Qualys 8.5 Release Notes

July 10, 2015

Qualys 8.5 is now available. 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)

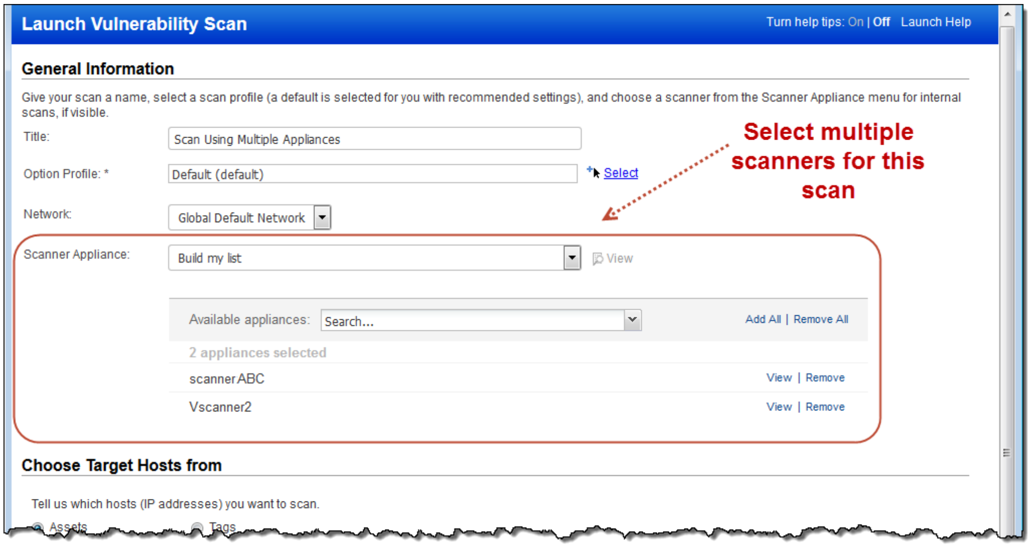
Qualys API Enhancements

Qualys Cloud Platform

Select Multiple Scanner Appliances for Scans

With this release you can select multiple scanner appliances for your internal vulnerability and compliance scans (PC and SCAP). This is especially useful when scanning a large number of hosts because it allows you to distribute the scan task across scanner appliances.

Simply choose "Build my list" from the Scanner Appliance menu when making your scan settings. Then select the appliances you want to use for the scan task.



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: Scan Using Multiple Appliances

Option Profile: * Default (default)

Network: Global Default Network

Scanner Appliance: Build my list

Available appliances: Search...

2 appliances selected

scanner ABC

Vscanner2

Select multiple scanners for this scan

Choose Target Hosts from

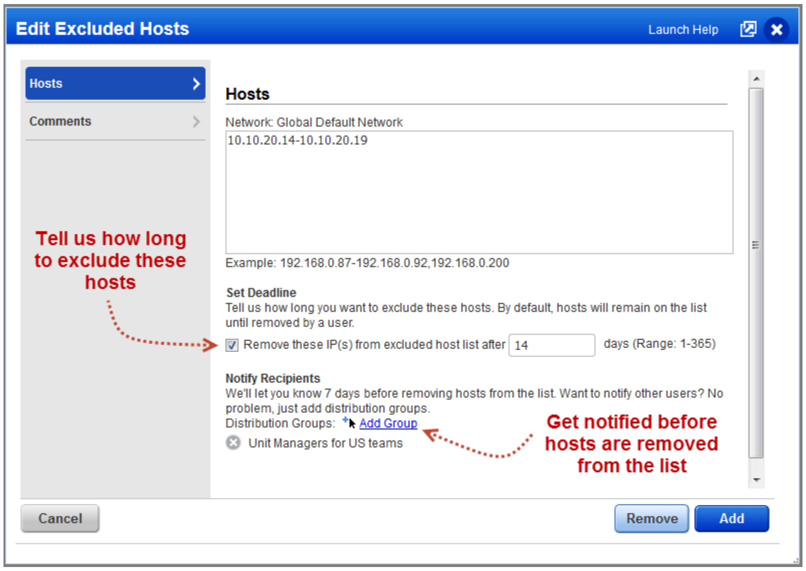
Tell us which hosts (IP addresses) you want to scan.

Scheduling your scans? No problem, you can select multiple scanner appliances for scheduled scans too.

Set Expiration Date for Excluded Hosts

You can now set an expiration date when adding IPs to the Excluded Hosts list. When the date is reached, the IPs are automatically removed from the list and made available again for scanning. We'll send you an email 7 days before removing the IPs, allowing you time to change the date if you want. To notify other users, simply add distribution groups and the email will be sent to them as well.

How do I exclude hosts for a set number of days? Go to Scans > Setup > Excluded Hosts. Click Edit to add IPs to the Excluded Hosts list. Enter the IPs you want to exclude, set a deadline and add distribution groups. Then add comments and click Add.



Edit Excluded Hosts

Hosts

Network: Global Default Network
10.10.20.14-10.10.20.19

Example: 192.168.0.87-192.168.0.92,192.168.0.200

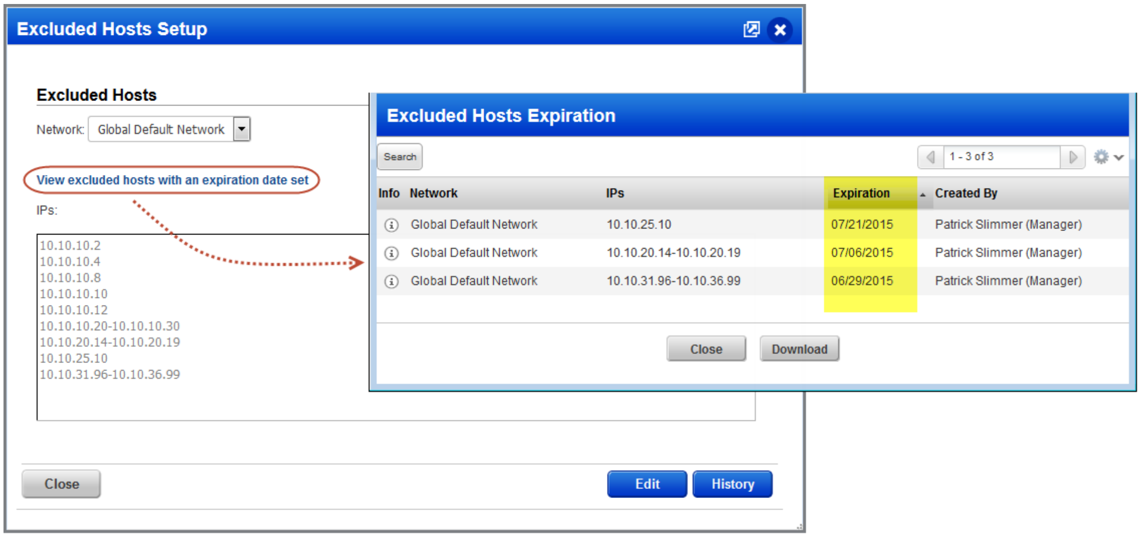
Set Deadline
Tell us how long you want to exclude these hosts. By default, hosts will remain on the list until removed by a user.
☑ Remove these IP(s) from excluded host list after 14 days (Range: 1-365)

Notify Recipients
We'll let you know 7 days before removing hosts from the list. Want to notify other users? No problem, just add distribution groups.
Distribution Groups: Add Group
Unit Managers for US teams

Tell us how long to exclude these hosts

Get notified before hosts are removed from the list

When viewing the Excluded Hosts list click the link "View excluded hosts with an expiration date set" to see when each IP/IP range is set to expire. You can sort this list by expiration date and download it in various formats like CSV and XML.



Excluded Hosts Setup

Excluded Hosts

Network: Global Default Network

View excluded hosts with an expiration date set

IPs:

```
10.10.10.2
10.10.10.4
10.10.10.8
10.10.10.10
10.10.10.12
10.10.10.20-10.10.10.30
10.10.20.14-10.10.20.19
10.10.25.10
10.10.31.96-10.10.36.99
```

Excluded Hosts Expiration

1 - 3 of 3

Info	Network	IPs	Expiration	Created By
ⓘ	Global Default Network	10.10.25.10	07/21/2015	Patrick Slimmer (Manager)
ⓘ	Global Default Network	10.10.20.14-10.10.20.19	07/06/2015	Patrick Slimmer (Manager)
ⓘ	Global Default Network	10.10.31.96-10.10.36.99	06/29/2015	Patrick Slimmer (Manager)

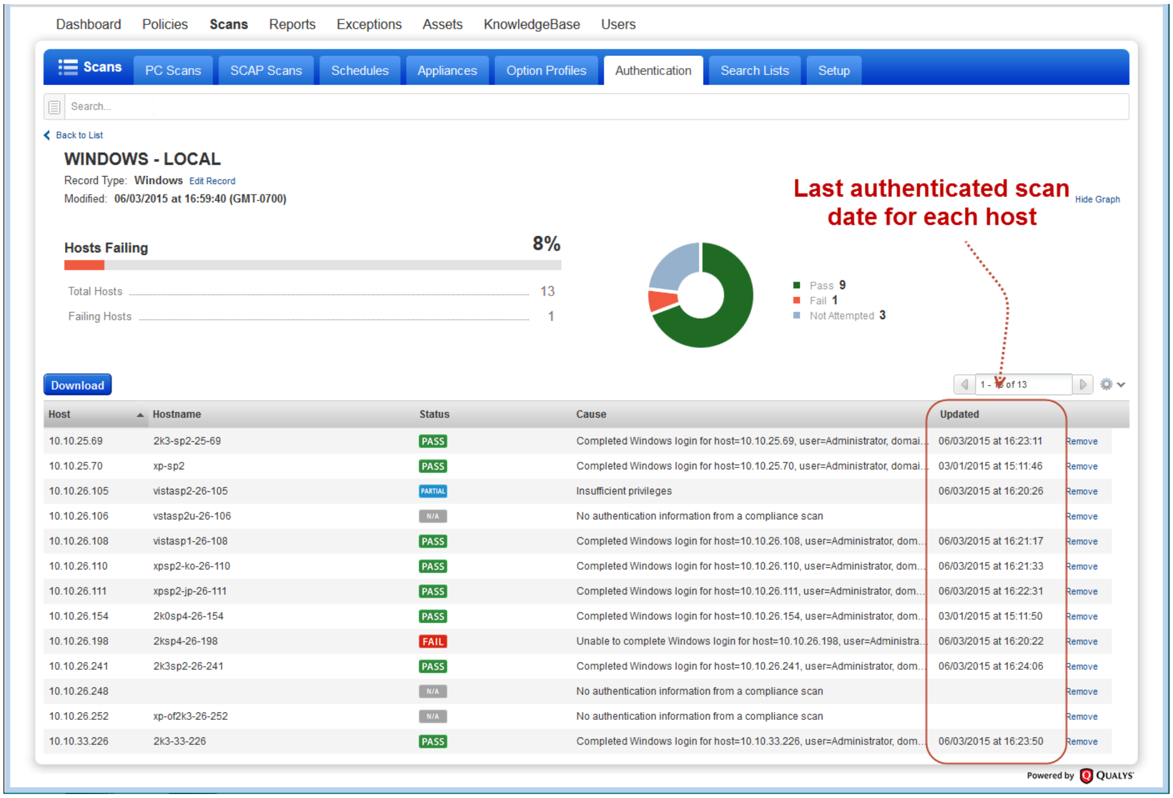
Want to change the expiration date for a host? Add the host to the list again and set a new deadline. The expiration date will be updated.

Last Scan Date added to Authentication Record Details

Drill down into authentication record details to see the date/time of the last authenticated scan for each host in the record. This is when the Pass/Fail status was last updated for the host.

Check it out

Go to Scans > Authentication and click the Details link for any record. When in VM, you'll see the vulnerability scan date. When in PC, you'll see the compliance scan date.



WINDOWS - LOCAL

Record Type: Windows Edit Record

Modified: 06/03/2015 at 16:59:40 (GMT-0700)

Hosts Failing 8%

Total Hosts 13

Failing Hosts 1

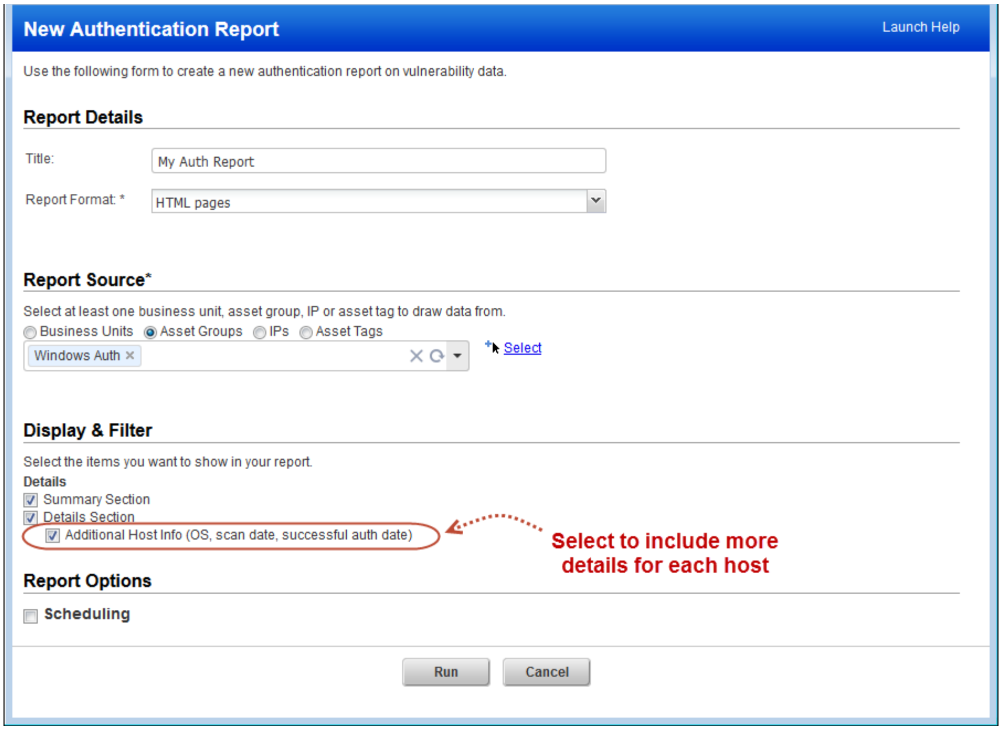
Last authenticated scan date for each host

Host	Hostname	Status	Cause	Updated	
10.10.25.69	2k3-sp2-25-69	PASS	Completed Windows login for host=10.10.25.69, user=Administrator, domai...	06/03/2015 at 16:23:11	Remove
10.10.25.70	xp-sp2	PASS	Completed Windows login for host=10.10.25.70, user=Administrator, domai...	03/01/2015 at 15:11:46	Remove
10.10.26.105	vistasp2-26-105	PARTIAL	Insufficient privileges	06/03/2015 at 16:20:26	Remove
10.10.26.106	vstasp2u-26-106	N/A	No authentication information from a compliance scan		Remove
10.10.26.108	vistasp1-26-108	PASS	Completed Windows login for host=10.10.26.108, user=Administrator, dom...	06/03/2015 at 16:21:17	Remove
10.10.26.110	xpsp2-ko-26-110	PASS	Completed Windows login for host=10.10.26.110, user=Administrator, dom...	06/03/2015 at 16:21:33	Remove
10.10.26.111	xpsp2-jp-26-111	PASS	Completed Windows login for host=10.10.26.111, user=Administrator, dom...	06/03/2015 at 16:22:31	Remove
10.10.26.154	2k0sp4-26-154	PASS	Completed Windows login for host=10.10.26.154, user=Administrator, dom...	03/01/2015 at 15:11:50	Remove
10.10.26.198	2ksp4-26-198	FAIL	Unable to complete Windows login for host=10.10.26.198, user=Administra...	06/03/2015 at 16:20:22	Remove
10.10.26.241	2k3sp2-26-241	PASS	Completed Windows login for host=10.10.26.241, user=Administrator, dom...	06/03/2015 at 16:24:06	Remove
10.10.26.248		N/A	No authentication information from a compliance scan		Remove
10.10.26.252	xp-of2k3-26-252	N/A	No authentication information from a compliance scan		Remove
10.10.33.226	2k3-33-226	PASS	Completed Windows login for host=10.10.33.226, user=Administrator, dom...	06/03/2015 at 16:23:50	Remove

Tip – The Credentials Breakdown options (on the authentication dashboard) only consider hosts scanned in the last 30 days. Now you can easily identify hosts that aren't being counted because they were scanned more than 30 days ago.

More Host Info in Authentication Reports

Select the option “Additional Host Info” when running your report to include this information for each host: 1) the host’s operating system, 2) the last time you scanned the host with authentication, and 3) the last time authentication was successful.



Use the following form to create a new authentication report on vulnerability data.

Report Details

Title: My Auth Report

Report Format: * HTML pages

Report Source*

Select at least one business unit, asset group, IP or asset tag to draw data from.

○ Business Units ● Asset Groups ○ IPs ○ Asset Tags

Windows Auth ×

Display & Filter

Select the items you want to show in your report.

Details

☑ Summary Section

☑ Details Section

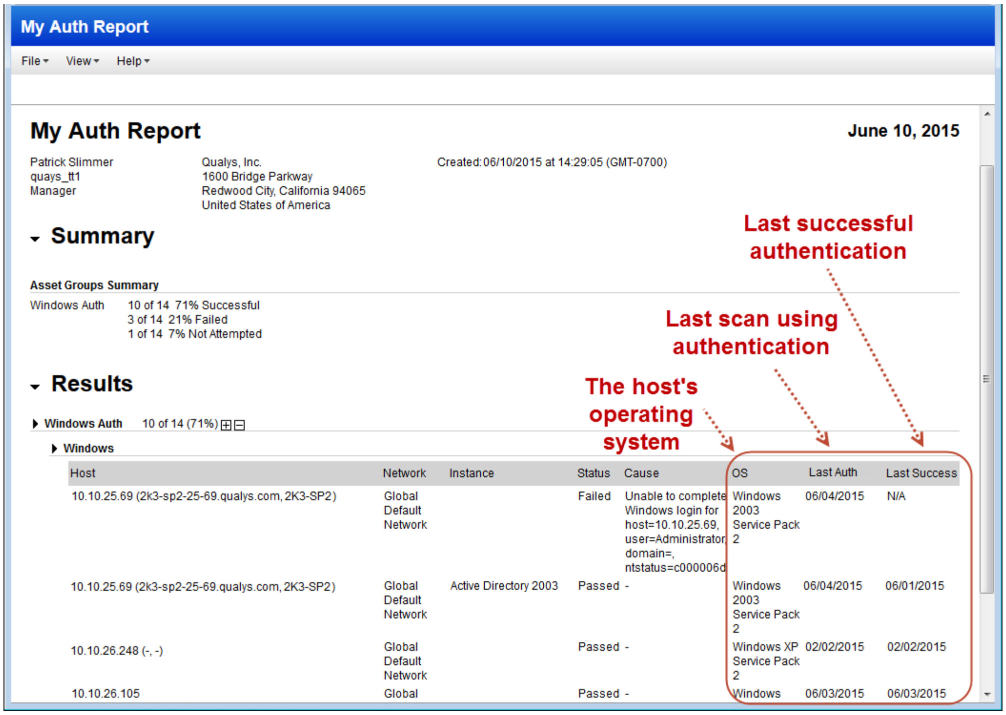
☑ Additional Host Info (OS, scan date, successful auth date)

Select to include more details for each host

Report Options

□ Scheduling

Here’s a sample report with host information included.



My Auth Report **June 10, 2015**

Patrick Slimmer
quays_tt1
Manager

Qualys, Inc.
1600 Bridge Parkway
Redwood City, California 94065
United States of America

Created: 06/10/2015 at 14:29:05 (GMT-0700)

Summary

Asset Groups Summary

Windows Auth	10 of 14 71% Successful 3 of 14 21% Failed 1 of 14 7% Not Attempted

Results

Windows Auth 10 of 14 (71%)

Windows

Host	Network	Instance	Status	Cause	OS	Last Auth	Last Success
10.10.25.69 (2k3-sp2-25-69.qualys.com, 2K3-SP2)	Global Default Network		Failed	Unable to complete Windows login for host=10.10.25.69, user=Administrator, domain=, ntstatus=c000006d	Windows 2003 Service Pack 2	06/04/2015	N/A
10.10.25.69 (2k3-sp2-25-69.qualys.com, 2K3-SP2)	Global Default Network	Active Directory 2003	Passed	-	Windows 2003 Service Pack 2	06/04/2015	06/01/2015
10.10.26.248 (-, -)	Global Default Network		Passed	-	Windows XP Service Pack 2	02/02/2015	02/02/2015
10.10.26.105	Global		Passed	-	Windows	06/03/2015	06/03/2015

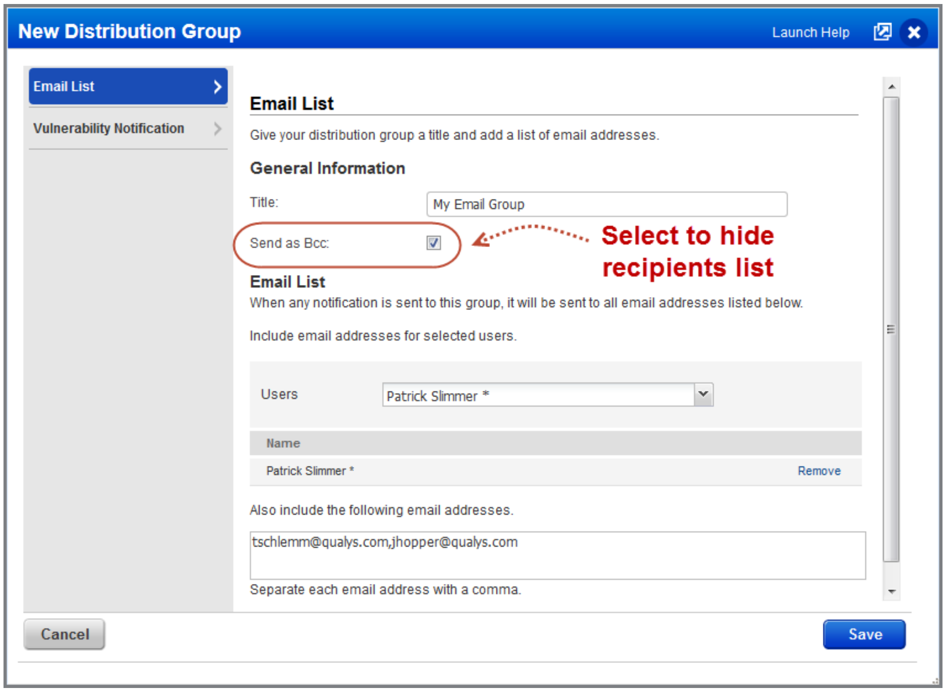
Last successful authentication

Last scan using authentication

The host's operating system

Send Email Notifications to Bcc List

It’s easy to do. Just select “Send as Bcc” in your distribution group settings. We’ll hide the list of recipients any time the distribution group is selected for a notification - scan notifications, report notifications, vulnerability notifications, etc.



Email List

Give your distribution group a title and add a list of email addresses.

General Information

Title: My Email Group

Send as Bcc: ☑

Select to hide recipients list

Email List

When any notification is sent to this group, it will be sent to all email addresses listed below.

Include email addresses for selected users.

Users: Patrick Slimmer *

Name	
Patrick Slimmer *	Remove

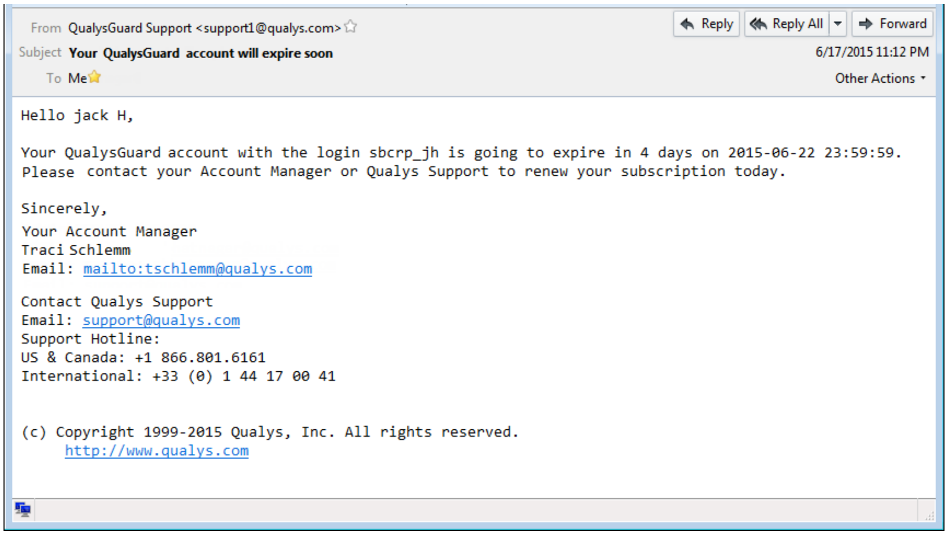
Also include the following email addresses.

tschlemm@qualys.com,jhopper@qualys.com

Separate each email address with a comma.

Get Notified Before Your Account Expires

The Manager Primary Contact (for the subscription) will now receive an email notification when the account is going to expire with details on how to renew. The email is sent 45 days, 30 days, 14 days and 7 days before the expiration date, and every day after that until the expiration date.



From QualysGuard Support <support1@qualys.com>

Subject **Your QualysGuard account will expire soon**

To Me

6/17/2015 11:12 PM

```
Hello jack H,

Your QualysGuard account with the login sbcrp_jh is going to expire in 4 days on 2015-06-22 23:59:59.
Please contact your Account Manager or Qualys Support to renew your subscription today.

Sincerely,
Your Account Manager
Traci Schlemm
Email: mailto:tschlemm@qualys.com

Contact Qualys Support
Email: support@qualys.com
Support Hotline:
US & Canada: +1 866.801.6161
International: +33 (0) 1 44 17 00 41


(c) Copyright 1999-2015 Qualys, Inc. All rights reserved.
     http://www.qualys.com
```

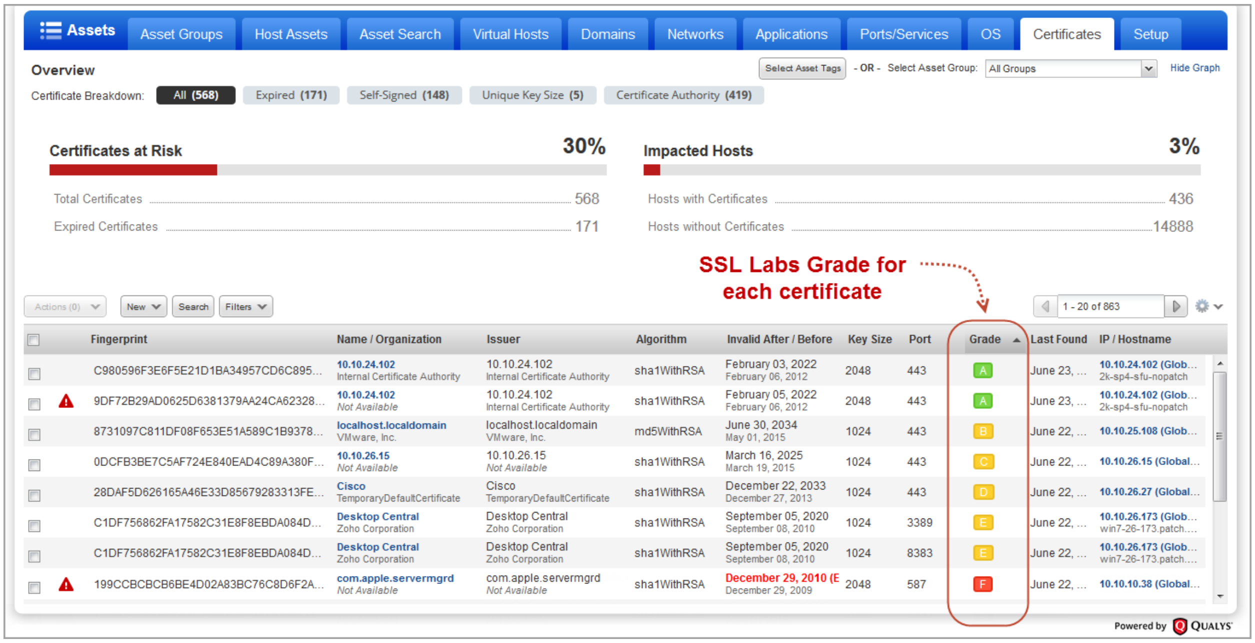
Qualys Vulnerability Management (VM)

SSL Labs Grade added to Certificates List

We're excited to announce that we've integrated SSL Labs with Qualys VM. When enabled, you'll get a letter grade (A+, A, A-, B, C, D, E, F, T, M, NA) for each certificate on your certificates list. Grades are updated automatically each time new vulnerability scan results are processed for your hosts.

Important – The SSL Labs Grade feature must be enabled for your subscription. Please contact your Technical Account Manager or Support to get this feature.

Go to VM > Assets > Certificates to see grades for your certificates. Not seeing a grade? Be sure to run new vulnerability scans on your hosts in order for grades to be calculated.



Overview

Select Asset Group: All Groups

Certificate Breakdown: All (568) Expired (171) Self-Signed (148) Unique Key Size (5) Certificate Authority (419)

Certificates at Risk 30%

Total Certificates 568

Expired Certificates 171

Impacted Hosts 3%

Hosts with Certificates 436

Hosts without Certificates 14888

SSL Labs Grade for each certificate

□		Fingerprint	Name / Organization	Issuer	Algorithm	Invalid After / Before	Key Size	Port	Grade	Last Found	IP / Hostname
□		C980596F3E6F5E21D1BA34957CD6C895...	10.10.24.102 Internal Certificate Authority	10.10.24.102 Internal Certificate Authority	sha1WithRSA	February 03, 2022 February 06, 2012	2048	443	A	June 23, ...	10.10.24.102 (Glob... 2k-sp4-sfu-nopatch
□	⚠	9DF72B29AD0625D6381379AA24CA62328...	10.10.24.102 *Not Available*	10.10.24.102 Internal Certificate Authority	sha1WithRSA	February 05, 2022 February 06, 2012	2048	443	A	June 23, ...	10.10.24.102 (Glob... 2k-sp4-sfu-nopatch
□		8731097C811DF08F653E51A589C1B9378...	localhost.localdomain VMware, Inc.	localhost.localdomain VMware, Inc.	md5WithRSA	June 30, 2034 May 01, 2015	1024	443	B	June 22, ...	10.10.25.108 (Glob...
□		0DCFB3BE7C5AF724E840EAD4C89A380F...	10.10.26.15 *Not Available*	10.10.26.15 *Not Available*	sha1WithRSA	March 16, 2025 March 19, 2015	1024	443	C	June 22, ...	10.10.26.15 (Global...
□		28DAF5D626165A46E33D85679283313FE...	Cisco TemporaryDefaultCertificate	Cisco TemporaryDefaultCertificate	sha1WithRSA	December 22, 2033 December 27, 2013	1024	443	D	June 22, ...	10.10.26.27 (Global...
□		C1DF756862FA17582C31E8F8EBDA084D...	Desktop Central Zoho Corporation	Desktop Central Zoho Corporation	sha1WithRSA	September 05, 2020 September 08, 2010	1024	3389	E	June 22, ...	10.10.26.173 (Glob... win7-26-173.patch....
□		C1DF756862FA17582C31E8F8EBDA084D...	Desktop Central Zoho Corporation	Desktop Central Zoho Corporation	sha1WithRSA	September 05, 2020 September 08, 2010	1024	8383	E	June 22, ...	10.10.26.173 (Glob... win7-26-173.patch....
□	⚠	199CCBCBCB6BE4D02A83BC76C8D6F2A...	com.apple.servermgrd *Not Available*	com.apple.servermgrd *Not Available*	sha1WithRSA	December 29, 2010 (E December 29, 2009	2048	587	F	June 22, ...	10.10.10.38 (Global...

You'll notice that if the same certificate is found multiple times on the same host (on different ports), then each instance of the certificate will now be listed and the Port column will show the port number. Each instance of the certificate can have a different grade.

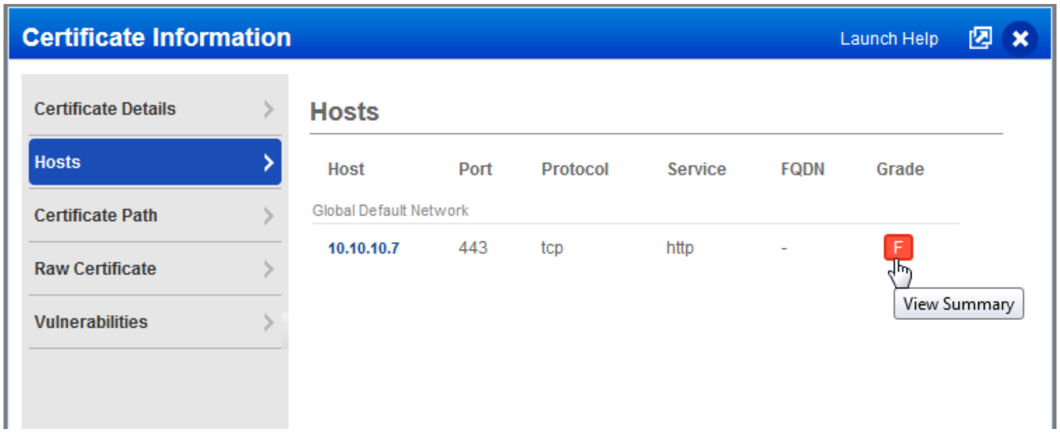
How are grades calculated?

We first look at the certificate to verify that it is valid and trusted. Then we inspect SSL configuration in three categories: 1) Protocol Support, 2) Key Exchange and 3) Cipher Strength. Each category is given a score and we combine these scores for an overall score of 0-100. (A zero in any category results in an overall score of zero.) The overall numerical score is translated into a letter grade (A-F) using a look-up table. Your A grade will be upgraded to A+ for exceptional configurations, and downgraded to A- when there are one or more warnings. Other grades you might see: T (certificate is not trusted), M (certificate name mismatch), and NA (not applicable, SSL server information not retrieved).

Want to know more? Go to https://www.ssllabs.com/projects/rating-guide/index.html

Can I update the grade without a new scan?

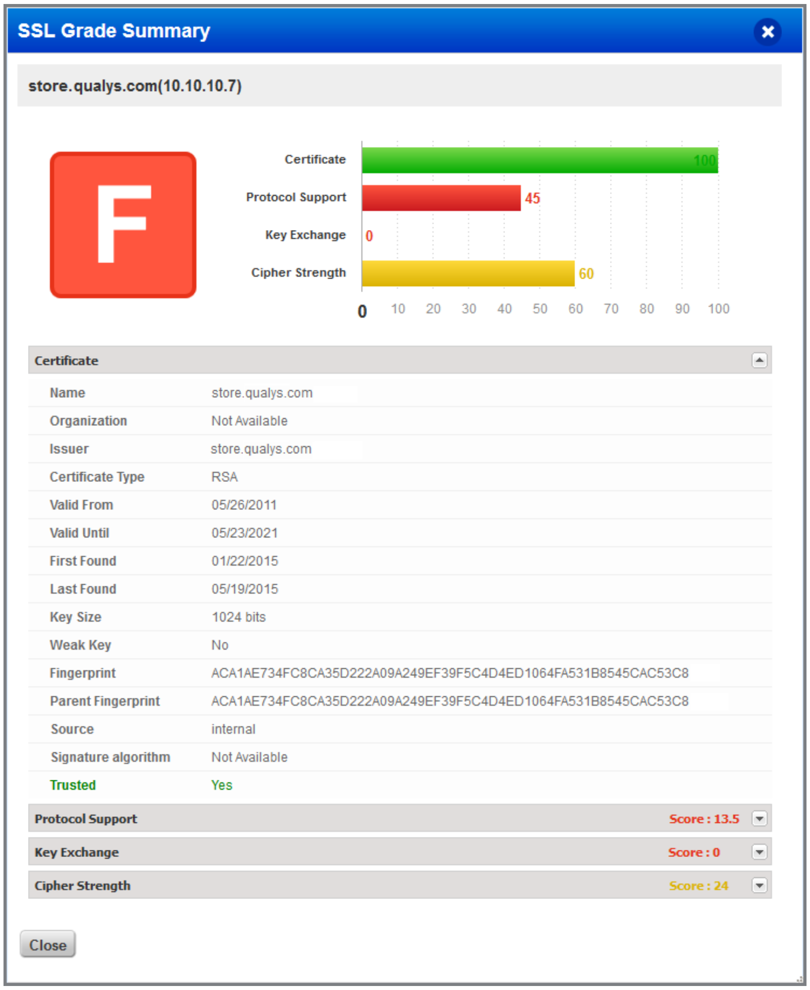
Yes. From your certificates list, choose Certificate Info from the Quick Actions menu and then go to the Hosts tab. The grade is automatically calculated based on the most recent host scan data. Optionally, click on the host's IP address in your certificates list and go to the Certificates tab to get a grade for any certificate on the host.



Hosts

Host	Port	Protocol	Service	FQDN	Grade
Global Default Network					
10.10.10.7	443	tcp	http	-	F

Click on the grade to view the SSL Grade Summary page. Here you'll see certificate information plus the score and details for these three categories: 1) Protocol Support, 2) Key Exchange and 3) Cipher Strength.



store.qualys.com(10.10.10.7)

Certificate

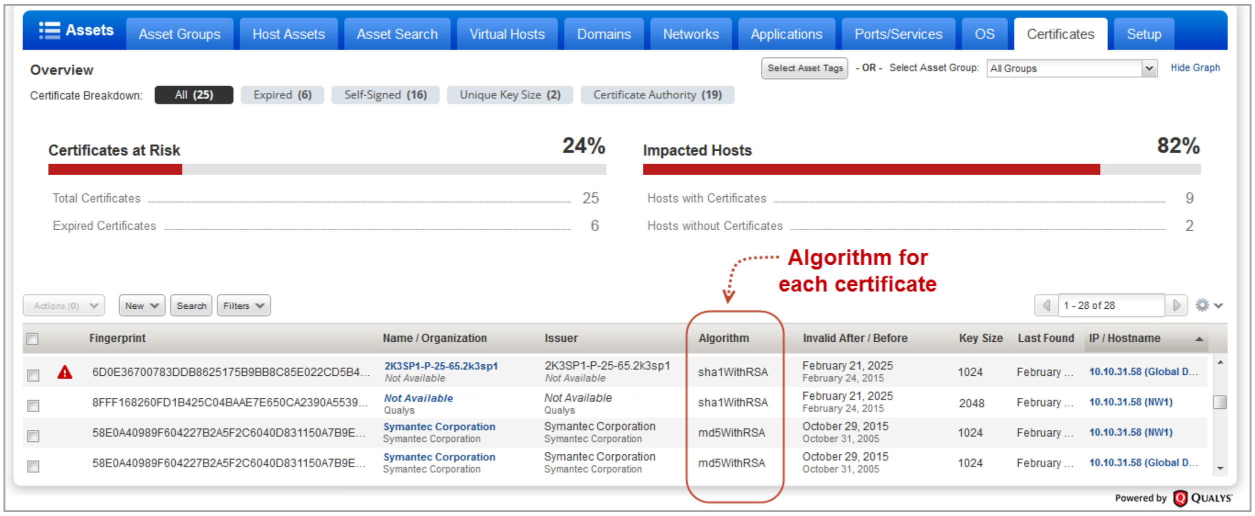
Name	store.qualys.com
Organization	Not Available
Issuer	store.qualys.com
Certificate Type	RSA
Valid From	05/26/2011
Valid Until	05/23/2021
First Found	01/22/2015
Last Found	05/19/2015
Key Size	1024 bits
Weak Key	No
Fingerprint	ACA1AE734FC8CA35D222A09A249EF39F5C4D4ED1064FA531B8545CAC53C8
Parent Fingerprint	ACA1AE734FC8CA35D222A09A249EF39F5C4D4ED1064FA531B8545CAC53C8
Source	internal
Signature algorithm	Not Available
Trusted	Yes

Protocol Support	Score : 13.5
Key Exchange	Score : 0
Cipher Strength	Score : 24

The Certificate score is either 0 (not trusted) or 100 (trusted). This score is not used when calculating the overall grade.

Algorithm added to Certificates List

For each certificate you’ll see the algorithm (sha1WithRSA, md5WithRSA, etc) in the new Algorithm column. Just go to VM > Assets > Certificates to see it.



Overview

Certificate Breakdown: All (25) Expired (6) Self-Signed (16) Unique Key Size (2) Certificate Authority (19)

Certificates at Risk 24%

Total Certificates	25
Expired Certificates	6

Impacted Hosts 82%

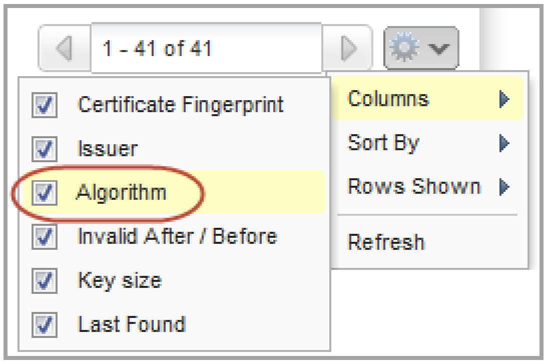
Hosts with Certificates	9
Hosts without Certificates	2

Algorithm for each certificate

☐		Fingerprint	Name / Organization	Issuer	Algorithm	Invalid After / Before	Key Size	Last Found	IP / Hostname
☐	⚠	6D0E36700783DDB8625175B9BB8C85E022CD5B4...	2K3SP1-P-25-65.2k3sp1 *Not Available*	2K3SP1-P-25-65.2k3sp1 *Not Available*	sha1WithRSA	February 21, 2025 February 24, 2015	1024	February ...	10.10.31.58 (Global D...
☐		8FFF168260FD1B425C04BAAE7E650CA2390A5539...	*Not Available* Qualys	*Not Available* Qualys	sha1WithRSA	February 21, 2025 February 24, 2015	2048	February ...	10.10.31.58 (NW1)
☐		58E0A40989F604227B2A5F2C6040D831150A7B9E...	Symantec Corporation Symantec Corporation	Symantec Corporation Symantec Corporation	md5WithRSA	October 29, 2015 October 31, 2005	1024	February ...	10.10.31.58 (NW1)
☐		58E0A40989F604227B2A5F2C6040D831150A7B9E...	Symantec Corporation Symantec Corporation	Symantec Corporation Symantec Corporation	md5WithRSA	October 29, 2015 October 31, 2005	1024	February ...	10.10.31.58 (Global D...

How do I show the new Algorithm column?

This column is hidden initially. Simply select it in the Tools menu (as shown on the right) to show it in the list.



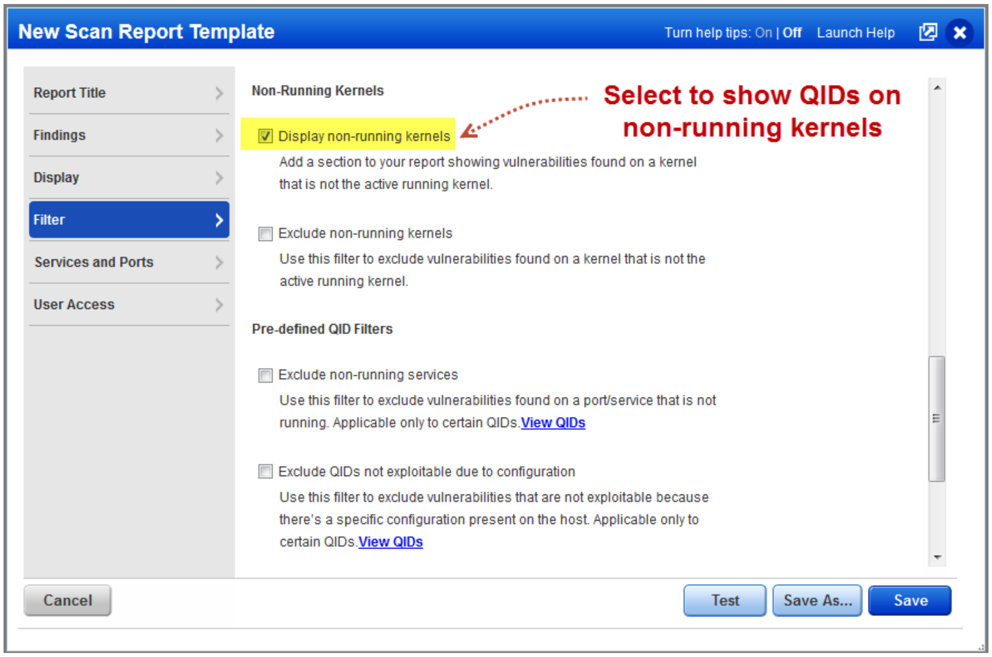
Will the algorithm appear in downloaded reports?

Yes. When the column is shown in the UI, then it will also appear when you download the Certificate’s report. Go to New > Download and choose a report format (XML, CSV, etc).

Identify Vulnerabilities on Non-Running Kernels

With this release, users can create reports that show non-running kernels in the vulnerability details. This way you can identify vulnerabilities found on a kernel that is not the active running kernel.

A new option “Display non-running kernels” has been added under “Non-Running Kernels” on the Filter tab of report templates for scan, patch, and scorecard reports.



Non-Running Kernels

☑ Display non-running kernels

Add a section to your report showing vulnerabilities found on a kernel that is not the active running kernel.

☐ Exclude non-running kernels

Use this filter to exclude vulnerabilities found on a kernel that is not the active running kernel.

Pre-defined QID Filters

☐ Exclude non-running services

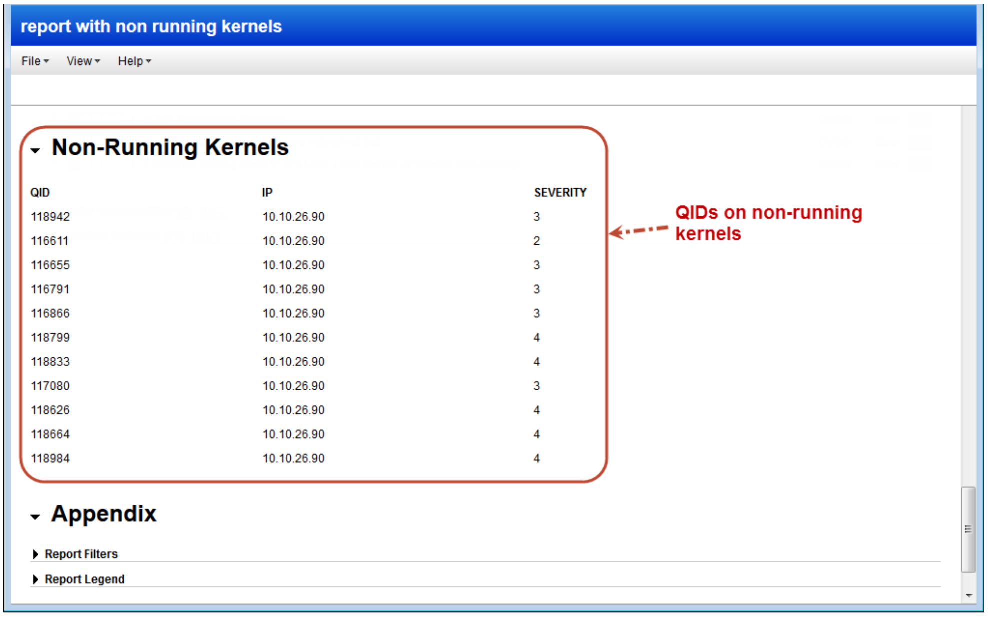
Use this filter to exclude vulnerabilities found on a port/service that is not running. Applicable only to certain QIDs. View QIDs

☐ 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

Select to show QIDs on non-running kernels

Here’s a sample report with vulnerabilities on non-running kernels for host 10.10.26.90.



Non-Running Kernels

QID	IP	SEVERITY
118942	10.10.26.90	3
116611	10.10.26.90	2
116655	10.10.26.90	3
116791	10.10.26.90	3
116866	10.10.26.90	3
118799	10.10.26.90	4
118833	10.10.26.90	4
117080	10.10.26.90	3
118626	10.10.26.90	4
118664	10.10.26.90	4
118984	10.10.26.90	4

QIDs on non-running kernels

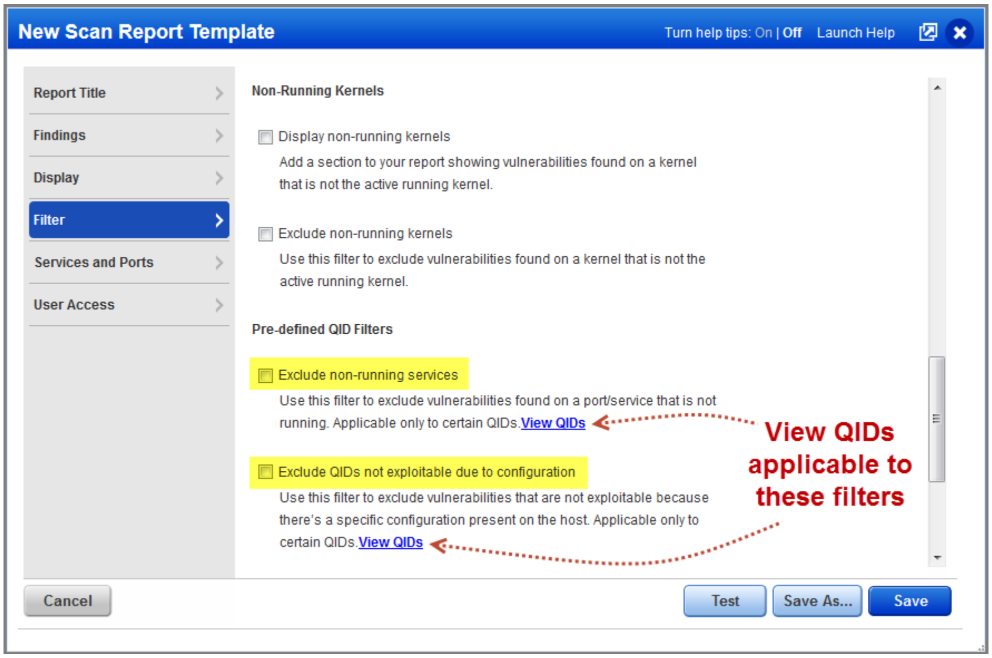
Appendix

Tip – When you run this report in CSV format you’ll see a new column “Non-running Kernel” with a value of Yes or No for each vulnerability to indicate whether it was found on a non-running kernel.

View QIDs Applicable to Report Filters

With this release you can identify the vulnerabilities that apply to these report template filters: “Exclude QIDs on non-running services” and “Exclude QIDs not exploitable due to configuration”. These filters appear in templates for scan reports, patch reports and scorecard reports.

In your report template, click the View QIDs link to see the list of the QIDs that may be filtered out when each filter option is selected.



Non-Running Kernels

□ Display non-running kernels

Add a section to your report showing vulnerabilities found on a kernel that is not the active running kernel.

□ Exclude non-running kernels

Use this filter to exclude vulnerabilities found on a kernel that is not the active running kernel.

Pre-defined QID Filters

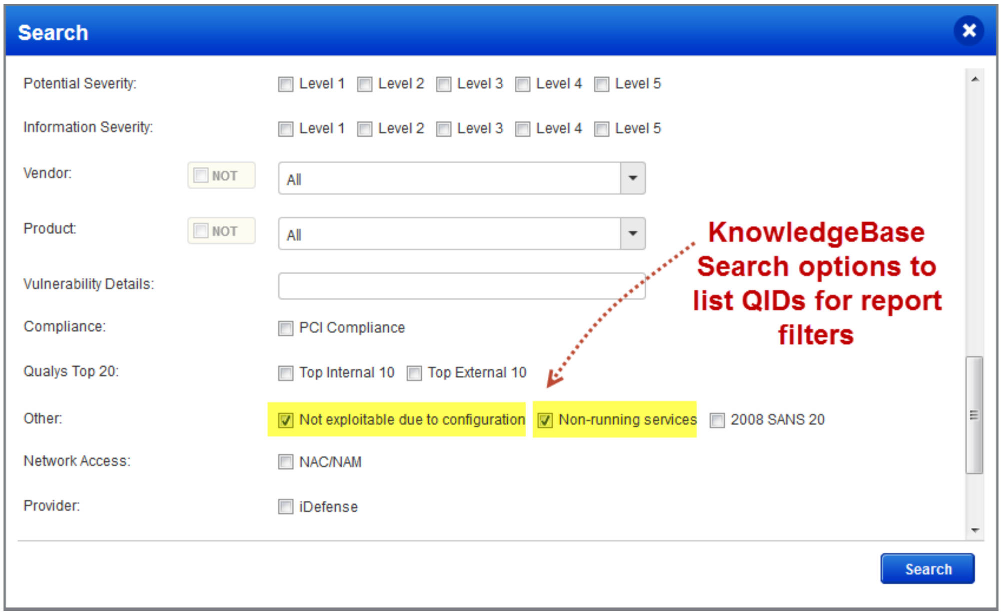
□ Exclude non-running services

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

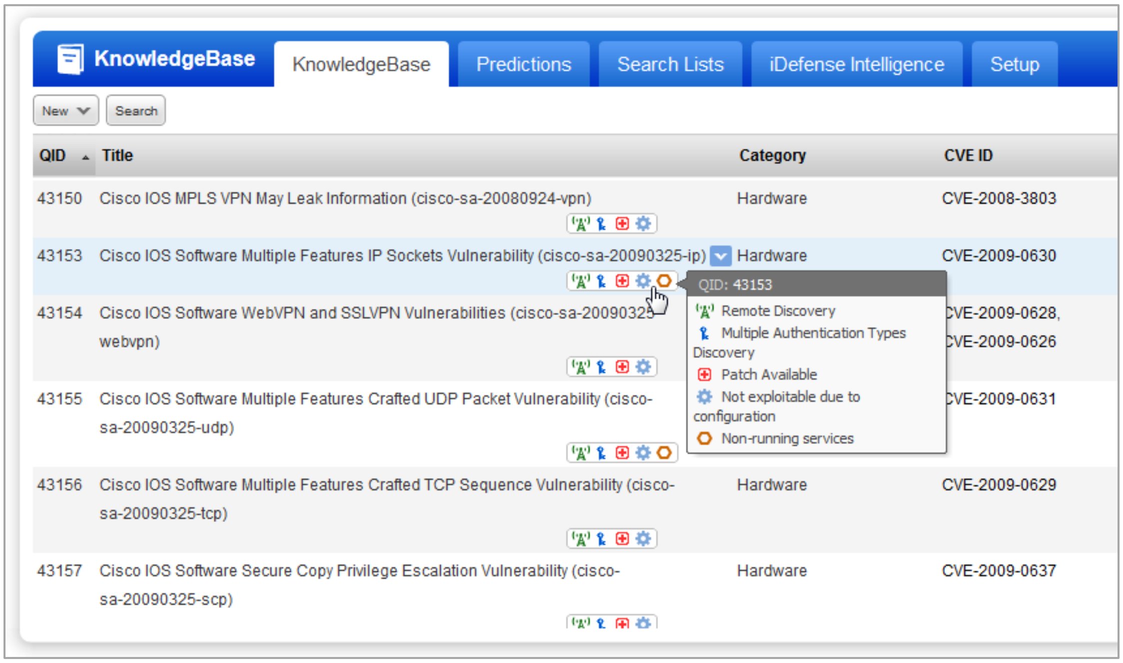
Use this filter to exclude vulnerabilities that are not exploitable because there's a specific configuration present on the host. Applicable only to certain QIDs. View QIDs

You can also find these QIDs in the KnowledgeBase and create a search list based on these options. Go to KnowledgeBase, click Search, and select the options “Not exploitable due to configuration” and “Non-running services” to find the QIDs applicable to the report filters.


Search
Search
KnowledgeBase Search options to list QIDs for report filters

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:		
Compliance:		□ PCI Compliance
Qualys Top 20:		□ Top Internal 10 □ Top External 10
Other:		☑ Not exploitable due to configuration ☑ Non-running services □ 2008 SANS 20
Network Access:		□ NAC/NAM
Provider:		□ iDefense

In the KnowledgeBase, QIDs that apply to the filter “Not exploitable due to configuration” are flagged with ⚙. QIDs that apply to the filter “Non-running services” are flagged with ○.



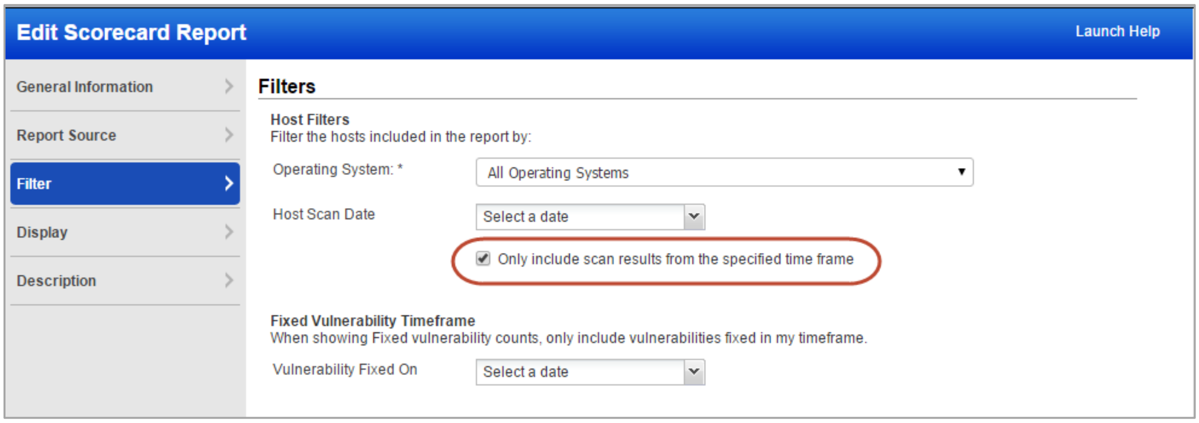
QID	Title	Category	CVE ID
43150	Cisco IOS MPLS VPN May Leak Information (cisco-sa-20080924-vpn)	Hardware	CVE-2008-3803
43153	Cisco IOS Software Multiple Features IP Sockets Vulnerability (cisco-sa-20090325-ip)	Hardware	CVE-2009-0630
43154	Cisco IOS Software WebVPN and SSLVPN Vulnerabilities (cisco-sa-20090325-webvpn)		CVE-2009-0628, CVE-2009-0626
43155	Cisco IOS Software Multiple Features Crafted UDP Packet Vulnerability (cisco-sa-20090325-udp)		CVE-2009-0631
43156	Cisco IOS Software Multiple Features Crafted TCP Sequence Vulnerability (cisco-sa-20090325-tcp)	Hardware	CVE-2009-0629
43157	Cisco IOS Software Secure Copy Privilege Escalation Vulnerability (cisco-sa-20090325-scp)	Hardware	CVE-2009-0637

QID: 43153
Remote Discovery
Multiple Authentication Types Discovery
Patch Available
Not exploitable due to configuration
Non-running services

Select time frame for Scorecard Reports

We have now enabled time frame selection for Scorecard reports. This means only the scan results during the period defined by you will be displayed in the Scorecard Report.

In the Edit Scorecard Report, the new option “Only include scan results from the specified time frame” is added so that only the scan results for the period of time you select from “Host Scan Date” are displayed. Using the Host Scan Date you have options like today, all dates before, all dates after, date range, in the previous day, week, month, year, etc, to define the time frame.



Filters

Host Filters
Filter the hosts included in the report by:

Operating System: * All Operating Systems

Host Scan Date Select a date

☑ Only include scan results from the specified time frame

Fixed Vulnerability Timeframe
When showing Fixed vulnerability counts, only include vulnerabilities fixed in my timeframe.

Vulnerability Fixed On Select a date

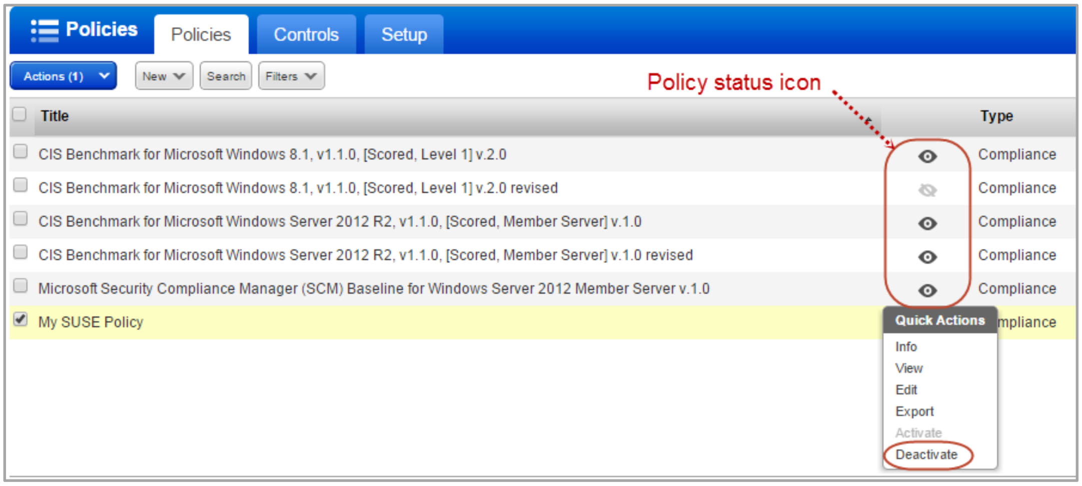
Qualys Policy Compliance (PC)

Make Policies Active or Inactive

Every policy in your account will now either be in an active or inactive state. The policies that are in inactive state will not be scanned or reported on. By default your polices are marked active.

You may want to hide a new policy while you're working on it and then publish it at a later time. Or let's say a policy has become out of date and you want to edit the policy before republishing it. In such cases you mark the policy inactive and make the required changes. Only after you activate the policy, it will be available for scanning and reporting.

You can easily mark an existing policy inactive. Go to your list of policies, identify the policy and select Deactivate from the Quick Actions menu. (Use Actions menu to select multiple policies at one go.)

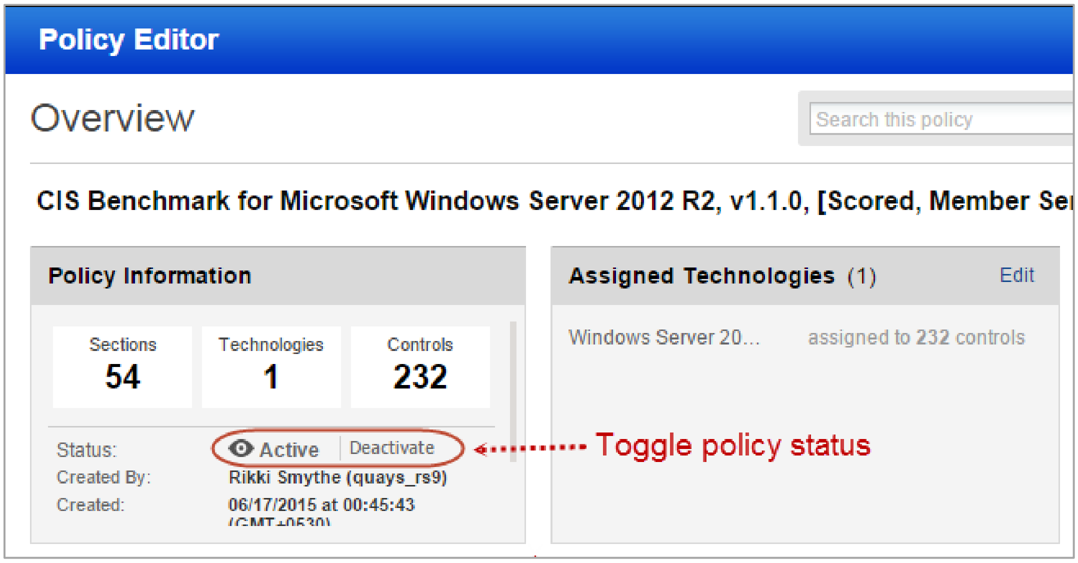


	Title		Type
□	CIS Benchmark for Microsoft Windows 8.1, v1.1.0, [Scored, Level 1] v.2.0	◉	Compliance
□	CIS Benchmark for Microsoft Windows 8.1, v1.1.0, [Scored, Level 1] v.2.0 revised	⊘	Compliance
□	CIS Benchmark for Microsoft Windows Server 2012 R2, v1.1.0, [Scored, Member Server] v.1.0	◉	Compliance
□	CIS Benchmark for Microsoft Windows Server 2012 R2, v1.1.0, [Scored, Member Server] v.1.0 revised	◉	Compliance
□	Microsoft Security Compliance Manager (SCM) Baseline for Windows Server 2012 Member Server v.1.0	◉	Compliance
☑	My SUSE Policy		mpliance

◉ means active

⊘ means inactive

You can also choose to Deactivate your policy using the Policy Editor.



CIS Benchmark for Microsoft Windows Server 2012 R2, v1.1.0, [Scored, Member Se

Policy Information

Sections	Technologies	Controls
54	1	232

Status: ◉ Active | Deactivate
Created By: Rikki Smythe (quays_rs9)
Created: 06/17/2015 at 00:45:43 (GMT+0530)

Assigned Technologies (1) Edit

Windows Server 20... assigned to 232 controls

What happens when I deactivate a policy?

- No posture evaluation will take place for the policy
- The policy will be hidden from your dashboard, reports and exceptions
- Any policy report schedules for the policy will be deactivated
- The policy will be removed from compliance scorecard reports
- The policy will be removed from option profiles (with the Scan by Policy option enabled)

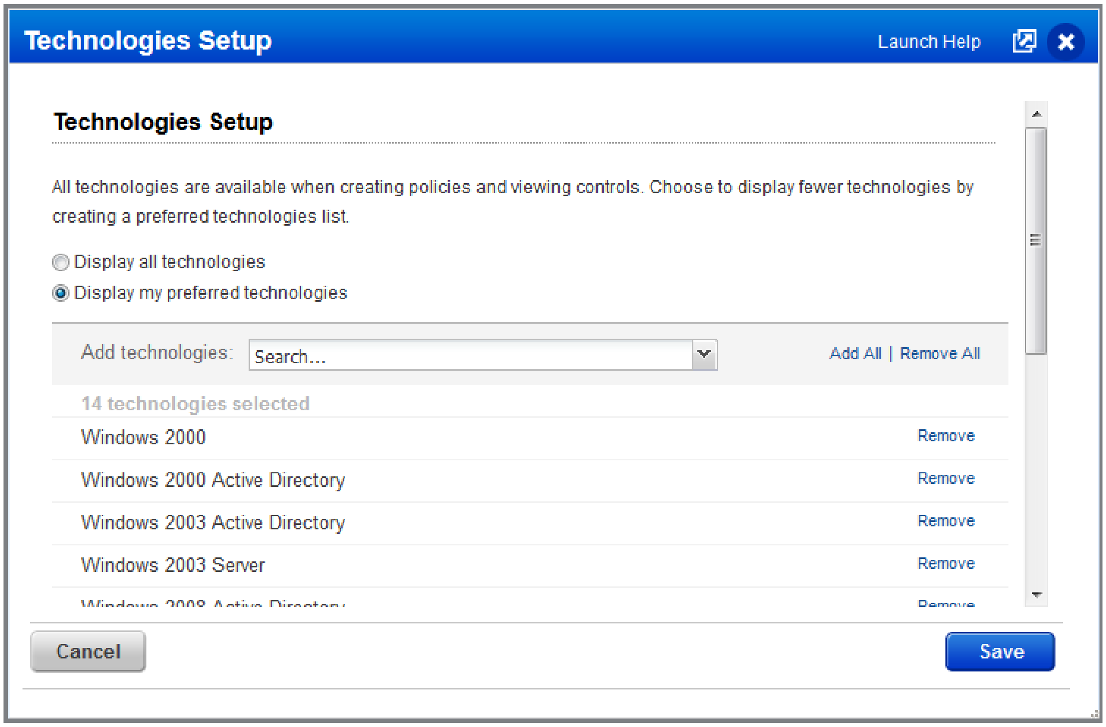
What happens if I re-activate the policy?

Posture evaluation will resume and the policy will be available again for scanning and reporting. You'll need to manually re-activate report schedules and add the policy back to your scorecard reports and option profiles. For policy report schedules, the policy will be selected for you.

Hide Technologies

You can now hide the technologies that you do not use on a regular basis. By hiding these technologies, you no longer need to go through the whole list of all the available technologies to select the ones you want. This is especially useful while searching controls by technologies. Only the controls related to the preferred technologies are displayed and are available for search.

Go to Policies > Setup > Technologies and create a list of preferred technologies that should be displayed. For example, let's say you're interested only in Windows. You add all the Windows technologies to your preferred list. All other technologies like Unix, Sybase, Solaris, etc will be hidden.



Technologies Setup

All technologies are available when creating policies and viewing controls. Choose to display fewer technologies by creating a preferred technologies list.

○ Display all technologies
● Display my preferred technologies

Add technologies: Search...

14 technologies selected

Windows 2000	Remove
Windows 2000 Active Directory	Remove
Windows 2003 Active Directory	Remove
Windows 2003 Server	Remove
Windows 2008 Active Directory	Remove

New Support for Tomcat Server Authentication

We now support compliance scans for tomcat servers running on Unix hosts. Simply create a new Tomcat Server authentication record with details about your Tomcat installation and instance. Unix authentication is required so you'll also need a Unix record for the host running the server.

Which technologies are supported?

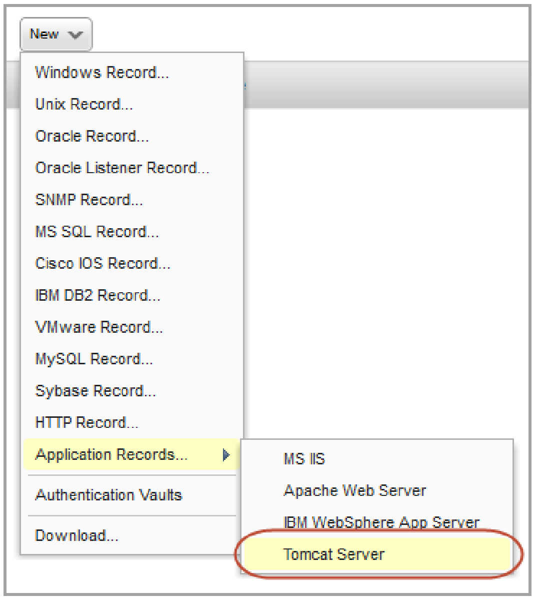
- Apache Tomcat 6.x and 7.x
- VMware vFabric tc Server 2.9.x
- Pivotal tc Server 3.x

How do I get started?

- Go to Scans > Authentication.

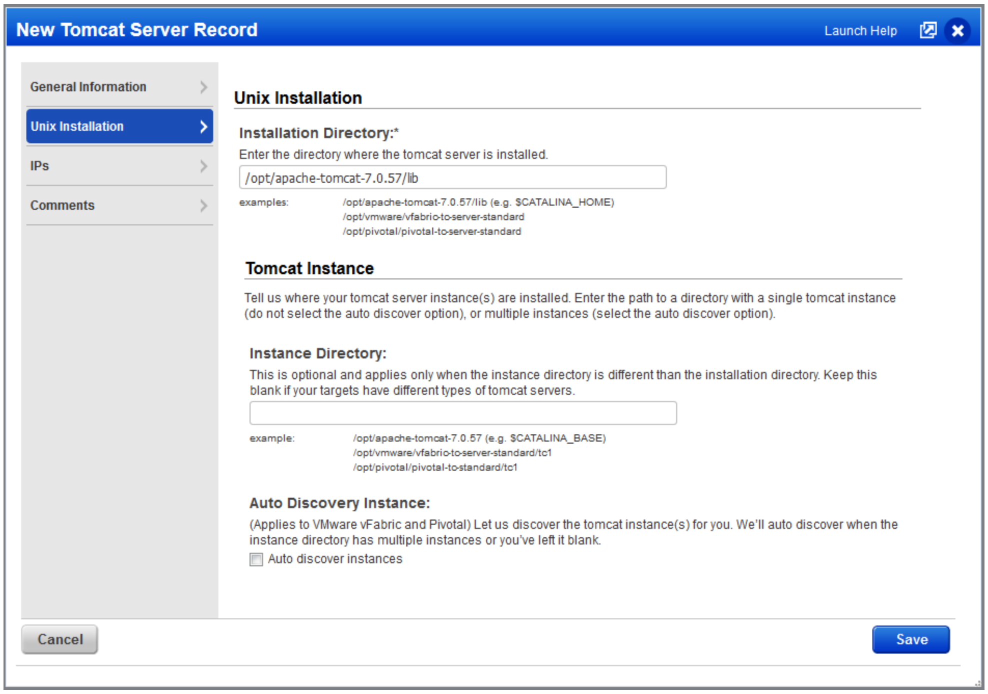
- Check that you have a Unix record already defined for each host running a tomcat server.

- Create a tomcat server record for the same host. Go to New > Application Records > Tomcat Server (as shown on the right).



Your Tomcat Server Record

You'll need to tell us where the tomcat server is installed. You may also need to tell us where the tomcat server instance(s) are installed – if different than the installation directory. Have multiple instances? Use the Auto Discover option and we'll find the instances for you (applies to VMware vFabric and Pivotal).



Unix Installation

Installation Directory:*

Enter the directory where the tomcat server is installed.

/opt/apache-tomcat-7.0.57/lib

examples: /opt/apache-tomcat-7.0.57/lib (e.g. $CATALINA_HOME)
/opt/vmware/vfabric-to-server-standard
/opt/pivotal/pivotal-to-server-standard

Tomcat Instance

Tell us where your tomcat server instance(s) are installed. Enter the path to a directory with a single tomcat instance (do not select the auto discover option), or multiple instances (select the auto discover option).

Instance Directory:

This is optional and applies only when the instance directory is different than the installation directory. Keep this blank if your targets have different types of tomcat servers.

example: /opt/apache-tomcat-7.0.57 (e.g. $CATALINA_BASE)
/opt/vmware/vfabric-to-server-standard/tc1
/opt/pivotal/pivotal-to-standard/tc1

Auto Discovery Instance:

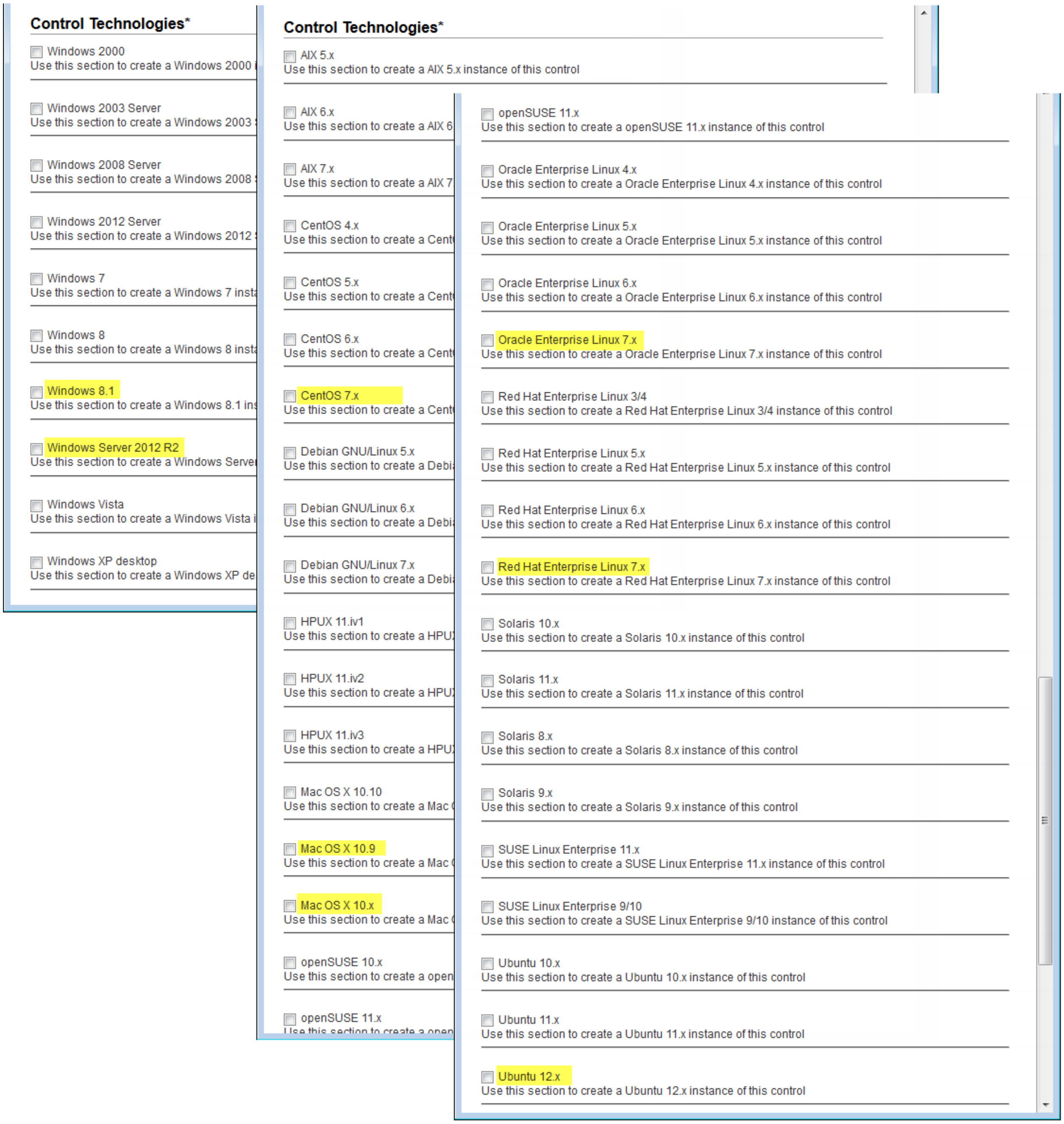
(Applies to VMware vFabric and Pivotal) Let us discover the tomcat instance(s) for you. We'll auto discover when the instance directory has multiple instances or you've left it blank.

☐ Auto discover instances

New Technologies Supported for UDCs

These Windows technologies are now supported for user defined controls: Windows 8.1 and Windows Server 2012 R2. These Unix technologies are now supported: Mac OS X 10.10, Mac OS X 10.9, Red Hat Enterprise Linux 7.x, Oracle Enterprise Linux 7.x, CentOS 7.x and Ubuntu 12.x.

Want to create controls for these technologies? Go to Policies > Controls, and choose New > Control. Then select the Windows or Unix control type you want to create. Tip - We already provide service-defined controls for these technologies in our Controls Library.



Control Technologies*

□ Windows 2000
Use this section to create a Windows 2000 i

□ Windows 2003 Server
Use this section to create a Windows 2003

□ Windows 2008 Server
Use this section to create a Windows 2008

□ Windows 2012 Server
Use this section to create a Windows 2012

□ Windows 7
Use this section to create a Windows 7 insta

□ Windows 8
Use this section to create a Windows 8 insta

□ Windows 8.1
Use this section to create a Windows 8.1 ins

□ Windows Server 2012 R2
Use this section to create a Windows Serve

□ Windows Vista
Use this section to create a Windows Vista i

□ Windows XP desktop
Use this section to create a Windows XP de

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

□ AIX 7.x
Use this section to create a AIX 7

□ CentOS 4.x
Use this section to create a Cent

□ CentOS 5.x
Use this section to create a Cent

□ CentOS 6.x
Use this section to create a Cent

□ CentOS 7.x
Use this section to create a Cent

□ Debian GNU/Linux 5.x
Use this section to create a Debi

□ Debian GNU/Linux 6.x
Use this section to create a Debi

□ Debian GNU/Linux 7.x
Use this section to create a Debi

□ HPUX 11.iv1
Use this section to create a HPU

□ HPUX 11.iv2
Use this section to create a HPU

□ HPUX 11.iv3
Use this section to create a HPU

□ Mac OS X 10.10
Use this section to create a Mac

□ Mac OS X 10.9
Use this section to create a Mac

□ Mac OS X 10.x
Use this section to create a Mac

□ openSUSE 10.x
Use this section to create a open

□ openSUSE 11.x
Use this section to create a open

□ openSUSE 11.x
Use this section to create a openSUSE 11.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

□ Oracle Enterprise Linux 6.x
Use this section to create a Oracle Enterprise Linux 6.x instance of this control

□ Oracle Enterprise Linux 7.x
Use this section to create a Oracle Enterprise Linux 7.x instance of this control

□ Red Hat Enterprise Linux 3/4
Use this section to create a Red Hat Enterprise Linux 3/4 instance of this control

□ Red Hat Enterprise Linux 5.x
Use this section to create a Red Hat Enterprise Linux 5.x instance of this control

□ Red Hat Enterprise Linux 6.x
Use this section to create a Red Hat Enterprise Linux 6.x 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

□ 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

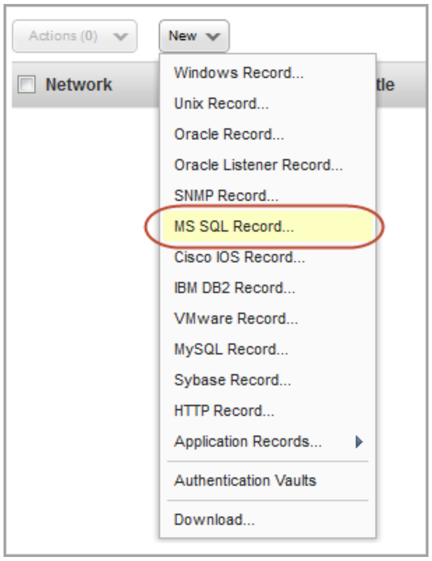
□ SUSE Linux Enterprise 9/10
Use this section to create a SUSE Linux Enterprise 9/10 instance of this control

□ Ubuntu 10.x
Use this section to create a Ubuntu 10.x instance of this control

□ Ubuntu 11.x
Use this section to create a Ubuntu 11.x instance of this control

□ Ubuntu 12.x
Use this section to create a Ubuntu 12.x instance of this control

Microsoft SQL Server 2014 Support



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

You'll need a MS SQL Server record to authenticate to your Microsoft SQL Server 2014 database, and scan it for compliance.

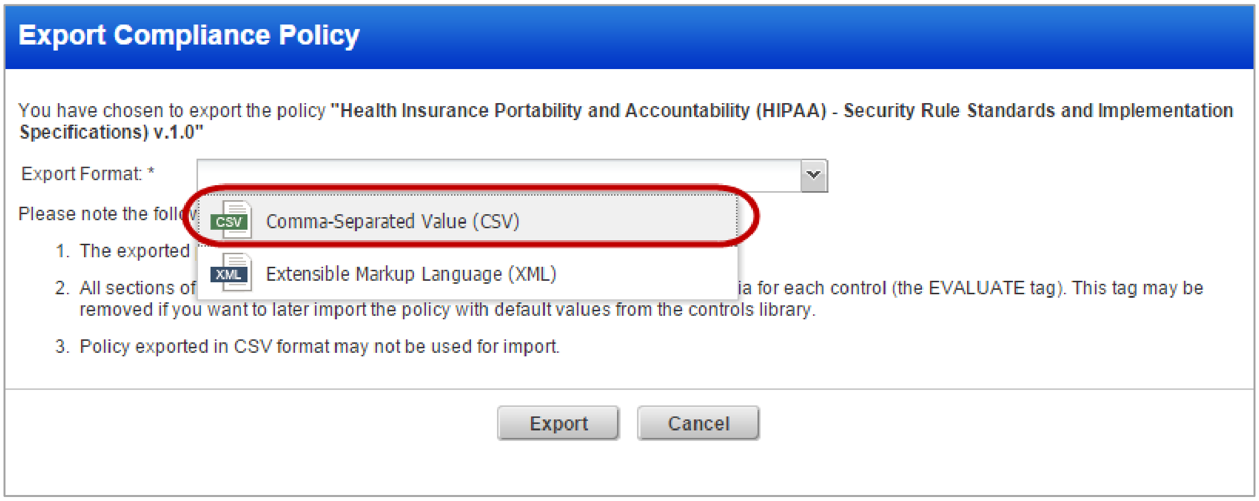
How do I get started?

Go to Scans > Authentication, and choose New > MS SQL Record (as shown on the right). This authentication type is supported for compliance scans only.

Export policies in CSV format

You can now export a policy to your local system in CSV format. This lets you quickly and easily share the policy and compare it to other policies you may have. A policy exported in CSV format will display information about Sections, Controls and Expected values.

To export a policy, simply go to Policies > Policies, choose the policy you want to export and click export from the Quick Actions menu and select "Comma-Separated Value (CSV)" as your Export Format.



Export Compliance Policy

You have chosen to export the policy **"Health Insurance Portability and Accountability (HIPAA) - Security Rule Standards and Implementation Specifications) v.1.0"**

Export Format: *

Please note the foll

1. The exported
2. All sections of ia for each control (the EVALUATE tag). This tag may be removed if you want to later import the policy with default values from the controls library.
3. Policy exported in CSV format may not be used for import.

Evidence added to SCAP Policy CSV Reports

By reviewing the evidence you can determine why a rule passed or failed for a host. The evidence content includes nodes (definitions and test sections) that represent the logic of the rule and the scan tests performed on the host.

For example, you might see this:

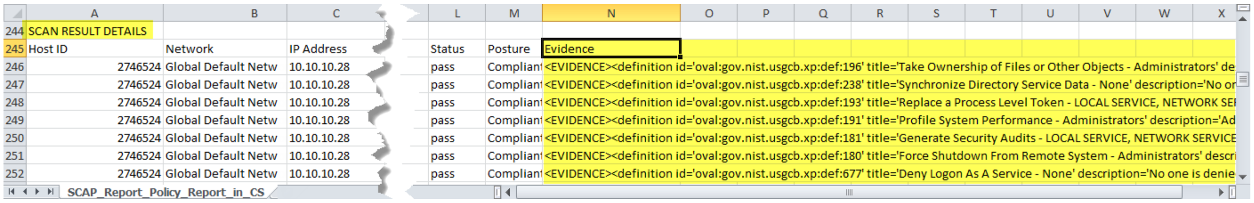
<EVIDENCE><definition id='oval:gov.nist.usgcb.xp:def:45' title='Access Audit for Global System Objects Disabled' description='Audit the access of global system objects is disabled' result='Pass'></definition><AND result='Pass'><definition id='oval:org.mitre.oval:def:105' title='Microsoft Windows XP is installed' description='The operating system installed on the system is Microsoft Windows XP.' result='Pass'></definition><test id='oval:gov.nist.usgcb.xp:tst:9' comment='Registry key HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Control\\Lsa\\AuditBaseObjects matches oval:gov.nist.usgcb.xp:var:45' result='Pass'><expected>type : reg_dword ^(0|1)$</expected><actual>HKEY_LOCAL_MACHINE System\CurrentControlSet\Control\Lsa AuditBaseObjects reg_dword 0 32_bit </actual></test></AND></EVIDENCE>

How do I run the SCAP Policy report?

Go to PC > Reports, and choose New > SCAP Report > Policy Report. Enter report details and be sure to select CSV for the report format. Then click Run.

Sample CSV report

The new Evidence column appears under Scan Result Details. (Tip - This is the last column in the report.)



	A	B	C	L	M	N
244	SCAN RESULT DETAILS					
245	Host ID	Network	IP Address	Status	Posture	Evidence
246	2746524	Global Default Netw	10.10.10.28	pass	Compliant	<EVIDENCE><definition id='oval:gov.nist.usgcb.xp:def:196' title='Take Ownership of Files or Other Objects - Administrators' de
247	2746524	Global Default Netw	10.10.10.28	pass	Compliant	<EVIDENCE><definition id='oval:gov.nist.usgcb.xp:def:238' title='Synchronize Directory Service Data - None' description='No or
248	2746524	Global Default Netw	10.10.10.28	pass	Compliant	<EVIDENCE><definition id='oval:gov.nist.usgcb.xp:def:193' title='Replace a Process Level Token - LOCAL SERVICE, NETWORK SEI
249	2746524	Global Default Netw	10.10.10.28	pass	Compliant	<EVIDENCE><definition id='oval:gov.nist.usgcb.xp:def:191' title='Profile System Performance - Administrators' description='Ad
250	2746524	Global Default Netw	10.10.10.28	pass	Compliant	<EVIDENCE><definition id='oval:gov.nist.usgcb.xp:def:181' title='Generate Security Audits - LOCAL SERVICE, NETWORK SERVICE
251	2746524	Global Default Netw	10.10.10.28	pass	Compliant	<EVIDENCE><definition id='oval:gov.nist.usgcb.xp:def:180' title='Force Shutdown From Remote System - Administrators' descri
252	2746524	Global Default Netw	10.10.10.28	pass	Compliant	<EVIDENCE><definition id='oval:gov.nist.usgcb.xp:def:677' title='Deny Logon As A Service - None' description='No one is denie

Qualys API Enhancements

Improvements for Managing Excluded IPs

The Excluded IP API v2 (/api/2.0/fo/asset/excluded_ip/) has been updated to 1) allow users to remove all IPs from the list, 2) allow users to set an expiration date when adding IPs to the list, and 2) show expiration dates in the list output.

User API Accepts Timezone Codes

With this release the User API (/msp/user.php) allows you to assign a timezone code to a user account using the new optional parameter "time_zone_code".

Launch Report API Accepts Recipient Groups

The Launch Report API has been updated to allow users to notify distribution groups when a report is complete, using the new optional parameter "recipient_group_id".

VM - Create Reports with Non-Running Kernels in Vulnerability Details

Several report DTDs have been updated to show vulnerabilities found on a kernel that is not the active running kernel. This option must be selected in the report template.

PC - New Tomcat Server Authentication API

The new Tomcat Server Authentication API (/api/2.0/fo/auth/tomcat/) lets you to list, create, update and delete Tomcat Server authentication records.

PC - Make Policies Active or Inactive

Policy status has been added to the XML output returned by the Compliance Policy List API (/api/2.0/fo/compliance/policy/?action=list) and the Export Compliance Policy API (/api/2.0/fo/compliance/policy/?action=export).

Want to learn more? See the *Qualys API Release Notes 8.5* for full details. You can download the release notes and our user guides from your account. Just go to Help > Resources.