QUALYS®

Qualys Cloud Suite 2.26

We're excited to tell you about improvements and enhancements in Qualys Cloud Suite 2.26.

AV AssetView

TP ThreatPROTECT

Search assets with last VM / Compliance scan date
Apply Tags to Multiple Assets
Use "*" Wildcard to Broaden Search Results

CA Cloud Agent

View activation job progress
View installation instructions for deploying Linux agents on Azure

SAQ Security Assessment Questionnaire

Create Rules for Dynamic Questionnaire

WAS Web Application Scanning

Custom Inline Comments for Whitelists and Blacklists
Ability to Change From Address in Scans and Scheduled Reports

Qualys Cloud Suite 2.26 brings you many more
Improvements and updates! Learn more

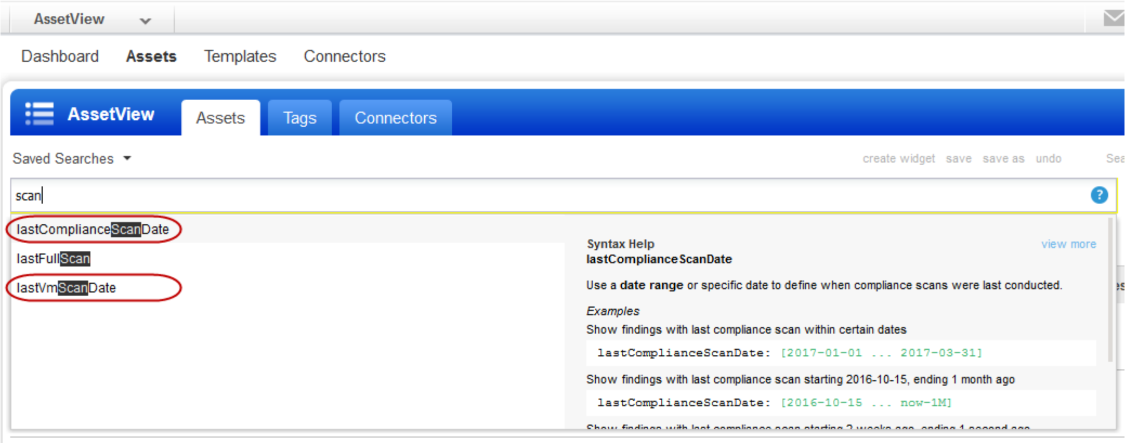
Copyright 2017 by Qualys, Inc. All Rights Reserved.

AV AssetView

TP ThreatPROTECT

Search assets with last VM / Compliance scan date

You can now search / filter assets with the last VM scan date or the last compliance scan date. The new fields can also be used for creating widgets, templates, saved searches, and dynamic asset tags.



Syntax Help
lastComplianceScanDate

Use a **date range** or specific date to define when compliance scans were last conducted.

Examples

Show findings with last compliance scan within certain dates

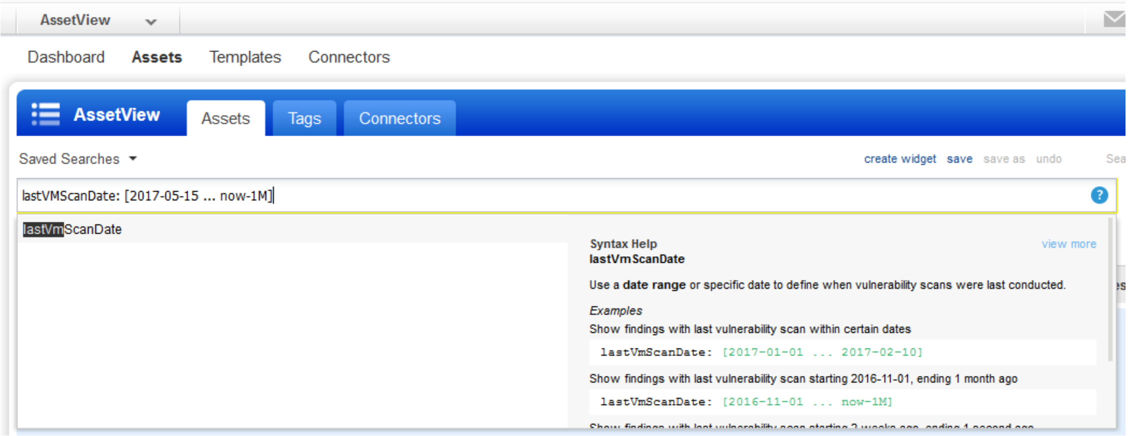
```
lastComplianceScanDate: [2017-01-01 ... 2017-03-31]
```

Show findings with last compliance scan starting 2016-10-15, ending 1 month ago

```
lastComplianceScanDate: [2016-10-15 ... now-1M]
```

Show findings with last compliance scan starting 2 weeks ago, ending 1 second ago

Simply go to the Assets tab, select the field name and enter your query (after the colon). The Syntax Help on the right gives helpful hints with writing your query.



```
lastVMScanDate: [2017-05-15 ... now-1M]
```

Syntax Help
lastVmScanDate

Use a **date range** or specific date to define when vulnerability scans were last conducted.

Examples

Show findings with last vulnerability scan within certain dates

```
lastVmScanDate: [2017-01-01 ... 2017-02-10]
```

Show findings with last vulnerability scan starting 2016-11-01, ending 1 month ago

```
lastVmScanDate: [2016-11-01 ... now-1M]
```

Show findings with last vulnerability scan starting 2 weeks ago, ending 1 second ago

Some examples,

Search for assets with a specific VM scan date or compliance scan date:

lastComplianceScanDate:'2016-01-10'
lastVMScanDate:'2016-01-10'

Search for assets having last VM / Compliance scan date within a date range:
lastComplianceScanDate: [2016-01-01 ... 2016-01-10]
lastVMScanDate: [2016-01-01 ... 2016-01-10]

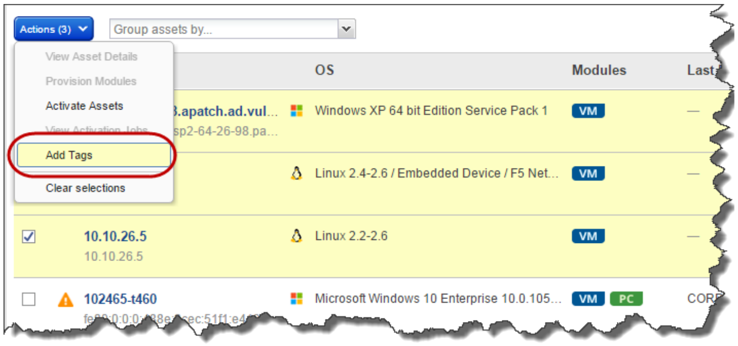
Search for assets having last VM / Compliance scan date between a specific date and a few months ago:
lastComplianceScanDate: [2015-10-01 ... now-3M]
lastVMScanDate: [2015-10-01 ... now-3M]

Apply Tags to Multiple Assets

You can now apply tags to multiple assets from the assets list at one go. Simply, select the assets you want to tag and from the Actions menu click Add Tags.

The selected tag is applied to all the chosen Assets and can be viewed in the Tags column in the Asset List.

While applying tags, dynamic tags are not displayed as such tags cannot be bulk assigned to assets.

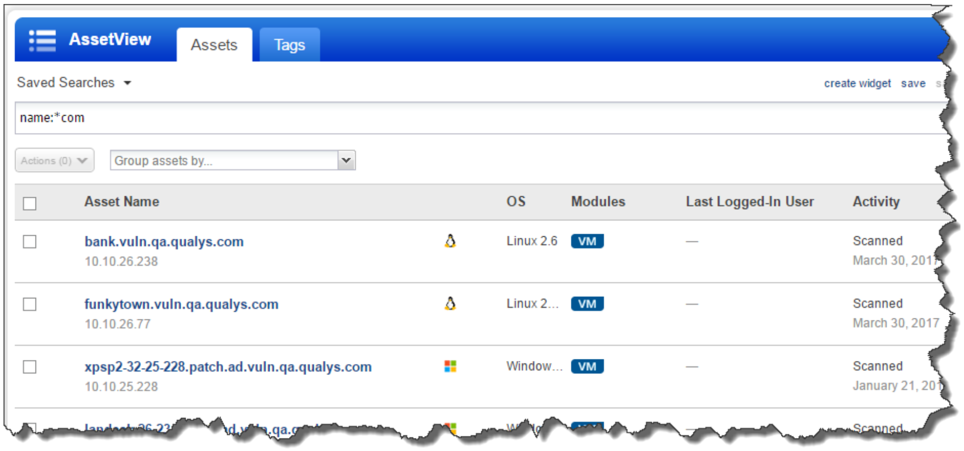


		OS	Modules	Last
	.apatch.ad.vul... sp2-64-26-98.pa...	Windows XP 64 bit Edition Service Pack 1	VM	—
		Linux 2.4-2.6 / Embedded Device / F5 Net...	VM	—
☑	10.10.26.5 10.10.26.5	Linux 2.2-2.6	VM	—
□	102465-t460	Microsoft Windows 10 Enterprise 10.0.105...	VM PC	COR

Use "*" Wildcard to Broaden Search Results

We have now added support to use "*" wildcard in the search criteria. When the query string starts with * all the assets "ending in" for the fields "name" and "tags.name" are matched and listed. Search results are case insensitive.

For example the query name:*com matches assets with hostname ending in ".com" including hostnames like this: qualys.com, asset.qualys.com, corp.us.domain123.com, etc.



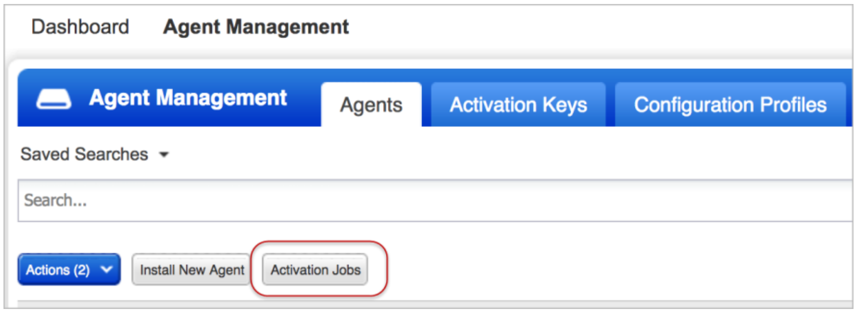
name:*com

□	Asset Name	OS	Modules	Last Logged-In User	Activity
□	bank.vuln.qa.qualys.com 10.10.26.238	Linux 2.6	VM	—	Scanned March 30, 2017
□	funkytown.vuln.qa.qualys.com 10.10.26.77	Linux 2...	VM	—	Scanned March 30, 2017
□	xpsp2-32-25-228.patch.ad.vuln.qa.qualys.com 10.10.25.228	Window...	VM	—	Scanned January 21, 201

CA Cloud Agent

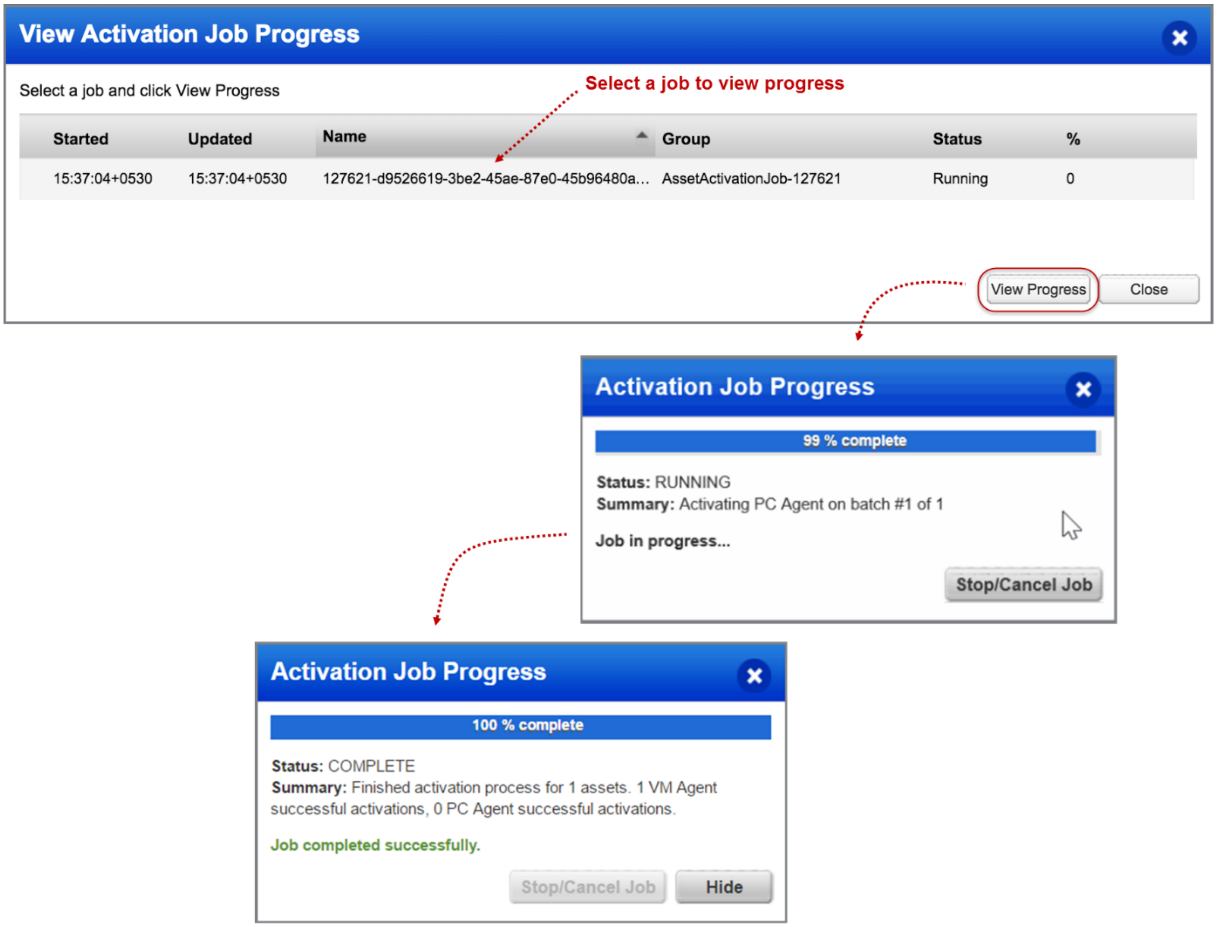
View activation job progress

Once you initiate activation of agents, it may take some time for the agents to get activated. You can now view the progress of the activation jobs which you have initiated for the agents.



To view the activation job progress, go to Agent Management > Agents, and then click Activation Jobs.

You will see a list of activation jobs you have initiated. Select a job and click View Progress to view the activation progress.


View Activation Job Progress

Select a job and click View Progress

Select a job to view progress

Started	Updated	Name	Group	Status	%
15:37:04+0530	15:37:04+0530	127621-d9526619-3be2-45ae-87e0-45b96480a…	AssetActivationJob-127621	Running	0

Activation Job Progress

99 % complete

Status: RUNNING
Summary: Activating PC Agent on batch #1 of 1

Job in progress...

Activation Job Progress

100 % complete

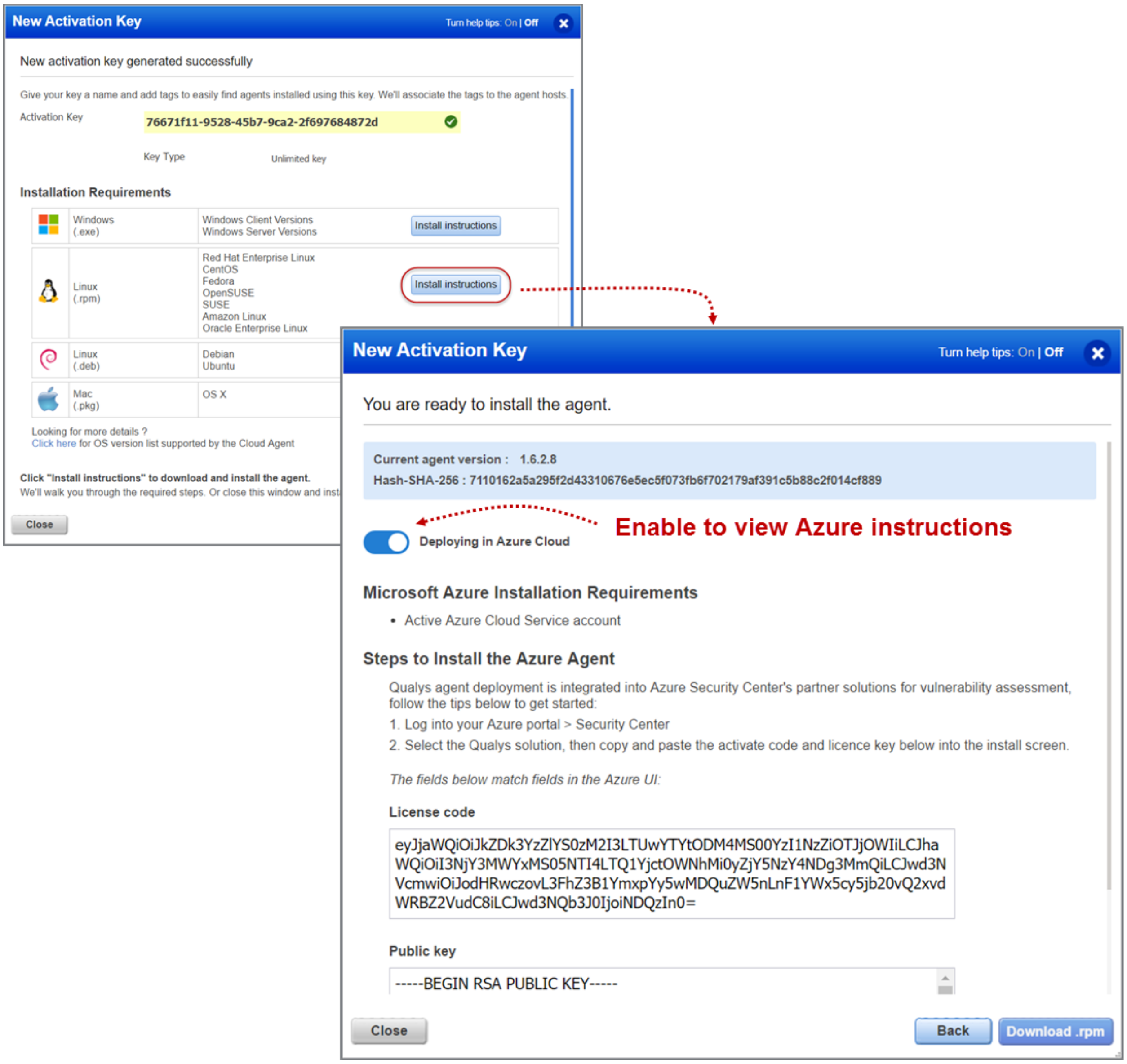
Status: COMPLETE
Summary: Finished activation process for 1 assets. 1 VM Agent successful activations, 0 PC Agent successful activations.

Job completed successfully.

Note: While the job is in progress you can use the Stop/Cancel Job option to cancel the agent activation if required. Once cancelled, you can activate the agent later.

View installation instructions for deploying Linux agents on Azure

You can now view the installation instructions for deploying Linux agents on Azure Cloud. The installation instructions are available once you generate an activation key.



New activation key generated successfully

Give your key a name and add tags to easily find agents installed using this key. We'll associate the tags to the agent hosts.

Activation Key 76671f11-9528-45b7-9ca2-2f697684872d ✓

Key Type Unlimited key

Installation Requirements

Windows (.exe)	Windows Client Versions Windows Server Versions	Install instructions
Linux (.rpm)	Red Hat Enterprise Linux CentOS Fedora OpenSUSE SUSE Amazon Linux Oracle Enterprise Linux	Install instructions
Linux (.deb)	Debian Ubuntu	
Mac (.pkg)	OS X	

Looking for more details ?
Click here for OS version list supported by the Cloud Agent

Click "Install instructions" to download and install the agent.
We'll walk you through the required steps. Or close this window and inst

You are ready to install the agent.

Current agent version : 1.6.2.8
Hash-SHA-256 : 7110162a5a295f2d43310676e5ec5f073fb6f702179af391c5b88c2f014cf889

Enable to view Azure instructions

Deploying in Azure Cloud

Microsoft Azure Installation Requirements

- Active Azure Cloud Service account

Steps to Install the Azure Agent

Qualys agent deployment is integrated into Azure Security Center's partner solutions for vulnerability assessment, follow the tips below to get started:

1. Log into your Azure portal > Security Center
2. Select the Qualys solution, then copy and paste the activate code and licence key below into the install screen.

The fields below match fields in the Azure UI:

License code

```
eyJjaWQiOiJkZDk3YzZlYS0zM2I3LTUwYTYtODM4MS00YzI1NzZiOTJjOWIiLCJha
WQiOiI3NjY3MWYxMS05NTI4LTQ1YjctOWNhMi0yZjY5NzY4NDg3MmQiLCJwd3N
VcmwiOiJodHRwczovL3FhZ3B1YmxpYy5wMDQuZW5nLnF1YWx5cy5jb20vQ2xvd
WRBZ2VudC8iLCJwd3NQb3J0IjoiNDQzIn0=
```

Public key

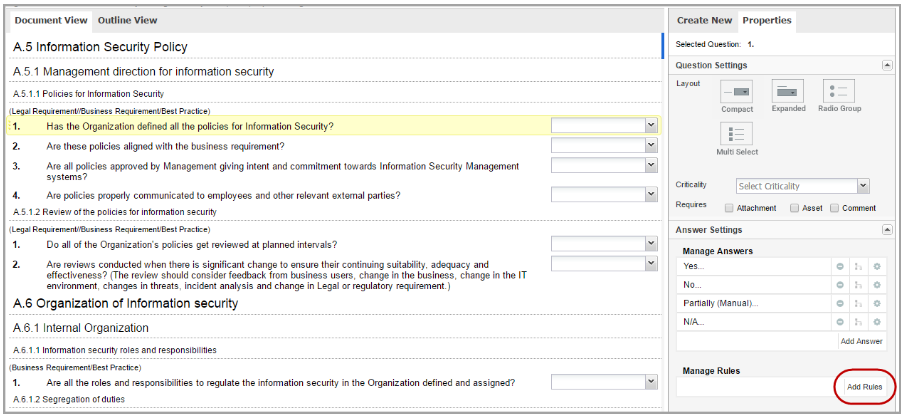
```
-----BEGIN RSA PUBLIC KEY-----
```

Create Rules for Dynamic Questionnaire

In a template, you can now configure questions to be dynamically shown or hidden based on a response to a single question or responses to a combination of questions.

To create rules in the template:

Simply navigate to Templates > My Templates and select the template you want to configure. Choose a question and add a Jump To or Hide rule.



A.5 Information Security Policy

A.5.1 Management direction for information security

A.5.1.1 Policies for Information Security

(Legal Requirement//Business Requirement/Best Practice)

1. Has the Organization defined all the policies for Information Security?
2. Are these policies aligned with the business requirement?
3. Are all policies approved by Management giving intent and commitment towards Information Security Management systems?
4. Are policies properly communicated to employees and other relevant external parties?

A.5.1.2 Review of the policies for information security

(Legal Requirement//Business Requirement/Best Practice)

1. Do all of the Organization's policies get reviewed at planned intervals?
2. Are reviews conducted when there is significant change to ensure their continuing suitability, adequacy and effectiveness? (The review should consider feedback from business users, change in the business, change in the IT environment, changes in threats, incident analysis and change in Legal or regulatory requirement.)

A.6 Organization of Information security

A.6.1 Internal Organization

A.6.1.1 Information security roles and responsibilities

(Business Requirement/Best Practice)

1. Are all the roles and responsibilities to regulate the information security in the Organization defined and assigned?

A.6.1.2 Segregation of duties

Selected Question: 1.

Question Settings

Layout: Compact, Expanded, Radio Group, Multi Select

Criticality: Select Criticality

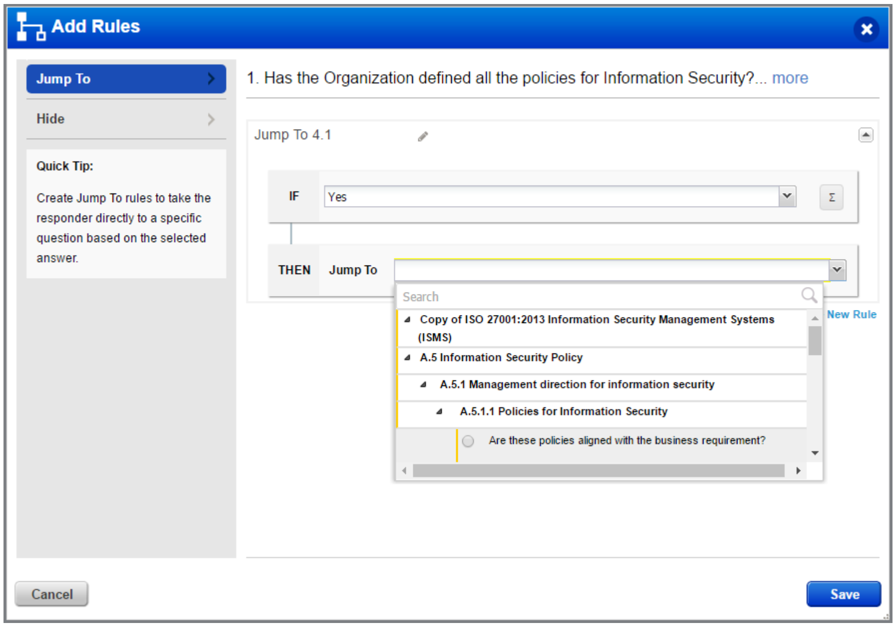
Requires: □ Attachment □ Asset □ Comment

Answer Settings

Manage Answers: Yes... No... Partially (Manual)... N/A...

Manage Rules

Configure a Jump To rule when you want to navigate the responder to a different question depending on the answer provided.



Quick Tip:

Create Jump To rules to take the responder directly to a specific question based on the selected answer.

1. Has the Organization defined all the policies for Information Security?... more

Jump To 4.1

IF Yes

THEN Jump To

Copy of ISO 27001:2013 Information Security Management Systems (ISMS)

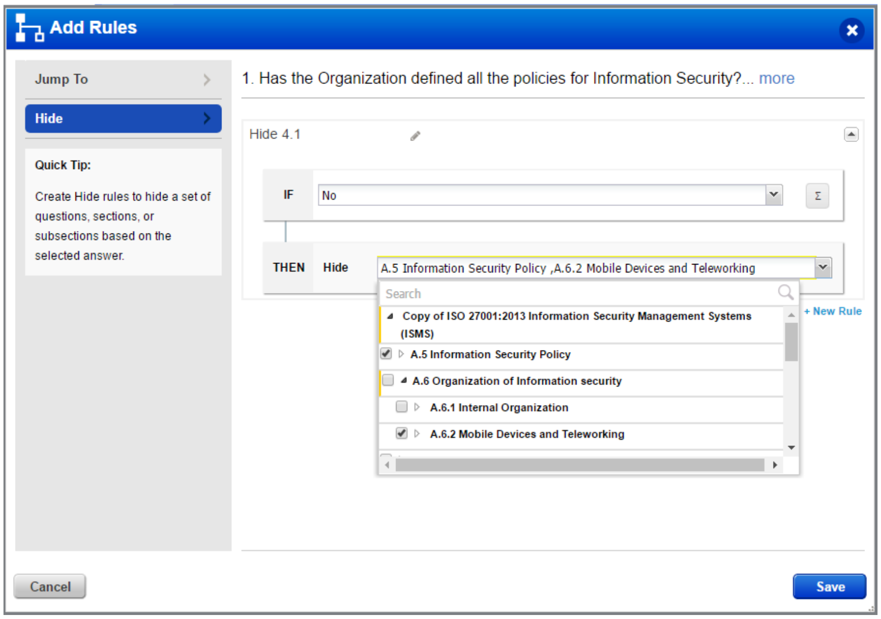
A.5 Information Security Policy

A.5.1 Management direction for information security

A.5.1.1 Policies for Information Security

○ Are these policies aligned with the business requirement?

Configure a Hide rule when you want to hide certain questions, sections, subsections from the responder depending on the answer provided.



Create Hide rules to hide a set of questions, sections, or subsections based on the selected answer.

1. Has the Organization defined all the policies for Information Security?... more

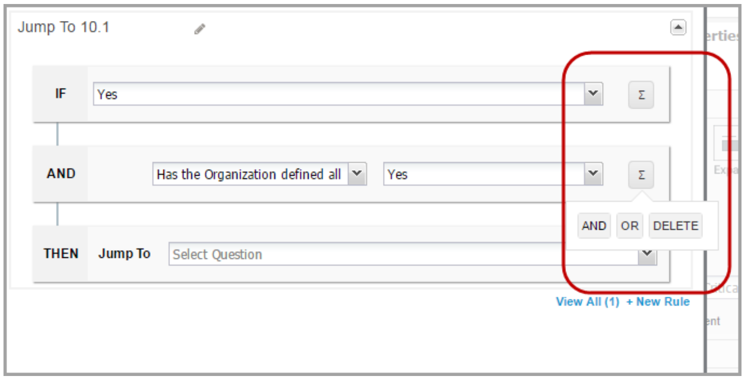
IF: No

THEN Hide: A.5 Information Security Policy ,A.6.2 Mobile Devices and Teleworking

Search

- Copy of ISO 27001:2013 Information Security Management Systems (ISMS)
  - ☑ A.5 Information Security Policy
  - □ A.6 Organization of Information security
    - □ A.6.1 Internal Organization
    - ☑ A.6.2 Mobile Devices and Teleworking

Create complex Jump To and Hide rules using the AND and OR operators.



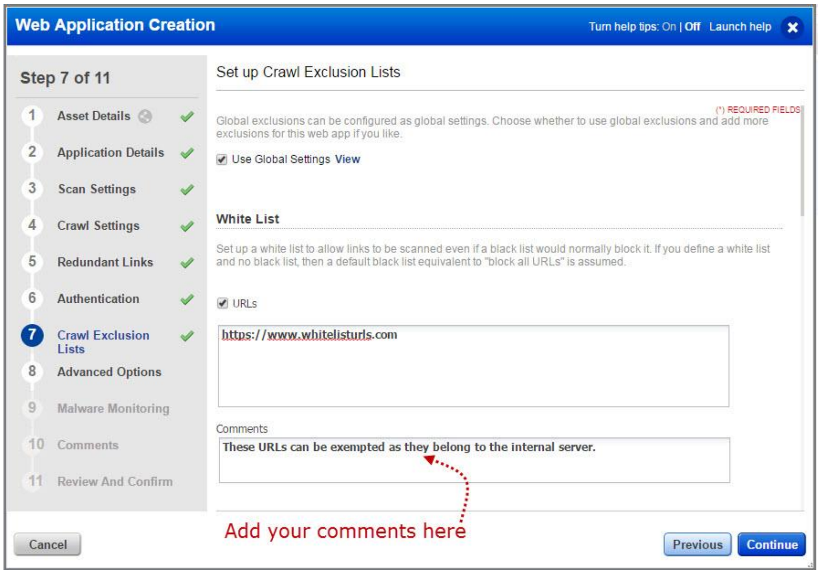
IF: Yes

AND: Has the Organization defined all: Yes

THEN Jump To: Select Question

Custom Inline Comments for Whitelists and Blacklists

With this release you can now enter verbose custom comments along with whitelist and blacklists scanning entries. This will visibly aid users on why specific blacklists or whitelists entries were created.



Set up Crawl Exclusion Lists

(*) REQUIRED FIELDS

Global exclusions can be configured as global settings. Choose whether to use global exclusions and add more exclusions for this web app if you like.

☑ Use Global Settings View

White List

Set up a white list to allow links to be scanned even if a black list would normally block it. If you define a white list and no black list, then a default black list equivalent to "block all URLs" is assumed.

☑ URLs

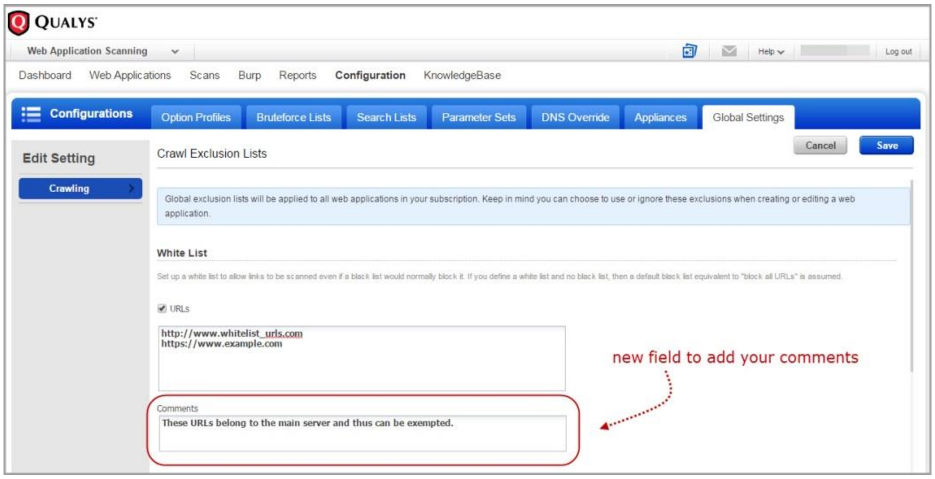
https://www.whitelisturls.com

Comments

These URLs can be exempted as they belong to the internal server.

To add comments to crawl exclusion list that is specific to a web application, edit the web application and go to Crawl Exclusion Lists. Select the field (URL/Regex) and enter your comments.

You could also add comments to the globally defined crawl exclusion lists. Go to Configuration > Global Settings and then click Edit.



Crawl Exclusion Lists

Global exclusion lists will be applied to all web applications in your subscription. Keep in mind you can choose to use or ignore these exclusions when creating or editing a web application.

White List

Set up a white list to allow links to be scanned even if a black list would normally block it. If you define a white list and no black list, then a default black list equivalent to "block all URLs" is assumed.

☑ URLs

http://www.whitelist_urls.com
https://www.example.com

Comments

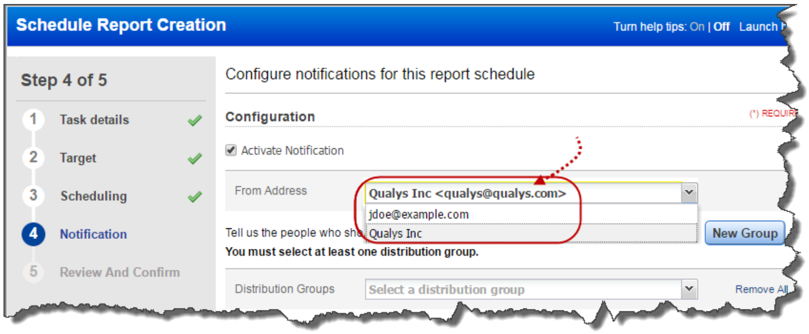
These URLs belong to the main server and thus can be exempted.

To view the comments added to a web application, click View from the quick actions menu and the Crawl Exclusion List panel will display the comments.

Ability to Change From Address in Scans and Scheduled Reports

We now provide you the ability to change the From address in the notifications that are sent for scans, scheduled scans and scheduled reports. You could select the email address when you create or edit scans or scheduled reports. Similarly, you could configure notifications for scheduled scan, re-scheduling a scan, scan completion, scheduled scan failure and scheduled report.

Scheduled Reports



Configure notifications for this report schedule

Configuration (*) REQUIR

☑ Activate Notification

From Address: Qualys Inc <qualys@qualys.com>
jdoe@example.com
Qualys Inc

Tell us the people who sh

You must select at least one distribution group.

Distribution Groups: Select a distribution group

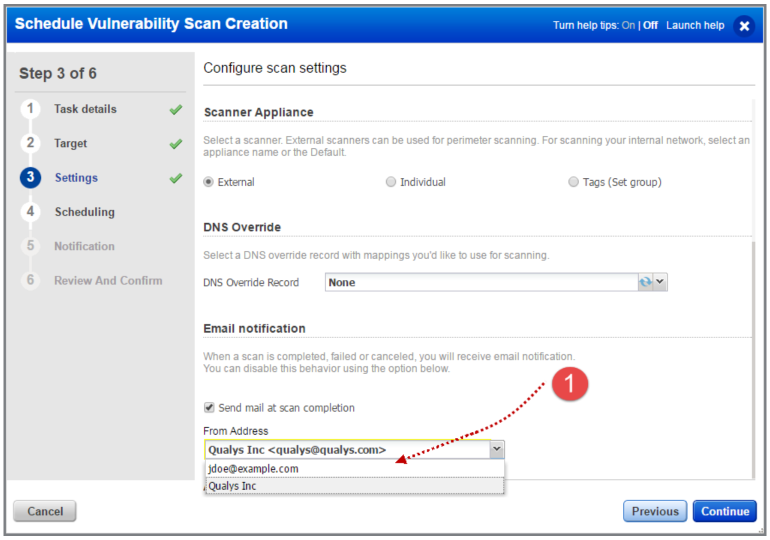
You can now tell us which email address should be used in scheduled report notification. The From Address dropdown populates two options: email address of the scheduled report owner and email address configured in your subscription (for example qualys@qualys.com). Choose one email address from the dropdown.

If the owner of the scheduled report changes, the From Address dropdown will accordingly reflect the email ID of the new owner.

Scheduled Scan

Go to Scans > Schedules > New Schedule and then launch Discovery or Vulnerability Scan.

1) You can configure the From Address for scan completion, scan failure and scan cancellation notifications from the Settings panel.



Configure scan settings

Scanner Appliance

Select a scanner. External scanners can be used for perimeter scanning. For scanning your internal network, select an appliance name or the Default.

● External ○ Individual ○ Tags (Set group)

DNS Override

Select a DNS override record with mappings you'd like to use for scanning.

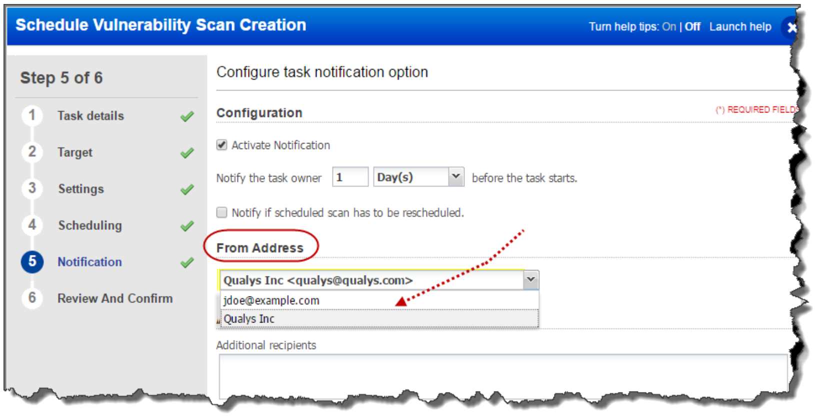
DNS Override Record: None

Email notification

When a scan is completed, failed or canceled, you will receive email notification.
You can disable this behavior using the option below.

☑ Send mail at scan completion

From Address: Qualys Inc <qualys@qualys.com>
jdoe@example.com
Qualys Inc



Configure task notification option

Configuration (*) REQUIRED FIELDS

☑ Activate Notification

Notify the task owner 1 Day(s) before the task starts.

☐ Notify if scheduled scan has to be rescheduled.

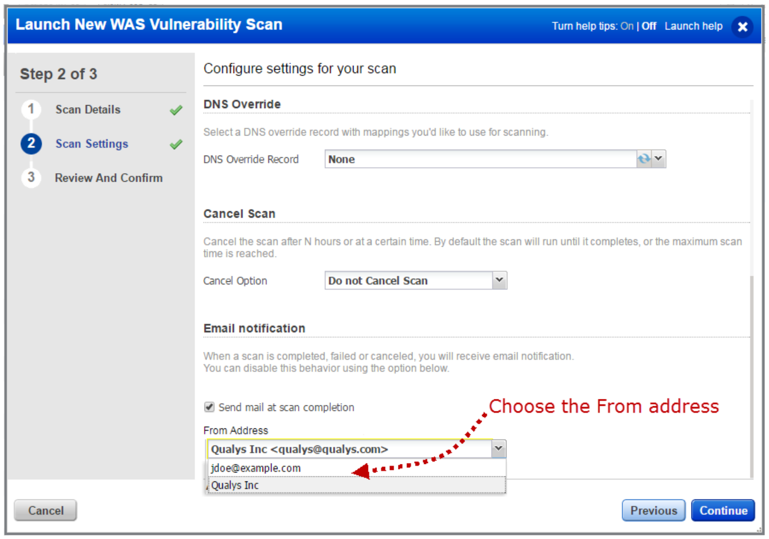
From Address: Qualys Inc <qualys@qualys.com>
jdoe@example.com
Qualys Inc

Additional recipients

2) You can configure the From Address for notification to be sent each time the scan is scheduled to start in the Notification panel.

Launch Scan

Similarly, you can select the From Address for the scan notification when you launch a new scan. Go to Scans > Scan List > New Scan and then launch Discovery or Vulnerability Scan. The Scan Settings panel allows you to select the email address.



Launch New WAS Vulnerability Scan

Step 2 of 3

1 Scan Details ✓

2 Scan Settings ✓

3 Review And Confirm

Configure settings for your scan

DNS Override

Select a DNS override record with mappings you'd like to use for scanning.

DNS Override Record: None

Cancel Scan

Cancel the scan after N hours or at a certain time. By default the scan will run until it completes, or the maximum scan time is reached.

Cancel Option: Do not Cancel Scan

Email notification

When a scan is completed, failed or canceled, you will receive email notification.
You can disable this behavior using the option below.

☑ Send mail at scan completion

From Address: Qualys Inc <qualys@qualys.com>

Choose the From address

Issues addressed in this release

Qualys Cloud Suite 2.26 brings you many more improvements and updates.

AV AssetView

TP ThreatPROTECT

- The saved search list will now be displayed completely without being truncated after setting the search as a favorite.
- Accurate queries are now generated after clicking on asset counts from the Group By vulnerabilities view.
- Tag rules which utilize regular expressions with negative look-behinds are now validated successfully.
- The quick actions menu is now displayed accurately on the UI.
- All assets with EC2 scan are now filtered accurately in Network Topology.
- The Trends graph is now displayed correctly even if data collection fails and there are missing data points.
- Now, in the Trends graph, when a trend value increases from zero it will display 100% instead of Infinity%.
- Dashboard widget filters are now populated correctly while creating a widget.
- The connectors tab would show up as empty at random; this issue is now fixed and appropriate information is displayed.
- In the Group by vulnerabilities view, now queries are executed correctly and accurate vulnerability count is displayed.
- The Asset Vulnerabilities list in Asset View will now display the correct date the vulnerabilities were detected.
- Queries are now accurately formed and results are properly displayed for Backdoors and Trojans Horses widget in ThreatPROTECT dashboard.

CA Cloud Agent

- In order to prevent complete stoppage of agent - platform communication, users are not allowed to set the blackout window for 24 hours a day for all 7 days a week.
- The text in the Uninstall Agent dialog box is now updated to communicate what actually happens during agent uninstall.
- Previously Cloud Agent was occasionally displaying the old search interface in place of the new search interface. This is now fixed, Cloud Agent will consistently display the new search interface.
- Previously the Configuration Profile Creation wizard was allowing the user to enter invalid values for fields in the Performance panel. This is fixed, and now the user cannot enter invalid values.
- In order to prevent complete stoppage of agent - platform communication, users are not allowed to set the blackout window for 24 hours a day for all 7 days a week through API.
- Previously the user could enter values that were less than the lower limit for Performance Level fields under Cloud Agent Configurations. This is fixed, and now the user cannot enter invalid values.

- Agent status reporting has now been improved. Henceforth the status "STATUS_REPORTED" is no longer visible for Agents that sync with the Qualys platform. The user will now see the appropriate status for each activity.

SAQ Security Assessment Questionnaire

- Appropriate link for remove delegation is now shown in the email.
- On submitting the questionnaire, incomplete questions are highlighted in red.
- A section in a questionnaire can no more be delegated once the campaign is in complete status.
- While deleting users from the Users tab, the number of users per page is now displayed as specified.
- Reviewer and approver names are now displayed accurately in the 3-stage and 4-stage type of workflows for a campaign.
- Published templates can no more be edited.
- A section once delegated to a user can no more be delegated to another user. The delegate section link is now hidden from the delegated user.

WAF Web Application Firewall

- Web Application Firewall now displays a warning when associating an SSL certificate profile to a non-SSL Web application.
- The Description field was missing from the Security Policy Creation wizard. This is fixed, and now you can add a description while creating a security policy.
- The Web Application Firewall KnowledgeBase now displays data for the Web Application Category by default.

WAS Web Application Scanning

- We have improved the text for error messages displayed when the Report or download link has expired.
- We have now fixed an issue so that report data URL that includes special characters such as "%isin" now function correctly.
- User will now see the message which explains the use of Cancel After and Cancel At options on WebApp Create, Scan Create and Schedule Create windows.
- Now DNS override field will not be disabled by default. If the proxy is set then DNS override dropdown will be disabled.
- We have fixed an issue so that the number of vulnerabilities under findings by severity graph is in sync with the number in tabular statistics in WAS report.
- We have now fixed an issue so that the WAS scan report now displays vulnerabilities detected in that particular instance of the scan every time you view the report. To see the latest vulnerabilities you must generate a new scan report.
- An accurate scanner is now selected while relaunching a WAS scan.
- We now ensure that every scan name and schedule name is unique.