

# **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

#### **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 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!

	New Unix Record	Turn help tips: On   Off Launch He
Get password for user login	Record Title >	Authentication
credentials from vault	Login Credentials	Provide login credentials to use for authenticated scanning. You have the option to get the login password from a vault available in your account.
	Private Keys / Certificates >	Username*: root
	Root Delegation >	Get password from vault <b>(YES)</b>
	Policy Compliance Ports	Vault Type: Cyber-Ark AIM
	IPs >	Vault Record*: Cyber-Ark PIM Suite
	Comments >	Vault Folder*: Cyber-Ark ALM Hitachi ID PAM
		Quest Vault
		Thycotic Secret Server
	New Unix Record	Tum help lips:
Use multiple private keys	Record Title >	Private Keys / Certificates
and/or certificates for	Login Credentials	Add private keys and/or certificates to be used for authentication - as many as you'd like. Any combination of
authentication. Any	Private Keys / Certificates 🗦	private keys (RSA, DSA, ECDSA, ED25519) and certificate types (X5.09, OpenSSH) can be added.
kove (PSA DSA ECDSA	Root Delegation >	Private Key
ED25510) and certificates	Policy Compliance Ports	Set private key / certificate for your Unix record
(OpenSSH X 509)	IPs >	Get private key from vault
(openson, 71.50))	Comments >	Private Key Type:
		Private Key Content: DSA
		ECDSA ED25519
	Record Title >	Private Keys / Certificates
New option to get private	Login Credentials	Add private keys and/or certificates to be used for authentication - as many as you'd like. Any combination of nyivate keys (PSA_DSA_ECDSA_ED25510) and certificate times (X5.09, OnenSSH) can be added
key from vault (CyberArk	Private Keys / Certificates 🗦	Private Key / Certificate
AIM vault only)	Root Delegation >	Private Key
	Policy Compliance Ports	Set private key / certificate for your Unix record
	IPs >	Get private key from vault. YES
	Comments >	Private Key Vault Type: Cyber-Ark AIM
		Vault Record*: My Vault  Vault Folder*-
		Vault File*: vault-file-name

<ol> <li>New option to get private key passphrase from vault. Choose from vaults available in your account.</li> <li>Choose certificate type OpenSSH or X.509</li> </ol>	Private Keys / Certificates     >       Root Delegation     >       Policy Compliance Ports     >       IPs     >       Comments     >	No Items a Private Key Ge Va Pa Va Va Co	ate Key / Certifica private key / certifica at passphrase from vault ult Username: ult Username: ult Folder*: ult Folder*: ult File*: ertificate Type: 2	Ite Ite for your Unix record VIES VYUE VYUE VYUE VYUE VYUE VYUE VYUE VYUE	×
Use multiple root delegation tools - Sudo, Pimsu, PowerBroker	New Unix Record       Record Title       Login Credentials       Private Key/Certificate       Root Delegation       Policy Compliance Ports       IPs       Comments	Root Delegation Add one or more root deleg This allows the login accou 3 items selected Root Delegation Pimsu PowerBroker Sudo	ation tools (Sudo, Pimsu, Pow nt to perform assessment tests Vault Username N/A N/A jgreene	rurr erBroker) to be used for authentication with the elevated privileges required. Vault Type N/A N/A Cyber-Ark AIM	Add Root Delegation Remove All Edit   Remove Edit   Remove Edit   Remove
New option to get password from vault. Choose from vaults available in your account.	Cogin Credentials     >       Private Key/ Certificate     >       Root Delegation     >       Qualys Shell     >       Policy Compliance Ports     >       IPs     >       Comments     >	Root Delegation Set the root delegation: Get password from v Vauit Usemame: Vauit Type: Vauit Record: Vauit Folder*: Vauit File*: Close	Cancel Cre Authentication gation below PowerBroker ault: YES MyVault Cyber-Ark PIM Suit Cyber-Ark PIM Suit Cyber-Ark PIM Suit Cyber-Ark AIM Hitachi ID PAM Lieberman ERPM Quest Vault Thycotic Secret Se	ate	Add Root D

#### 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!

New Cyber-Ark AIM Vault Launch Help	<b>^</b>	
Vault Title		Required credentials
Title: * My Vault		<ul> <li>Application ID (CCP web services)</li> </ul>
Vault Credentials		<ul> <li>Name of digital password safe</li> </ul>
Application ID: * Qualys-Scan-App-ID Safe: * VaultSafeName URL: * https://mydomain.com/AIMWebService/v1.1/AIM.asmx [example: https://host.domain/AIMWebService/v1.1/AIM.asmx]	l	- URL to AIM web service (choose SSL Verify and we'll verify the server's SSL certificate is valid and trusted)
SSL Verify:  Certificate:	l	The following is also required if your server requires a certificate for authentication:
Private key:		<ul> <li>Certificate (X.509 in PEM format)</li> </ul>
Passphrase:	1	<ul> <li>Private key that corresponds to public key stored on certificate</li> </ul>
Comments		- 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.

New 🕶	
Windows Record	
Unix Record	
Oracle Record	
Oracle Listener Record	
SNMP Record	
MS SQL Record	
Cisco Record	
IBM DB2 Record	
VMware Record	
MySQL Record	
Sybase Record	
Checkpoint Firewall	
HTTP Record	
Application Records	
Authentic ation Vaults	
Download	

New Cisco Record			Launch Help
Record Title	Login Credentials		
Login Credentials	Use the basic login credential or cho	ose to use authentication vault for au <ul> <li>Authentication Vault</li> </ul>	uthenticated scanning.
IPs >	User Name: *	root	]
Comments >	Password:	•••••	Clear Text Password
	Confirm Password:	•••••	]
	Enable Password:		
	Confirm Enable Password:		
	Policy Compliance		
	If services (SSH, telnet, rlogin) are no below.	ot running on well known ports (22, 2	3, 513 respectively) enter the ports in the custom field
	Ports:	Well Known Ports (22,23,513)     Custom Ports:	
		example: 2222, 2223	
	Canc	el Save	

#### **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.

New MS SQL Server F	Record Launch Help	
Record Title >	IPs or Member Domain	
Login Credentials	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.	
IPs or Member Domain	Enter or Select IPs/Ranges: Select IPs/Ranges   Select Asset Group   Remove   Clear	
Comments	Example: 192.168.0.87-192.168.0.92, 192.168.0.200  Display each IP/Range on new line Member Domain: webdomain.com	
	Cancel Save	

# 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.

Scanner Appliance In	nformation		Launch Help	Ø 🗙					
General Information	General Information			<u>^</u>					
Scanner Options	Scanner Appliance:	is_quays_an							
WAN Settings	Network: Type:	QWEB Network Physical Scanner							
LAN Settings	Serial Number: Polling Interval:	0 180 seconds		=					
Proxy Settings	User Login:	quays_an							
Users	Status:	Connected	Edit Scan	ner Appl	iance			Launch Help	🛛 🗶
Asset Groups	Active:	Yes	General Info	rmation	>	General Information			~
Versions	Created:	-	Scanner Opt	tions	>	Reboot			
VLANs	Modified By: Modified:	-	Versions		>	Scanner Appliance: *	is_quays_an		
Static Routes	Scanner Tags: Model:	QGSA-0000-A1	VLANs		>	Network:	QWEB Network		
Comments	•		Static Route	s	>	User Login:	quays_an		=
Close			Comments		>	Type:	Physical Scanner		
						Polling Interval : *	180		
						Notification:	Email status if scanner appliance mis	ses	
							1 heartbeat checks (4 hour interva	ls)	
					(	Model:	QGSA-0000-A1		
						•	III		F.
			Cancel					s	ave

# **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.

Scheduled Scans Setup
Scheduled Scans Setup
Prevent Overlapping Scans The Manager primary contact has the option to prevent the service from starting a new scheduled scan when there's an instance of it running. In this case the service skips launching the second scan, sets the next launch date to the future, and counts the skipped scan as an occurrence.
Relaunch Scan on Finish The Manager primary contact has the option to allow users to configure a scheduled scan to relaunch once a scan instance finishes. This gives users the ability to perform continuous scanning by launching a new scan as soon as the previous one finishes. Relaunch Scan on Finish
Save Cancel

# 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 Vulnerab	lity Scan	Turn help tips: On   Off Launch He
General Information	1	
Give your scan a name, sel scans, if visible.	ect a scan profile (a default is selected for you with recommended settings), an	d choose a scanner from the Scanner Appliance menu for internal
Title:	Vulnerability Scan_1	2
Option Profile: *	Initial Options (default)	Select
Processing Priority:	2 - Ultimate 🔻	
Network:	Net1 V	
Scanner Appliance:	Default v Default External	View
Choose Target Hos	All Scanners in Asset Group All Scanners in TagSet All Scanners in Network Puild my list	
Tell us which hosts (IP ad	ABC_VT_Scanner1	1
Assets	Tags	
		and the second and a second and

#### Launch Compliance Scans:

Launch Compliar	ice Scan	Turn help tips: On   Off Launch Helt
General Information	1	
Give your scan a name, sel scans, if visible.	ect a scan profile (a default is selected for you with recommended settings)	, and choose a scanner from the Scanner Appliance menu for internal
Title:	Compliance Scan_1	
Compliance Profile:	Initial PC Options	□ Ø <u>View</u>
Network:	Net1 🔻	(
Scanner Appliance:	Default •	View
	Default External	
Choose Target Hos	All Scanners in Asset Group All Scanners in TagSet All Scanners in Network	
Tell us which hosts (IP ad	Build my list ABC_VT_Scanner1	(
Assets	Tags	
and the second second	and a second and a second	south on production for

# 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.

Dashboard Scans Reports	Remediatio	on Assets KnowledgeBase Use	rs		
Users         Users         Busines           New Y         Search         Filters Y	ss Units Dis	tribution Groups Activity Log Setu	q	4 51 - 100 of	248 🕨 🏶 🗸
Date Action	n 🛦 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 Ownersandt_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 Improved log details for so tasks (maps, scans or repo	cm_scan heduled orts) that fai	Scheduled cm_scan 'with [id:24718 Title ScheduleComplianceScan_Retesting_chec Ownersandt_rr Role manager[ deactivated: Scheduledcm_scan validation failed while launching : Error loading Option Profile : No record was found	Rujuta Paithankar <mark>k</mark>	sandt_rp Manager	
10/13/2016 at 13:25:02 (GMT+0530) error	scan	Scheduled scan 'with [id:24719] Title:ScheduleScan_Retesting_Ruj123 Owner.sand_rp Role.managerj deactivated: Scheduledscan validation failed while launching Error loading Option Profile : No record was foun	Rujuta Paithankar : d	sandt_rp Manager	
10/12/2016 at 15:07:02 (GMT+0530) error	report	Scheduled report With (id 20528 Title-PolicyReport_Retesting_Check Ownersand_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 j	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.

New User				
General Information	>	User Role		
Locale	>	User Role: *	Scanner	•
User Role	>	Allow access to:	Manager Unit Manager	
Asset Groups	>	Business Unit: *	Auditor Scanner	
Permissions	>		Contact Remediation User	
Options	>			
Security	>			

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.

Vulnerability Management 🗸 🗸							5	Help 🗸			Logout
Remediation Knowledge	Base										
Remediation         Tickets           Actions (0)         New         Search	Filters 🗸								1 - 20 of 3	0	▶
			Displaying tickets modified within t	he last 30 days. Use Setu	p menu to cha	nge.					
Ticket # State     Due D	ate + IP	Port # Instance	DNS Hostname	NetBIOS Hostname	Severity	QID	Vulnerability Title	Owner	Modified	Created	Resolved
000133 Closed/Ignored 10/04/2	2016 10.11.65.97	3389	qw81esqp3-65-97	QW81ESQP3-65-97	3	90882	Windows Remote Desktop Protocol Weak Encryption Method Allowed	Swati Vijayan 1	09/30/2016	09/27/2016	09/30/2 🔺
000134 Closed/Ignored 10/04/2	016 10.11.65.98	3389	qw81esqp3-65-98	QW81ESQP3-65-98	3	90882	Windows Remote Desktop Protocol Weak Encryption Method Allowed	Swati ∨ijayan 1	09/27/2016	09/27/2016	09/27/2
000135 Open 10/04/2	10.11.65.200	)		QWV/SQP3-65-200	5	90783	Microsoft Windows Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-020)	Swati Vijayan	09/27/2016	09/27/2016	
000136 Open 10/04/2	016 10.11.65.200	3389		QWVSQP3-65-200	3	90882	Windows Remote Desktop Protocol Weak Encryption	Swati Vijayan 1	09/27/2016	09/27/2016	*

#### **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.

Launch Vulnera	bility Scan Turn help tips: On   Off Launch Help	Ê
General Informati	on	
Give your scan a name, s scans, if visible.	select a scan profile (a default is selected for you with recommended settings), and choose a scanner from the Scanner Appliance menu for internal	
Title:		
Option Profile: *	Initial Options (default) * Select	
Processing Priority:	0 - No Priority	
Scanner Appliance:	2 - Ultimate vailable Set priority for 3 - Critical this scan	ш
Choose Target Ho	S - High	
Tell us which hosts (IP	6 - Standard and a standard san.	
Assets	9 - Low 0 0 - No Priority	
Asset Groups	Select items C - * <u>Select</u>	
IPs/Ranges	*► <u>Select</u>	
	Example: 192.168.0.87-192.168.0.92, 192.168.0.200	
Exclude IPs/Ranges	*k <u>Select</u>	
	Example: 192.168.0.87-192.168.0.92, 192.168.0.200	

#### 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	В	С	D	E	F	G	н	1	J	К	L	E
1	Company	User	ReportTitle	AssetGroups	IPs	Users	CreatedDate	Network	AssetTage				Ē
2	Qualys, Inc.	Patrick Slimmer	Tickets per Vuln	All		All Users	10/24/2016 at 12:02:06 (GMT-0700)	Global De	fault Netw	vork			
3	QID	Title	Туре	Disabled	Severity	OriginalS	Tickets	Open	Resolved	Closed	AvgResolu	Overdue	
4	90783	Microsoft Windo	Confirmed	no	5		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 R	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 C	Confirmed	no	5		Date/time when 4	4	0	0	N/A	0	
1	0 90596	Microsoft Windo	Confirmed	no	5		the report was 4	4	0	0	N/A	0	
1	1 90606	Microsoft Media	Confirmed	no	5		4	4	0	0	N/A	0	
1	2 90616	Microsoft Windo	Confirmed	no	5		created 4	4	0	0	N/A	0	
1	3 90923	Microsoft Cumul	Confirmed	no	5		4	4	0	0	N/A	0	

# 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.

Edit Scorecard Repo	Drt Launch Help
General Information	> Define contents to display in your report
General Information Report Source Filter Display Description	<ul> <li>Define contents to display in your report</li> <li>The optional report content selected below applies to the QID selected in "Filter"</li> <li>Included</li> <li>Report Description</li> <li>Report Summary</li> <li>Vulnerability data about each selected asset group or tag</li> <li>Business Risk Coal</li> <li>Configure the business risk goal using the slider below. This goal is the maximum accepted risk, expressed as a percentage of vulnerabile hosts, for each asset group or tag. A host is considered witherability data about each selected asset group or tag. A host is considered witherability data by 0 50 60 70 80 90 100</li> <li>Wulnerability Type Show vulnerability conts by type (confirmed and potential).</li> <li>Vulnerability Status</li> <li>Show vulnerability conts by type (confirmed and potential).</li> <li>Vulnerability Age Show vulnerability conts by status (New, Active, Re-Opened and Fixed), enclude Vulnerability Ignore Status</li> <li>Vulnerability Age Show counts of New, Active and Re-Opened vulnerabilities by age (in days).</li> <li>Sow Included &amp; Excluded &amp; Search Lists summary</li> </ul>
	Include this text in the report footer

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

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



# **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.

Policy Edito	or		Turn help tips: On   Off Launch Help
Overview		Search this po	policy
Windows Pol	licy		<u>^</u>
Policy Inform	ation	Assigned Technologies (1)	Edit Hosts (1) Tags (0)
Sections 2	Technologies Controls 1 702	Windows XP desktop assigned to 70	702 controls Windows Hosts
Status: Locking: Last Evaluated:	Active Deactivate     Deactivate     Deactivate     OFF     09/27/2016 at 10:03:36     (GMT-0700)		Click Edit to add tags to your policy <sup>■</sup>

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

Policy Editor	Turn help tips: On	Off Launch Hel	
Overview	Edit Assets X	~	1
Windows Polic	Edit policy assets. Tell us the hosts you want to analyze for compliance with this policy. Have Cloud Agent? You can also include agent hosts.		^
Policy Informa	Choose Target Hosts from	Edit Hide	
Sections 2	Add Tags to Include		
Status:	Include hosts that have Any of the tags below. (2) Add Tag win		
Locking: Last Evaluated:	Windows XP X		
	(3)		
Sections	Select tags for		
Add Section	your policy		
Section Ti			
1 U	Cancel		÷
Cancel		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 Com	pliance Policy	
You have chosen to	export the policy "Windows Policy"	
Export Compliance Policy         You have chosen to export the policy "Windows Policy"         Export Format *       Comma-Separated Value (CSV)         Image: Comma-Separated Value (CSV)       Image: Comma-Separated Value (CSV)		
	Include user defined controls	
Please note the foll	owing:	
1. All sections removed if y	of the exported policy may be edited except for the evaluation criteria for each control (the EVALUATE tag). This tag may be ou want to later import the policy with default values from the controls library.	
2. Policy expor	ted 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 REQUID	8ED
My Policy	
V 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	
Enabling this checkbox will create new user defined controls mentioned in the xml. Newly created controls will have policy's name appended to it's 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.

Policies Policies Controls Setup				
Actions (0) V New V Search		4	- 20 of 6910	▶ * ~
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	
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		
	Policies	Contro	ols Setu	p				
Actions (1)	New 🗸 Search	Filters 🕶						
Title							🔒 Cre	ated By
UM Chrome test	t						Quick Actions	anager User
CIS Benchmark v.1.0	for Microsoft SC	QL Server 20	08 R2 Databas	se Engine Benchm	ark v1.0.0, [Sc	ored, Level 1]	Info View Edit	anager User
UM Chrome test							Export Activate	
ID:	1755	7					Lock	
Policy Title:	UM C	Chrome test					Unlock	7
Lock Status:	Unlo	cked					Evaluate	
Active:	Activ	e 💿						_
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.
- Mangers can unlock any policy, but Unit Managers can unlock only the polices 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.

Policy Edito	or				Turn help tips:	On   Off Launch H		
Dverview			Search this policy					
Windows Pol	icy							
Policy Informa	ation	Assigned Technologies (1)	Edit	Hosts (1)	Tags (2)	Edit Hide		
Sections 2	Technologies Controls 1 702	Windows XP desktop assigned	to 702 controls	Windows	XP Windows H	losts		
Status: Locking: Last Evaluated:	Active Deactivate     Active Deactivate     Block other users OFF     09/27/2016 at 10:03:36     (GMT-0700)							
		🗋 Cover page	9					
Add Section	Reorder							
Section 1	litle							
1 4	UDCs Add Controls   Copy Controls   Remove	Click to evalua	te the		Con 2	trols		
Cancel		policy upon \$	Save	Eval	uate now Save	As Save		



#### **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	ŕ
This control type chec	cks for the existence of a user-specified Windows registry key.			
General Inform	nation			
Statement: *				E
Category: *		•		
-Sub-Categoor*	True		] Lock Value	~
Control Techn	ologies*			
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 / Use this section to	Active Directory create a Windows 2003 Active Directory instance of this control			
Windows 2003 S Use this section to	Server create a Windows 2003 Server instance of this control		New Active Directory — technologies	
Windows 2008 / Use this section to	Active Directory create a Windows 2008 Active Directory instance of this control		supported	
Windows 2008 S Use this section to	Server create a Windows 2008 Server instance of this control			
Windows 2012 F Use this section to	R1/R2 Active Directory create a Windows 2012 R1/R2 Active Directory instance of this control			
Mindawa 0040 (	2			