



Qualys 8.9 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

- Unix Authentication Improvements
- New Authentication Vault for Cyber-Ark AIM
- Cisco NX-OS Authentication Supported
- MS SQL Server Authentication - Member Domain Support
- EC2 Scanning is Now Available to Unit Managers
- View Scanner Appliance Model Information
- Enhancement to the Prevent Overlapping Scans Feature
- Use External Scanners to Scan custom networks in VM and PC
- Improved Log Entries for Scheduled Tasks

Qualys Vulnerability Management (VM)

- Introducing a new user role: Remediation User
- Enhancements to Vulnerability Scan Processing
- New Scan Option – Purge Hosts when OS is Changed
- Created Date Added to Remediation Reports in CSV Format
- Vulnerability Scorecard Report – Display Ignored Vulnerability Status
- CVSS3 Final Score in XML, CSV Scan Reports
- Vulnerability Counts by Severity Added to Scan Report CSV

Qualys Policy Compliance (PC/SCAP)

- Support Asset Tags in Compliance Policies
- Include UDCs in Policy Export/Import
- Ability to Lock a Compliance Policy
- Start Policy Evaluation Anytime
- Active Directory Technologies Supported for Windows UDCs

Qualys API Enhancements

See the *Qualys API Release Notes 8.9* for details. You can download the release notes and our user guides from your account. Just go to Help > Resources.

Qualys 8.9 brings you many more Improvements and updates! [Learn more](#)

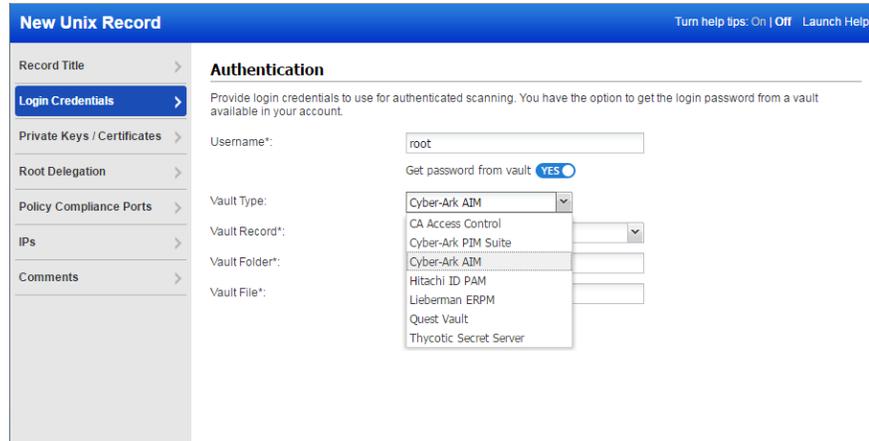
Qualys Cloud Platform

Unix Authentication Improvements

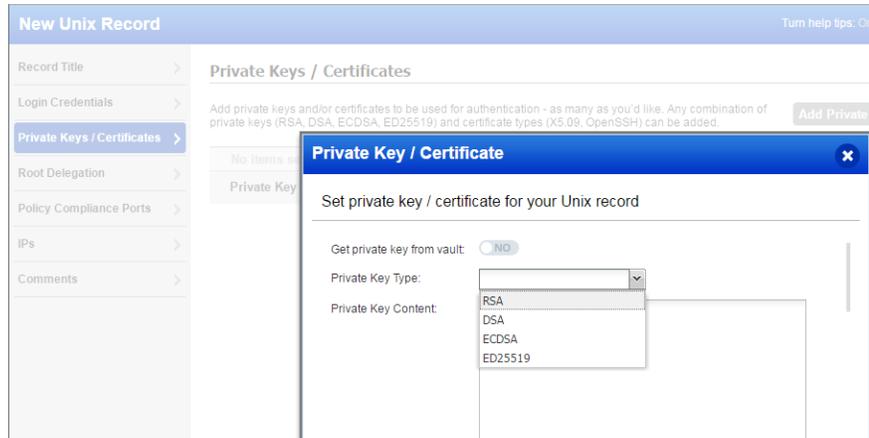
We're excited to tell you about the many enhancements we've made to Unix in this release. All enhancements are available for the Unix Record, using Qualys Cloud Suite UI and API. Now you can configure a single authentication record that supports better integration with third party vaults, and lets you define a variety of private keys and root delegation tools.

Here's what you can do!

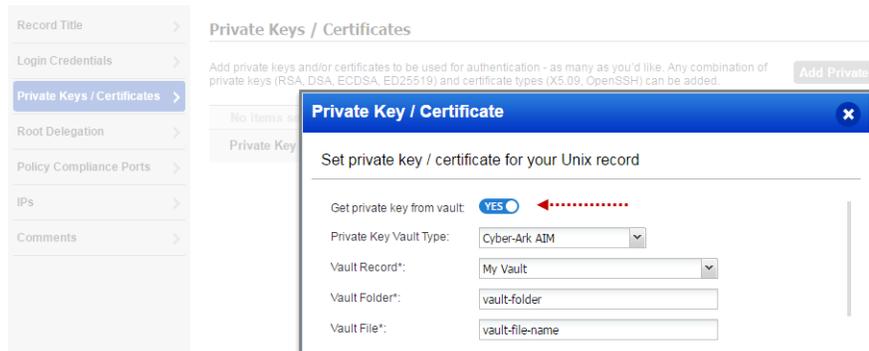
Get password for user login credentials from vault



Use multiple private keys and/or certificates for authentication. Any combination of private keys (RSA, DSA, ECDSA, ED25519) and certificates (OpenSSH, X.509)

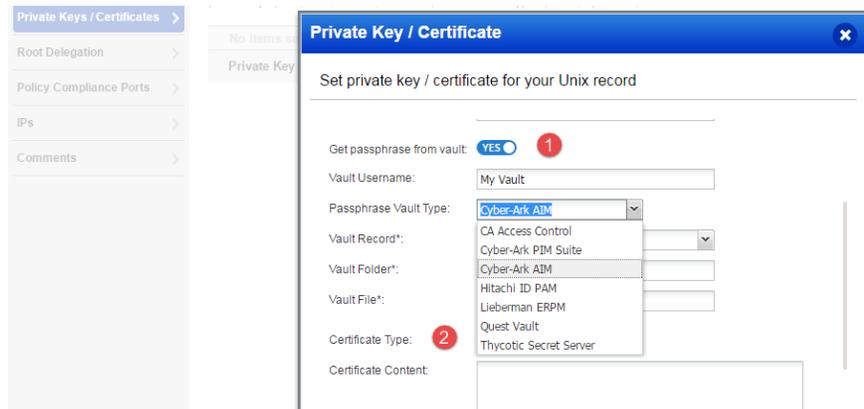


New option to get private key from vault (CyberArk AIM vault only)

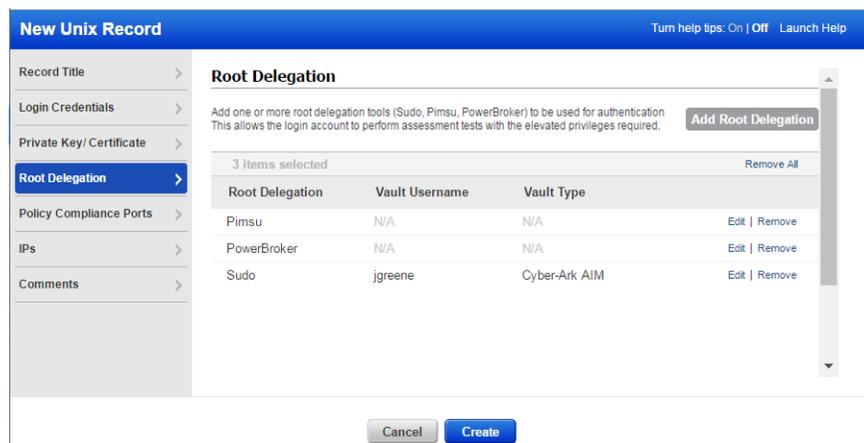


(1) New option to get private key passphrase from vault. Choose from vaults available in your account.

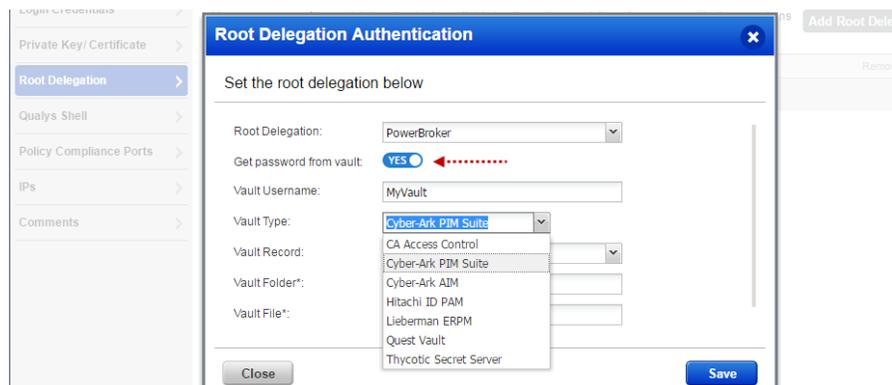
(2) Choose certificate type OpenSSH or X.509



Use multiple root delegation tools - Sudo, Pimsu, PowerBroker



New option to get password from vault. Choose from vaults available in your account.



Your existing Unix records

We'll upgrade all of your existing Unix records to add SSH2 authentication support and use the new Unix Record wizard. Upgraded records will function exactly as before and do not require any changes by you.

Good to Know - Cisco records and CheckPoint Firewall records will remain the same and will not be upgraded.

New Authentication Vault for Cyber-Ark AIM

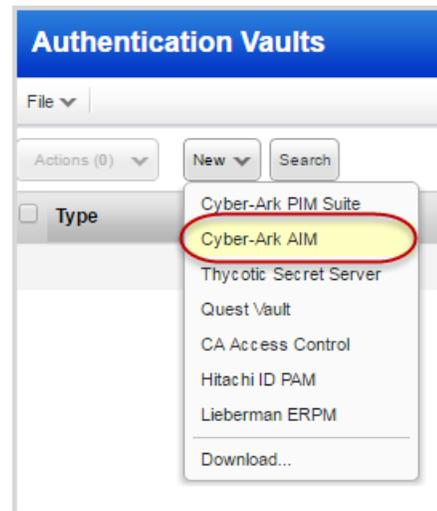
Our new authentication vault supports Cyber-Ark Application Identity Manager (AIM) configured with Cyber-Ark Central Credential Provider (CCP). This new vault can be used to securely retrieve authentication credentials at scan time, for many authentication types, from your Cyber-Ark AIM/CCP solution.

Windows - In a Windows Record you can choose to get the login password from your Cyber-Ark AIM solution.

Unix - In a Unix Record you can choose to get this authentication information from your Cyber-Ark AIM solution: login password, private key and private key passphrase.

And More ! Many more authentication records let you choose to get the login password from your Cyber-Ark AIM solution.

These include Cisco, Checkpoint Firewall, Oracle, Oracle Listener, IBM DB2, MS SQL, Sybase, MySQL and VMware.



How do I get started?

Configure your Cyber-Ark authentication vault (vault credentials), configure authentication records for your authentication types (safe location in Cyber-Ark AIM), and start your scans. That's it!

Required credentials

- Application ID (CCP web services)
- Name of digital password safe
- URL to AIM web service (choose SSL Verify and we'll verify the server's SSL certificate is valid and trusted)

The following is also required if your server requires a certificate for authentication:

- Certificate (X.509 in PEM format)
- Private key that corresponds to public key stored on certificate
- Private key passphrase

Cisco NX-OS Authentication Supported

We now support authentication for Cisco NX-OS devices as well.

Simply create a new Cisco authentication record (authentication record for all supported Cisco devices is now grouped as Cisco Record.)

How do I get started?

Just go to Scans > Authentication and click New > Cisco Record to create a new Cisco authentication record (as shown on right).

Your Cisco Authentication Record

You'll notice that the settings are the same for all supported Cisco devices (Cisco NX-OS, Cisco IOS, Cisco ASA and Cisco IOS XE technologies). If the "enable" command on the target hosts requires a password, then you must also provide the enable password in the authentication record.

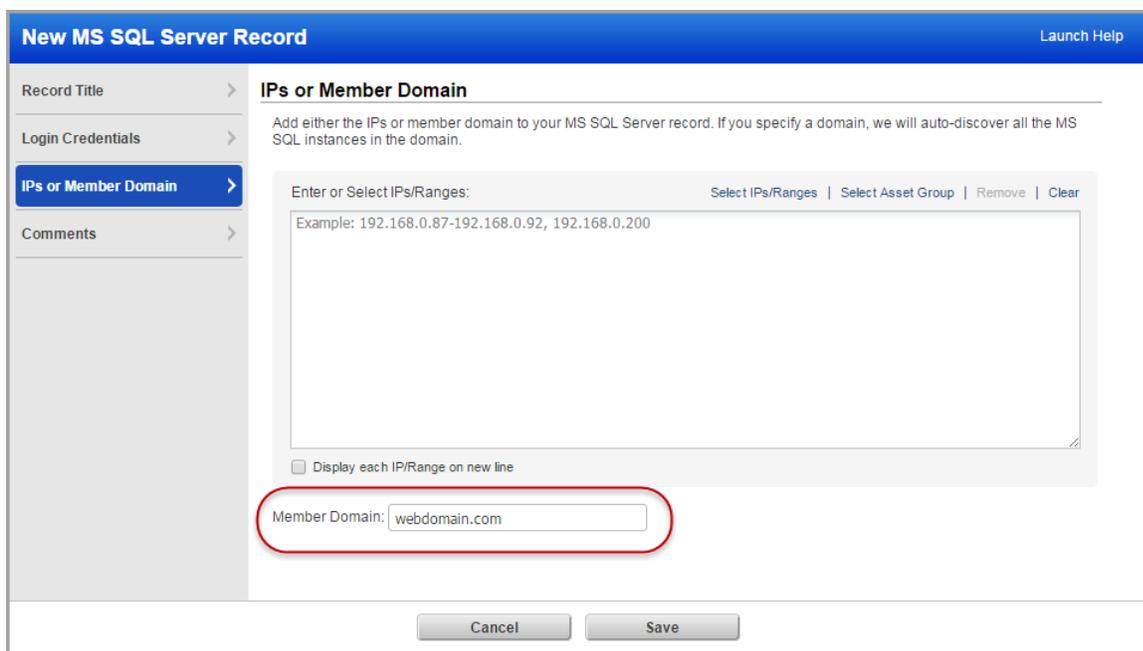
A screenshot of the 'New Cisco Record' form. The form has a blue header with 'New Cisco Record' on the left and 'Launch Help' on the right. On the left side, there is a sidebar with 'Record Title', 'Login Credentials', 'IPs', and 'Comments'. The main content area is divided into two sections: 'Login Credentials' and 'Policy Compliance'.
Login Credentials
Use the basic login credential or choose to use authentication vault for authenticated scanning.
 Basic authentication Authentication Vault
User Name: *
Password: Clear Text Password
Confirm Password:
Enable Password:
Confirm Enable Password:
Policy Compliance
If services (SSH, telnet, rlogin) are not running on well known ports (22, 23, 513 respectively) enter the ports in the custom field below.
Ports: Well Known Ports (22,23,513) Custom Ports:
example: 2222, 2223
At the bottom of the form are 'Cancel' and 'Save' buttons.

MS SQL Server Authentication - Member Domain Support

You can now create a single record for all MS SQL server targets that are members of your domain. In the MS SQL record wizard the “IPs” tab is renamed to “IPs or Member Domain”. To use domain based support, provide your active directory or NetBIOS domain name on the “IPs or Member Domain” tab in the new Member Domain field.

When Member Domain is provided:

- We’ll auto discover all MS SQL servers in the domain.
- It’s not possible to provide IP addresses for the same record.



The screenshot shows a web interface for creating a new MS SQL server record. The title bar reads "New MS SQL Server Record" with a "Launch Help" link on the right. A left-hand navigation pane contains tabs for "Record Title", "Login Credentials", "IPs or Member Domain" (which is selected and highlighted in blue), and "Comments". The main content area is titled "IPs or Member Domain" and contains the following text: "Add either the IPs or member domain to your MS SQL Server record. If you specify a domain, we will auto-discover all the MS SQL instances in the domain." Below this is a text input field with the placeholder "Enter or Select IPs/Ranges:" and buttons for "Select IPs/Ranges", "Select Asset Group", "Remove", and "Clear". An example text "Example: 192.168.0.87-192.168.0.92, 192.168.0.200" is shown in the input field. Below the input field is a checkbox labeled "Display each IP/Range on new line". At the bottom of the main area, the "Member Domain:" label is followed by a text input field containing "webdomain.com", which is circled in red. At the very bottom of the form are "Cancel" and "Save" buttons.

EC2 Scanning is Now Available to Unit Managers

EC2 Scanning must be enabled for your subscription. Contact your Account Manager or Support to get it.

EC2 scanning is not just for Managers anymore! Now Unit Managers can start and schedule EC2 scans as long as the IPs for the EC2 environment are in the Unit Manager’s Business Unit.

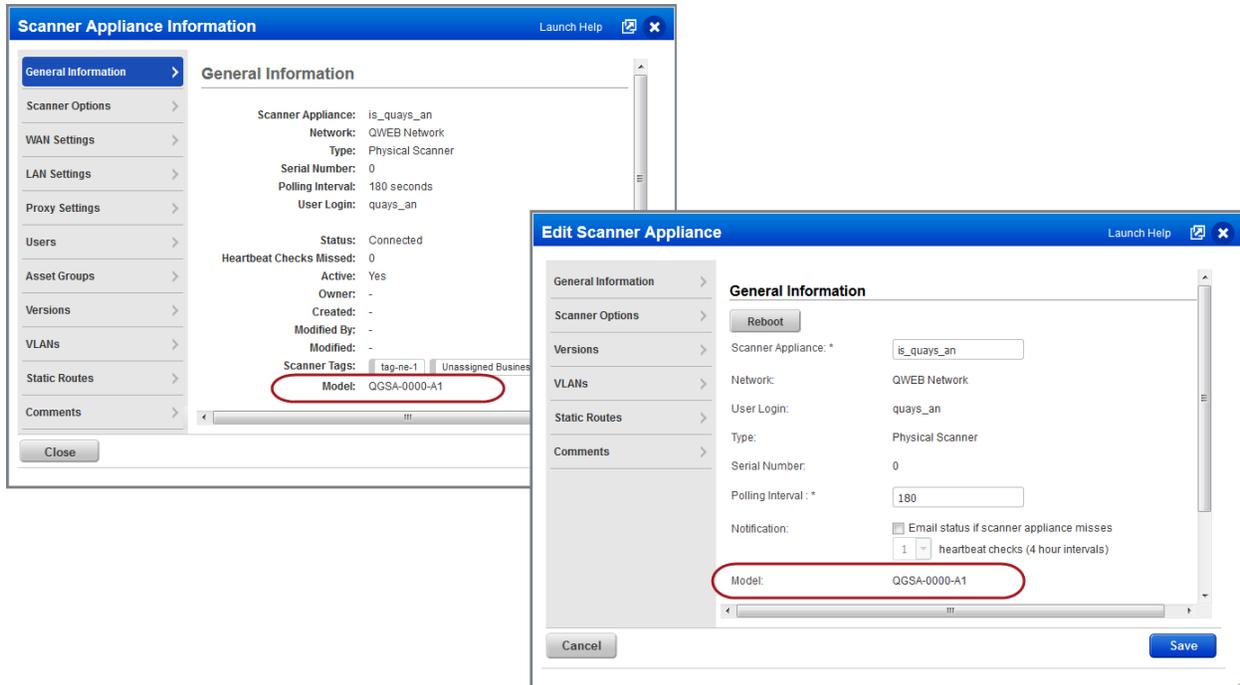
Unit Managers have these permissions:

- Perform vulnerability scans and/or compliance scans on your EC2 assets
- Configure a virtual scanner using Amazon EC2/VPC
- Create EC2 connectors (in the AssetView application)

Refer to the online help for details on how to set up and run EC2 scans.

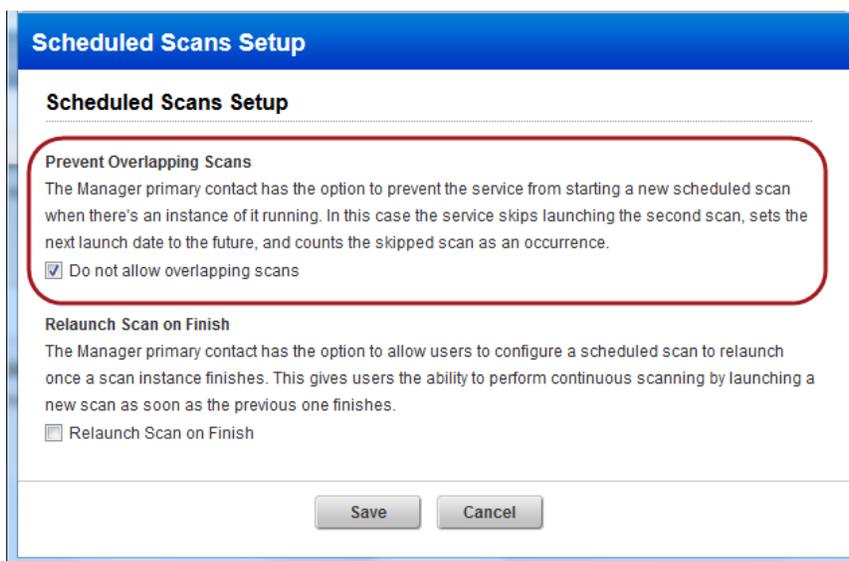
View Scanner Appliance Model Information

We'll show the model of the appliance on the Scanner Appliance Information page and the Edit Scanner Appliance page. Note that you'll see cvscanner for virtual scanners and oscanner for offline scanners.



Enhancement to the Prevent Overlapping Scans Feature

We've enhanced this feature to also consider paused scans. When you select "Do not allow overlapping scans", a new scheduled scan will not be started when there's already an instance of the scan running or paused. Go to Scans > Setup > Scheduled Scans to enable this option.



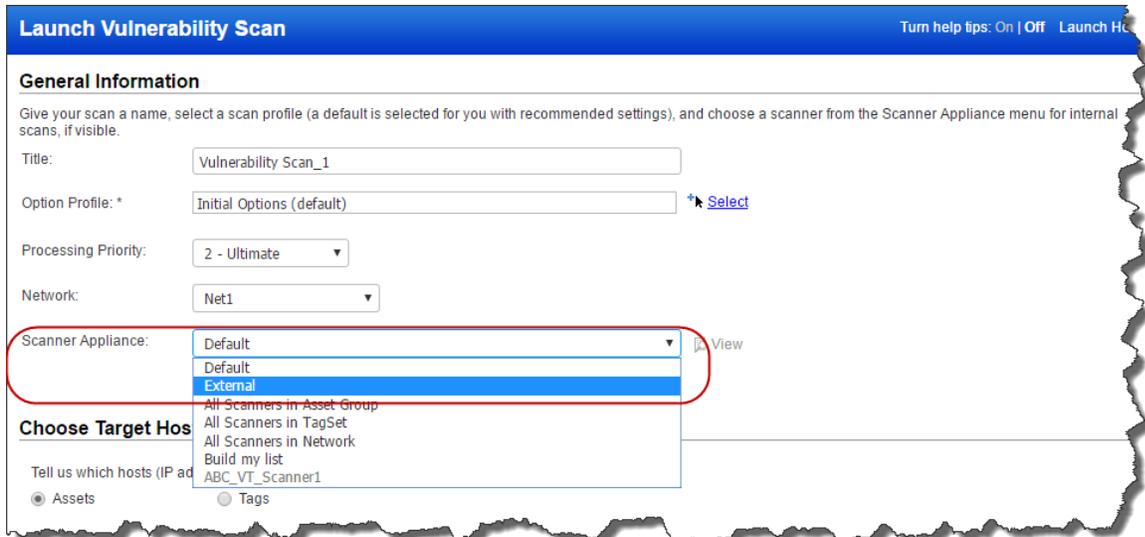
Use External Scanners to Scan custom networks in VM and PC

You can now use External scanners for scanning custom networks. Simply choose the "External" scanner appliance option at scan time or when you schedule your scan.

Ready to start your scan?

Go to Scans > New > Scan, select the network you want to scan, select the External scanner appliance option, and target IPs on your network perimeter.

Launch Vulnerability scans:



Launch Vulnerability Scan Turn help tips: On | Off Launch Help

General Information

Give your scan a name, select a scan profile (a default is selected for you with recommended settings), and choose a scanner from the Scanner Appliance menu for internal scans, if visible.

Title:

Option Profile: * [Select](#)

Processing Priority:

Network:

Scanner Appliance: [View](#)

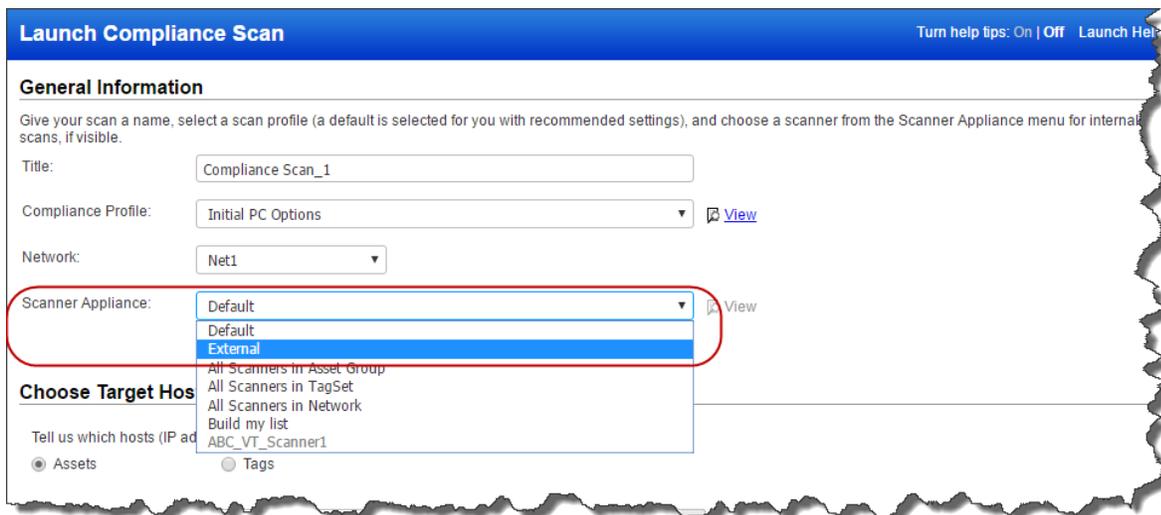
- Default
- External**
- All Scanners in Asset Group
- All Scanners in TagSet
- All Scanners in Network
- Build my list
- ABC_VT_Scanner1

Choose Target Hosts

Tell us which hosts (IP address) you want to scan:

Assets Tags

Launch Compliance Scans:



Launch Compliance Scan Turn help tips: On | Off Launch Help

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:

Compliance Profile: [View](#)

Network:

Scanner Appliance: [View](#)

- Default
- External**
- All Scanners in Asset Group
- All Scanners in TagSet
- All Scanners in Network
- Build my list
- ABC_VT_Scanner1

Choose Target Hosts

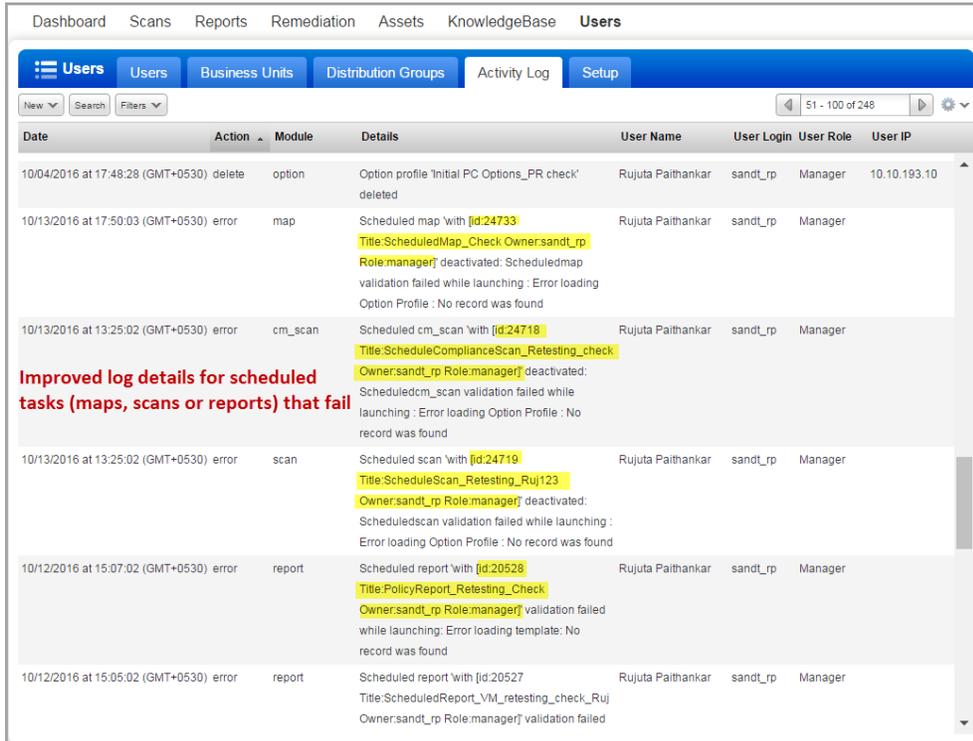
Tell us which hosts (IP address) you want to scan:

Assets Tags

Improved Log Entries for Scheduled Tasks

We have simplified troubleshooting by providing additional details in the activity log for a failed scheduled task. Along with the cause of failure, we now provide task id, title, task owner and user role for a scheduled task (maps, scan or reports) that fails.

Here's an example of failed scheduled map and scheduled scan.



The screenshot shows the 'Users' section of a management interface, specifically the 'Activity Log' tab. The table lists several failed tasks. A red text overlay on the left side of the table reads: 'Improved log details for scheduled tasks (maps, scans or reports) that fail'. The table columns are: Date, Action, Module, Details, User Name, User Login, User Role, and User IP. The 'Details' column contains expanded error messages for failed tasks, including task IDs, titles, and owner information.

Date	Action	Module	Details	User Name	User Login	User Role	User IP
10/04/2016 at 17:48:28 (GMT+0530)	delete	option	Option profile 'Initial PC Options_PR check' deleted	Rujuta Paithankar	sandt_rp	Manager	10.10.193.10
10/13/2016 at 17:50:03 (GMT+0530)	error	map	Scheduled map with [id:24733] [Title:ScheduledMap_Check,Owner:sandt_rp,Role:manager] deactivated: Scheduledmap validation failed while launching : Error loading Option Profile : No record was found	Rujuta Paithankar	sandt_rp	Manager	
10/13/2016 at 13:25:02 (GMT+0530)	error	cm_scan	Scheduled cm_scan with [id:24718] [Title:ScheduleComplianceScan_Retesting_check,Owner:sandt_rp,Role:manager] deactivated: Scheduledcm_scan validation failed while launching : Error loading Option Profile : No record was found	Rujuta Paithankar	sandt_rp	Manager	
10/13/2016 at 13:25:02 (GMT+0530)	error	scan	Scheduled scan with [id:24719] [Title:ScheduleScan_Retesting_Ruj123,Owner:sandt_rp,Role:manager] deactivated: Scheduledscan validation failed while launching : Error loading Option Profile : No record was found	Rujuta Paithankar	sandt_rp	Manager	
10/12/2016 at 15:07:02 (GMT+0530)	error	report	Scheduled report with [id:20528] [Title:PolicyReport_Retesting_Check,Owner:sandt_rp,Role:manager] validation failed while launching: Error loading template: No record was found	Rujuta Paithankar	sandt_rp	Manager	
10/12/2016 at 15:05:02 (GMT+0530)	error	report	Scheduled report with [id:20527] [Title:ScheduledReport_VM_retesting_check_Ruj,Owner:sandt_rp,Role:manager] validation failed	Rujuta Paithankar	sandt_rp	Manager	

Go to Users > Activity Log.

The details column in the now provides additional task details - task id, task title, task owner and user role.

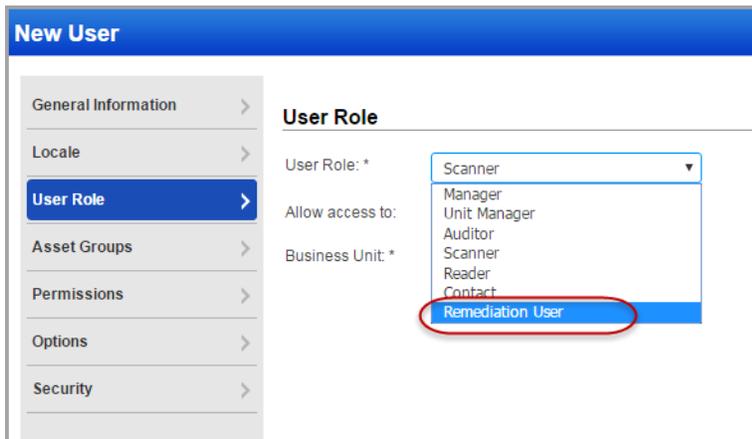
Qualys Vulnerability Management (VM)

Introducing a new user role: Remediation User

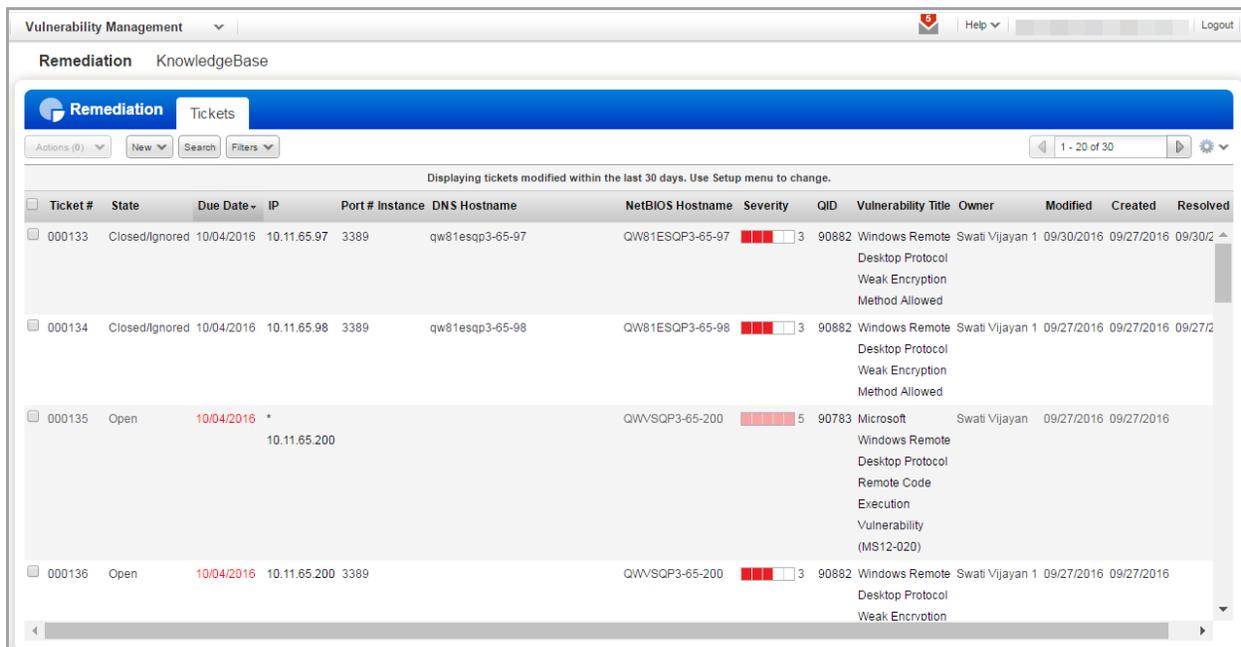
Users with this role will only have access to remediation tickets and the vulnerability knowledgebase. These users do not have any scanning or reporting privileges.

Good to know:

- Manager can assign Business Unit and Asset Groups to the user.
- Manager can assign tickets generated by policy rules for assets (asset groups) associated with the user.
- While creating or editing a policy, a manager can assign a remediation user, who will be assigned all tickets originating from the policy.



The user will have same permissions that are applicable to the assets. The user can view, edit or resolve remediation tickets that are assigned to the user or owned by the user.



Enhancements to Vulnerability Scan Processing

Host scan time is now based on scan end time

We've changed the way we report the host scan time when updating vulnerabilities and tickets. The host scan time will now be based on when the scan finished, not when the scan started. We'll get the scan end date/time from QID 45038 "Host Scan Time". If this QID was not included in your vulnerability scan then we'll use the scan start date/time.

Choose a priority level for each scan

Now you can tell us which of your vulnerability scans has the highest priority and should be processed first. You'll do this at the time you launch/schedule your scan. By default, 0-No Priority is selected. You can choose from nine priority levels with the highest priority being 1-Emergency and the lowest priority being 9-Low.

The screenshot shows the 'Launch Vulnerability Scan' interface. The 'Processing Priority' dropdown menu is open, displaying the following options: 0 - No Priority, 1 - Emergency, 2 - Ultimate, 3 - Critical, 4 - Major, 5 - High, 6 - Standard, 7 - Medium, 8 - Minor, 9 - Low, and 0 - No Priority. A red arrow points to the '1 - Emergency' option with the text 'Set priority for this scan'. The interface also includes fields for 'Title', 'Option Profile', 'Scanner Appliance', 'Asset Groups', 'IPs/Ranges', and 'Exclude IPs/Ranges'. The 'Assets' radio button is selected under 'Tell us which hosts (IP address) to scan'.

Finished scans are processed before running scans

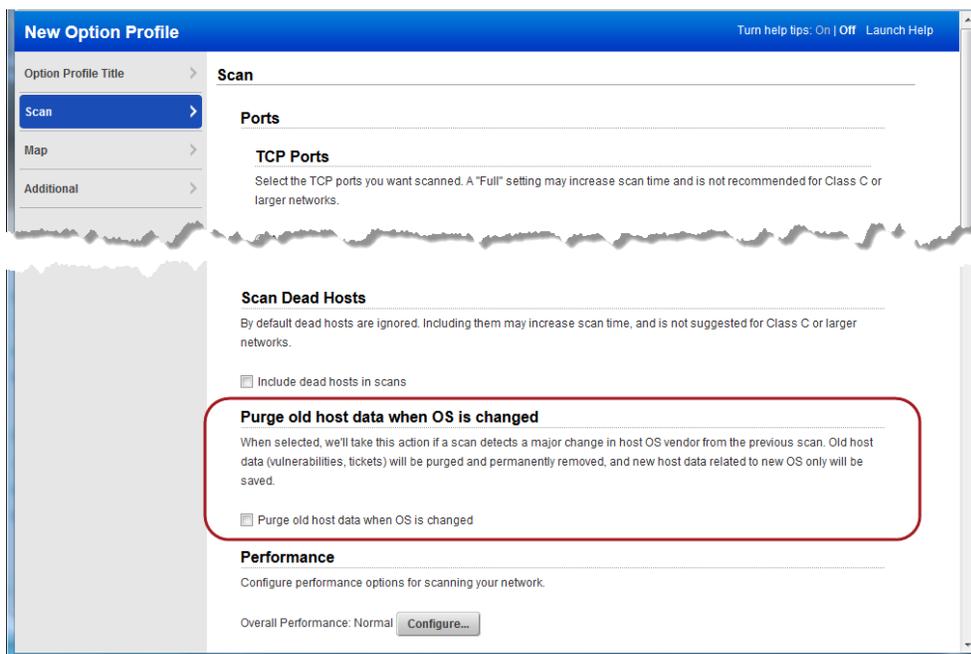
We'll process scans in this order:

- finished scan with priority set
- finished scan with no priority
- running scan with priority set
- running scan with no priority

New Scan Option – Purge Hosts when OS is Changed

This feature must be enabled for your subscription. Contact your Account Manager or Support to get it.

This option is useful if you have systems that are regularly decommissioned or replaced. By selecting this option in your option profile, you're telling us you want to purge a host if we detect a change in the host's Operating System (OS) vendor at scan time. For example, the OS changes from Linux to Windows or Debian to Ubuntu. We will not purge the host for an OS version change like Linux 2.8.13 to Linux 2.9.4.



Created Date Added to Remediation Reports in CSV Format

Remediation reports in CSV format will now show the date/time when the report was created. This appears in the new column CreatedDate.

Sample CSV Report

This sample remediation report was created on October 24, 2016.

	A	B	C	D	E	F	G	H	I	J	K	L		
1	Company	User	ReportTitle	AssetGroups	IPs	Users	CreatedDate	Network	AssetTags					
2	Qualys, Inc.	Patrick Slimmer	Tickets per Vuln	All		All Users	10/24/2016 at 12:02:06 (GMT-0700)	Global Default Network						
3	QID	Title	Type	Disabled	Severity	OriginalSe	Tickets	Open	Resolved	Closed	AvgResolu	Overdue		
4	90783	Microsoft Windo	Confirmed	no				5	5	0	0	N/A	1	
5	90464	Microsoft Windo	Confirmed	no				5	4	2	0	2	0.5	1
6	90477	Microsoft SMB Re	Confirmed	no				5	4	4	0	0	N/A	1
7	90517	Microsoft Windo	Confirmed	no				5	4	4	0	0	N/A	0
8	90572	Microsoft WordP	Confirmed	no				5	4	4	0	0	N/A	0
9	90577	Microsoft SMB Cl	Confirmed	no				5	4	4	0	0	N/A	0
10	90596	Microsoft Windo	Confirmed	no				5	4	4	0	0	N/A	0
11	90606	Microsoft Media	Confirmed	no				5	4	4	0	0	N/A	0
12	90616	Microsoft Windo	Confirmed	no				5	4	4	0	0	N/A	0
13	90923	Microsoft Cumuli	Confirmed	no				5	4	4	0	0	N/A	0

Date/time when the report was created

Vulnerability Scorecard Report – Display Ignored Vulnerability Status

You'll notice a new option in the vulnerability scorecard report template to display ignored vulnerability when reporting vulnerability counts by status. This option is available only for scorecard reports.

Tip: You can choose this option when you edit the Scorecard Report template.

Checkout the following report sample with the ignored vulnerability status information.

Status	Count	Percentage
New	10	7%
Active	74	51%
Fixed	48	33%
Re-Opened	0	0%
Ignored	13	9%
Total	145	100%

Age Range (Days)	Count	Percentage
0 - 30 days	10	7%
31 - 60 days	74	51%
61 - 90 days	48	33%
91 - 180 days	0	0%
181 - 270 days	13	9%
> 270 days	0	0%
Total	145	100%

Title	Asset Group	Hosts Scanned	Severities (Vulnerable Hosts)			Vulnerable Hosts	Total Goal %	Vulnerability Type	Vulnerability Status					
			Level 5	Level 4	Level 3				Confirmed	Potential	New	Active	Fixed	Re-Opened
ALL		13	18 (7)	0 (0)	36 (8)	8	61.5%	54	0	10	44	12	0	4
10.10.10.9_conf_5		1	3 (1)	0 (0)	4 (1)	1	100%	7	0	0	7	0	0	1
10.10.10.7_N_9		2	3 (1)	0 (0)	4 (1)	1	50%	7	0	0	7	11	0	1
10.10.32.6_Conf1_Pot3		1	2 (1)	0 (0)	2 (1)	1	100%	4	0	0	4	0	0	0
10.10.32.5_POT_5432		1	0 (0)	0 (0)	12 (1)	1	100%	12	0	0	12	0	0	0
10.10.10.11		1	0 (0)	0 (0)	0 (0)	0	0%	0	0	0	0	1	0	2
10.10.10.7_conf_3N2		1	0 (0)	0 (0)	0 (0)	0	0%	0	0	0	0	11	0	0
10.10.32.11_Conf_L4		1	0 (0)	0 (0)	0 (0)	0	0%	0	0	0	0	0	0	1
AG - Scanner_AfterIgn_532		1	0 (0)	0 (0)	0 (0)	0	0%	0	0	0	0	1	0	2
AG-Empty		0	0 (0)	0 (0)	0 (0)	0	0%	0	0	0	0	0	0	0
QWEB-12947		2	0 (0)	0 (0)	0 (0)	0	0%	0	0	0	0	12	0	2
Total		24	26 (10)	0 (0)	58 (12)	12	50%	84	0	10	74	48	0	13

CVSS3 Final Score in XML, CSV Scan Reports

We've added the CVSS3 final score in scan reports with host based findings (also known as asset data reports). XML and CSV formats were updated in this release. See the *Qualys API Release Notes 8.9* for details, including DTD changes.

Sample XML Report

```
...
<VULN_INFO>
  <QID id="qid_66021">66021</QID>
  <TYPE>Vuln</TYPE>
  <SSL>>false</SSL>
  <RESULT>
<![CDATA[ @(#)pcnfsd_v2.c 1.6 - rpc.pcnfsd V2.0 (c) 1991 Sun Technology
Enterprises, Inc.]]>
  </RESULT>
  <FIRST_FOUND>2016-07-13T06:54:15Z</FIRST_FOUND>
  <LAST_FOUND>2016-07-13T06:54:15Z</LAST_FOUND>
  <TIMES_FOUND>1</TIMES_FOUND>
  <VULN_STATUS>New</VULN_STATUS>
  <CVSS_FINAL>4</CVSS_FINAL>
  <CVSS3_FINAL>3.2</CVSS3_FINAL>
</VULN_INFO>
...
```

Sample CSV Report

```
...
"IP","DNS","NetBIOS","Tracking Method","OS","IP
Status","QID","Title","VulnStatus","Type","Severity","Port","Protocol","F
QDN","SSL","First Detected","Last Detected","Times Detected","CVE
ID","Vendor Reference","Bugtraq ID","CVSS","CVSS Base","CVSS
Temporal","CVSS Environment","CVSS3","CVSS3 Base","CVSS3 Temporal",...

"10.10.24.72","2k3x64sp2-24-72","2K3X64SP2-24-72","IP","Windows 2003 R2
Service Pack 2","host scanned, found vuln","38626","OpenSSL oracle padding
vulnerability(CVE-2016-2107)","New","Vuln","4","2381","tcp",,"over
ssl","08/12/2016 16:34:37","08/12/2016 16:34:37","1","CVE-2016-
2107","OpenSSL Security Advisory 20160503","91787","4.3","2.6
(AV:N/AC:H/Au:N/C:P/I:N/A:N)","2 (E:POC/RL:OF/RC:C)","Asset Group: AG 24,
Collateral Damage Potential: Medium-High, Target Distribution: Medium,
Confidentiality Requirement: High, Integrity Requirement: Medium,
Availability Requirement: High","5.2","5.8","5.2",...
```

...

Vulnerability Counts by Severity Added to Scan Report CSV

This update applies to a scan report with host based findings. Now when you sort your scan report by vulnerability you'll see a section in the CSV output that shows the total number of vulnerabilities detected at each severity level.

For each severity level (1-5), you'll see the total number of vulnerabilities, plus the number of vulnerabilities for each vulnerability type - Confirmed, Potential and Information Gathered (edit your report template to change the types included). When your report includes trending, you'll also see Trend columns showing the changes to vulnerability counts for your report timeframe.

Sample CSV Report

This sample report includes all vulnerability types - Confirmed, Potential and Information Gathered - and it includes trending for the last month.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	All Vuln Types	10/11/2016 at 11:21:26 (GMT-0700)										
2	Qualys, Inc.	1600 Bridge Parkway	Redwood City	California	USA	94065						
3	Patrick Slimme	qualys_ps	Manager									
4												
5	Asset Groups	IPs	Active Hosts	Hosts Matching	Trend Analysis	Date Range	Network	Asset Tags				
6	Windows Hosts:	NONE	11	11	Last 1 month	09/10/2016 - 10/	Global De	NONE				
7												
8	Total Vulnerab	Avg Security Ri	Business Risk									
9	4324	3.8	33/100									
10												
11	IP	Network	Total Vulner	Security Risk								
12	10.10.10.11	Global Default	451	4								
13	10.10.10.28	Global Default	326	3.9								
14	10.10.10.46	Global Default	353	3.9								
15	10.10.10.66	Global Default	485	4								
16	10.10.10.77	Global Default	292	3.9								
17	10.10.10.86	Global Default	251	3.8								
18	10.10.10.88	Global Default	248	3.8								
19	10.10.10.113	Global Default	420	4.1								
20	10.10.10.180	Global Default	802	3.9								
21	10.10.10.215	Global Default	143	3.1								
22	10.10.10.221	Global Default	553	3.8								
23												
24												
25	Severity	Total	Trend	Confirmed	Trend	Potential	Trend	Information Gathered				
26	5	1043	2	1036	2	7	0	0				
27	4	1572	0	1559	0	13	0	0				
28	3	893	1	815	0	35	1	43				
29	2	377	4	187	3	39	1	151				
30	1	439	2	23	0	17	2	399				
31	Total	4324	9	3620	5	111	4	593				
32												
33	IP	Network	DNS	NetBIOS	Tracking Metho	OS	IP Status	QID	Title	Vuln Statu	Type	Severity
34	10.10.10.77	Global Default	com2k12dc.c	COM2K12DC	IP	Windows 2012	host scanr	91264	Microsoft	Active	Vuln	5
35	10.10.10.86	Global Default	2012r2dtr-10	2012R2DTR-10-8	IP	Windows 2012 R	host scanr	91264	Microsoft	Active	Vuln	5
36	10.10.10.88	Global Default	com2k12r2-c	COM2K12R2-DC	IP	Windows 2012	host scanr	91264	Microsoft	Active	Vuln	5

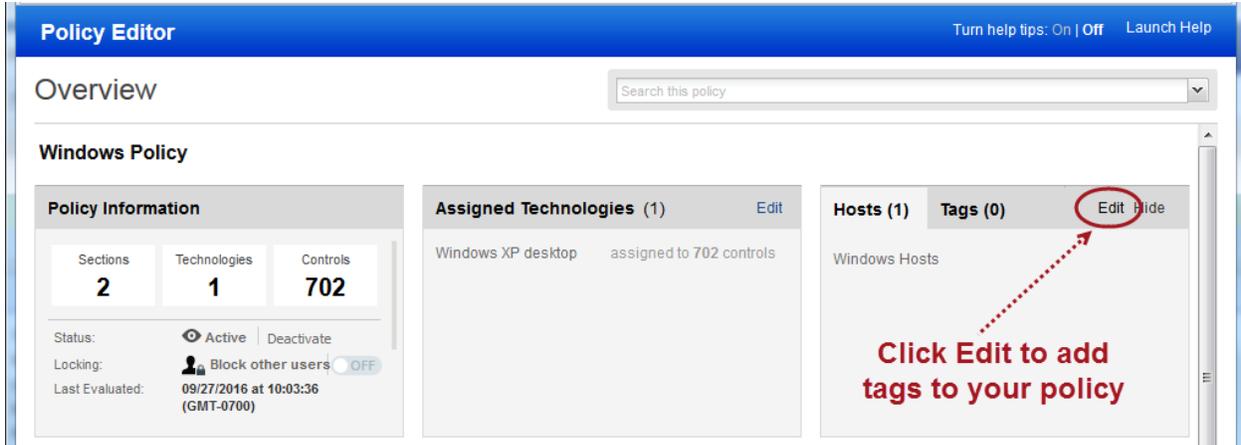
new section with vulnerabilities by severity (applicable when you sort by vulnerability)

Qualys Policy Compliance (PC)

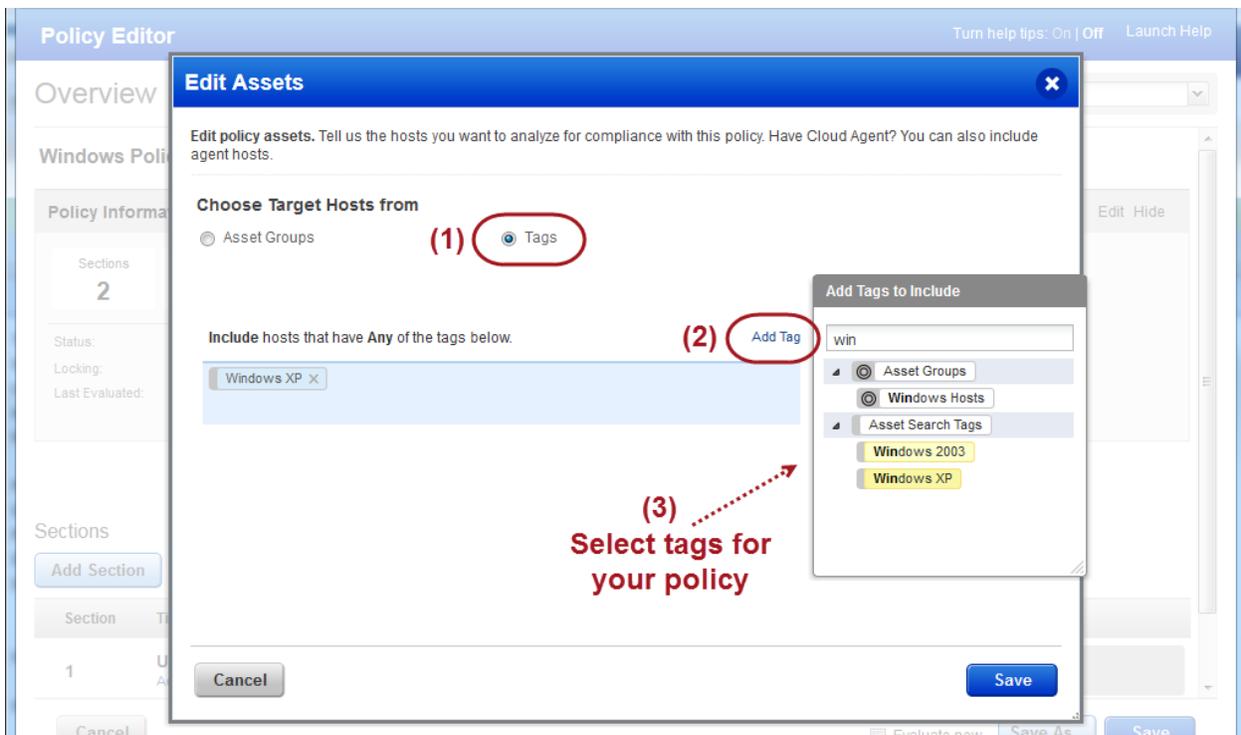
Support Asset Tags in Compliance Policies

This release introduces the ability to add asset tags to compliance policies. Hosts that match any of the tags will be included in the policy. Managers and Auditors always have this permission. Unit Managers can add tags when they have the “Create/edit compliance policies” permission.

Start by clicking Edit to add tags to your policy.



Then 1) click Tags, 2) click Add Tag, and 3) select one or more tags for your policy. Hit Save.



Include UDCs in Policy Export/Import

You can now include user-defined controls (UDCs) when you export a policy from your account to CSV or XML, and when you import a policy to your account from XML. By default, only service-provided controls are included during policy export and import.

Export a policy

Identify the policy you want on your policies list and select Export from the Quick Actions menu. Choose a format, select the “Include user defined controls” option, and click the Export button. Your exported policy will include all service-provided controls and user-defined controls in the policy.

Export Compliance Policy

You have chosen to export the policy "Windows Policy"

Export Format: * Comma-Separated Value (CSV)

Include user defined controls ←..... Select to include UDCs

Please note the following:

1. All sections of the exported policy may be edited except for the evaluation criteria 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.
2. Policy exported in CSV format may not be used for import.

Export Cancel

Import a policy

Go to Policies > New > Policy > Import from XML file. Follow the wizard to select an XML file, give your policy a name, select the “Create user defined controls” option, and click the Create button.

Create a New Policy

Policy from XML File: Import an XML file from your local file system.
Give your policy a name. The policy name will appear in your policies list for quick identification.
For Example: CIS Windows Server 2003 Benchmark v1.2

Name your policy REQUIRED

My Policy

Activate this policy
Your policy will be available for scanning and reporting. Clear this check box to activate the policy at a later time.

Create user defined controls ←..... Select to include UDCs
Enabling this checkbox will create new user defined controls mentioned in the xml. Newly created controls will have policy's name appended to its statement.

Back Choose XML File Create

What happens next?

The imported policy appears in your policies list where you can assign assets to the policy and customize the policy settings. The UDCs from the policy appear on your controls list. We'll append the policy name to the control statement for each UDC added, as shown below.



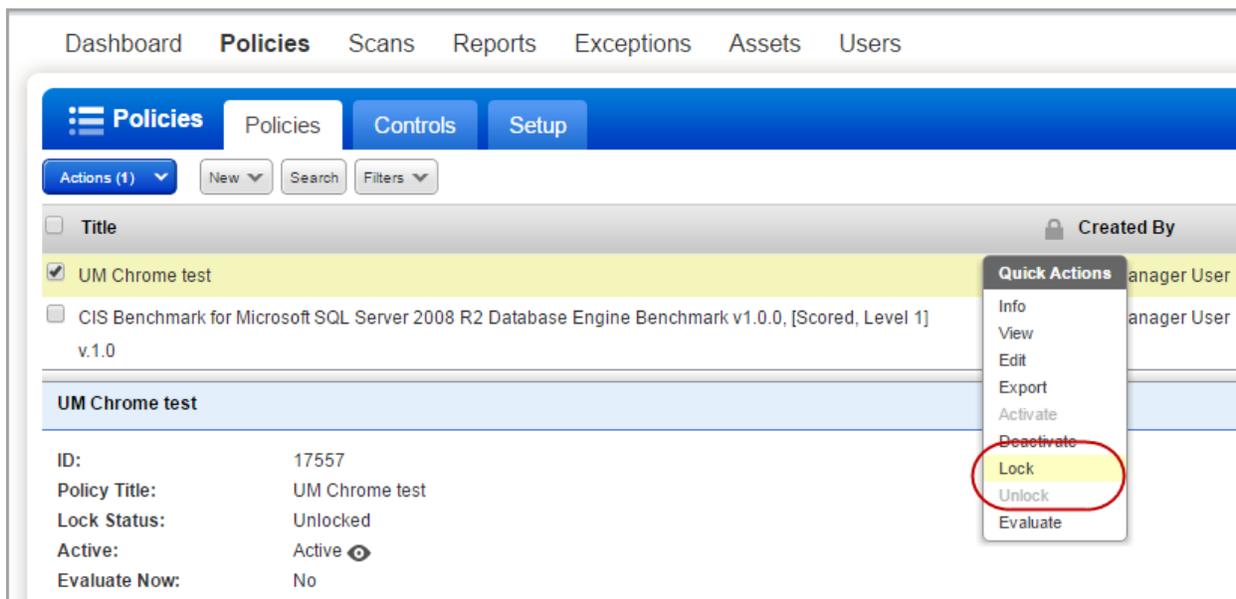
CID	Statement	Category	Created	Modified	Criticality
100004	permissions for registry key HKLM\SYSTEM\My Policy	Access Control Requirements	10/05/2016	10/05/2016	CRITICAL
100003	check for registry key HKLM\SYSTEM\My Policy	Access Control Requirements	10/05/2016	10/05/2016	MEDIUM
100002	check for registry key HKLM\SYSTEM	Access Control Requirements	09/09/2016	09/09/2016	MEDIUM
100001	permissions for registry key HKLM\SYSTEM	Access Control Requirements	09/09/2016	09/09/2016	CRITICAL
100000	Find lines in the /etc/passwd file that end with /bin/bash	Access Control Requirements	09/09/2016	09/09/2016	SERIOUS

Ability to Lock a Compliance Policy

You can now lock a policy so that you can restrict other users from updating it.

Simply, navigate to Policies > Policies and select the policy you want to lock. Select Lock from the Quick Actions menu.

You can use the Actions menu to lock multiple policies in one go.



Dashboard Policies Scans Reports Exceptions Assets Users

Actions (1) New Search Filters

Title	Created By
<input checked="" type="checkbox"/> UM Chrome test	anager User
<input type="checkbox"/> CIS Benchmark for Microsoft SQL Server 2008 R2 Database Engine Benchmark v1.0.0, [Scored, Level 1] v.1.0	anager User

Quick Actions

- Info
- View
- Edit
- Export
- Activate
- Deactivate
- Lock**
- Unlock
- Evaluate

UM Chrome test

ID: 17557
Policy Title: UM Chrome test
Lock Status: Unlocked
Active: Active 
Evaluate Now: No

Similarly, you can unlock a locked policy.

Good to know:

- Locked policies cannot be edited, however they are still available for reporting. Policies must be unlocked to enable editing.
- Only Managers and Unit Managers have permission to lock a policy.
- Managers can unlock any policy, but Unit Managers can unlock only the policies locked by them.
- Policies that are locked while importing and SCAP policies cannot be locked or unlocked.

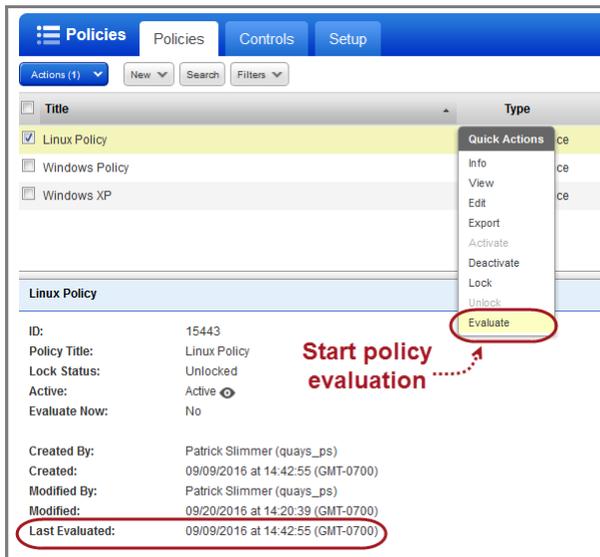
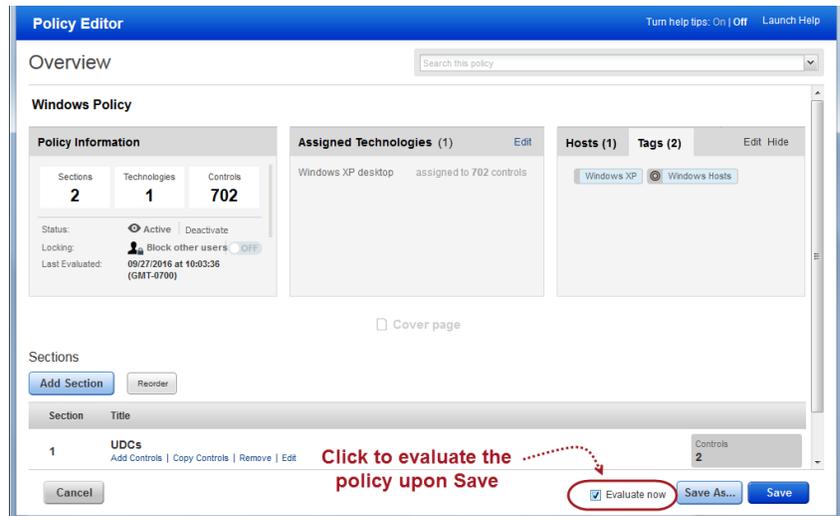
Start Policy Evaluation Anytime

We always evaluate policies when new scan results are processed for the hosts in your policy. With this release, you can also start policy evaluation when saving changes to a policy or anytime from the policies data list.

Evaluate from Policy Editor

Select the Evaluate Now check box before you click Save. This option is especially useful if you've added asset tags to your policy and you want to immediately evaluate the policy against matching hosts.

Note that this option is not selected by default and we will no longer evaluate a policy when you save changes unless you pick this option.



Evaluate from Policies List

Select any policy in the list and choose Evaluate from the Quick Actions menu (as shown).

Want to evaluate multiple policies in bulk? Select the policies and choose Evaluate from the Actions menu above the list.

Note that the date/time of the last policy evaluation appears in the Preview Pane.

Active Directory Technologies Supported for Windows UDCs

These technologies are now supported: Windows 2003 Active Directory, Windows 2008 Active Directory and Windows 2012 R1/R2 Active Directory. These new technologies are supported for all Windows UDCs (previously supported for WMI Query Check).

Want to create a UDC for these technologies? Go to Policies > Controls > New > Control, and select any of the Windows control types. Scroll down to the Control Technologies section to provide a rationale statement and expected value for each technology you're interested in.

New Control: Registry Key Existence Turn help tips: On | Off Launch Help

This control type checks for the existence of a user-specified Windows registry key.

General Information

Statement: *

Category: *

Sub-Category: *

Default Value: True Lock Value

Control Technologies*

- Windows 10
Use this section to create a Windows 10 instance of this control
- Windows 2000
Use this section to create a Windows 2000 instance of this control
- Windows 2003 Active Directory
Use this section to create a Windows 2003 Active Directory instance of this control
- Windows 2003 Server
Use this section to create a Windows 2003 Server instance of this control
- Windows 2008 Active Directory
Use this section to create a Windows 2008 Active Directory instance of this control
- Windows 2008 Server
Use this section to create a Windows 2008 Server instance of this control
- Windows 2012 R1/R2 Active Directory
Use this section to create a Windows 2012 R1/R2 Active Directory instance of this control
- Windows 2012 Server
Use this section to create a Windows 2012 Server instance of this control

New Active Directory technologies supported

Issues Addressed

- The Applications Report CSV file now downloads for large reports from the Assets > Applications tab. We are now streaming the data for downloading the CSV.
- Reports in PDF format are now displayed in the browser when finished. You may need to download HTML reports to view them.
- PDF and XML reports now get downloaded when you choose to download the reports.
- Fixed two issues for MHT Scan results Report: the “Expand All” option in the file now expands all root nodes and the scan results also lets the user scroll smoothly.
- We now display the QID indicator [1] for CVSS3 in PDF/HTML/MHT report formats. Earlier, only the docx report format displayed the indicator.
- Fixed an issue in Scan Reports where we displayed the wrong asset group for the CVSS Environment value. This was an issue when the same IP belonged to multiple asset groups in different networks and we returned the asset group from the wrong network.
- Policy scorecard report now renders graphs correctly for both PDF and HTML formats.
- We have now added a colon to display correct formatting in the Technologies section of the Policy report (Policy Compliance > Reports > Reports> Policy Report).
- The New Policy Report page now contains properly aligned text.
- Fixed an issue where the special characters in the policy name are now correctly displayed in the Policy drop-down of Policy Compliance > Reports > Policy Summary tab.
- When the results table is split across multiple pages, the Authentication report now displays only a single entry for the last row of the current page, instead of duplicating that entry on the next page.
- When you download an Asset Search Report using the API, the Company name in the Header section of DTD will now be wrapped in CDATA to allow for special characters in the Company name of the API Header.
- Fixed an issue in Asset Search Reports when hosts are specified using asset tags and you’ve entered one or more QIDs. Only hosts with at least one of the QIDs will be included in the report.
- Fixed an issue where users were not able to purge more than 3986 hosts at once from their Asset Search Report.
- The Asset Search Report is now generated properly in all supported formats and can be viewed accurately.
- Fixed an issue with tags display in Asset Search Report. Users were seeing many non-associated tags for each host. Also parent child tag hierarchy issues are now resolved.
- We removed the Create Tag button from Asset Search Reports in HTML format, generated from the Reports section.
- Fixed missing images and logos in Asset Search Reports that are generated from the Reports section.
- Added back the Help menu in Asset Search Reports generated in HTML format from the Reports section.
- We’ve improved the performance of the Asset Search Report “batch edit” option. Now you can select a large number of hosts and edit them without waiting for the UI to populate the Edit Hosts window.

- Fixed an issue for Asset Search Report where Purge or Purge All action for IP addresses from multiple networks now displays correct error message.
- While performing an Asset Search, the “Select Asset Groups” dialog now shows all asset groups irrespective of the selected network.
- The Asset Groups drop-down will now include all asset groups and show the correct asset group count. We have also improved the asset group widget now to load all asset groups faster than before.
- Fixed an issue where creating a tag during Asset Search with service criteria displayed an error. Now, the tag is created without any error.
- If a VM or PC license expires, instead of getting a fatal error and an incident, you will now see the appropriate license expire message in the API response.
- A subscription expired message is now shown for an expired VM or PC subscription. In case there are other modules in the subscription, the user is redirected to the AssetView module.
- We’ve modified certificate processing to update certificate source for each scan during scan processing. If certificate source is updated since the previous scan the new source will be updated for the host.
- When you remove IPs from your subscription, we’ll remove the same IPs from your authentication records all at once.
- We now display the Manage SCAP scans link in the introduction page only when the subscription has SCAP add-on enabled.
- Fixed reordering issue of remediation policy rules.
- The Host List API v2 (resource /api/2.0/fo/asset/host/) now displays accurate values for vm_scan_since parameter. All the hosts which were scanned before enabling “New scan Processing” are now displayed in host list.
- PC scan results now show “authentication fail” if authentication fails for Oracle.
- We now correctly display the Last Fixed date information for the vulnerability in the Remediation > Ticket > Vulnerability Information.
- Fixed the issue where the email signature displayed Account Manager in place of Business Unit Manager.
- We’ve improved the layout of the email template contact message so that it appears clearly in all mail clients. The mailto format changed to userlogin@qualys.com “Firstname Lastname”
- We will now display each instance of a certificate vulnerability (QID). A QID may be found on different ports on the same host or on different hosts. You’ll see this in the Certificate Information.
- We will now display multiple locations for a certificate when the certificate is found at multiple locations. A certificate may be found at different locations on the same host or on different hosts. You’ll see this in the Certificate Information.
- New Qualys API Quick Reference covers all Qualys APIs going forward. We’ve updated to add 8.9 API features. Log in to Qualys and go to Help > Resources to download it.
- The Appliance API (/api/2.0/fo/appliance/) now displays accurate values for ML_LATEST and VULNSIGS_LATEST elements.

- AWS HVM AMI images for Qualys Virtual Scanner Appliance have been released and are available at Amazon marketplace. We've updated the Qualys Virtual Scanner Appliance wizard and links in the wizard point to step by step configuration instructions at the Qualys Community.
- When you make an API request to update a virtual scanner appliance (/api/2.0/fo/appliance/?action=update) and you do not include required input parameters, the response will now list the parameters that are allowed.
- Added validation to check that IP_ADDRESS is not blank when using "set_routes" to specify a static route for a virtual scanner appliance using the Virtual Scanner Appliance API (/api/2.0/fo/appliance/?action=update). The static route format is IP_ADDRESS|NETMASK|GATEWAY|NAME.
- For subscriptions with Network Support, we will always show the Network and Scanner Appliance options on the Launch Scan page.
- Now the scanner appliances related to a specific network are visible only while creating an asset group within that network.
- Now a scheduled scan task is not created if a scanner is not associated with the custom network.
- Fixed reordering issue of remediation policy rules.
- Editing a remediation policy rule works as expected for a network disabled account and does not show an "Invalid network selected" error.
- While downloading a new virtual appliance, the "Add New Virtual Scanner" dialog now displays the complete text for the link "Click here for guidance".
- (Applicable when IPv6 Scanning is enabled for your subscription.) When you edit a scanner appliance to enable IPv6 you'll see these changes: 1) we renamed the field "Address/Netmask" to "Address/Prefix" and 2) we added validation to only allow an IPv6 prefix range of /1 to /64.
- The incorrectly displayed "checkpoint firewall" text is now removed from the Options profile for new, info, and edit window.
- Fixed an issue where users were receiving a Completed Scan Notification when their scan was Paused. Now you'll get a Paused Scan Notification. This applies when you've checked the "Send notification when this scan is finished" option when launching or scheduling your scan.
- Fixed an issue where users were seeing the error "User unauthorized to provision virtual scanner" when adding an Offline Scanner when the subscription didn't also have Virtual Scanner support.
- Fixed an issue where a host's DNS and/or NetBIOS hostname detected by a vulnerability scan was being overwritten with empty text when a subsequent compliance scan did not return a hostname.
- Fixed an issue where, if a Locked policy has include all hosts with PC agents check box selected in the policy editor, it is retained as selected.
- We now display the host-based Scan Report with correct indentation for output blocks in XML format.
- We now display an appropriate error when an IP is provided for the scanners_in_ag parameter while choosing the scanner option as "All scanners in asset group" in the API.
- The Scorecard Report will now be generated properly via UI and API.
- The word QualysGuard is replaced with Qualys at a few places on the Qualys Support page.
- API Release Notes 8.9 clarifies CSV updates and provides sample output for CSV updates.

- Updated the API v1 User Guide to explain that scan_report_list.php function returns all saved scans in the user's account.
- A VMware Authenticated Scanning document is now available! Log in to Qualys and go to Help > Resources to download it.
- Updated the online help to better explain that the option to remove hosts from only the VM module or only the PC module is not available in subscriptions with the Cloud Agent module.
- Update to the System Requirements help to note that the Edge browser is not supported for PCI module.
- Updated the Vulnerability Scorecard Report help to better explain the Previous options for the Host Scan Date filter.