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.

Copyright 2016 by Qualys, Inc. All Rights Reserved.

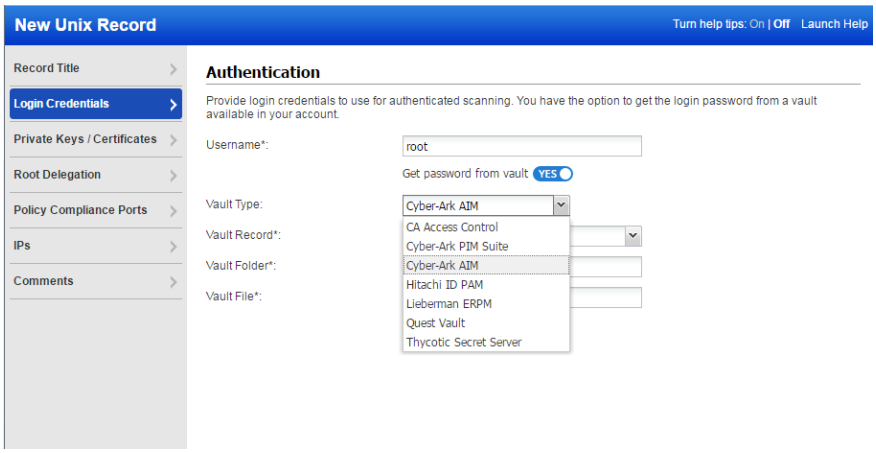
Qualys Cloud Platform

Unix Authentication Improvements

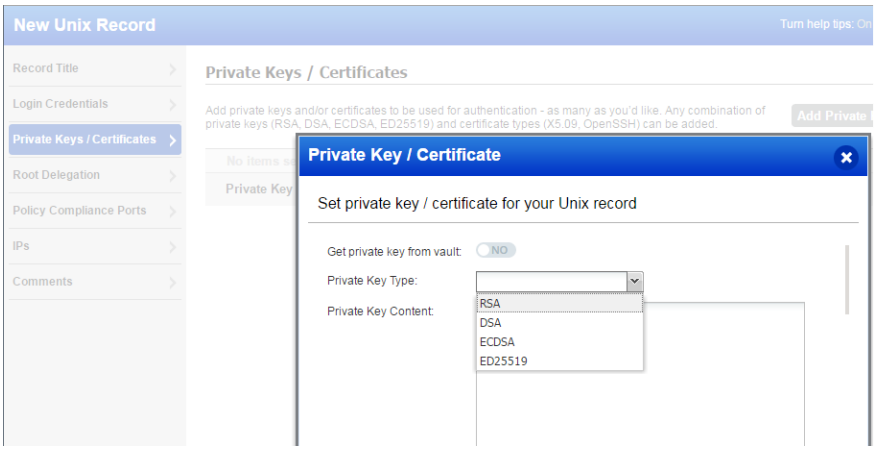
We're excited to tell you about the many enhancements we've made to Unix in this release. All enhancements are available for the Unix Record, using Qualys Cloud Suite UI and API. Now you can configure a single authentication record that supports better integration with third party vaults, and lets you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

Here's what you can do!

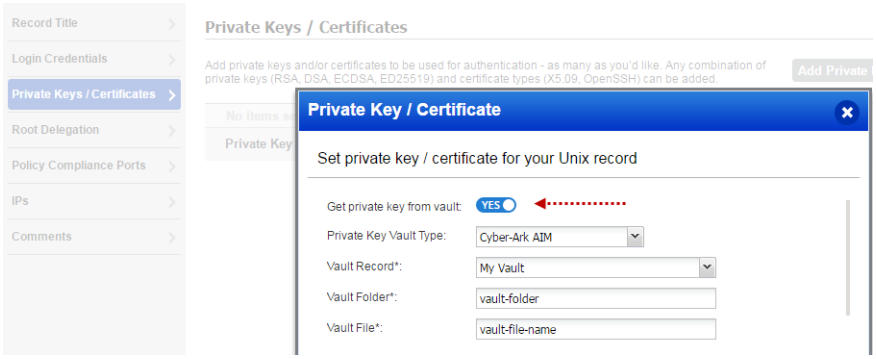
Get password for user login credentials from vault



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

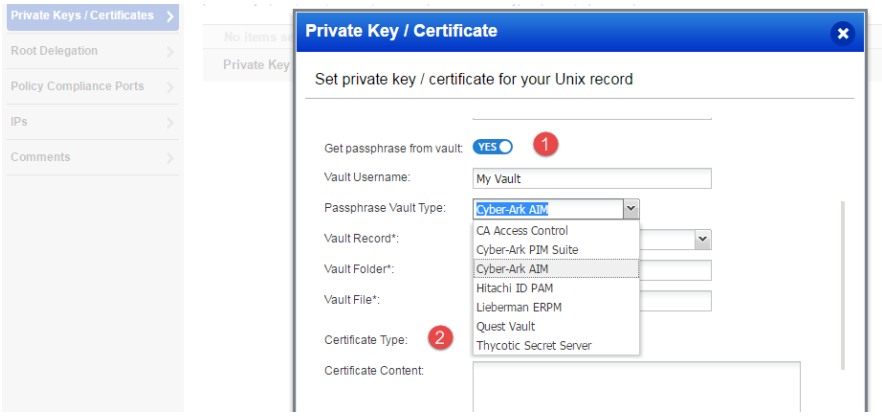


New option to get private key from vault (CyberArk AIM vault only)

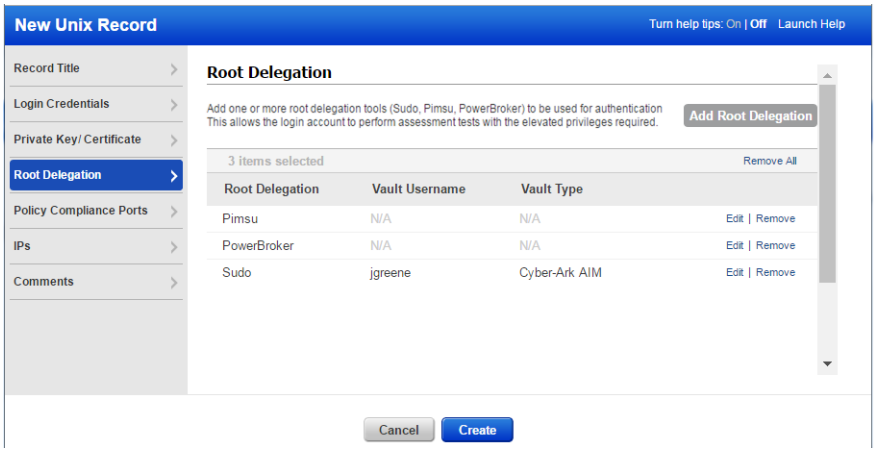


(1) New option to get private key passphrase from vault. Choose from vaults available in your account.

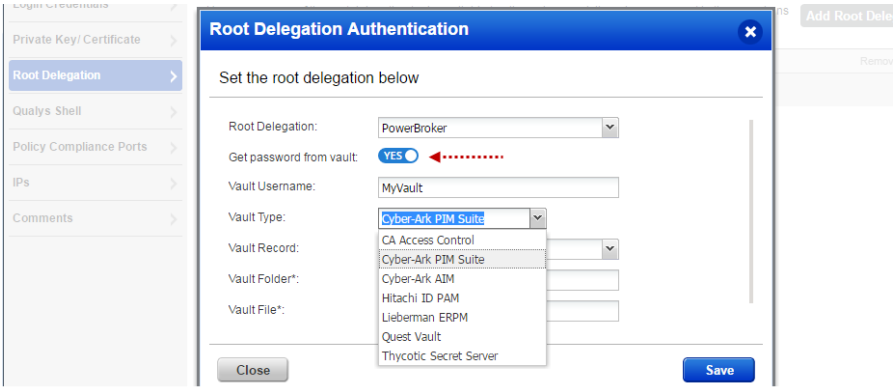
(2) Choose certificate type OpenSSH or X.509



Use multiple root delegation tools - Sudo, Pimsu, PowerBroker



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

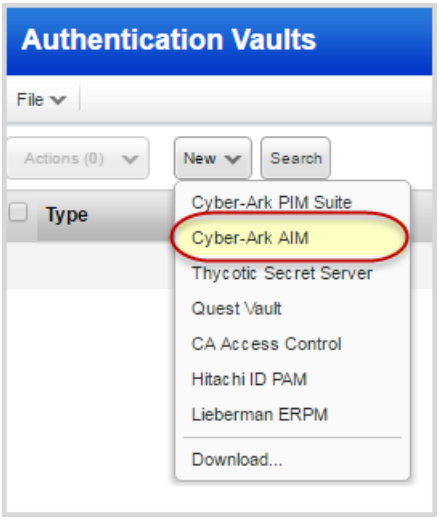


Your existing Unix records

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.

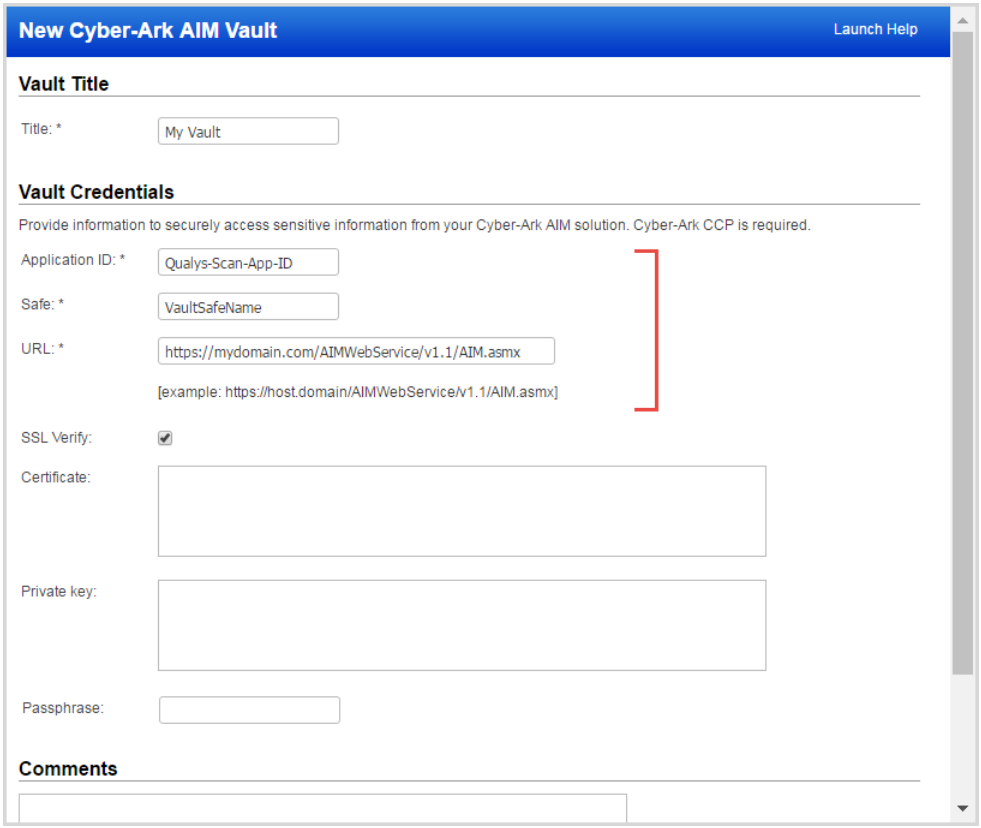
Windows - In a Windows Record you can choose to get the login password from your Cyber-Ark AIM solution.

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.

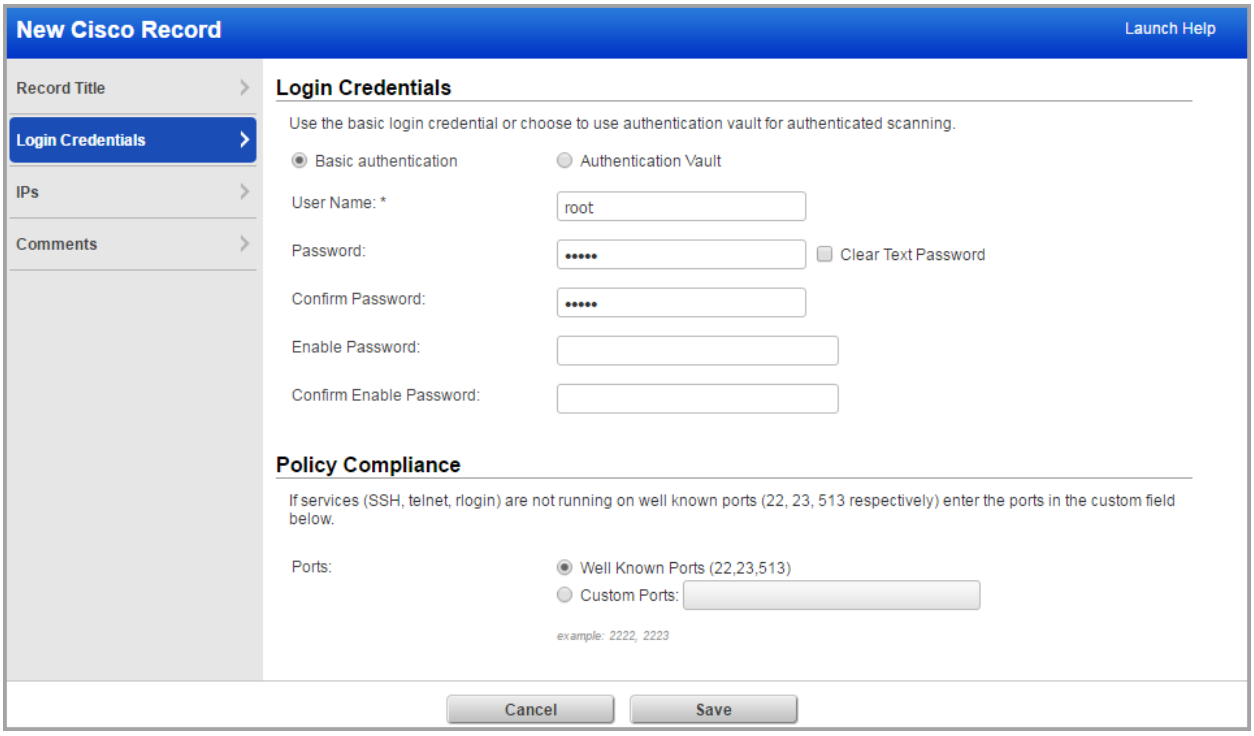
Simply create a new Cisco authentication record (authentication record for all supported Cisco devices is now grouped as Cisco Record.)

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

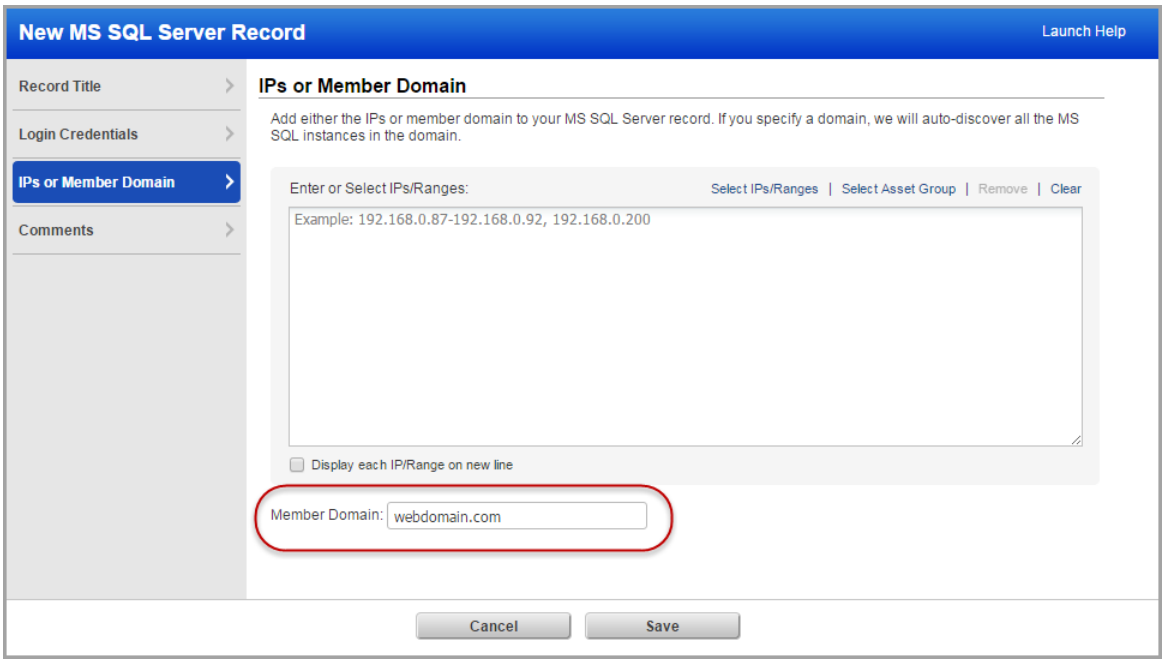
You'll notice that the settings are the same for all supported Cisco devices (Cisco NX-OS, Cisco IOS, Cisco ASA and Cisco IOS XE technologies). If the "enable" command on the target hosts requires a password, then you must also provide the enable password in the authentication record.



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.



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.

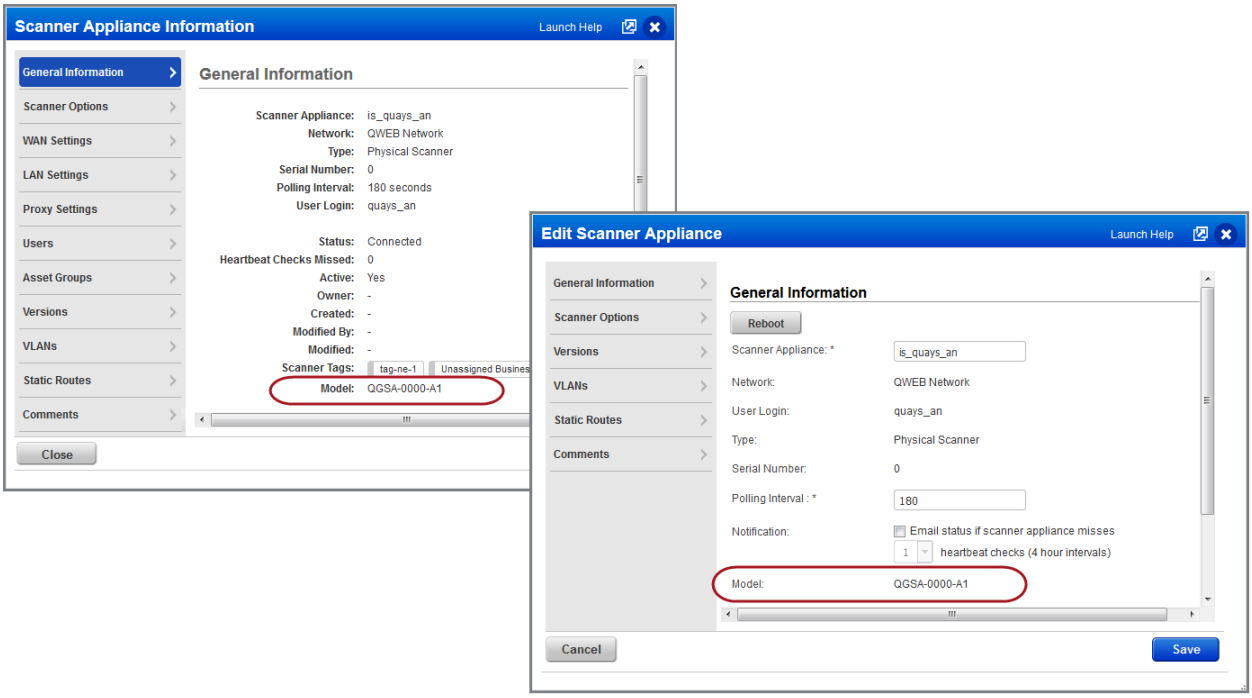
EC2 scanning is not just for Managers anymore! Now Unit Managers can start and schedule EC2 scans as long as the IPs for the EC2 environment are in the Unit Manager’s Business Unit.

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.

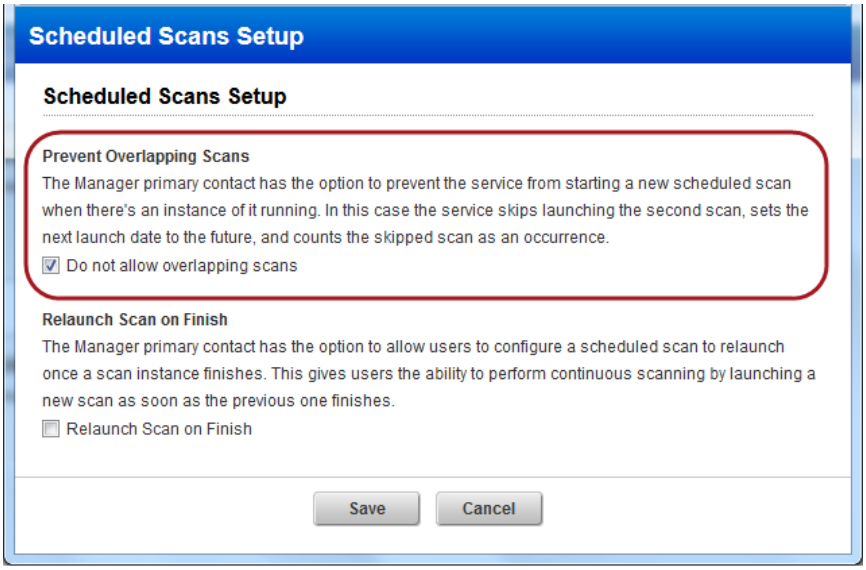
View Scanner Appliance Model Information

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.

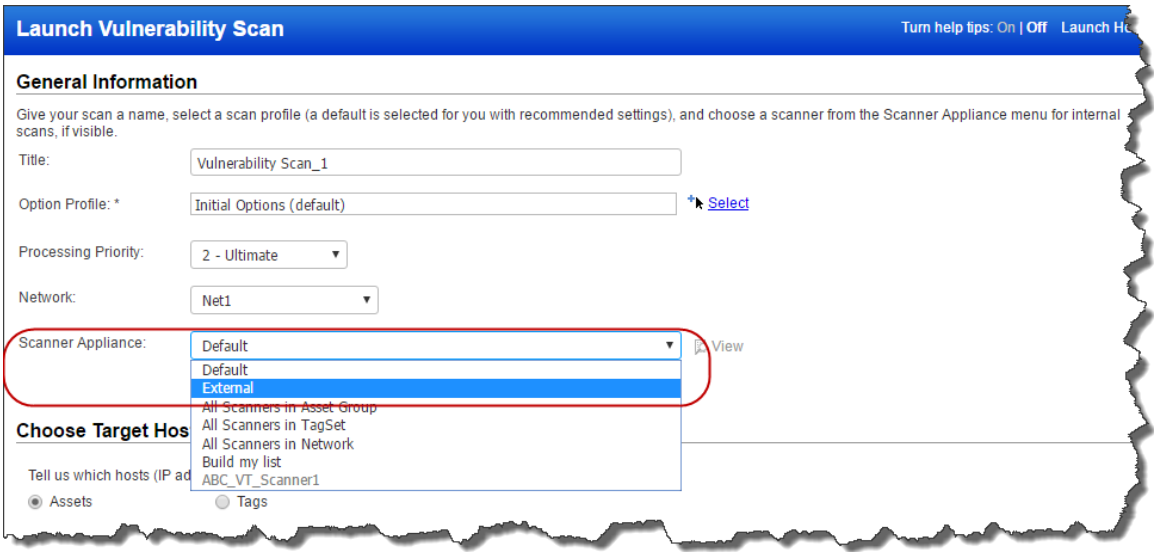


Use External Scanners to Scan custom networks in VM and PC

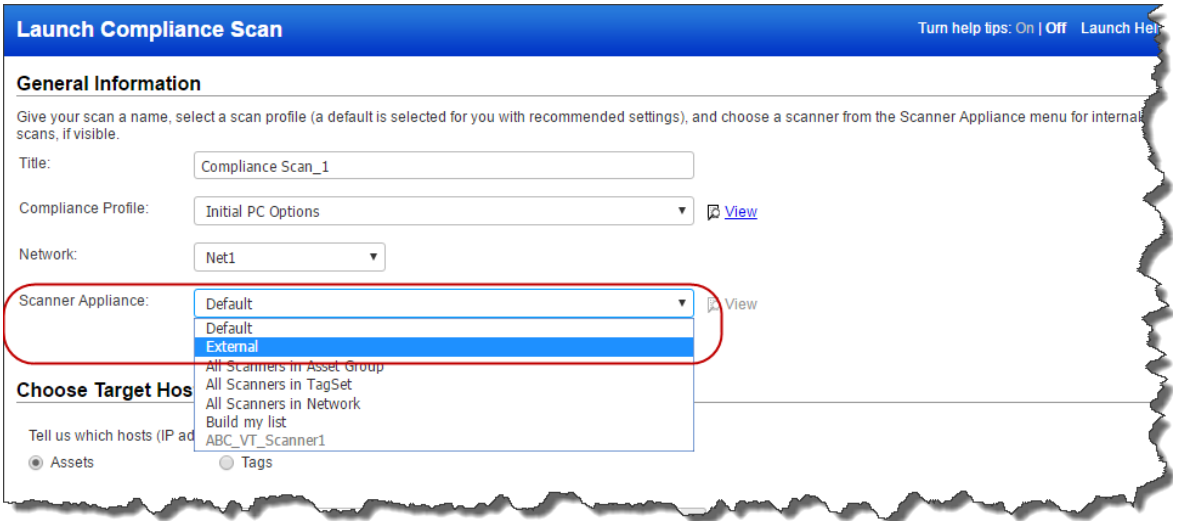
You can now use External scanners for scanning custom networks. Simply choose the "External" scanner appliance option at scan time or when you schedule your scan.

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:



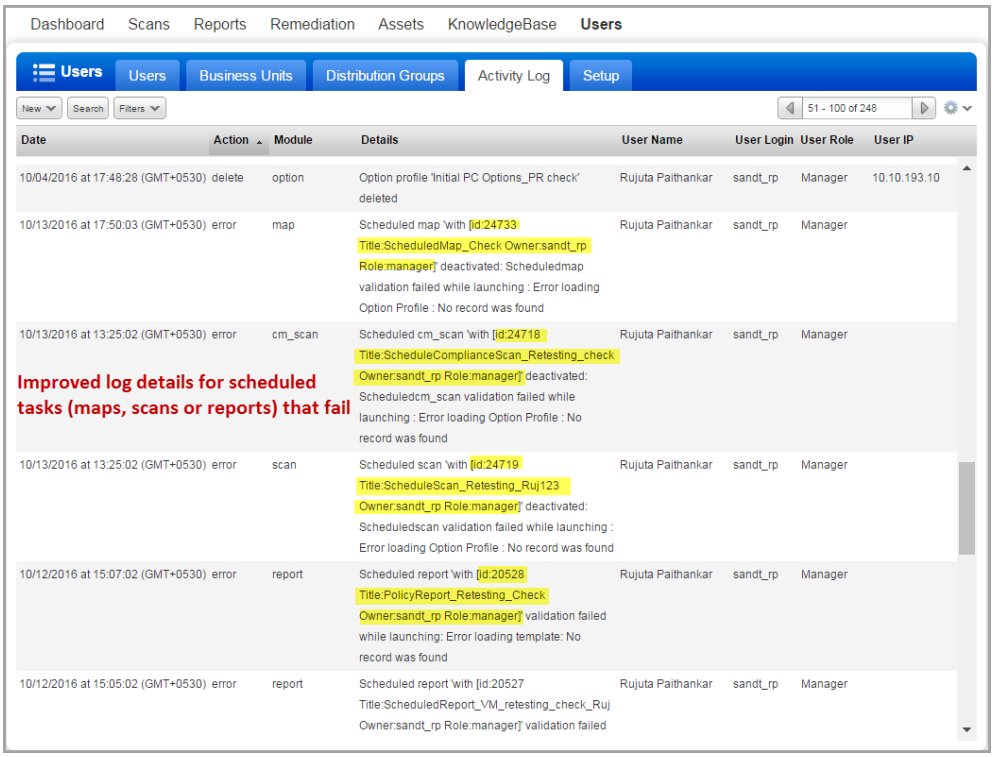
Launch Compliance Scans:



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.



Go to Users > Activity Log.

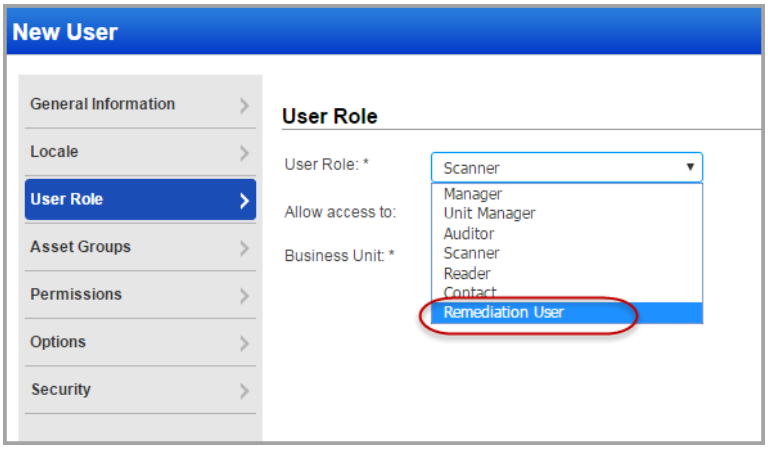
The details column in the now provides additional task details - task id, task title, task owner and user role.

Qualys Vulnerability Management (VM)

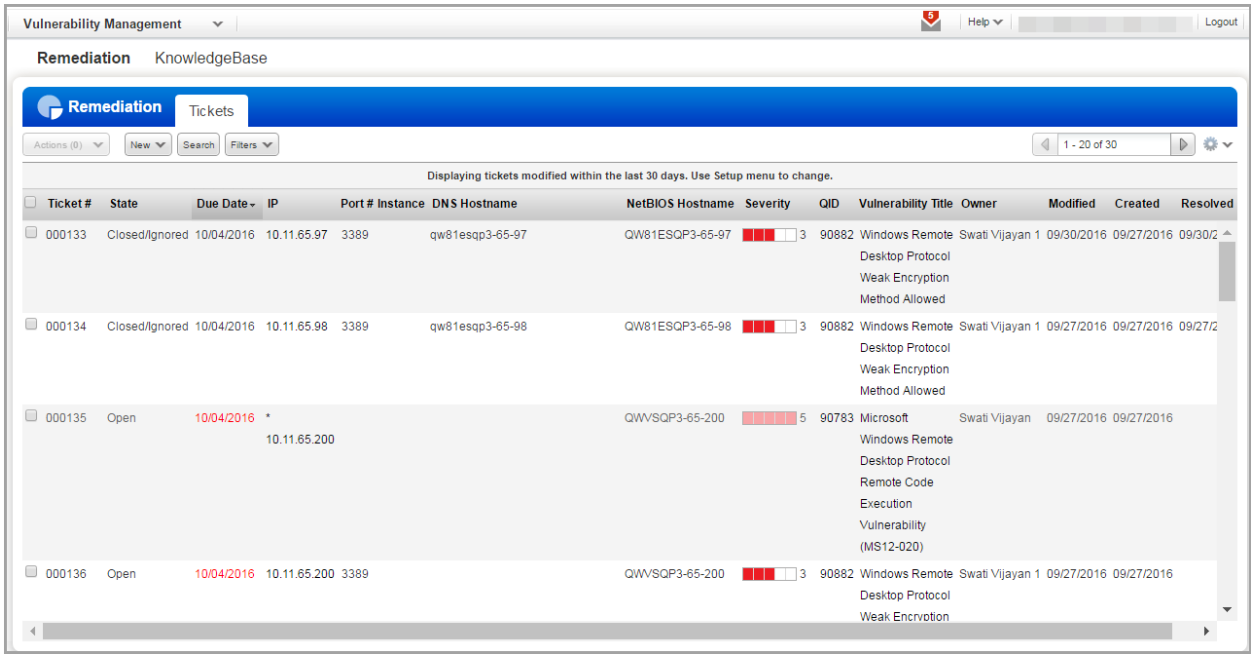
Introducing a new user role: Remediation User

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.



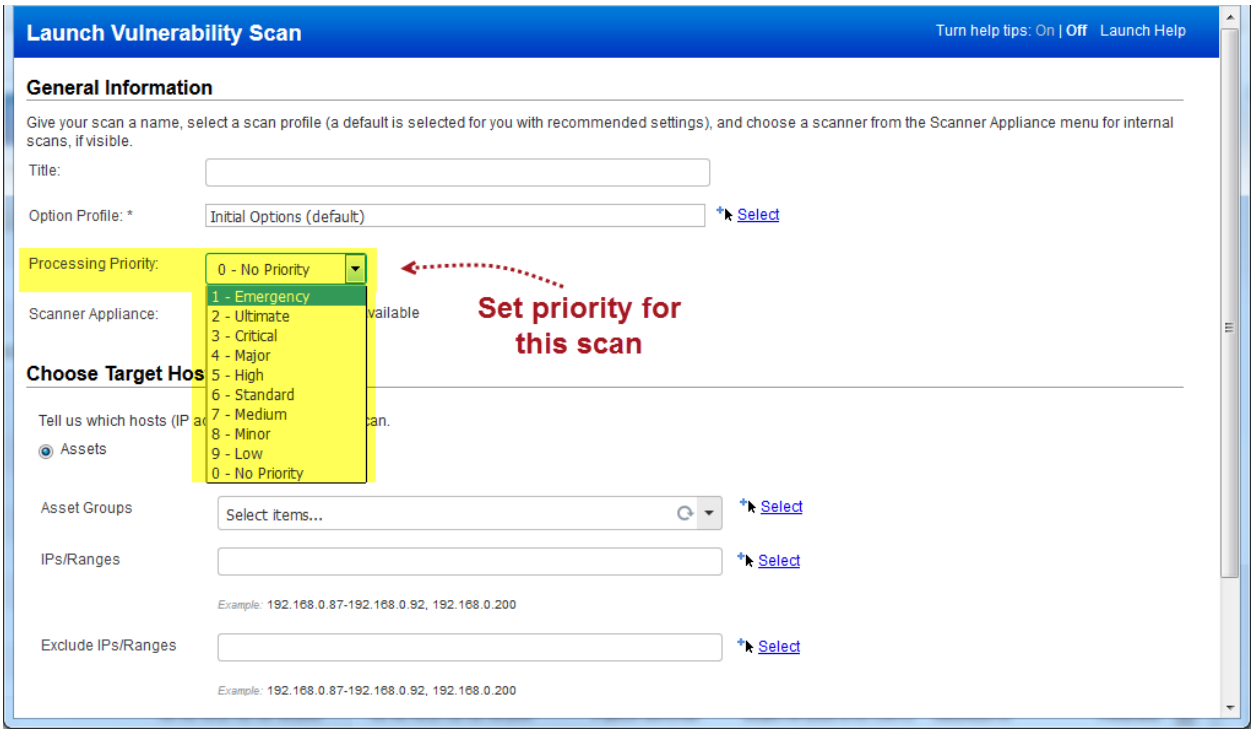
Enhancements to Vulnerability Scan Processing

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.



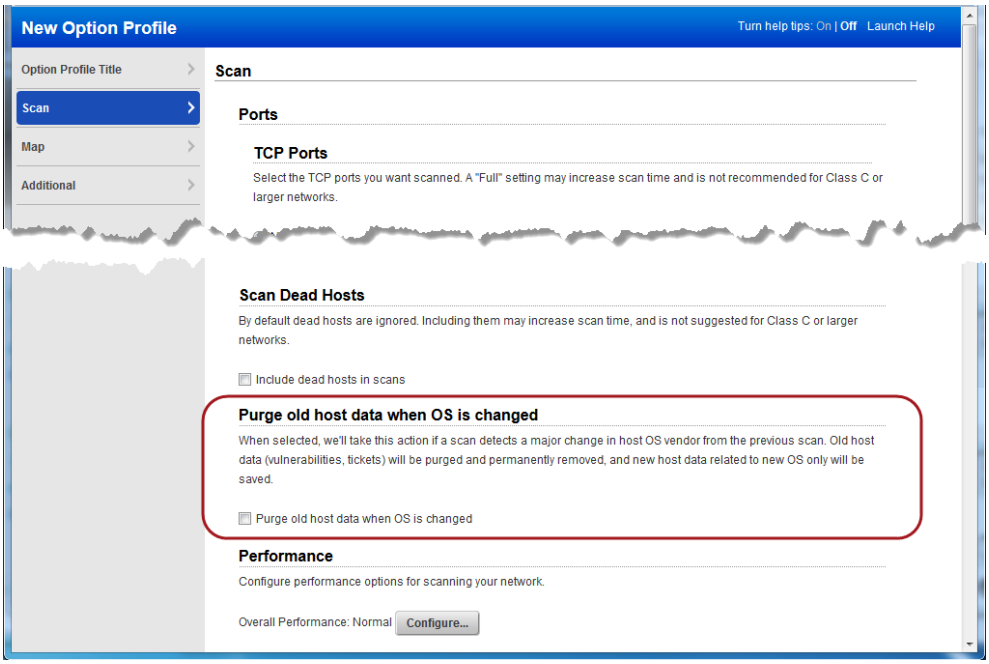
Finished scans are processed before running scans

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

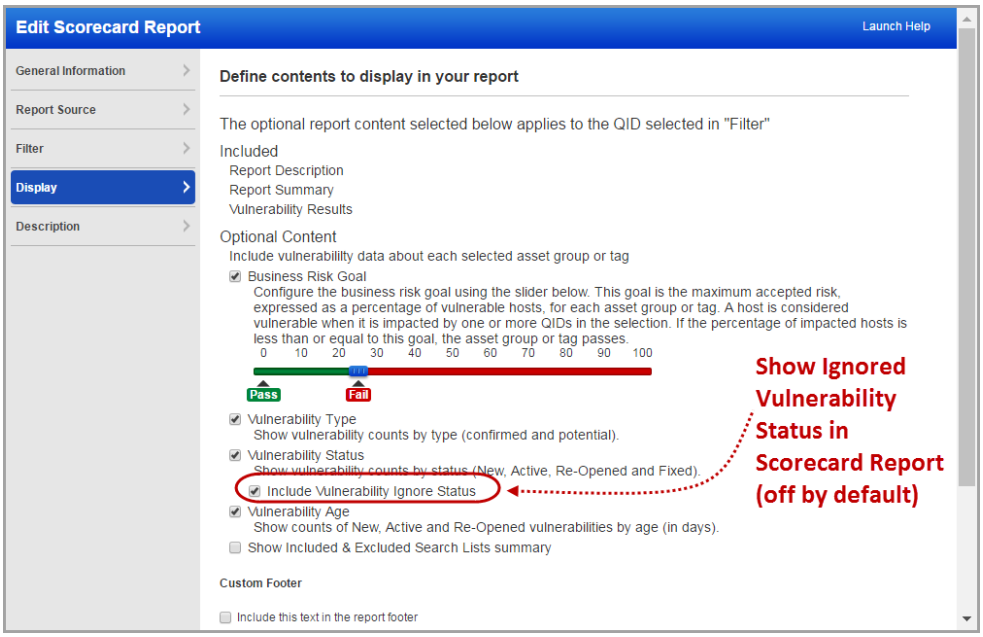
This sample remediation report was created on October 24, 2016.

	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	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 Cumul	Confirmed	no	5		4	4	0	0	N/A	0

Date/time when the report was created

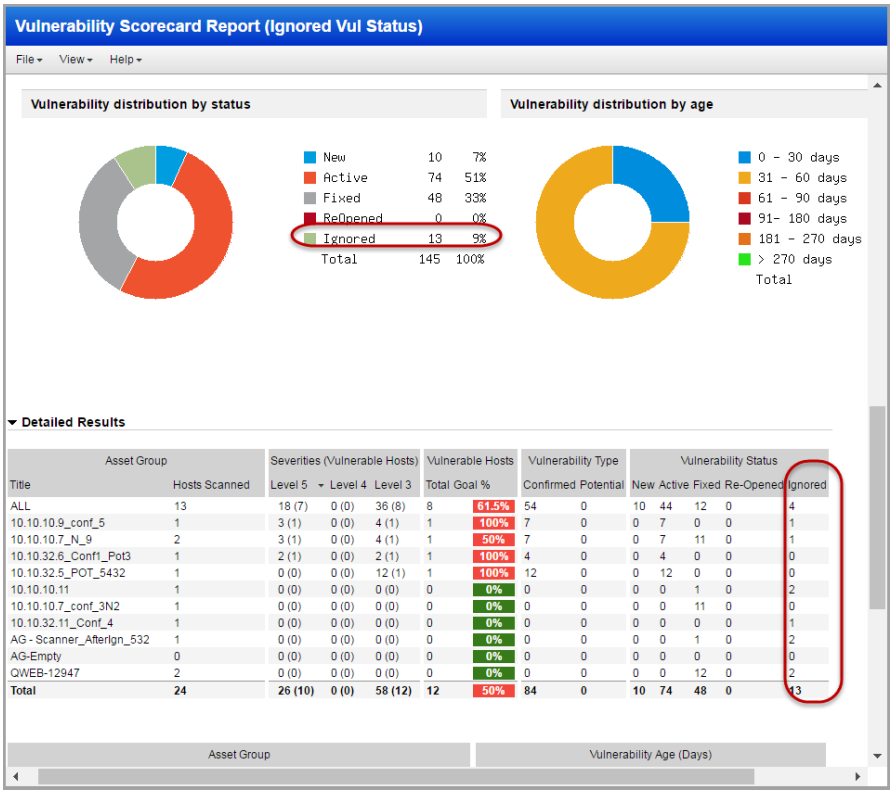
Vulnerability Scorecard Report – Display Ignored Vulnerability Status

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 chose this option when you edit the Scorecard Report template.

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

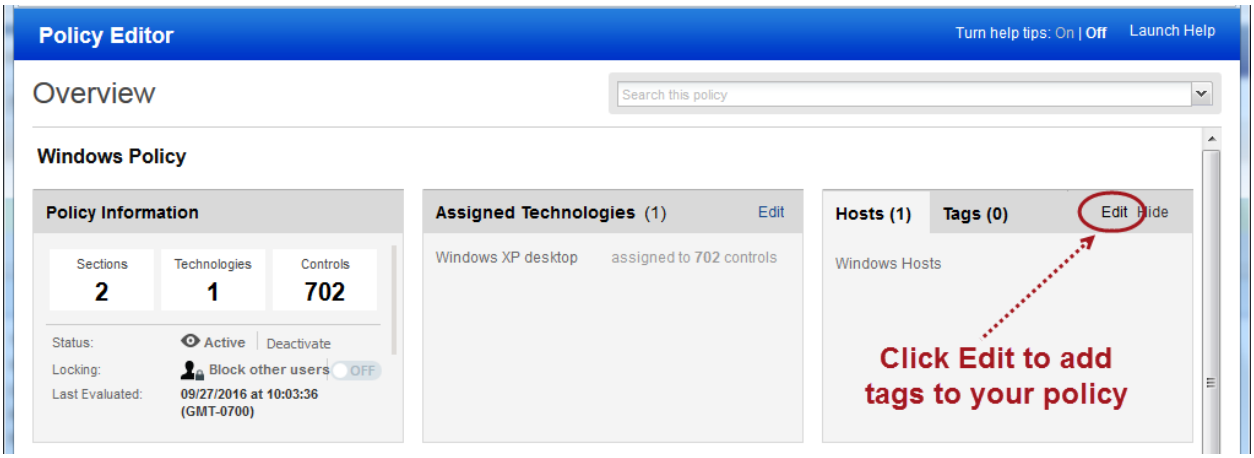


Qualys Policy Compliance (PC)

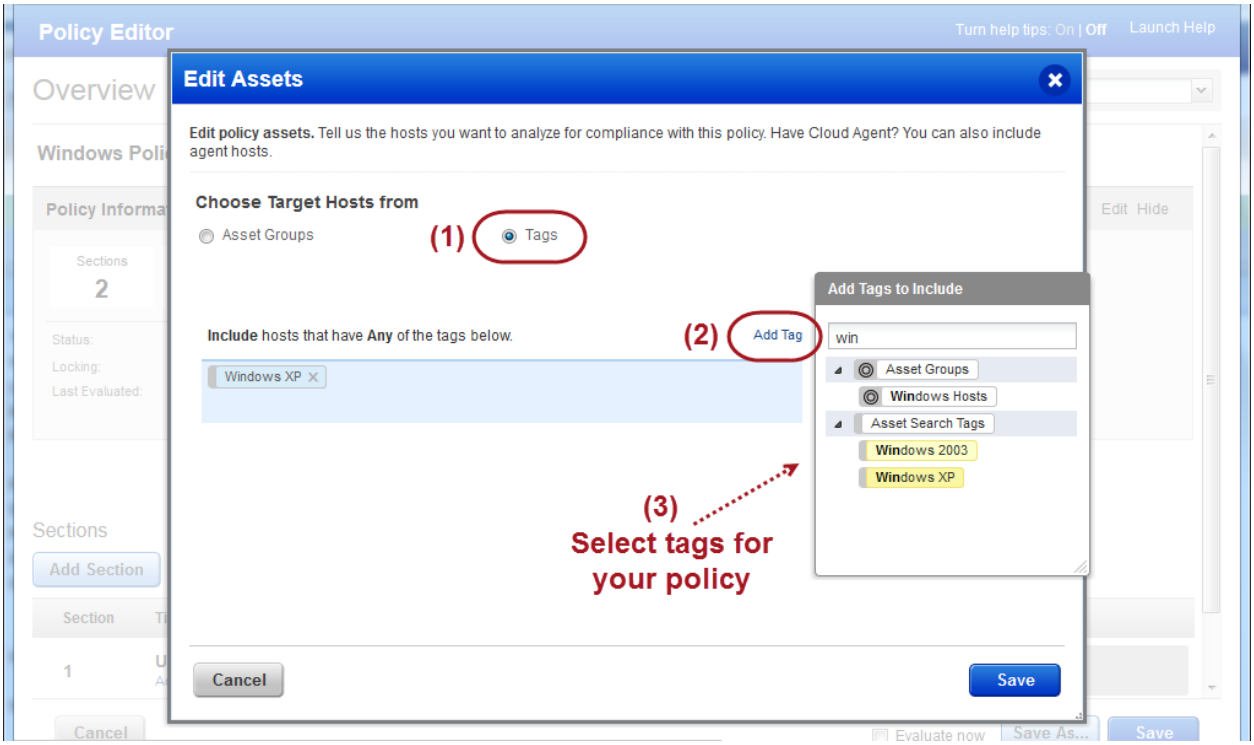
Support Asset Tags in Compliance Policies

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.



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

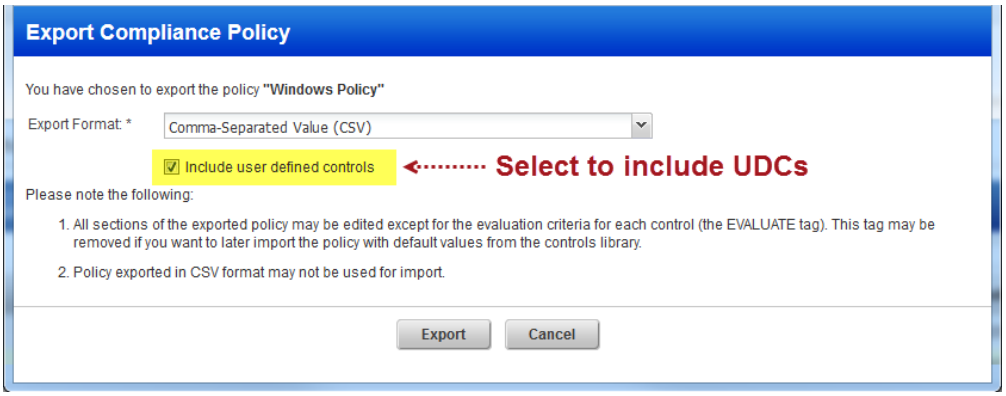


Include UDCs in Policy Export/Import

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.

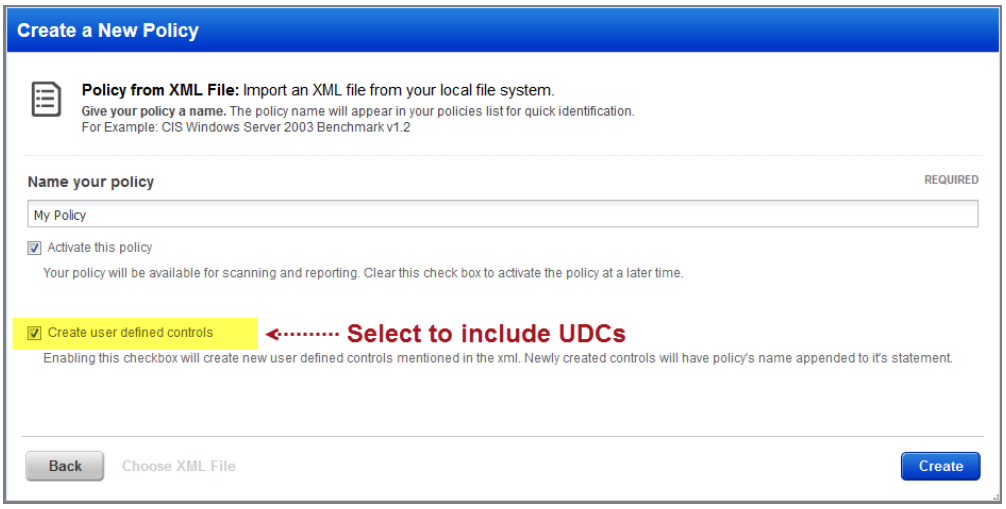
Export a policy

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.



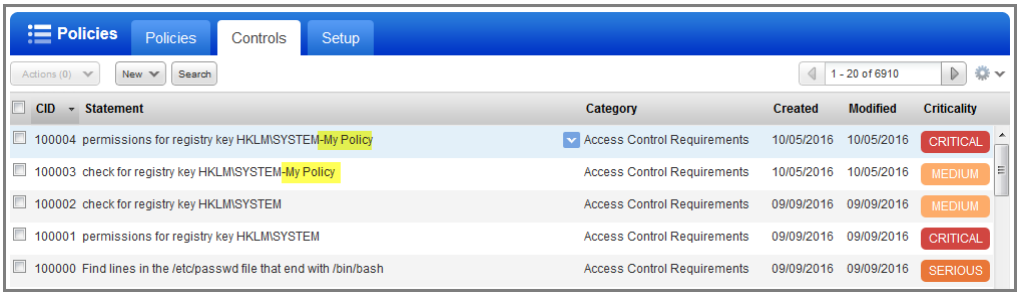
Import a policy

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.



What happens next?

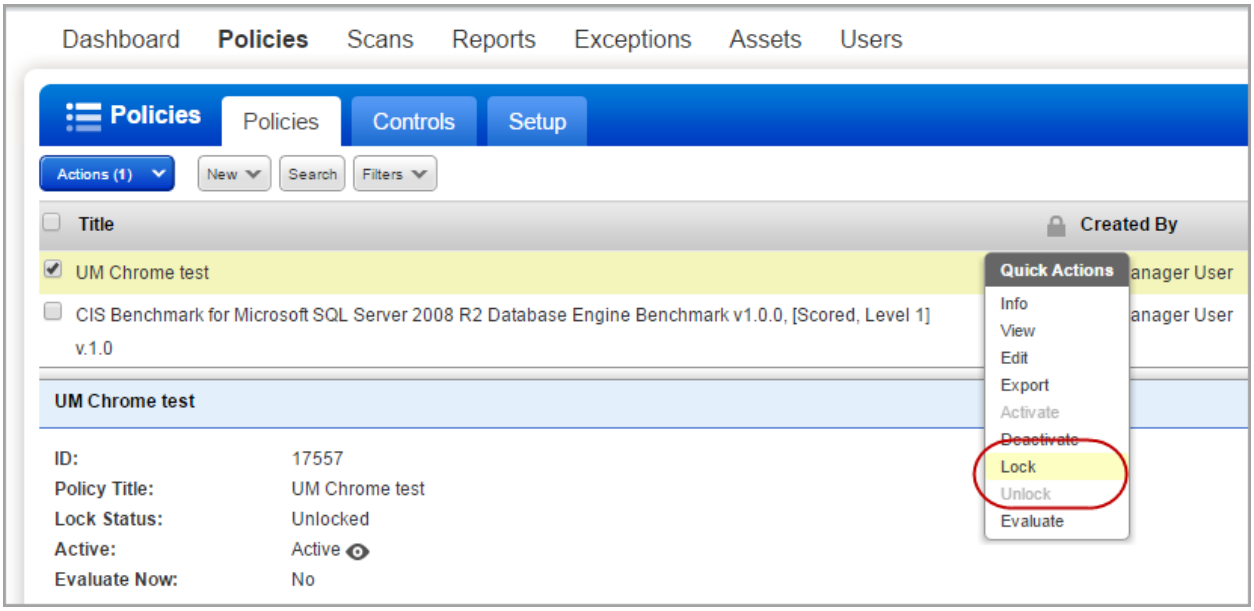
The imported policy appears in your policies list where you can assign assets to the policy and customize the policy settings. The UDCs from the policy appear on your controls list. We'll append the policy name to the control statement for each UDC added, as shown below.



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.



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.

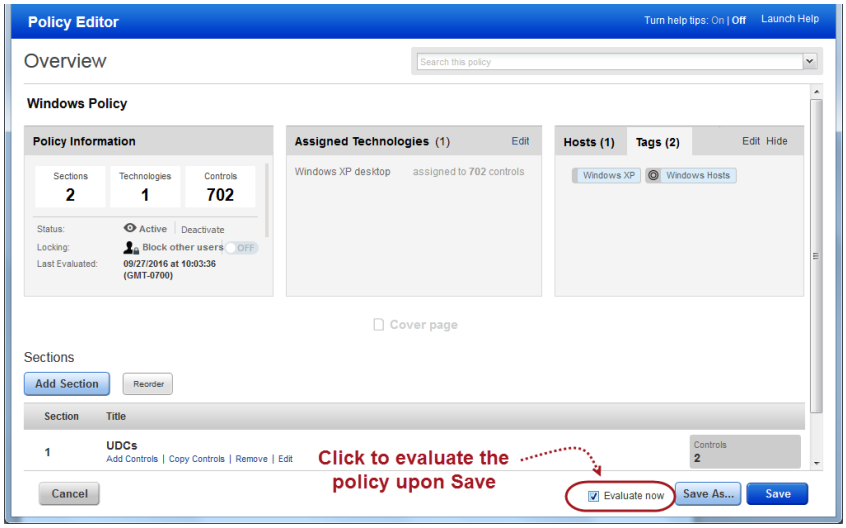
Start Policy Evaluation Anytime

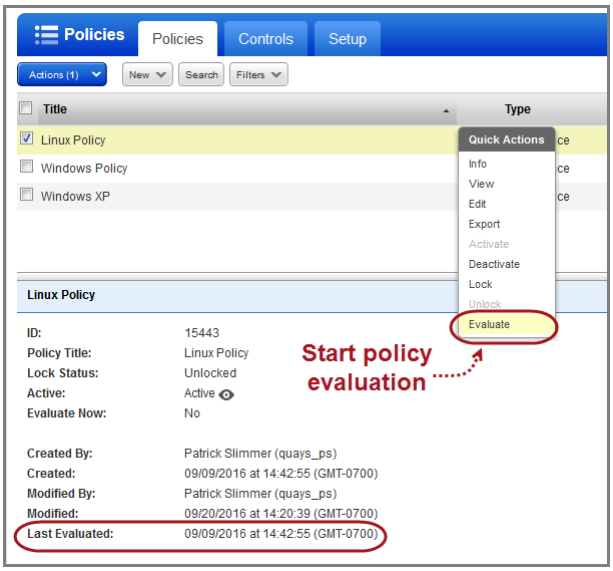
We always evaluate policies when new scan results are processed for the hosts in your policy. With this release, you can also start policy evaluation when saving changes to a policy or anytime from the policies data list.

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.





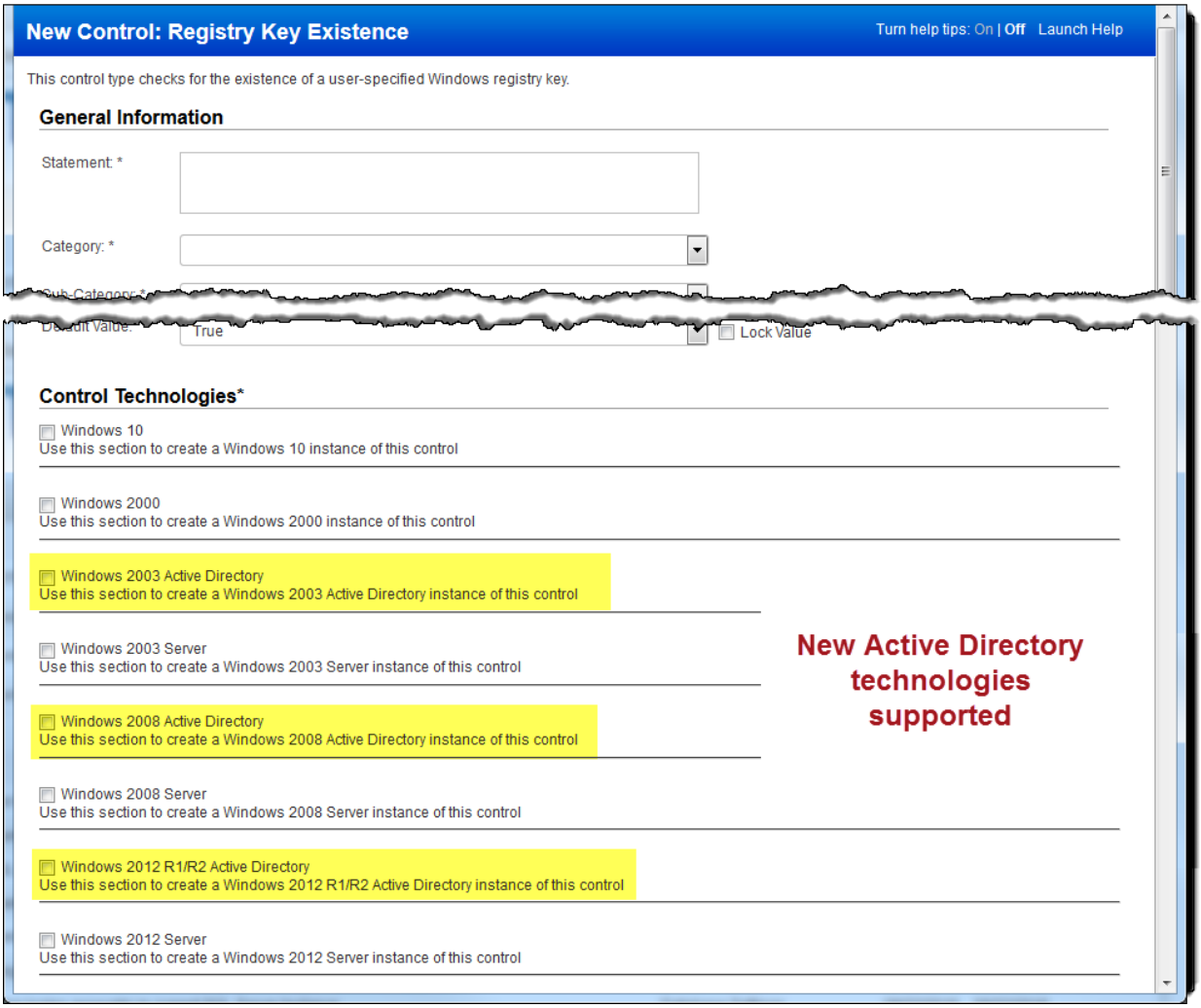
Evaluate from Policies List

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.