Qualys 8.11 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

More Granular Schedule Settings
Tomcat Server Authentication - Extended Support to Windows
Support for Palo Alto Networks Firewall Authentication
Support for MongoDB Authentication
Authorized Use Only Message

Qualys Vulnerability Management (VM)

New Scan Option - Do Not Overwrite OS
Show QID Changes in KnowledgeBase
More about for Information Gathered Detections

Qualys Policy Compliance (PC/SCAP/SCA)

Select a Timeframe for Policy Reports
New UDC: Directory Integrity Check

Qualys 8.11 brings you many more Improvements and updates! Learn more

Copyright 2017 by Qualys, Inc. All Rights Reserved.

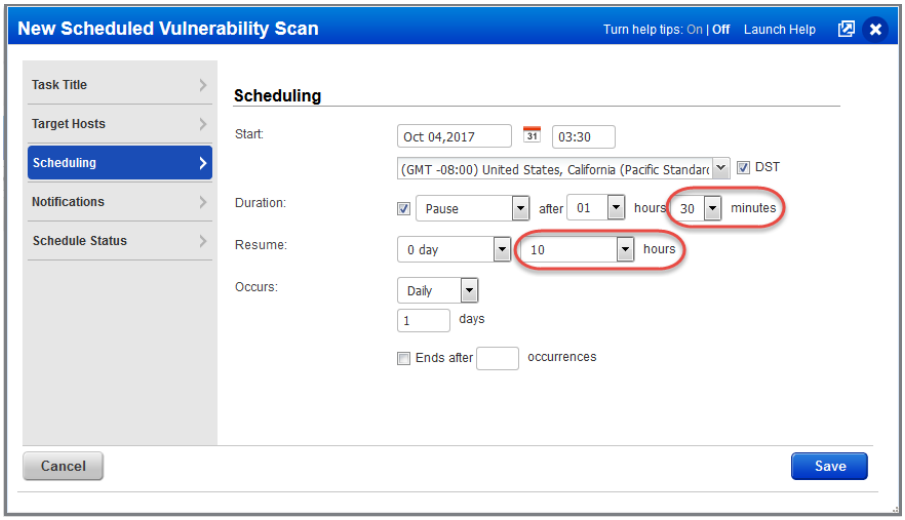
Qualys Cloud Platform

More Granular Schedule Settings

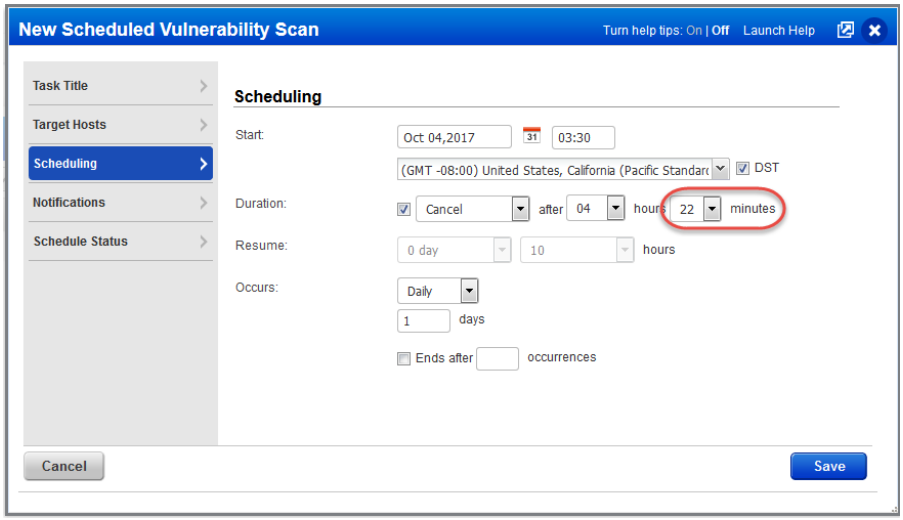
With this release you can set minutes when defining when to pause or cancel a scan, and set hours for when to resume a scan.

Good to Know – The value you set for pause will determine the minimum value you can set for resume. For example, if you set the scan to pause after 1 hour then you can set it to resume in 2 or more hours. If you set the scan to pause between 1-2 hours (from 1hr, 1min to 1 hr, 59min) then you can set it to resume in 3 hours or more.

Pause and Resume



Cancel



Tomcat Server Authentication - Extended Support to Windows

We now support vulnerability and compliance scans for tomcat servers running on Windows hosts. Simply create a Tomcat Server record with details about your Apache Tomcat installation and instance. Your Tomcat Server records may include details for both Windows and Unix installations (previously supported). A Windows record is also required.

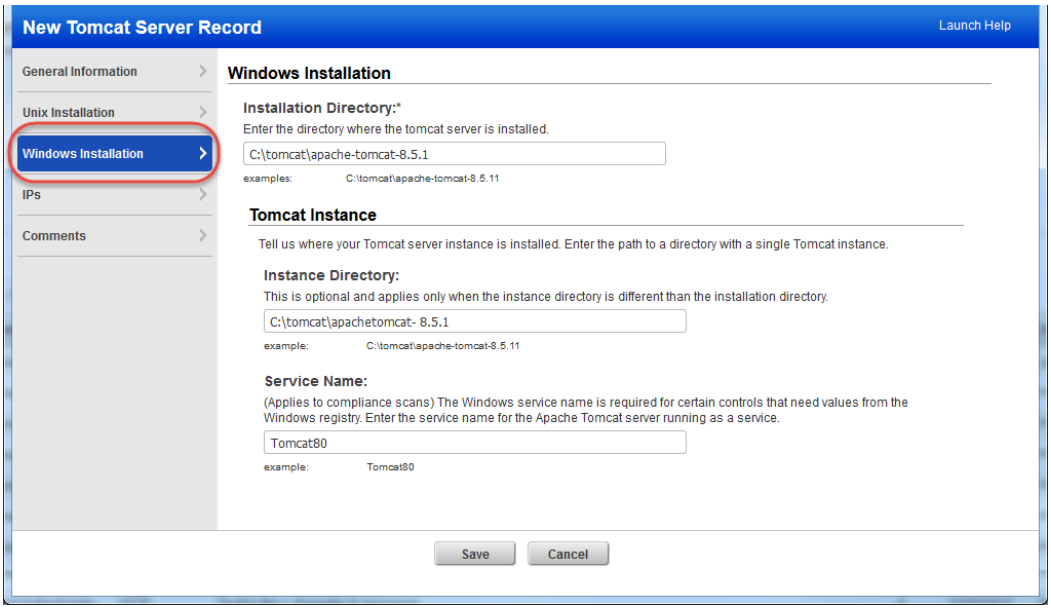
Which technologies are supported?

For Windows, we support Apache Tomcat 7.x and 8.x.

For Unix, we added support for Apache Tomcat 8.x. We also support Apache Tomcat 6.x and 7.x, VMware vFabric tc Server 2.9.x and Pivotal tc Server 3.x.

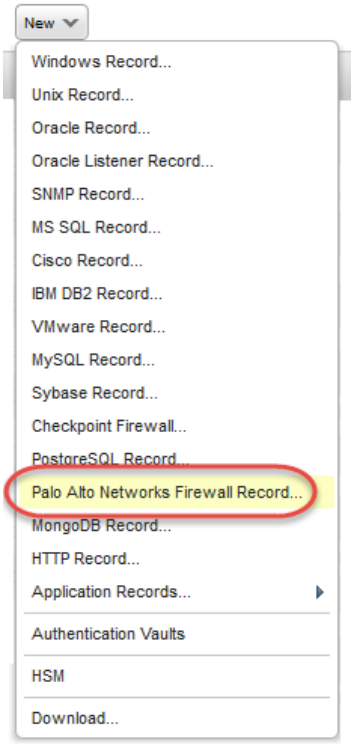
Updated Tomcat Server Record

You'll see a new section for providing details about your Windows installation, including the Windows directory where the tomcat server is installed, the directory where the tomcat server instance is installed, and the Windows service name (applies to compliance scans only). The Windows service name is required for certain controls that need values from the Windows registry.



Support for Palo Alto Networks Firewall Authentication

Create a Palo Alto Networks Firewall record in order to authenticate to a firewall instance running on hosts in your account. This authentication type is supported for vulnerability scans and compliance scans using VM, PC and SCA.



Which technologies are supported?

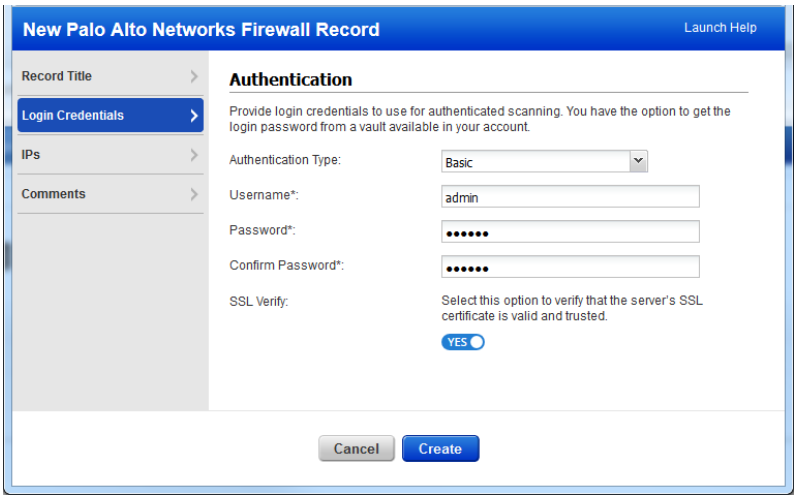
PANOS 6, 7 and 8

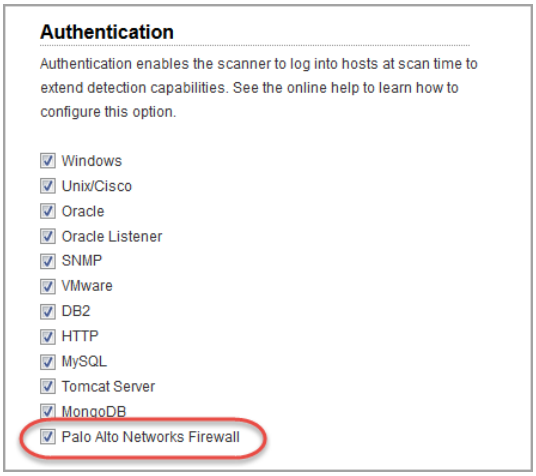
How do I get started?

Go to Scans > Authentication, and choose New > Palo Alto Networks Firewall Record (as shown on the right).

Your Palo Alto Networks Firewall Record

Provide basic login credentials (username and password) to be used for authentication or get the password from a supported password vault. See the online help for user account requirements.



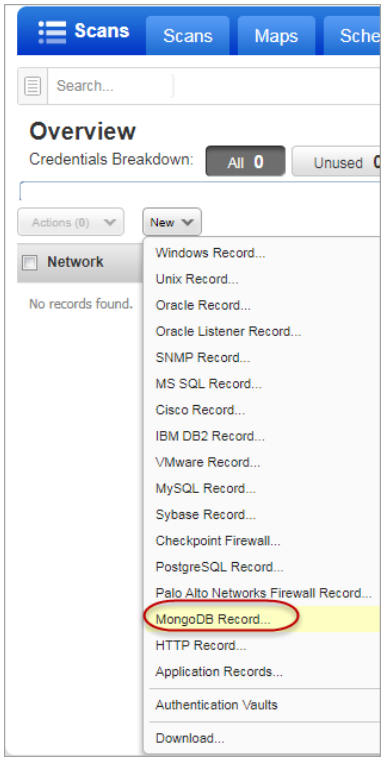


Enable Palo Alto Networks Firewall authentication

Running vulnerability scans? Be sure to select this new authentication type in your option profile.

Support for MongoDB Authentication

We now support MongoDB authentication for vulnerability scans and compliance scans using Qualys apps VM, PC, SCA. Simply create a new MongoDB authentication record with details about your to authenticate to a MongoDB database instance running on a Unix host, and scan it for compliance.



Unix authentication is required so you'll also need a Unix record for the host running the database. Make sure the IP addresses you define in your MongoDB records are also defined in Unix records.

Which technologies are supported?

- MongoDB 3.x

How do I get started?

- Go to Scans > Authentication.

- Check that you have a Unix record already defined for the host running the database.

- Create a MongoDB record for the same host. Go to New > MongoDB Record.

Your MongoDB authentication record

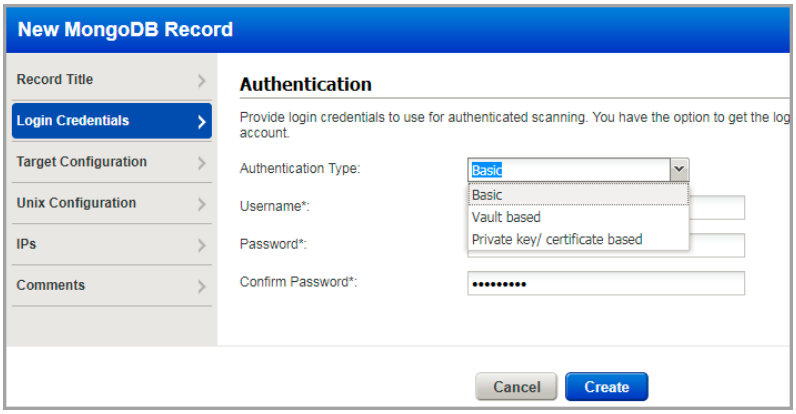
The type of authentication method you use depends on your server settings and how you've configured client authentication.

You can use:

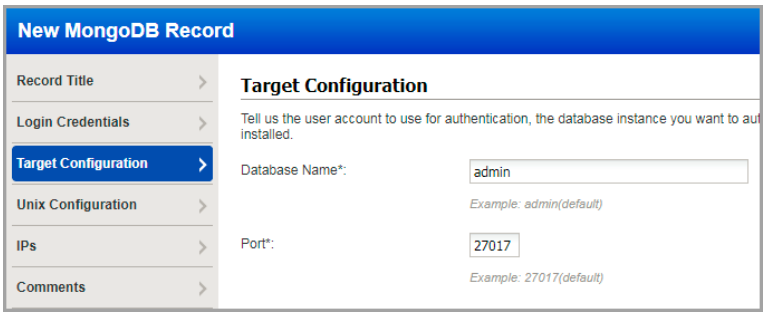
- Basic to authenticate with the credentials you provide

- Vault based to retrieve password from the Vault

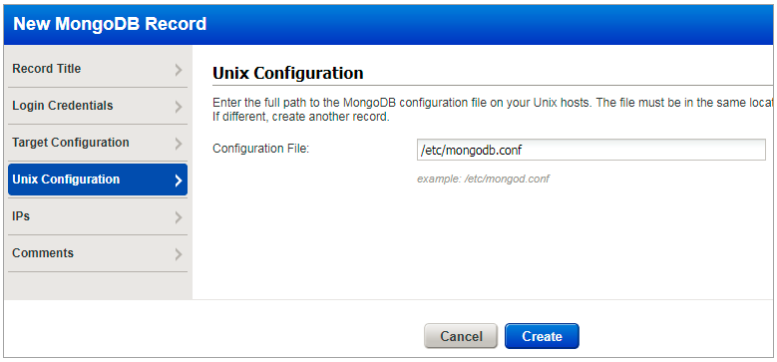
- Private key/certificate based password retrieval



Tell us the database name to authenticate to and the port the database is running on (or use the default database name and port).



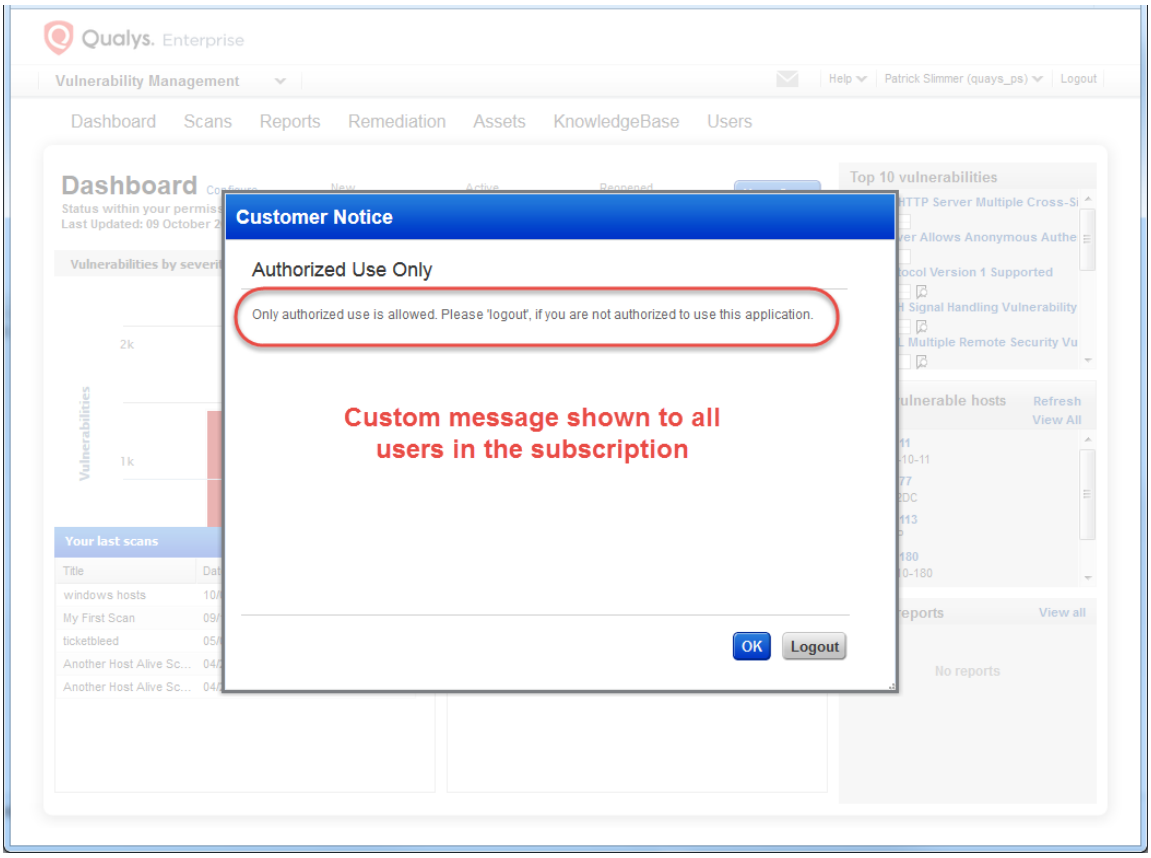
On the Unix tab, tell us the full path to the MongoDB configuration file on your Unix hosts. The file must be in the same location on all IPs listed in the record. If the file is in a different location for some hosts you must create additional records for those hosts.



Authorized Use Only Message

You can now choose to display an “Authorized Use Only” message to users after they log in. Contact Qualys Support or your Technical Account Manager if you’re interested in this feature.

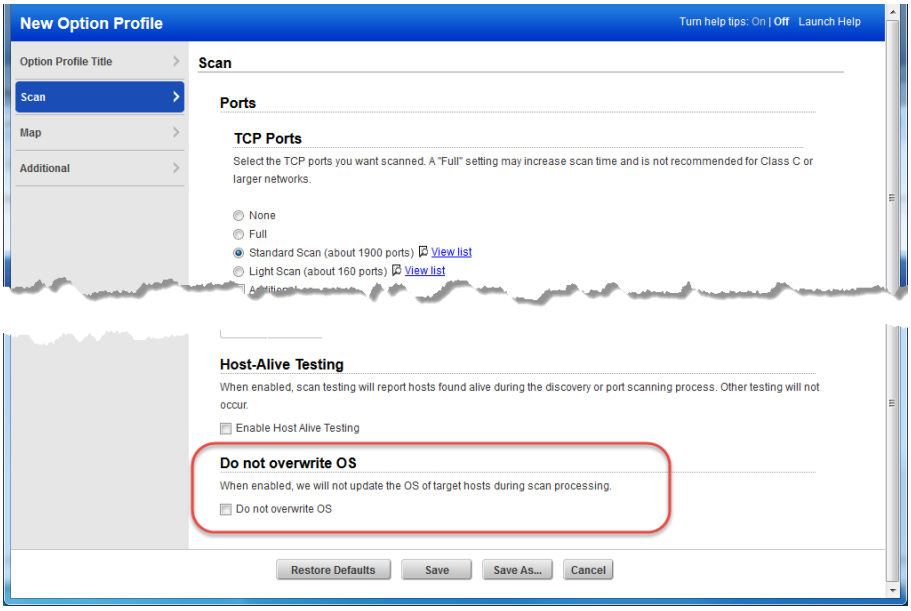
Your custom message will appear to all users in your subscription each time they log in. The user must hit OK to acknowledge that they are authorized in order to continue into the application. This is required by some customers for compliance purposes.



Qualys Vulnerability Management (VM)

New Scan Option - Do Not Overwrite OS

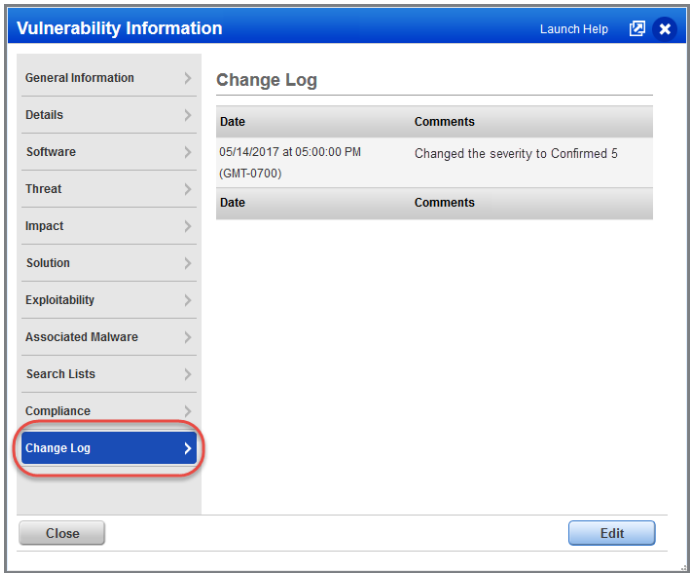
This new option appears in your option profile – scroll to the bottom of the Scan tab to see it. When selected, we will not update the operating system for your target hosts. This is especially useful if you're running a light or custom scan and you don't want to overwrite the OS detected by a Full scan.



Show QID Changes in KnowledgeBase

You'll now be able to view a list of changes made by Qualys to any QID in the Vulnerability KnowledgeBase including changes to detection logic, severity level and vulnerability type (confirmed, potential, information gathered).

Go to the KnowledgeBase and choose Info or Edit for any QID. Then go to the Change Log section. For each change you'll see the date of the change and comments provided by the Qualys Vulnerability Signatures team.



Good to Know

Only new changes made by Qualys will be listed. We will not display changes to QIDs made prior to this release.

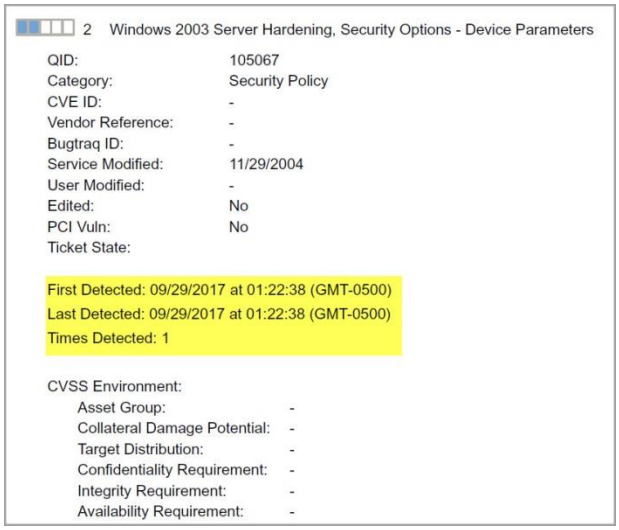
More about for Information Gathered Detections

We now display first time the vulnerability was detected (first detected), last time when the vulnerability was detected (last detected), and the count of the vulnerability (times detected) in host based reports.

How to view the information

Go to Reports > Reports > New and then select any type of report. Generate a scan report in various formats.

Scan Report (PDF format) - - >



2 Windows 2003 Server Hardening, Security Options - Device Parameters

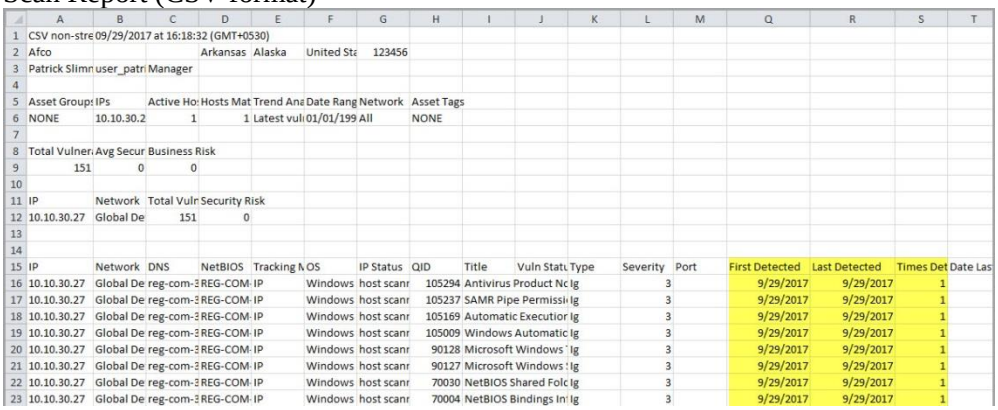
QID:	105067
Category:	Security Policy
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/29/2004
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

First Detected: 09/29/2017 at 01:22:38 (GMT-0500)
Last Detected: 09/29/2017 at 01:22:38 (GMT-0500)
Times Detected: 1

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

Scan Report (CSV format)



	A	B	C	D	E	F	G	H	I	J	K	L	M	Q	R	S	T
1	CSV non-stre	09/29/2017 at 16:18:32 (GMT+0530)															
2	Afco			Arkansas	Alaska	United Sta	123456										
3	Patrick Slimn	user_patri	Manager														
4																	
5	Asset Groups	IPs	Active Ho	Hosts Mat	Trend Ana	Date Rang	Network	Asset Tags									
6	NONE	10.10.30.2	1	1	Latest vuli	01/01/199	All	NONE									
7																	
8	Total Vulner	Avg Secur	Business Risk														
9	151	0	0														
10																	
11	IP	Network	Total Vuln	Security Risk													
12	10.10.30.27	Global De	151	0													
13																	
14																	
15	IP	Network	DNS	NetBIOS	Tracking N	OS	IP Status	QID	Title	Vuln Statu	Type	Severity	Port	First Detected	Last Detected	Times Det	Date Las
16	10.10.30.27	Global De	reg-com-3	REG-COM-	IP	Windows	host scanr	105294	Antivirus Product Nc		Ig	3		9/29/2017	9/29/2017	1	
17	10.10.30.27	Global De	reg-com-3	REG-COM-	IP	Windows	host scanr	105237	SAMR Pipe Permissi		Ig	3		9/29/2017	9/29/2017	1	
18	10.10.30.27	Global De	reg-com-3	REG-COM-	IP	Windows	host scanr	105169	Automatic Executior		Ig	3		9/29/2017	9/29/2017	1	
19	10.10.30.27	Global De	reg-com-3	REG-COM-	IP	Windows	host scanr	105009	Windows Automatic		Ig	3		9/29/2017	9/29/2017	1	
20	10.10.30.27	Global De	reg-com-3	REG-COM-	IP	Windows	host scanr	90128	Microsoft Windows '		Ig	3		9/29/2017	9/29/2017	1	
21	10.10.30.27	Global De	reg-com-3	REG-COM-	IP	Windows	host scanr	90127	Microsoft Windows '		Ig	3		9/29/2017	9/29/2017	1	
22	10.10.30.27	Global De	reg-com-3	REG-COM-	IP	Windows	host scanr	70030	NetBIOS Shared Folc		Ig	3		9/29/2017	9/29/2017	1	
23	10.10.30.27	Global De	reg-com-3	REG-COM-	IP	Windows	host scanr	70004	NetBIOS Bindings In		Ig	3		9/29/2017	9/29/2017	1	

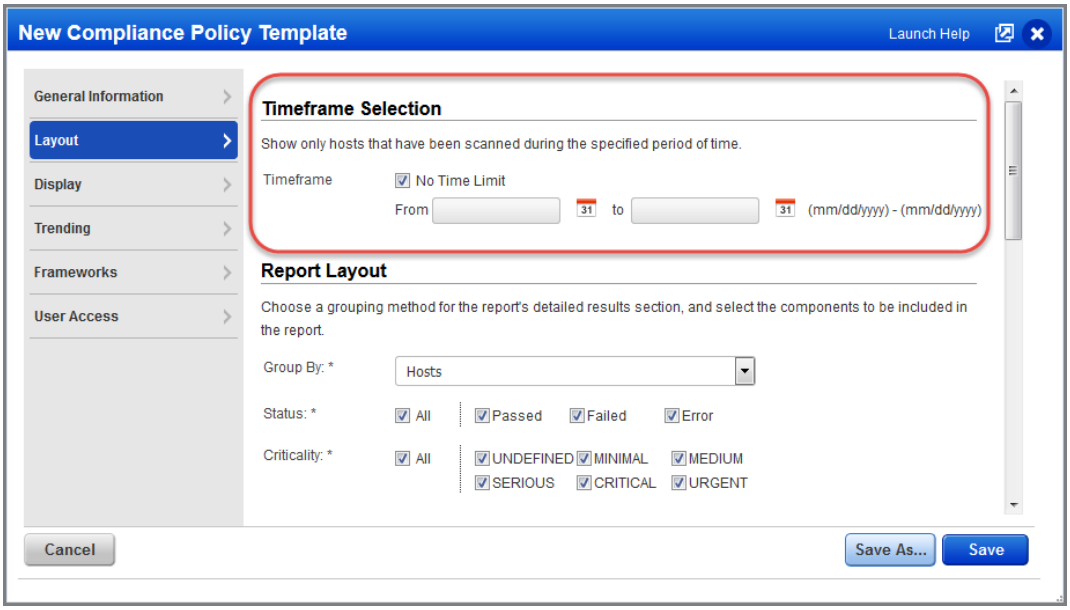
Scan Report (XML format)

```
<VULN_INFO_LIST>
  <VULN_INFO>
    <QID id="qid_105067">105067</QID>
    <TYPE>Ig</TYPE>
    <SSL>false</SSL>
    <RESULT format="table"><![CDATA[Device Parameter  Server Default  Legacy Client  Er
------------------------------ -------------  --------------- --------------  --------------
Allow undock without having to log on   1   0   0   0   1
Allowed to format and eject removable media 0   0   0   0   0
Prevent users from installing printer drivers   1   1   1   1   1
Restrict CD-ROM access to locally logged-on user only   0   Not Set Not Set 1   0
Restrict Floppy access to locally logged-on user only   0   Not Set Not Set 1   0]]></RESULT>
    <FIRST_FOUND>2017-09-29T06:22:38Z</FIRST_FOUND>
    <LAST_FOUND>2017-09-29T06:22:38Z</LAST_FOUND>
    <TIMES_FOUND>1</TIMES_FOUND>
  </VULN_INFO>
```

Qualys Policy Compliance (PC)

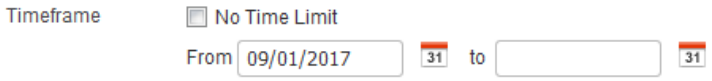
Select a Timeframe for Policy Reports

You now have the option to report compliance data for hosts scanned within a certain timeframe. The report summary, host statistics and detailed results sections of your report will be based on the timeframe you specify. *Note - The trend summary and trend graphs are based on the trend duration set in the template (under Trending).*

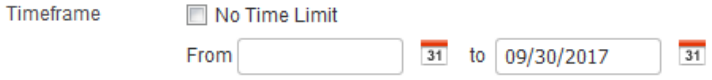


By default, hosts scanned anytime will be included (no time limit). You can specify a start date, end date or date range to select a timeframe. Check out these samples.

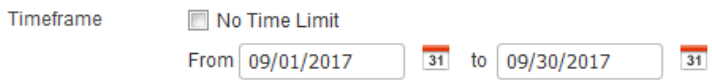
Include hosts scanned from September 1st to the current date:



Include hosts scanned anytime up to and including September 30th:



Include hosts scanned from September 1st to September 30th:

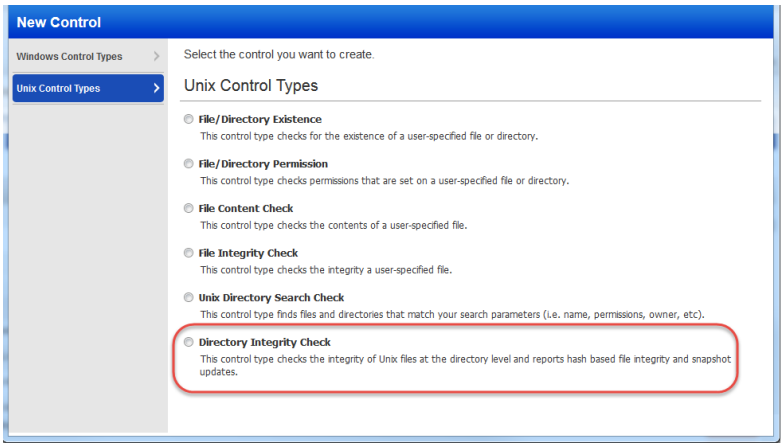


New UDC: Directory Integrity Check

This new User-Defined Control checks the integrity of files and directories that you're interested in and gives you up to the minute visibility on changes to files/directories and their permissions. It calculates hash based file integrity at the directory level, and automatically updates snapshots after changes.

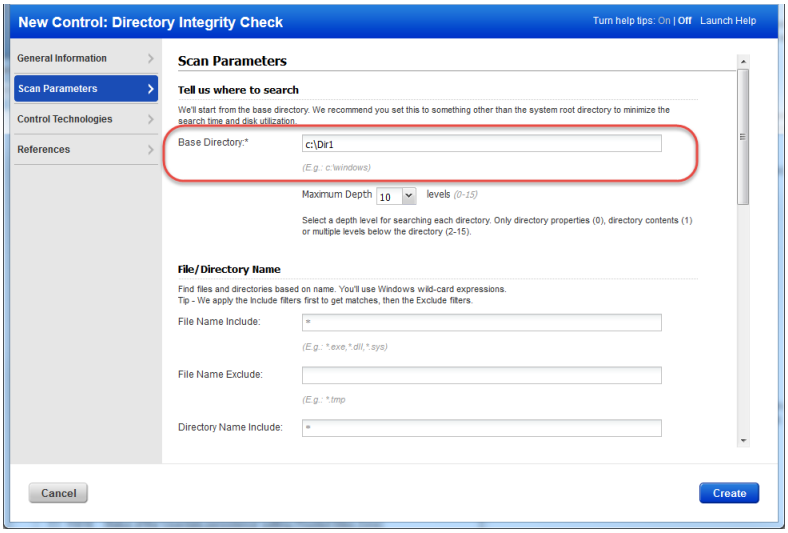
It's easy to get started!

Go to PC > Policies > Controls > New > Control, and choose Directory Integrity Check for Windows or Unix.



We start from the base directory

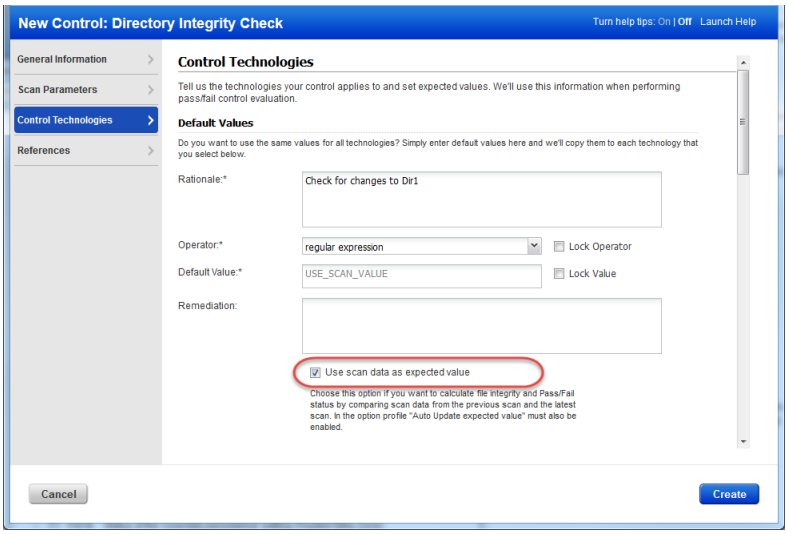
Tell us the base directory and set other scan parameters and search limits for this control.



Use scan data as expected value

This option is enabled by default and recommended. This means the files/directories evaluated are based on the control's scan parameters.

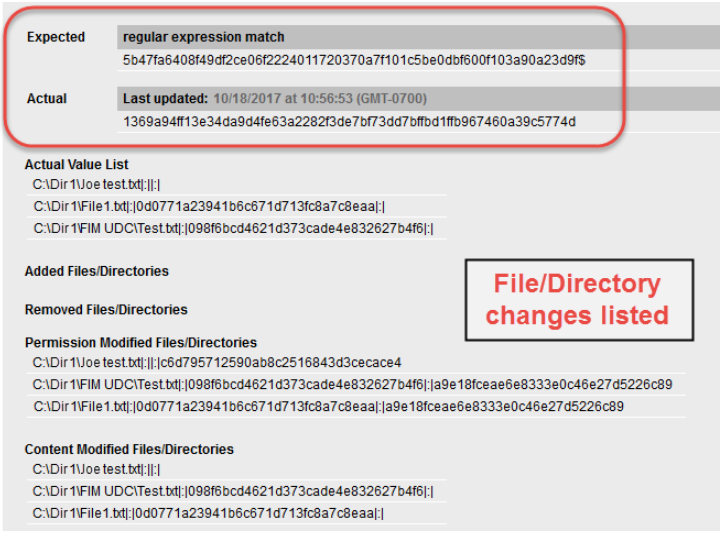
Note - You must also enable "Auto Update expected value" in the option profile you'll use for scanning.



Check out these sample results

Sample 1 - Expected and Actual digest values match (Pass). This means no changes were found to the files/directories.

Sample 2 - Expected and Actual digest values do not match (Fail). This means there were changes to files/directories as listed.



Customize file/directory selection

When "Use scan data as expected value" is disabled in the control you can customize what directories/files are included in snapshots used to calculate Pass/Fail status. We recommend you set the default value to .* (to match any value) and then check the actual value returned by the scan in a policy report. Then you can copy/paste the actual value into your policy.

Sample 1 - Expected and Actual values match (Pass). This means no changes were found.

Sample 2 - Expected and Actual values do not match (Fail). There were changes to files/directories. You'll notice that the digest for File1.txt is different because the file contents changed.

Issues Addressed

- Removed the limitation of 3900 ASCII characters for IP/range fields when you re-launch a scan.
- The Thycotic Secret Server vault is now supported for private key retrieval. The following authentication records are affected: Unix, PostgreSQL and MongoDB.
- Fixed an issue where searching for multiple IPs or specifying an IP range in the Scans > Authentication tab did not show results for all the specified IPs or IP range.
- Correct text message is shown when a network is deleted which at that time is running scans or reports.
- We updated the list of supported platforms in the Add New Virtual Scanner Appliance wizard.
- Now Compliance Reports in PDF are properly formatted using a template with multiple technologies.
- Fixed an issue in HTML Policy Reports where the Actual values were displayed as a single text line.
- The UDC detail values are now displayed in a tabular format in the Policy as well as the PDF format of the Policy Report.
- An appropriate validation error message is displayed if technology is removed from a control.
- An appropriate error message is displayed if the required Base directory field on Unix Directory Search Create/Edit window is left blank.
- The Remediation field on the Control Technology window for Directory Integrity Check, now has the [*] mark to signify that it is a mandatory field.
- The required field symbol [*] is now correctly displayed as [:*] where applicable.
- Search tracking method no longer shows Agent as an option while creating a policy.
- Fixed an issue where an exception was reopened due to change of evidence when there was no change in evidence.
- Fixed an issue where incorrect results were included in the user's Asset Search Report.
- Fixed an issue where Header was being displayed in CSV in certain corner cases when it was requested to Hide the header at the time of report generation.
- Fixed an issue where duplicate records were created even when the "Show unified views of hosts" option is enabled to display a merged record for host results from your vulnerability scans and agent.
- Fixed an issue where reports including multiple IP addresses were not formatted correctly.
- If you check the "Exclude Account ID from filename and report" option in report template, then a report generated using that template will not contain the username.
- Fixed an issue where user was getting error when creating a report template.
- Fixed an issue where searching for IPs contained in a map, using the Map > Search > Target option, returned incorrect results.
- Now when the user selects hosts to add to an approved hosts list for a map, the selected hosts appear in the Approved Hosts popup as expected.
- Fixed an issue where some map XML reports were not encoding certain special characters, and therefore the reports didn't pass validation. Now proper HTML encoding is applied to those map XML reports.

- Fixed an issue where users got an error when trying to ignore a vulnerability on an agent host (tracking method AGENT).
- Sorting by Targets column on VM Scans > Schedules tab now will not blank out the values in the Targets column for tag based scans.
- Fixed an issue now to display the timezone into schedule report as per the user profile setting rather than scheduled report timezone . Report will be run according to the selected timezone during scheduling.
- Now when the user chooses the link to download a report that is no longer available, we'll show a message telling the user the reason. The report will need to be regenerated.
- Host based scan reports now display the FQDN in the report header.
- Fixed an issue concerning auto closing of Open remediation tickets. Now Open remediation tickets will be auto closed based on the remediation policy rules as expected.
- Now users can add comments to CyberArk AIM vault records using the UI and API.
- Activity Logs now correctly reflect accurate log entries for SSH2 authentication record updates.
- Now the same business unit user will be able to see Excluded Hosts History as expected.
- We've made improvements and query optimizations for the Authentication Report.
- Fixed an issue where Auto Timezone was not detected properly for users using Japanese version of Microsoft Windows OS.
- Now users can log in to Qualys Cloud Platform using Safari/iOS.
- An email is sent to the user when a scan/map is trying to execute on a scanner appliance that is offline or unavailable. We've improved the text in this email for better understanding and clarity.
- Now Unit Managers can add hosts using the Host Asset API v2 (/api/2.0/fo/asset/ip/) to Asset Group ALL, when they have the Add IPs permission.
- PCAP scanning support in Express Lite subscription - You can now run a PCAP scan to get full capture data of a scan from an Express Lite subscription.
- Fixed issue where the old Qualys logo still appeared in a few spots in the UI.
- The From field will be set to noreply@qualys.con instead of support@qualys.com for iDefense email notifications.
- Made a fix to the instructions on how to create an administrator account in the Qualys Windows Authentication guide.
- Updated description of configurable vulnerability notification section in online help to clarify this is available to Manager users only.
- We updated the Unix Authenticated Scanning document to include a list of supported Cisco technologies.
- The Windows Authentication document is now updated with a new section "WMI Service Configuration" to describe how to lift WMI authentication level on target on new controls in PC.