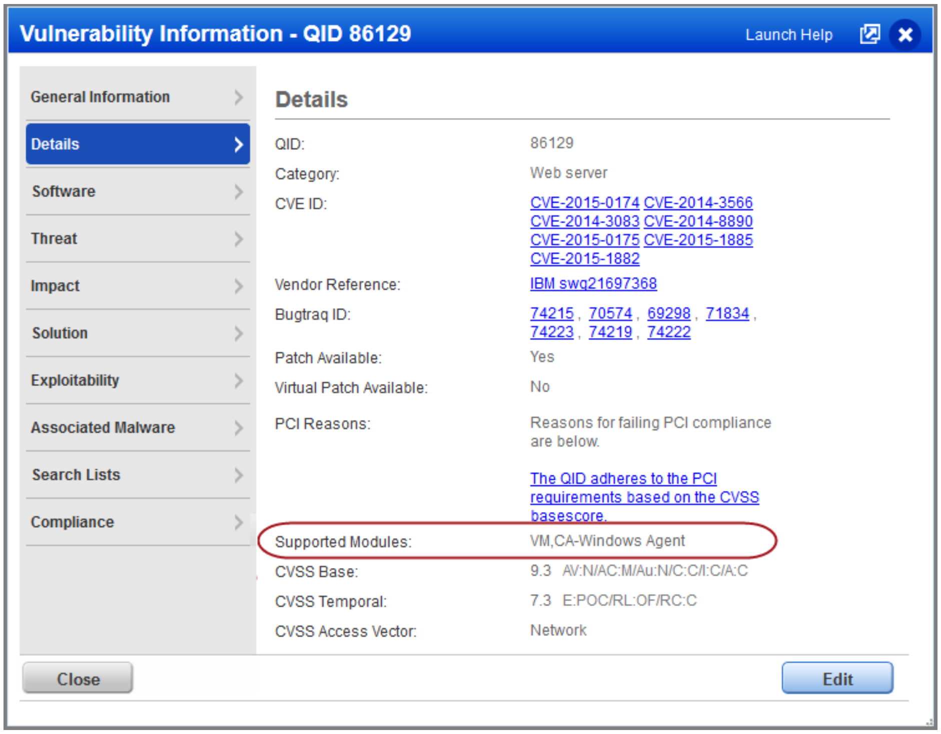
Vendor: □ NOT All

Product: □ NOT All

Vulnerability Details:

Supported Modules: □ VM □ CA-Windows Agent □ CA-Linux Agent □ WAS □ WAF □ MD

We’ve added a supported modules section to the vulnerability (QID) information, and this is where you’ll see the Qualys modules that may be used to detect each QID. For example, QID 86129 can be detected by a vulnerability scan and also by a Windows Cloud Agent.

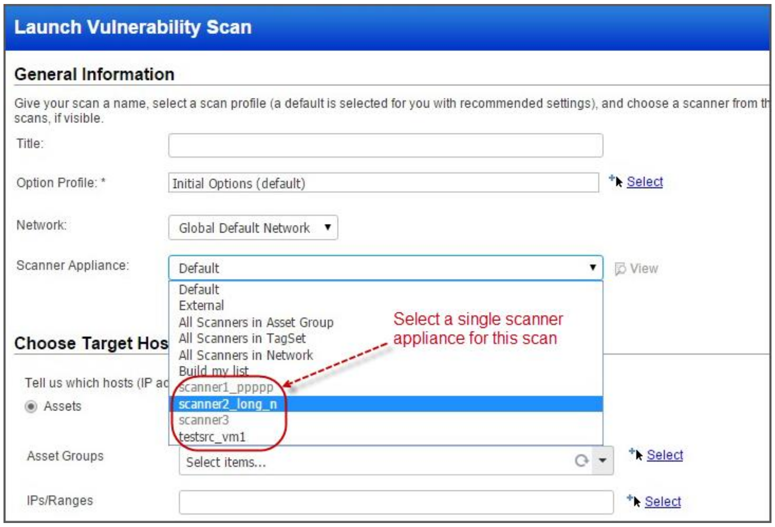


Details

QID:	86129
Category:	Web server
CVE ID:	CVE-2015-0174 CVE-2014-3566 CVE-2014-3083 CVE-2014-8890 CVE-2015-0175 CVE-2015-1885 CVE-2015-1882
Vendor Reference:	IBM swg21697368
Bugtraq ID:	74215 , 70574 , 69298 , 71834 , 74223 , 74219 , 74222
Patch Available:	Yes
Virtual Patch Available:	No
PCI Reasons:	Reasons for failing PCI compliance are below. The QID adheres to the PCI requirements based on the CVSS basescore.
Supported Modules:	VM,CA-Windows Agent
CVSS Base:	9.3 AV:N/AC:M/Au:N/C:C/I:C/A:C
CVSS Temporal:	7.3 E:POC/RL:OF/RC:C
CVSS Access Vector:	Network

Select Single Scanner Appliance for Scans

Quickly select a single scanner appliance for your internal vulnerability and compliance scans (PC and SCAP). We'll show all available scanners in the scanner appliance list so you don't have to use the Build my list option.



Launch Vulnerability Scan

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 th scans, if visible.

Title:

Option Profile: * Initial Options (default)

Network: Global Default Network

Scanner Appliance: Default

Select a single scanner appliance for this scan

Choose Target Hos

Tell us which hosts (IP ac

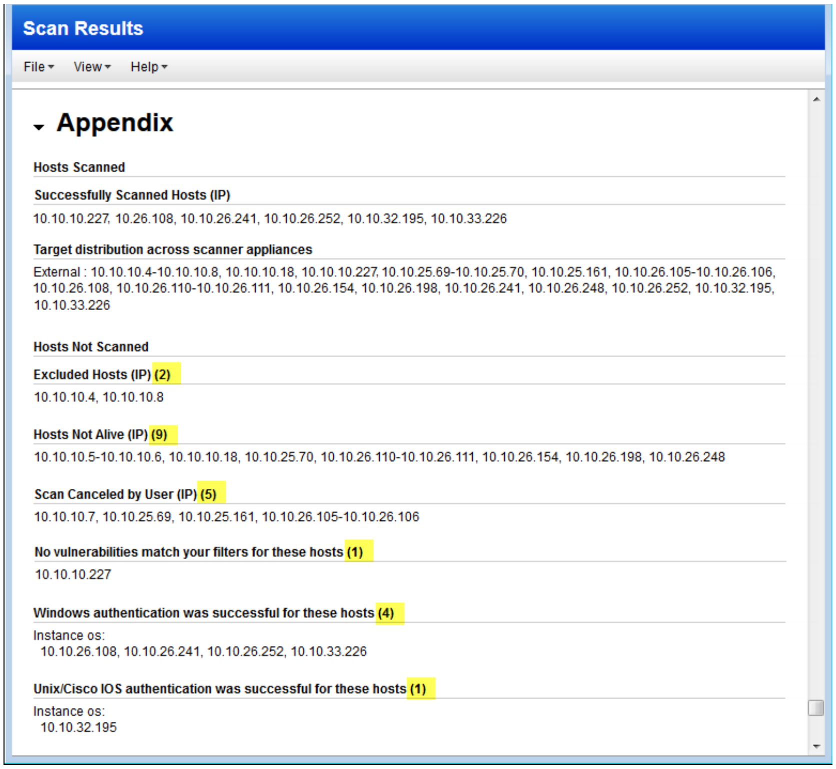
● Assets

Asset Groups: Select items...

IPs/Ranges

Host Counts Added to Scan Results Appendix

See at-a-glance the number of hosts that were scanned / not scanned for various reasons. Host counts appear in the Appendix section of your vulnerability scan results, as shown in this sample report.



Scan Results

Appendix

Hosts Scanned

Successfully Scanned Hosts (IP)

10.10.10.227, 10.26.108, 10.10.26.241, 10.10.26.252, 10.10.32.195, 10.10.33.226

Target distribution across scanner appliances

External : 10.10.10.4-10.10.10.8, 10.10.10.18, 10.10.10.227, 10.10.25.69-10.10.25.70, 10.10.25.161, 10.10.26.105-10.10.26.106, 10.10.26.108, 10.10.26.110-10.10.26.111, 10.10.26.154, 10.10.26.198, 10.10.26.241, 10.10.26.248, 10.10.26.252, 10.10.32.195, 10.10.33.226

Hosts Not Scanned

Excluded Hosts (IP) (2)

10.10.10.4, 10.10.10.8

Hosts Not Alive (IP) (9)

10.10.10.5-10.10.10.6, 10.10.10.18, 10.10.25.70, 10.10.26.110-10.10.26.111, 10.10.26.154, 10.10.26.198, 10.10.26.248

Scan Canceled by User (IP) (5)

10.10.10.7, 10.10.25.69, 10.10.25.161, 10.10.26.105-10.10.26.106

No vulnerabilities match your filters for these hosts (1)

10.10.10.227

Windows authentication was successful for these hosts (4)

Instance os:
10.10.26.108, 10.10.26.241, 10.10.26.252, 10.10.33.226

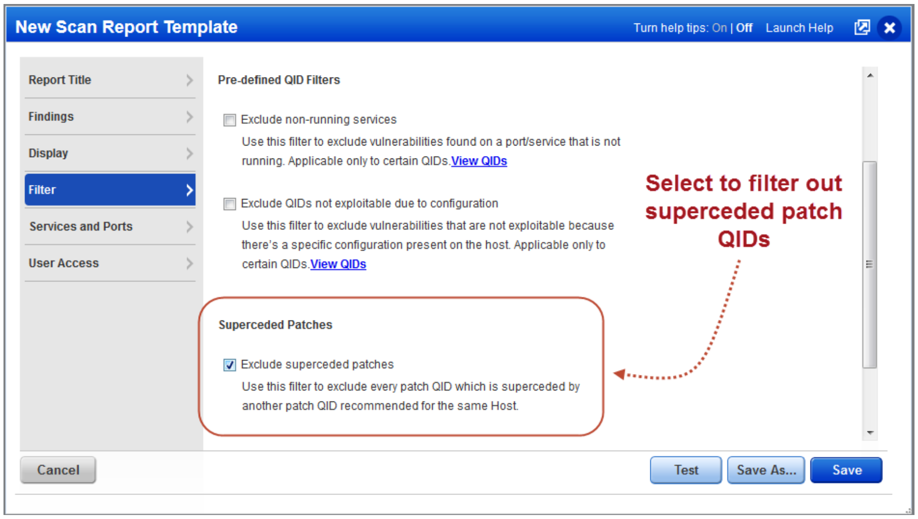
Unix/Cisco IOS authentication was successful for these hosts (1)

Instance os:
10.10.32.195

Scan Reports – Exclude Superceded Patches

We've integrated some of the patch report functionality into your scan reports by introducing a new filter for superceded patches. With this option enabled, we'll report only the recommended patches for each host and filter out patches that have been superceded.

How it works – A missing patch is identified by a QID like any other vulnerability. We'll report all missing patches (even those that have been superceded by newer patches) unless you select this option.



Pre-defined QID Filters

□ Exclude non-running services

Use this filter to exclude vulnerabilities found on a port/service that is not running. Applicable only to certain QIDs. View QIDs

□ Exclude QIDs not exploitable due to configuration

Use this filter to exclude vulnerabilities that are not exploitable because there's a specific configuration present on the host. Applicable only to certain QIDs. View QIDs

Superceded Patches

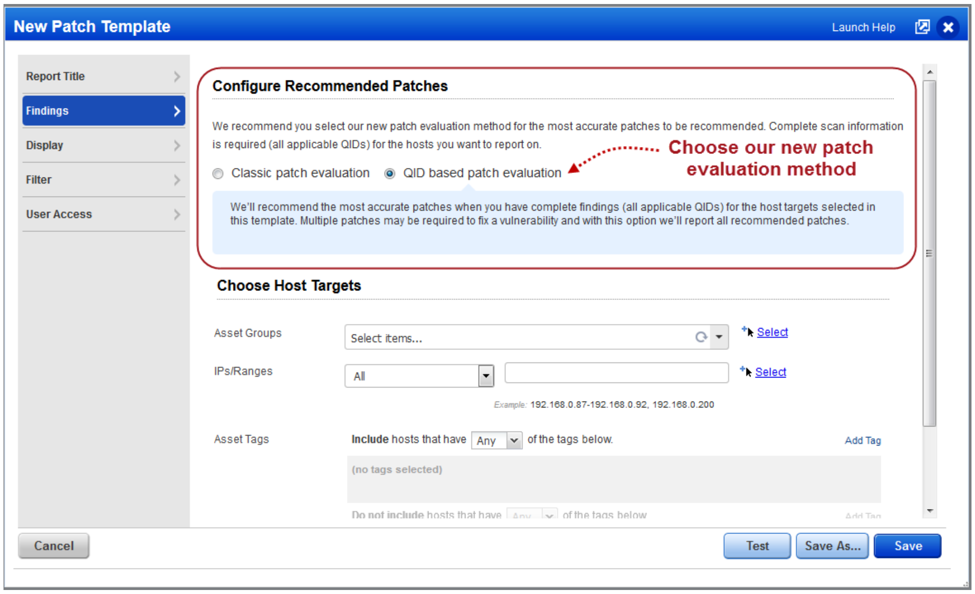
☑ Exclude superceded patches

Use this filter to exclude every patch QID which is superceded by another patch QID recommended for the same Host.

Select to filter out superceded patch QIDs

Patch Reports – New Patch Evaluation Method

Get the most accurate patch recommendations by selecting our new patch evaluation method in your patch report template. This new method works when you have complete scan findings (all applicable QIDs) for your target hosts. We'll determine the best patches to recommend based on the QIDs detected on each host. Also, when multiple patches are required to fix a vulnerability you'll now see multiple patches recommended in your report. This way you have all the information you need in one report.



Configure Recommended Patches

We recommend you select our new patch evaluation method for the most accurate patches to be recommended. Complete scan information is required (all applicable QIDs) for the hosts you want to report on.

○ Classic patch evaluation ● QID based patch evaluation

Choose our new patch evaluation method

We'll recommend the most accurate patches when you have complete findings (all applicable QIDs) for the host targets selected in this template. Multiple patches may be required to fix a vulnerability and with this option we'll report all recommended patches.

Choose Host Targets

Asset Groups: Select items... Select

IPs/Ranges: All Select

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

Asset Tags: **Include** hosts that have Any of the tags below. Add Tag

(no tags selected)

Do not include hosts that have Any of the tags below Add Tag

Prefer our old method or don't have complete scan findings?

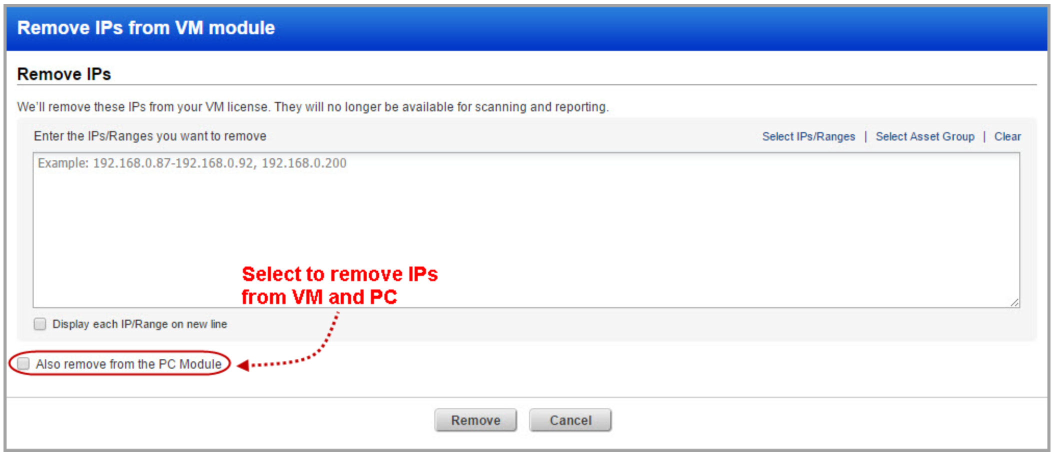
No problem. The Classic evaluation method is for you.

Ability to Remove Host IPs from the VM module only

You'll notice we've improved the Remove IPs wizard in the VM module (under Assets > Host Assets > New > Remove IPs). You'll enter host IP addresses/ranges you want to remove from your subscription in the field provided, as before. Now these IPs will be removed from the VM module only by default. If you want to remove IPs from your PC module too, be sure to select "Also remove from the PC module".

Good to know

- Once IPs have been removed, they will no longer be available for scanning and reporting.
- Host IPs with agents installed will not be removed (i.e. hosts with Agent tracking method).



Remove IPs from VM module

Remove IPs

We'll remove these IPs from your VM license. They will no longer be available for scanning and reporting.

Enter the IPs/Ranges you want to remove

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

Select to remove IPs from VM and PC

□ Display each IP/Range on new line

□ Also remove from the PC Module

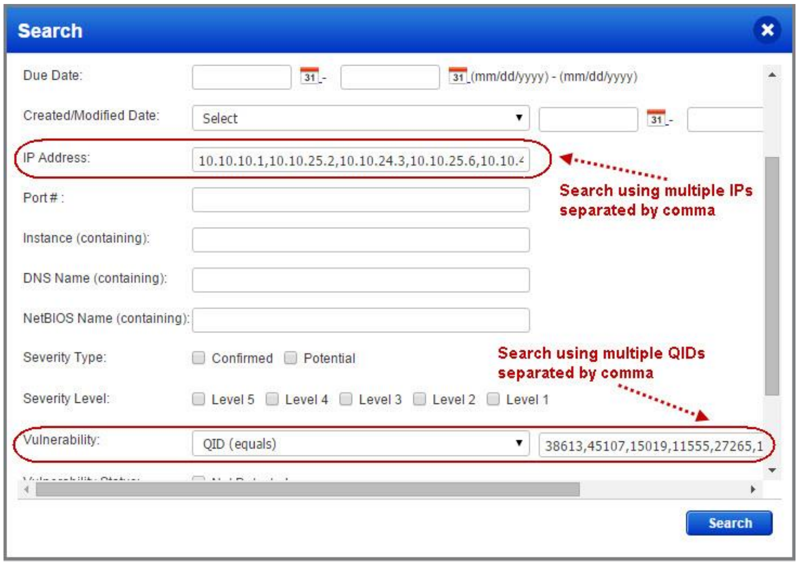
Improvements to scan reports with trending

We've updated template based scan reports in CSV format, created using a template with trending option enabled. These changes apply when the report template includes Fixed vulnerabilities (Findings > Vulnerability Filters):

- Reports include vulnerabilities fixed in the timeframe selected
- A new Date Last Fixed column appears in the CSV output

Improved Remediation Ticket Search

With this release, you can search for remediation tickets associated with multiple hosts and/or multiple vulnerabilities. The search window (Remediation > Tickets > Search) lets you enter multiple IP addresses and QIDs in the fields provided. You can specify multiple IPs or QIDs separated by a comma.



Search

Due Date: (mm/dd/yyyy) - (mm/dd/yyyy)

Created/Modified Date: Select

IP Address: 10.10.10.1,10.10.25.2,10.10.24.3,10.10.25.6,10.10.4

Search using multiple IPs separated by comma

Port # :

Instance (containing):

DNS Name (containing):

NetBIOS Name (containing):

Severity Type: □ Confirmed □ Potential

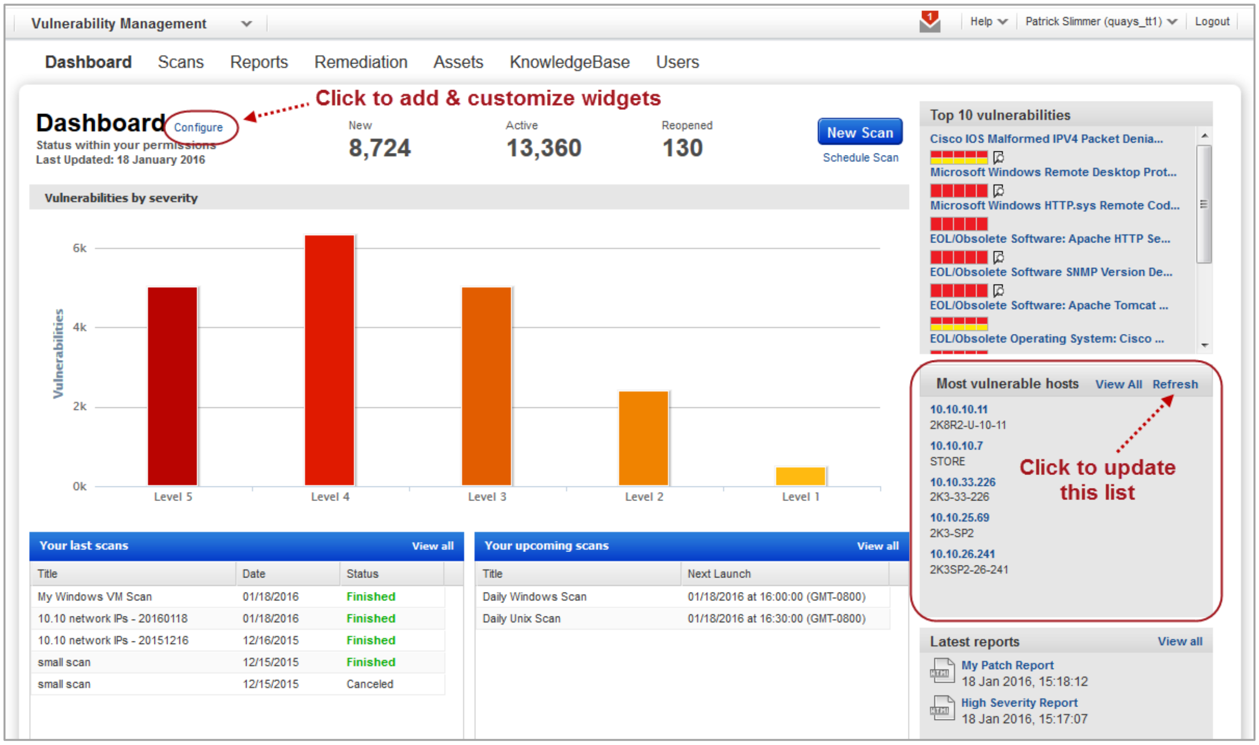
Severity Level: □ Level 5 □ Level 4 □ Level 3 □ Level 2 □ Level 1

Search using multiple QIDs separated by comma

Vulnerability: QID (equals) 38613,45107,15019,11555,27265,1

New Refresh Option for Most Vulnerable Hosts List

Click Refresh to instantly update the Most Vulnerable Hosts list on your Dashboard. This is especially useful when there have been changes made to the assets assigned to you or your business unit. Not seeing the Most Vulnerable Hosts list? Click the Configure link to add & customize this widget.



Dashboard
Status within your permissions
Last Updated: 18 January 2016

New	Active	Reopened
8,724	13,360	130

Top 10 vulnerabilities

- Cisco IOS Malformed IPV4 Packet Denia...
- Microsoft Windows Remote Desktop Prot...
- Microsoft Windows HTTP.sys Remote Cod...
- EOL/Obsolete Software: Apache HTTP Se...
- EOL/Obsolete Software SNMP Version De...
- EOL/Obsolete Software: Apache Tomcat ...
- EOL/Obsolete Operating System: Cisco ...

Most vulnerable hosts

10.10.10.11	2K8R2-U-10-11
10.10.10.7	STORE
10.10.33.226	2K3-33-226
10.10.25.69	2K3-SP2
10.10.26.241	2K3SP2-26-241

Your last scans

Title	Date	Status
My Windows VM Scan	01/18/2016	Finished
10.10 network IPs - 20160118	01/18/2016	Finished
10.10 network IPs - 20151216	12/16/2015	Finished
small scan	12/15/2015	Finished
small scan	12/15/2015	Canceled

Your upcoming scans

Title	Next Launch
Daily Windows Scan	01/18/2016 at 16:00:00 (GMT-0800)
Daily Unix Scan	01/18/2016 at 16:30:00 (GMT-0800)

Latest reports

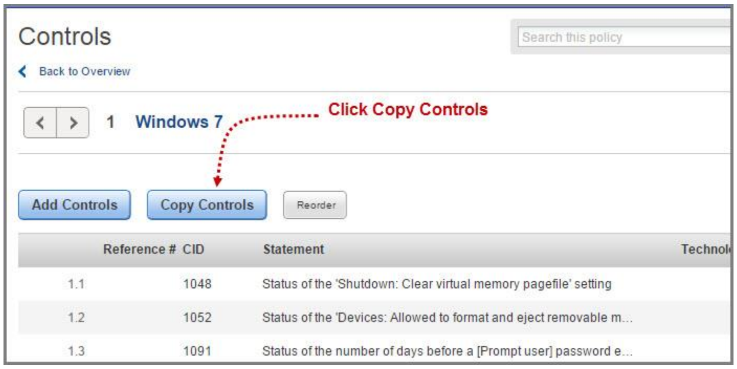
- My Patch Report 18 Jan 2016, 15:18:12
- High Severity Report 18 Jan 2016, 15:17:07

Qualys Policy Compliance (PC)

Copy Control Settings

Adding controls to a policy? You can now save time by copying controls already defined in another policy. We'll add them to your policy and copy over the control settings in 3-easy steps:

Click Copy Controls in a new section or existing section in your policy.



Controls

Search this policy

Back to Overview

1 Windows 7

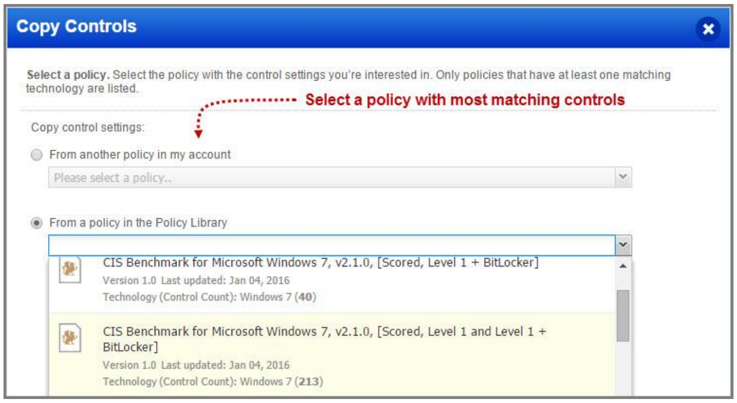
Click Copy Controls

Add Controls | Copy Controls | Reorder

Reference #	CID	Statement	Technol
1.1	1048	Status of the 'Shutdown: Clear virtual memory pagefile' setting	
1.2	1052	Status of the 'Devices: Allowed to format and eject removable m...	
1.3	1091	Status of the number of days before a [Prompt user] password e...	

Tell us which policy has the controls you're looking for.

You'll notice that you can select another policy in your account or a policy in the Library. We only list the policies that have at least one matching technology.



Copy Controls

Select a policy. Select the policy with the control settings you're interested in. Only policies that have at least one matching technology are listed.

Select a policy with most matching controls

Copy control settings:

○ From another policy in my account

Please select a policy..

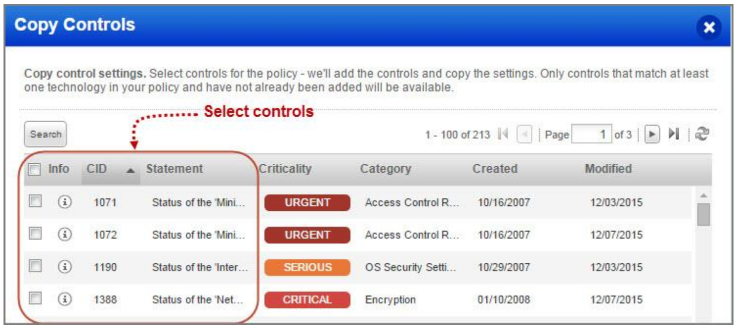
● From a policy in the Policy Library

CIS Benchmark for Microsoft Windows 7, v2.1.0, [Scored, Level 1 + BitLocker]
Version 1.0 Last updated: Jan 04, 2016
Technology (Control Count): Windows 7 (**40**)

CIS Benchmark for Microsoft Windows 7, v2.1.0, [Scored, Level 1 and Level 1 + BitLocker]
Version 1.0 Last updated: Jan 04, 2016
Technology (Control Count): Windows 7 (**213**)

Select the controls you want to copy, and click Copy. You can pick service-defined controls (non-deprecated) and user-defined controls.

That's it! The controls and their settings are added to your policy.



Copy Controls

Copy control settings. Select controls for the policy - we'll add the controls and copy the settings. Only controls that match at least one technology in your policy and have not already been added will be available.

Select controls

Search

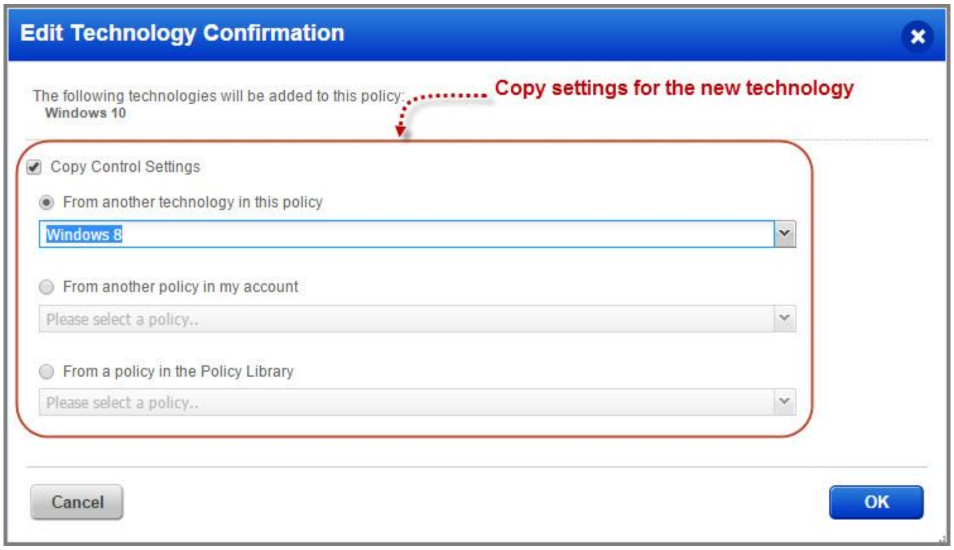
1 - 100 of 213 | Page 1 of 3

□	Info	CID	Statement	Criticality	Category	Created	Modified
□	ⓘ	1071	Status of the 'Mini...	URGENT	Access Control R...	10/16/2007	12/03/2015
□	ⓘ	1072	Status of the 'Mini...	URGENT	Access Control R...	10/16/2007	12/07/2015
□	ⓘ	1190	Status of the 'Inter...	SERIOUS	OS Security Setti...	10/29/2007	12/03/2015
□	ⓘ	1388	Status of the 'Net...	CRITICAL	Encryption	01/10/2008	12/07/2015

Copy settings from one Technology to another

Similarly, when you add a new technology to your policy, you can copy control settings from 1) another technology in the same policy, 2) another policy in your account or 3) a policy in the Library.

For example, let's say you're adding Windows 10 to your policy and you choose to copy settings from another technology like Windows 8. We will apply settings from all applicable Windows 8 controls to Windows 10 controls.



Edit Technology Confirmation

The following technologies will be added to this policy:
Windows 10

☑ Copy Control Settings

● From another technology in this policy

Windows 8

○ From another policy in my account

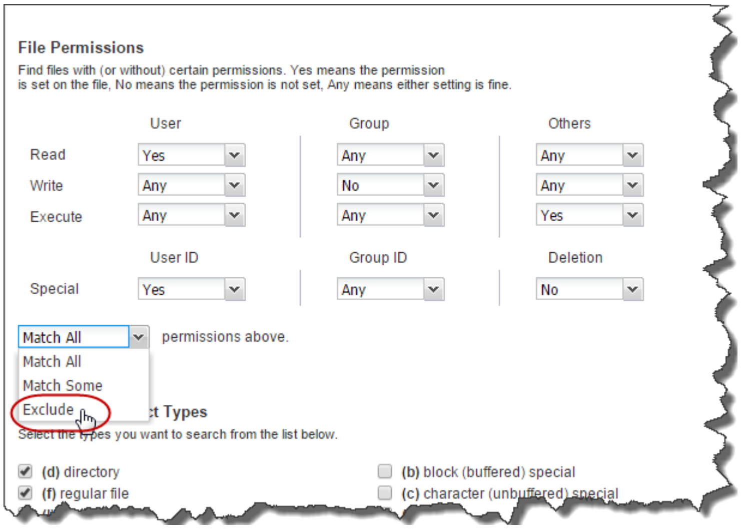
Please select a policy..

○ From a policy in the Policy Library

Please select a policy..

Unix Directory Search Check – Find files without certain permissions

You can now select “Exclude” to return files that exclude your permission settings from Scan Parameters while creating new Unix Directory Search checks.



File Permissions

Find files with (or without) certain permissions. Yes means the permission is set on the file, No means the permission is not set, Any means either setting is fine.

	User	Group	Others
Read	Yes	Any	Any
Write	Any	No	Any
Execute	Any	Any	Yes
	User ID	Group ID	Deletion
Special	Yes	Any	No

Match All permissions above.

ct Types

Select the types you want to search from the list below.

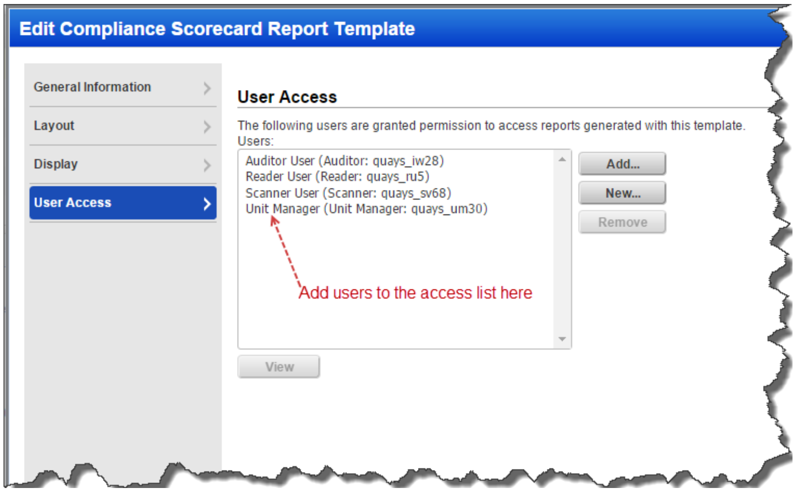
☑ (d) directory ☐ (b) block (buffered) special
☑ (f) regular file ☐ (c) character (unbuffered) special

Navigate to Policies > Controls and in New Control go to the Scan Parameters.

In the File Permissions section define the permissions you want to exclude during the search and select “Exclude”.

Make reports available to other users

You can now make Policy Compliance reports available to users who don’t already have access to them. Simply create a user access list in your compliance report templates. Users added to the template can view all reports generated from the template. Finished reports appear on the Reports tab.


Edit Compliance Scorecard Report Template

User Access

The following users are granted permission to access reports generated with this template.

Users:

Auditor User (Auditor: quays_iw28)
Reader User (Reader: quays_ru5)
Scanner User (Scanner: quays_sv68)
Unit Manager (Unit Manager: quays_um30)

Add users to the access list here

Sound familiar? That’s because this option is already available in VM scan reports and patch reports

Who can edit the access list?
Managers, Unit Managers and Auditors can add and remove users from the access list.

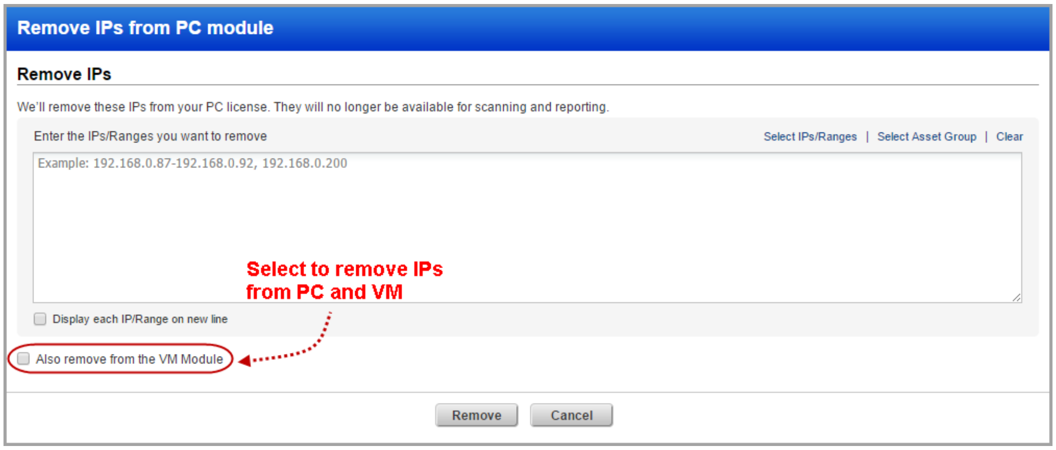
What happens when a user is removed from the list?
The user can no longer view the completed report in the Reports tab.

Can a user access a report on IPs that are not in the user’s account?
Yes, once a user is given access to a report template, the user can view all report content even if the IPs in the report are not in the user’s account.

Ability to Remove IPs from the PC module only

In this release, we’ve enhanced the Remove IPs wizard in the PC module (under Assets > Host Assets > New > Remove IPs). You’ll enter host IP addresses/ranges you want to remove from your subscription in the field provided, as before. Now these IPs will be removed from the PC module only by default. To remove them from your VM module too, be sure to select “Also remove from the VM module”.

Good to know
- Once IPs have been removed, they will no longer be available for scanning and reporting.
- Host IPs with agents installed will not be removed (i.e. hosts with the Agent tracking method).


Remove IPs from PC module

Remove IPs

We’ll remove these IPs from your PC license. They will no longer be available for scanning and reporting.

Enter the IPs/Ranges you want to remove

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

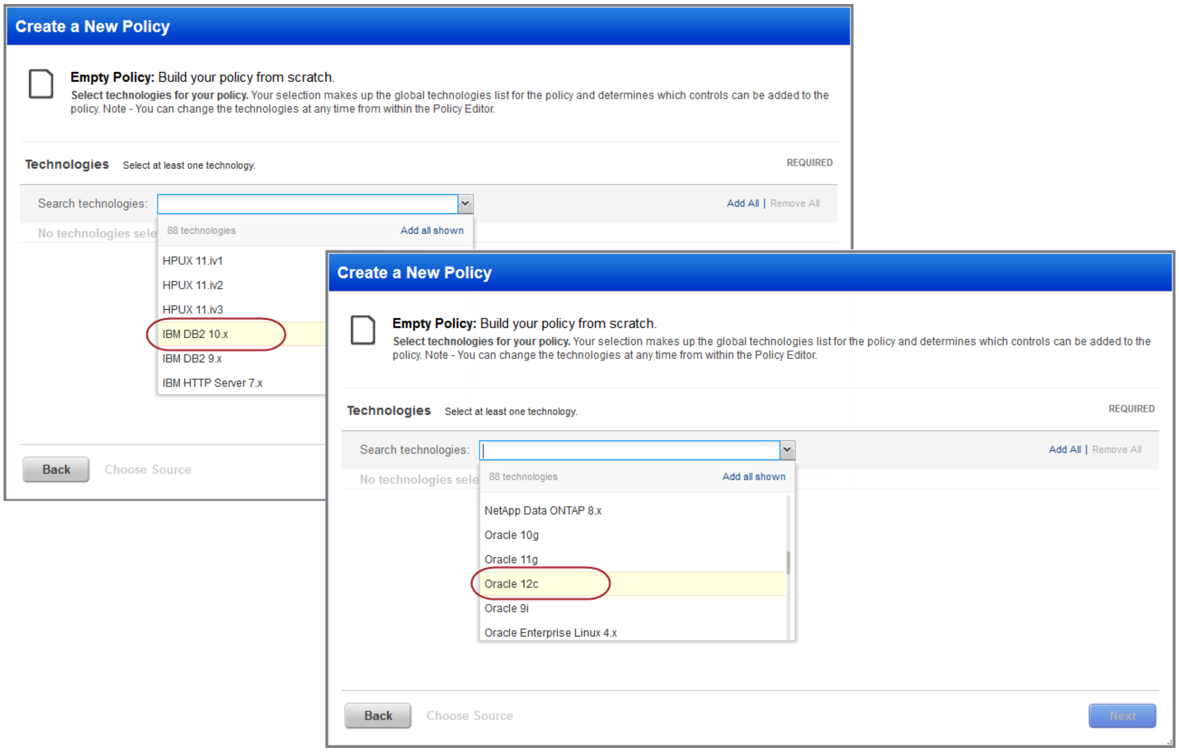
□ Display each IP/Range on new line

□ Also remove from the VM Module

Select to remove IPs from PC and VM

New Technologies Supported – IBM DB2 10.x and Oracle 12c

You can now evaluate compliance status for hosts running IBM DB2 10.x or Oracle 12c. It's easy to create new policies for these technologies. Simply choose the Create from Scratch option and then select technologies from the list. Optionally, add new technologies to your existing policies.



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 sele… 88 technologies Add all shown

HPUX 11.iv1
HPUX 11.iv2
HPUX 11.iv3
IBM DB2 10.x
IBM DB2 9.x
IBM HTTP Server 7.x

Back Choose Source

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

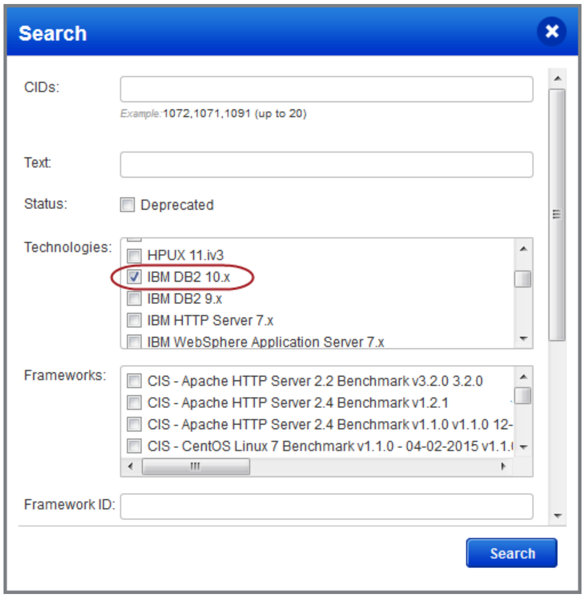
Search technologies: Add All | Remove All

No technologies sele… 88 technologies Add all shown

NetApp Data ONTAP 8.x
Oracle 10g
Oracle 11g
Oracle 12c
Oracle 9i
Oracle Enterprise Linux 4.x

Back Choose Source Next

Go to Policies > Controls > Search to quickly find controls applicable to new technologies.



Search

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

Text:

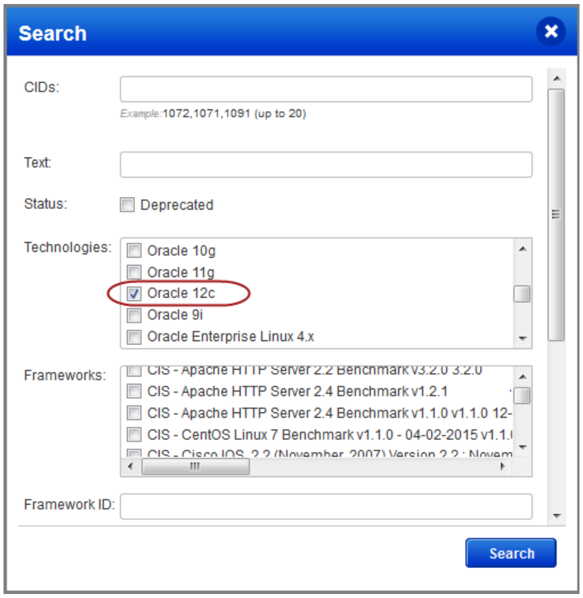
Status: □ Deprecated

Technologies:
□ HPUX 11.iv3
☑ IBM DB2 10.x
□ IBM DB2 9.x
□ IBM HTTP Server 7.x
□ IBM WebSphere Application Server 7.x

Frameworks:
□ CIS - Apache HTTP Server 2.2 Benchmark v3.2.0 3.2.0
□ CIS - Apache HTTP Server 2.4 Benchmark v1.2.1
□ CIS - Apache HTTP Server 2.4 Benchmark v1.1.0 v1.1.0 12-
□ CIS - CentOS Linux 7 Benchmark v1.1.0 - 04-02-2015 v1.1.

Framework ID:

Search



Search

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

Text:

Status: □ Deprecated

Technologies:
□ Oracle 10g
□ Oracle 11g
☑ Oracle 12c
□ Oracle 9i
□ Oracle Enterprise Linux 4.x

Frameworks:
□ CIS - Apache HTTP Server 2.2 Benchmark v3.2.0 3.2.0
□ CIS - Apache HTTP Server 2.4 Benchmark v1.2.1
□ CIS - Apache HTTP Server 2.4 Benchmark v1.1.0 v1.1.0 12-
□ CIS - CentOS Linux 7 Benchmark v1.1.0 - 04-02-2015 v1.1.
□ CIS - Cisco IOS 2.2 (November 2007) Version 2.2 : Novem

Framework ID:

Search

Qualys API Enhancements

Scan Report List – New Target Element

Now the Scan Report List API (/msp/scan_report_list.php) returns the IP addresses/ranges that were scanned in the XML output. A new target element was added to the Scan Report List Output DTD (scan_report_list.dtd).

New Schedule Report API

The new Schedule Report API v2 (/api/2.0/fo/schedule/report/) allows you to list scheduled reports in your account and launch new scheduled reports.

VM – Easily Identify Vulnerabilities Supported by Module

We've added a supported modules section to the vulnerability (QID) information. We updated these APIs: Dynamic Search List API v2, KnowledgeBase API v2, KnowledgeBase Download API v1.

VM – First Found Date added to Asset Search Report CSV, XML

We updated the Asset Search Report output in CSV and XML format. New elements were added to the Asset Search Report DTD (asset_search_report.dtd).

VM – Show Detections Since Certain Time

With this release you can filter detection list output to show updates since a certain time (date or number of days) using the Detection List API (/api/2.0/fo/asset/host/vm/detection/).

PC – New Exception API

Our new Exception API (/api/2.0/fo/compliance/exception/) lets you list, request, update and delete exceptions.

Want to learn more? See the *Qualys API Release Notes 8.7* for full details. You can download the release notes and our user guides from your account. Just go to Help > Resources.