Qualys 8.10 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

Qualys Vulnerability Management (VM)

Qualys Policy Compliance (PC/SCAP)

Qualys 8.10 brings you many more
Improvements and updates! Learn more

Qualys Cloud Platform

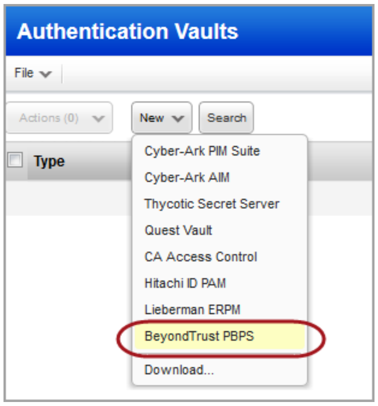
New Authentication Vault for BeyondTrust PBPS

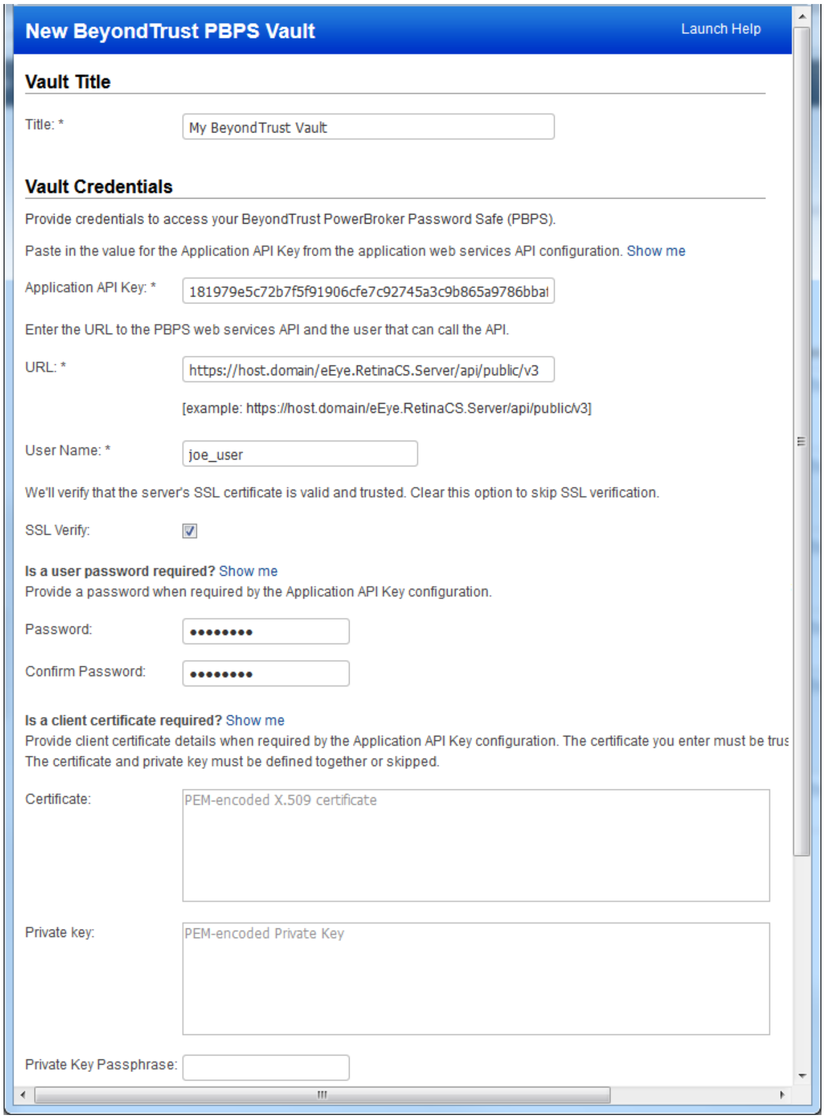
This new vault type can be used to retrieve authentication credentials from a BeyondTrust PowerBroker Password Safe (PBPS).

What are the steps? You’ll configure BeyondTrust PBPS vaults (vault credentials), configure authentication records for your authentication types (Windows, Unix, etc), and start your scans.

Configure your BeyondTrust PBPS Vault

Go to Scans > Authentication > New > Authentication Vaults. Then choose New > BeyondTrust PBPS.





New BeyondTrust PBPS Vault Launch Help

Vault Title

Title: * My BeyondTrust Vault

Vault Credentials

Provide credentials to access your BeyondTrust PowerBroker Password Safe (PBPS).

Paste in the value for the Application API Key from the application web services API configuration. Show me

Application API Key: * 181979e5c72b7f5f91906cfe7c92745a3c9b865a9786bba

Enter the URL to the PBPS web services API and the user that can call the API.

URL: * https://host.domain/eEye.RetinaCS.Server/api/public/v3

[example: https://host.domain/eEye.RetinaCS.Server/api/public/v3]

User Name: * joe_user

We'll verify that the server's SSL certificate is valid and trusted. Clear this option to skip SSL verification.

SSL Verify: ☑

Is a user password required? Show me
Provide a password when required by the Application API Key configuration.

Password: ••••••••

Confirm Password: ••••••••

Is a client certificate required? Show me
Provide client certificate details when required by the Application API Key configuration. The certificate you enter must be trus
The certificate and private key must be defined together or skipped.

Certificate: PEM-encoded X.509 certificate

Private key: PEM-encoded Private Key

Private Key Passphrase:

Provide vault credentials.

Application API Key - The application key (alpha-numeric string) for the BeyondTrust PBPS web services API.

URL - The HTTP or HTTPS URL to access the BeyondTrust PBPS web services API.

User Name - The user account that can call the BeyondTrust PBPS web services API.

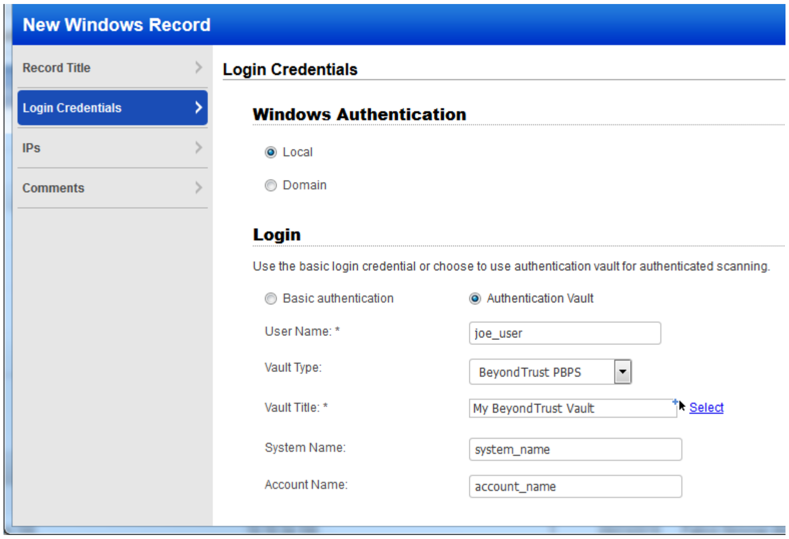
SSL Verify - Applies when the URL uses HTTPS. We’ll verify the SSL certificate of the web server to make sure it’s valid and trusted, unless you clear (un-check) this option.

Password - Provide a password when required by the Application API Key configuration.

Certificate / Private Key - Provide a certificate & private key when required by the Application API Key configuration. The certificate must be trusted by the PBPS web server. Enter a passphrase for the private key, if applicable.

Configure authentication records

The BeyondTrust PBPS vault is supported in all authentication record types except Cisco, IBM DB2, Sybase and PostgreSQL. Here's a sample Windows record with the vault selected.



Login Credentials

Windows Authentication

● Local

○ Domain

Login

Use the basic login credential or choose to use authentication vault for authenticated scanning.

○ Basic authentication ● Authentication Vault

User Name: * joe_user

Vault Type: BeyondTrust PBPS

Vault Title: * My BeyondTrust Vault Select

System Name: system_name

Account Name: account_name

Provide these settings:

Vault Type – BeyondTrust PBPS

Vault Title – Your vault record.

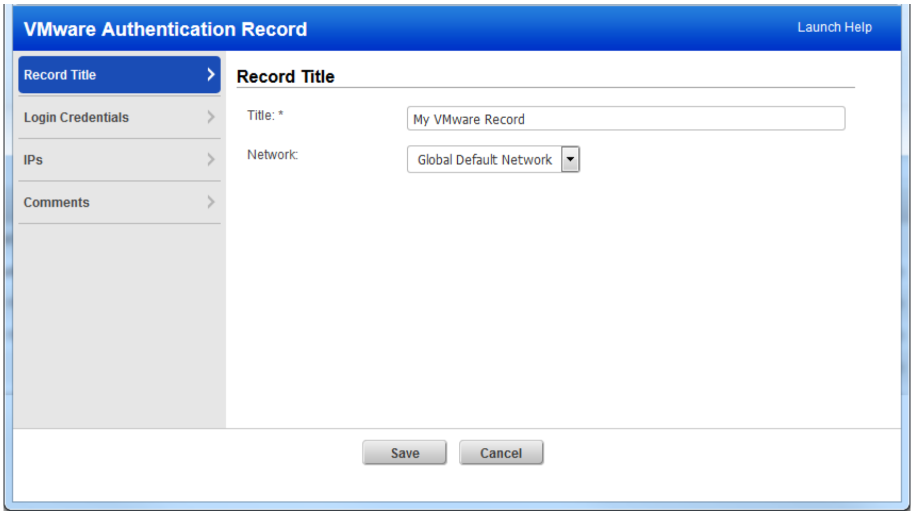
System Name – Enter the managed system name (also known as asset name). When not provided, we'll attempt to auto-discover the system name for you at scan time.

Account Name – The account name. When not provided, we'll try the username entered in the authentication record.

Authentication Records Improved

We improved some of our authentication record types: VMware, MySQL, Sybase, HTTP and Application Records (MS IIS, Apache Web Server, IBM WebSphere App Server, Tomcat Server, Oracle WebLogic Server) to retain consistency with other records. These records now open in a new window.

Example: Create a VMware authentication record



Record Title

Title: * My VMware Record

Network: Global Default Network

How do I get started?

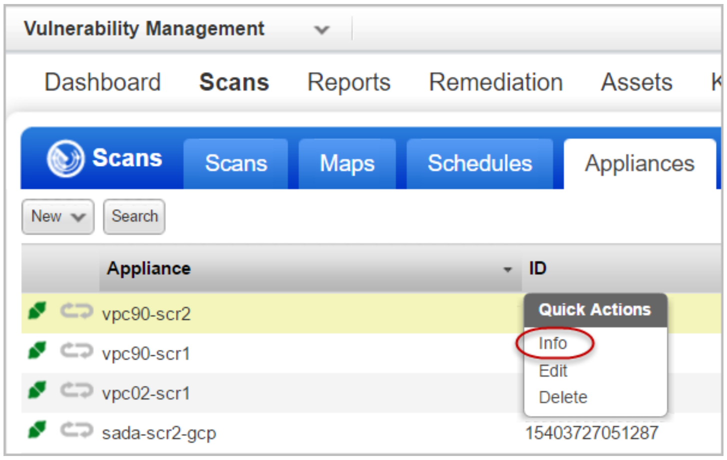
Go to Scans > Authentication and choose New and select the required authentication record. The listed authentication records now open in a new window.

Your Authentication Record

Give a title to the record, provide the login credentials and the required details for the authentication record. Finally, hit Save!

View Cloud Instance Information for a Scanner Appliance

Now you can view information about the instance on which a scanner appliance is deployed on the cloud.

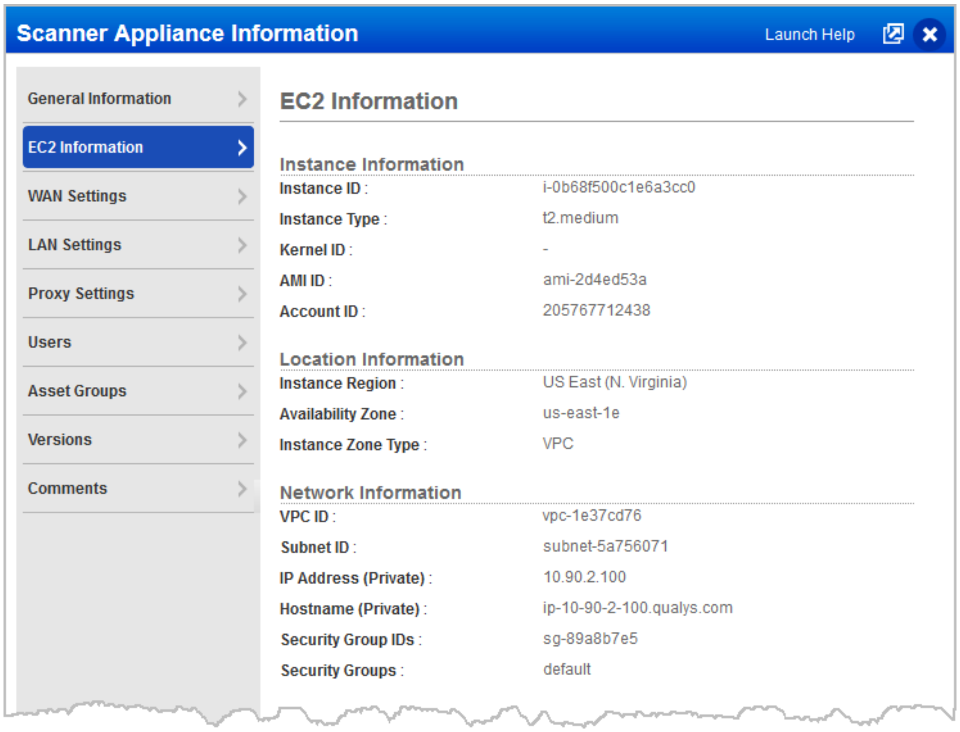


Appliance	ID
vpc90-scr2	
vpc90-scr1	
vpc02-scr1	
sada-scr2-gcp	15403727051287

How to view the instance information

Go to Scans > Appliances, and then click Info on the Quick Actions menu of the required appliance.

Example of EC2 instance information displayed for an appliance.



EC2 Information

Instance Information

Instance ID :	i-0b68f500c1e6a3cc0
Instance Type :	t2.medium
Kernel ID :	-
AMI ID :	ami-2d4ed53a
Account ID :	205767712438

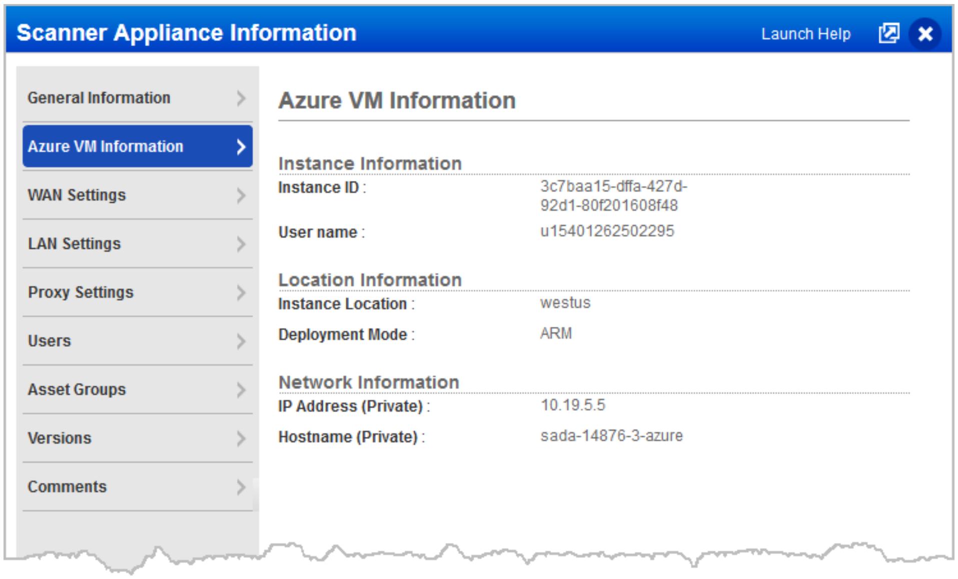
Location Information

Instance Region :	US East (N. Virginia)
Availability Zone :	us-east-1e
Instance Zone Type :	VPC

Network Information

VPC ID :	vpc-1e37cd76
Subnet ID :	subnet-5a756071
IP Address (Private) :	10.90.2.100
Hostname (Private) :	ip-10-90-2-100.qualys.com
Security Group IDs :	sg-89a8b7e5
Security Groups :	default

Example of Azure instance information displayed for an appliance.



Azure VM Information

Instance Information

Instance ID :	3c7baa15-dffa-427d-92d1-80f201608f48
User name :	u15401262502295

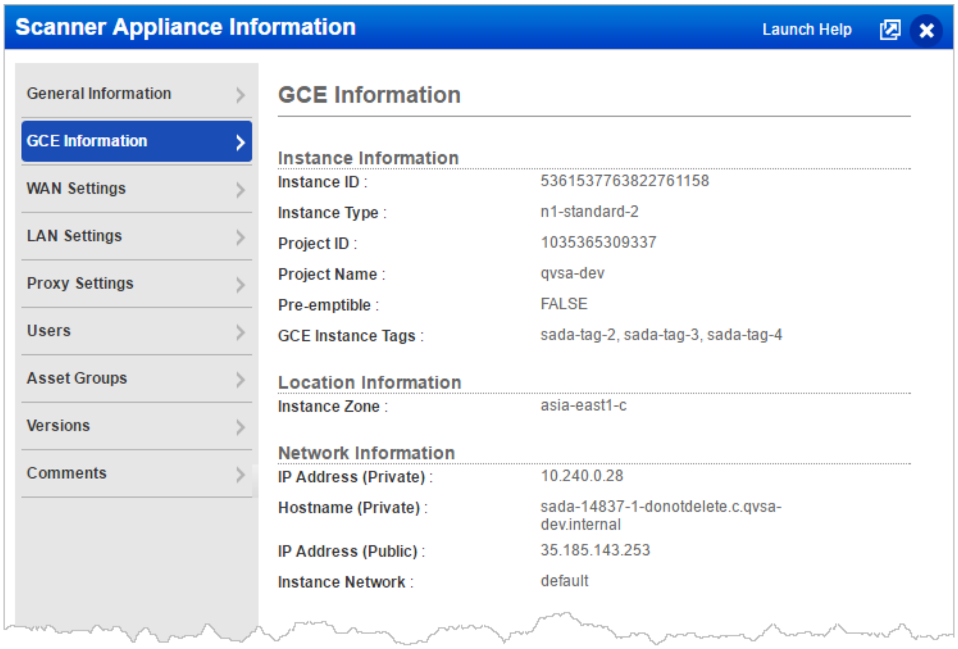
Location Information

Instance Location :	westus
Deployment Mode :	ARM

Network Information

IP Address (Private) :	10.19.5.5
Hostname (Private) :	sada-14876-3-azure

Example of Google GCE instance information displayed for an appliance.



GCE Information

Instance Information

Instance ID :	5361537763822761158
Instance Type :	n1-standard-2
Project ID :	1035365309337
Project Name :	qvsa-dev
Pre-emptible :	FALSE
GCE Instance Tags :	sada-tag-2, sada-tag-3, sada-tag-4

Location Information

Instance Zone :	asia-east1-c

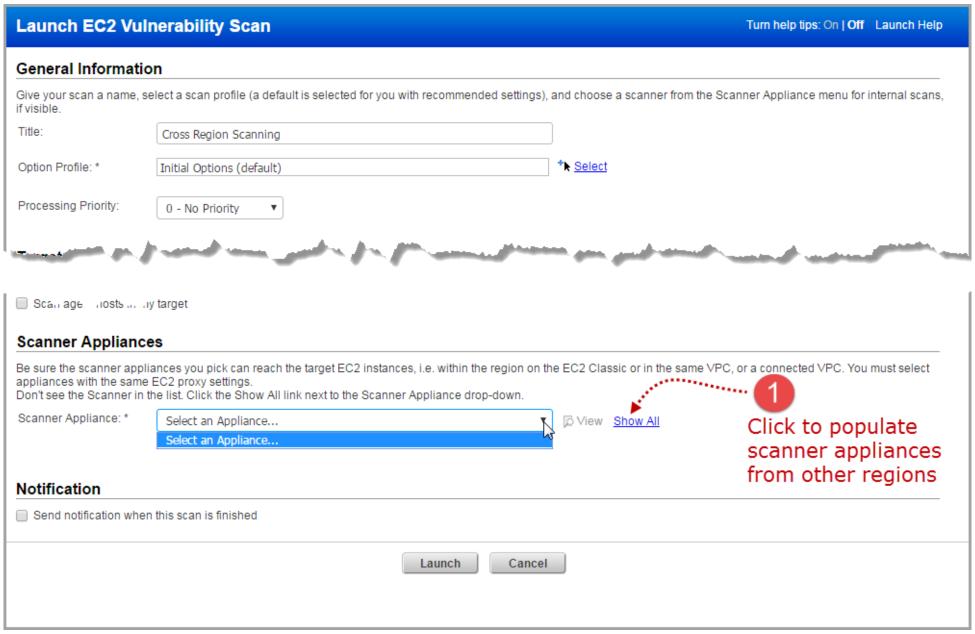
Network Information

IP Address (Private) :	10.240.0.28
Hostname (Private) :	sada-14837-1-donotdelete.c.qvsa-dev.internal
IP Address (Public) :	35.185.143.253
Instance Network :	default

Cross-Region Scanning Support for EC2 Scans

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

You can now assign a scanner appliance from a different region when scanner appliances in your region are unavailable. We now support availability of scanner appliances across regions.



Launch EC2 Vulnerability Scan

General Information

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

Title:	Cross Region Scanning
Option Profile: *	Initial Options (default) Select
Processing Priority:	0 - No Priority ▾

□ Sca.. age ..osts ... ..y target

Scanner Appliances

Be sure the scanner appliances you pick can reach the target EC2 instances, i.e. within the region on the EC2 Classic or in the same VPC, or a connected VPC. You must select appliances with the same EC2 proxy settings.
Don't see the Scanner in the list. Click the Show All link next to the Scanner Appliance drop-down.

Scanner Appliance: * Select an Appliance... ▾ View Show All

1 Click to populate scanner appliances from other regions

Notification

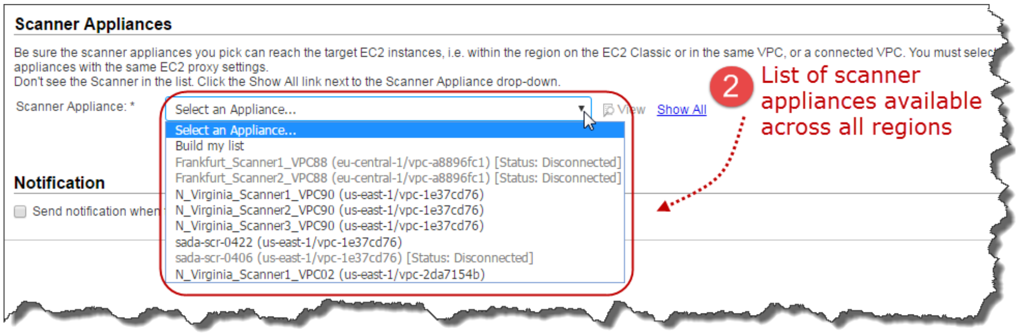
□ Send notification when this scan is finished

Go to Scans > Scans > New and then launch EC2 Scan.

The Scanner Appliance dropdown lists the scanner appliances that are available only in your region.

Click the Show All link to also see scanner appliances in other regions.

The Scanner Appliance dropdown will list all the scanner appliances that are available across all regions.



Scanner Appliances

Be sure the scanner appliances you pick can reach the target EC2 instances, i.e. within the region on the EC2 Classic or in the same VPC, or a connected VPC. You must selec
appliances with the same EC2 proxy settings.
Don't see the Scanner in the list. Click the Show All link next to the Scanner Appliance drop-down.

Scanner Appliance: * Select an Appliance... ▾ View Show All

- Select an Appliance...
- Build my list
- Frankfurt_Scanner1_VPC88 (eu-central-1/vpc-a8896fc1) [Status: Disconnected]
- Frankfurt_Scanner2_VPC88 (eu-central-1/vpc-a8896fc1) [Status: Disconnected]
- N_Virginia_Scanner1_VPC90 (us-east-1/vpc-1e37cd76)
- N_Virginia_Scanner2_VPC90 (us-east-1/vpc-1e37cd76)
- N_Virginia_Scanner3_VPC90 (us-east-1/vpc-1e37cd76)
- sada-scr-0422 (us-east-1/vpc-1e37cd76)
- sada-scr-0406 (us-east-1/vpc-1e37cd76) [Status: Disconnected]
- N_Virginia_Scanner1_VPC02 (us-east-1/vpc-2da7154b)

2 List of scanner appliances available across all regions

Notification

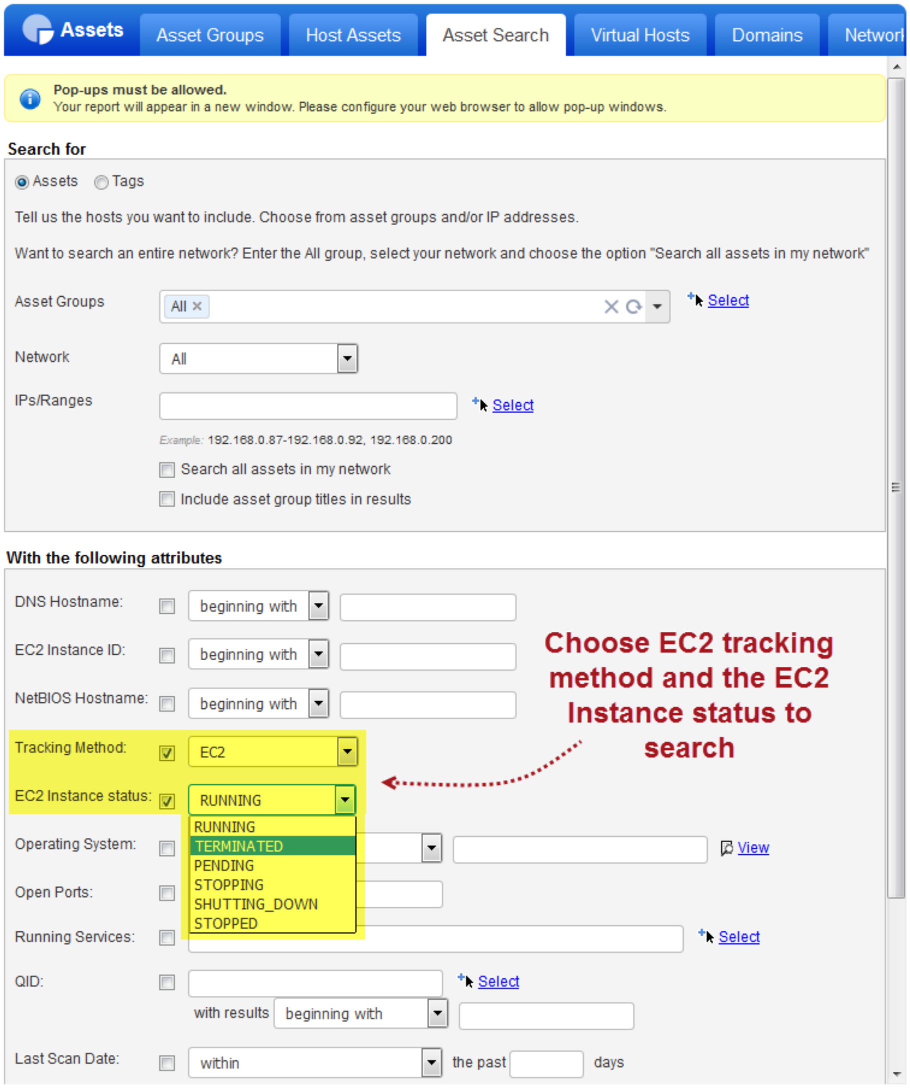
□ Send notification when

Find EC2 Assets by Instance Status and Take Action

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

With this release, you can easily find all of your Amazon EC2 assets with a particular status (running, terminated, stopped, etc) and take action on them. For example, find EC2 instances that are terminated in order to purge or remove them from your account. *Warning – When you purge a host the action cannot be undone. All vulnerability and compliance data collected from your scans will be deleted. See the online help to learn more about purging hosts.*

Go to Assets > Asset Search and choose the EC2 Instance status you're interested in. You must also pick the EC2 tracking method. Then click Search to see the results. (Tip – You can go to Reports > New > Asset Search Report to generate a report that you can easily share with others.)



Pop-ups must be allowed.
Your report will appear in a new window. Please configure your web browser to allow pop-up windows.

Search for

● Assets ○ Tags

Tell us the hosts you want to include. Choose from asset groups and/or IP addresses.

Want to search an entire network? Enter the All group, select your network and choose the option "Search all assets in my network"

Asset Groups: All × — Select

Network: All

IPs/Ranges: — Select

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

□ Search all assets in my network

□ Include asset group titles in results

With the following attributes

DNS Hostname: □ beginning with

EC2 Instance ID: □ beginning with

NetBIOS Hostname: □ beginning with

Tracking Method: ☑ EC2

EC2 Instance status: ☑ RUNNING

RUNNING
TERMINATED
PENDING
STOPPING
SHUTTING_DOWN
STOPPED

Operating System: □ — View

Open Ports: □

Running Services: □ — Select

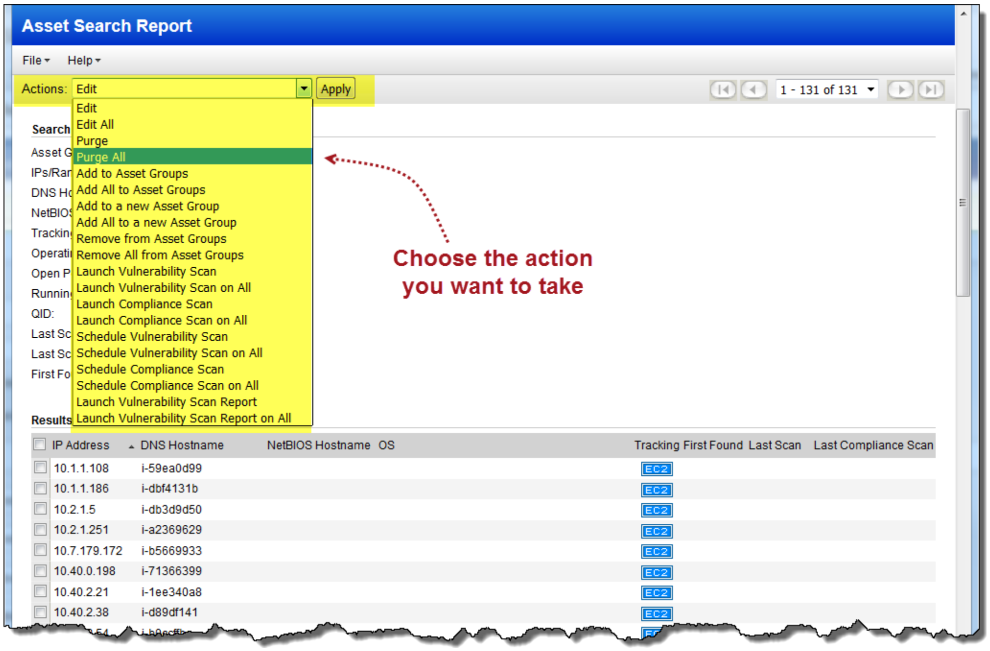
QID: □ — Select
with results beginning with

Last Scan Date: □ within the past days

Choose EC2 tracking method and the EC2 Instance status to search

Don't see this option? The EC2 Scanning feature must be enabled for your subscription.

Your Asset Search Report appears in a new window where you can take action on all or some of the EC2 assets that matched your search criteria. Choose an action from the menu at the top of the report.



Choose the action you want to take

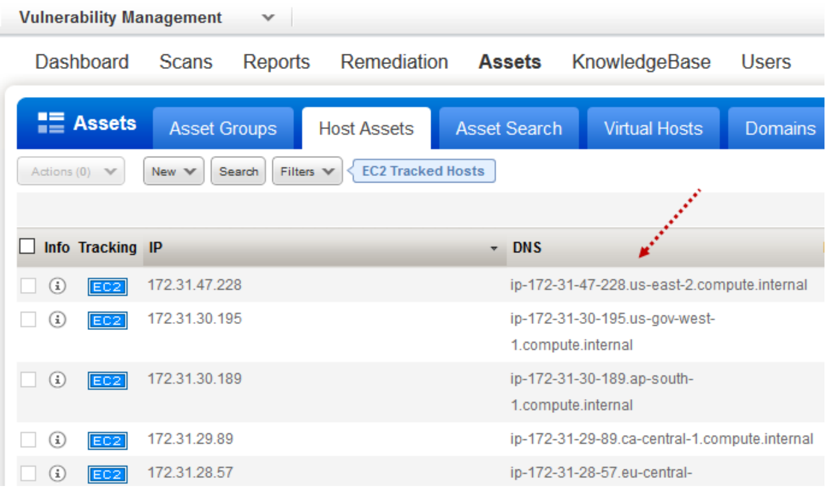
□	IP Address	DNS Hostname	NetBIOS Hostname	OS	Tracking	First Found	Last Scan	Last Compliance Scan
□	10.1.1.108	i-59ea0d99			EC2			
□	10.1.1.186	i-dbf4131b			EC2			
□	10.2.1.5	i-db3d9d50			EC2			
□	10.2.1.251	i-a2369629			EC2			
□	10.7.179.172	i-b5669933			EC2			
□	10.40.0.198	i-71366399			EC2			
□	10.40.2.21	i-1ee340a8			EC2			
□	10.40.2.38	i-d89df141			EC2			

Improved Reporting on EC2 Assets

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

We’ve improved reporting on EC2 assets, using the Qualys UI and API, to help you manage your EC2 assets within Qualys. For EC2 assets now we report EC2 Instance ID, private DNS name plus EC2 instance information. We’ll show you the UI improvements here.

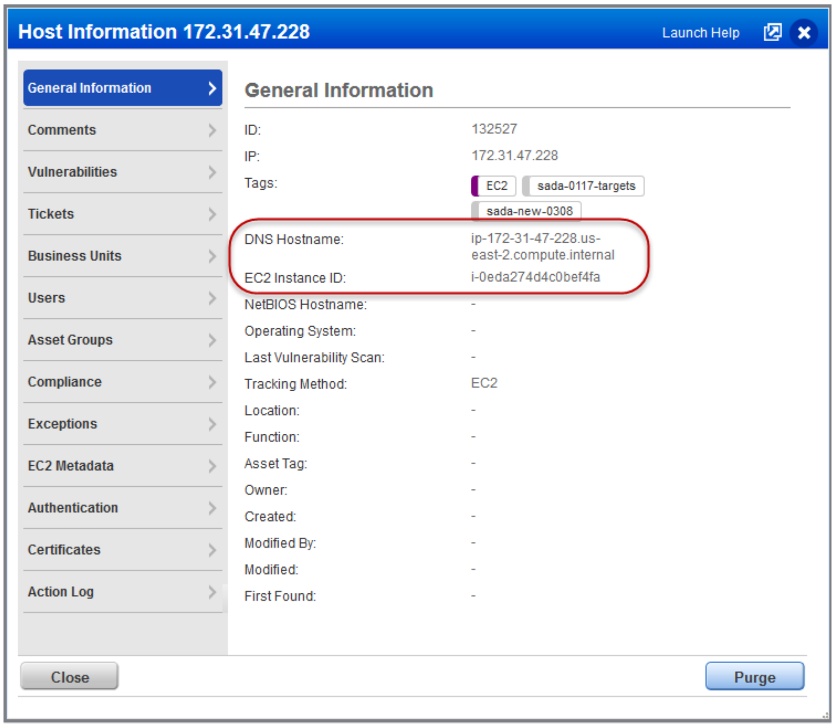
Using the Qualys API? Be sure to check out *Qualys 8.10 API Release Notes* to learn about EC2 reporting enhancements.



□	Info	Tracking	IP	DNS
□	ⓘ	EC2	172.31.47.228	ip-172-31-47-228.us-east-2.compute.internal
□	ⓘ	EC2	172.31.30.195	ip-172-31-30-195.us-gov-west-1.compute.internal
□	ⓘ	EC2	172.31.30.189	ip-172-31-30-189.ap-south-1.compute.internal
□	ⓘ	EC2	172.31.29.89	ip-172-31-29-89.ca-central-1.compute.internal
□	ⓘ	EC2	172.31.28.57	ip-172-31-28-57.eu-central-

Host Assets list

For EC2 assets the DNS column now shows the EC2 asset’s private DNS name.

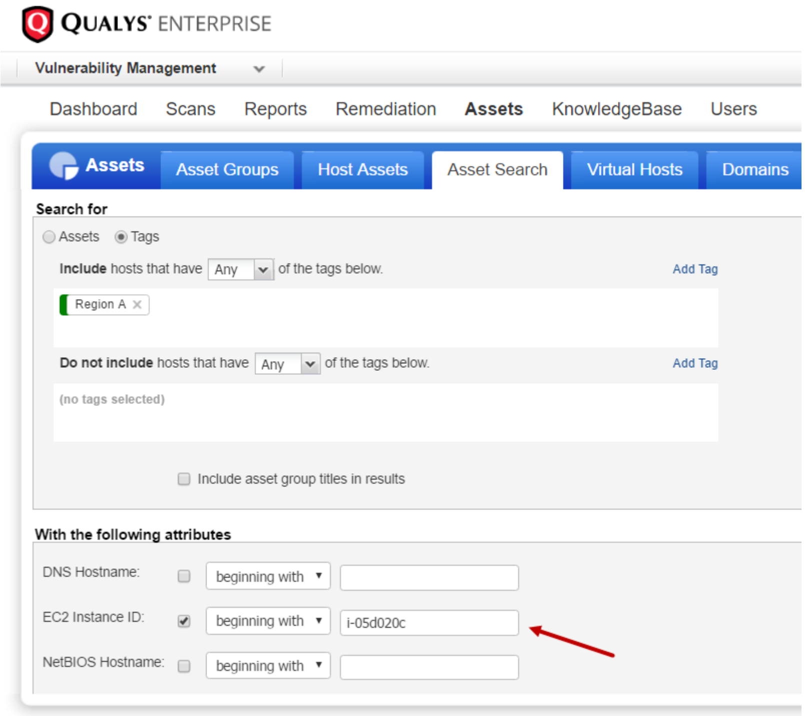


General Information

ID: 132527
IP: 172.31.47.228
Tags: EC2 sada-0117-targets sada-new-0308
DNS Hostname: ip-172-31-47-228.us-east-2.compute.internal
EC2 Instance ID: i-0eda274d4c0bef4fa
NetBIOS Hostname: -
Operating System: -
Last Vulnerability Scan: -
Tracking Method: EC2
Location: -
Function: -
Asset Tag: -
Owner: -
Created: -
Modified By: -
Modified: -
First Found: -

Host Information

Now the private DNS name is shown for Hostname and EC2 Instance ID is shown separately.



Search for
○ Assets ● Tags
Include hosts that have Any of the tags below.
Region A ×
Do not include hosts that have Any of the tags below.
(no tags selected)
□ Include asset group titles in results

With the following attributes
DNS Hostname: □ beginning with
EC2 Instance ID: ☑ beginning with i-05d020c
NetBIOS Hostname: □ beginning with

Asset Search

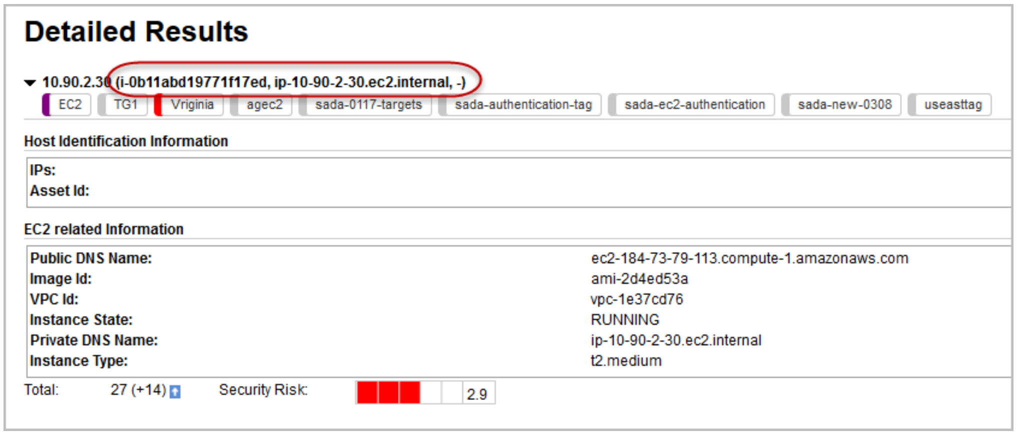
Now you can easily search your EC2 assets.

We've added a new option to search by EC2 Instance ID, and the DNS Hostname attribute lets you search across private EC2 names.

For EC2 assets the Asset Search report now shows EC2 Instance ID and the private DNS name.

We've added new EC2 information in the Scan Report

HTML, PDF, DOCx format - Now we include the private DNS name along with EC2 Instance ID at the host level. There's a new EC2 related information section i.e. Public DNS name, Image ID etc.



Detailed Results

▼ 10.90.2.30 (i-0b11abd19771f17ed, ip-10-90-2-30.ec2.internal, -)

EC2 | TG1 | Vriginia | agec2 | sada-0117-targets | sada-authentication-tag | sada-ec2-authentication | sada-new-0308 | useasttag

Host Identification Information

IPs:
Asset Id:

EC2 related Information

Public DNS Name:	ec2-184-73-79-113.compute-1.amazonaws.com
Image Id:	ami-2d4ed53a
VPC Id:	vpc-1e37cd76
Instance State:	RUNNING
Private DNS Name:	ip-10-90-2-30.ec2.internal
Instance Type:	t2.medium

Total: 27 (+14) Security Risk: 2.9

XML format - For an EC2 asset now we return the <EC2_INSTANCE_ID> tag as well as the <EC2_INFO> tag, and the <DNS> tag shows the private DNS name. The asset_data_report.dtd has been updated (see *Qualys 8.10 API Release Notes* for details).

```
...
   </ASSET_TAGS>
   <DNS><![CDATA[ip-10-90-2-30.ec2.internal]]></DNS>
   <EC2_INSTANCE_ID><![CDATA[i-0b11abd19771f17ed]]></EC2_INSTANCE_ID>
   <EC2_INFO>
       <PUBLIC_DNS_NAME><![CDATA[ec2-184-73-79-113.compute-
     1.amazonaws.com]]></PUBLIC_DNS_NAME>
       <IMAGE_ID><![CDATA[ami-2d4ed53a]]></IMAGE_ID>
       <VPC_ID><![CDATA[vpc-1e37cd76]]></VPC_ID>
       <INSTANCE_STATE><![CDATA[RUNNING]]></INSTANCE_STATE>
       <PRIVATE_DNS_NAME><![CDATA[ip-10-90-2-
     30.ec2.internal]]></PRIVATE_DNS_NAME>
      <INSTANCE_TYPE><![CDATA[t2.medium]]></INSTANCE_TYPE>
   </EC2_INFO>
...
```

CSV format - A new column for EC2 Instance ID has been added right after DNS name. For an EC2 asset the DNS column shows a private DNS name.

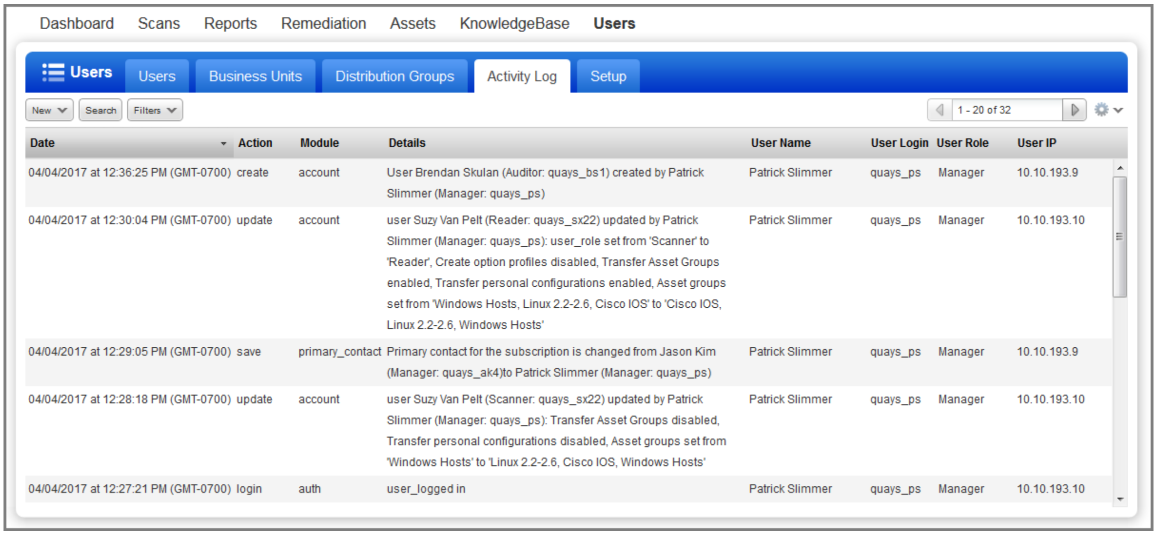
```
"IP","DNS","EC2 INSTANCE
ID","NetBIOS","QG_HOSTID","IP_INTERFACES","PUBLIC_DNS_NAME","IMAGE_ID","V
PC_ID”,”INSTANCE_STATE”,”PRIVATE_DNS”,”INSTANCE_TYPE","Tracking
Method","OS","IP Status","QID","Title","Vuln
Status","Type","Severity","Port","Protocol","FQDN","SSL","First
Detected","Last Detected","Times Detected","CVE ID","Vendor
Reference","Bugtraq ID","Results","PCI Vuln","Ticket
State","Instance","Category","Associated Tags","Date Last Fixed"
"10.90.2.100","ip-10-90-2-100.ec2.internal","i-0b68f500c1e6a3cc0",,,,"ec2-52-
87-152-105.compute-1.amazonaws.com","ami-2d4ed53a","vpc-
1e37cd76”,”RUNNING”,ip-10-90-2-100.ec2.internal”,”t2.medium","EC2","Linux
2.4-2.6 / Embedded Device / F5 Networks Big-IP","host scanned, found
vuln","38047","SSH daemon information
retrieving",,"Ig","1","22","tcp",,,,,,"CVE-1999-0634",,,"SSH1 supportedno
```

More User Details in the Activity Log

The Details section of the Activity Log will now include the user role and user login for new and updated user accounts. You'll also see these details when the primary contact for the subscription or business unit has changed.

User details appear in this format:
`firstname lastname (user role: user login)`

This example shows details for: create account, update account and save primary contact.



Date	Action	Module	Details	User Name	User Login	User Role	User IP
04/04/2017 at 12:36:25 PM (GMT-0700)	create	account	User Brendan Skulan (Auditor: quays_bs1) created by Patrick Slimmer (Manager: quays_ps)	Patrick Slimmer	quays_ps	Manager	10.10.193.9
04/04/2017 at 12:30:04 PM (GMT-0700)	update	account	user Suzy Van Pelt (Reader: quays_sx22) updated by Patrick Slimmer (Manager: quays_ps): user_role set from 'Scanner' to 'Reader', Create option profiles disabled, Transfer Asset Groups enabled, Transfer personal configurations enabled, Asset groups set from 'Windows Hosts, Linux 2.2-2.6, Cisco IOS' to 'Cisco IOS, Linux 2.2-2.6, Windows Hosts'	Patrick Slimmer	quays_ps	Manager	10.10.193.10
04/04/2017 at 12:29:05 PM (GMT-0700)	save	primary_contact	Primary contact for the subscription is changed from Jason Kim (Manager: quays_ak4)to Patrick Slimmer (Manager: quays_ps)	Patrick Slimmer	quays_ps	Manager	10.10.193.9
04/04/2017 at 12:28:18 PM (GMT-0700)	update	account	user Suzy Van Pelt (Scanner: quays_sx22) updated by Patrick Slimmer (Manager: quays_ps): Transfer Asset Groups disabled, Transfer personal configurations disabled, Asset groups set from 'Windows Hosts' to 'Linux 2.2-2.6, Cisco IOS, Windows Hosts'	Patrick Slimmer	quays_ps	Manager	10.10.193.10
04/04/2017 at 12:27:21 PM (GMT-0700)	login	auth	user_logged in	Patrick Slimmer	quays_ps	Manager	10.10.193.10

Qualys Vulnerability Management (VM)

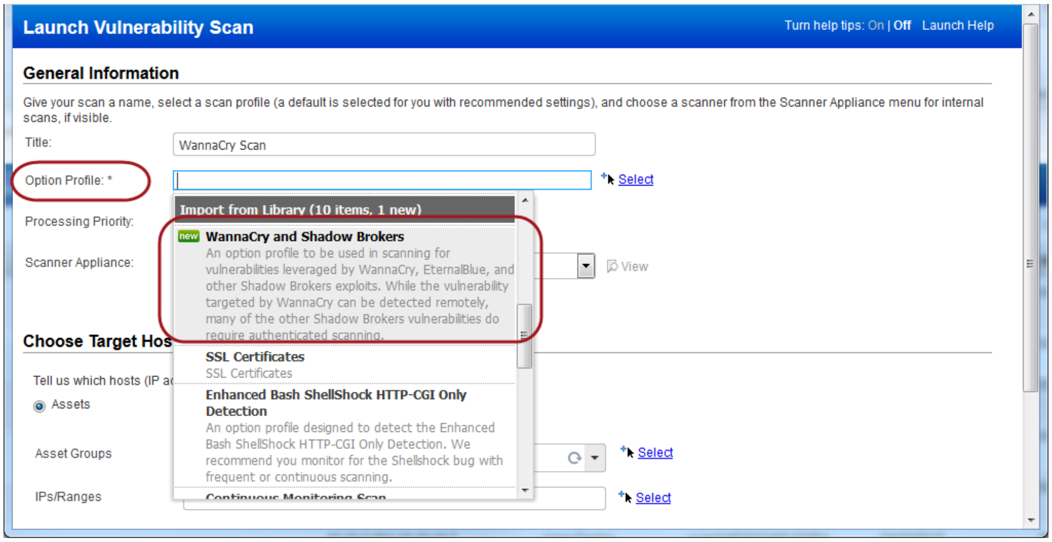
New Library Items to Detect WannaCry and Other Vulnerabilities

Import the new WannaCry and Shadow Brokers Option Profile and WannaCry and Shadow Brokers Search List from our Library to quickly identify vulnerabilities leveraged by WannaCry, EternalBlue, and other Shadow Brokers exploits.

Learn more from the Qualys Blog
How to Rapidly Identify Assets at Risk to WannaCry Ransomware and ETERNALBLUE Exploit

Import Option Profiles from our Library

Import the new WannaCry and Shadow Brokers option profile at scan launch time by simply choosing it from the Option Profile menu. The corresponding search list is imported with the option profile and you'll be given the option to make them globally available to all users in your subscription.



Launch Vulnerability Scan

Turn help tips: On | Off   Launch Help

General Information

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

Title: WannaCry Scan

Option Profile: *

Import from Library (10 items, 1 new)

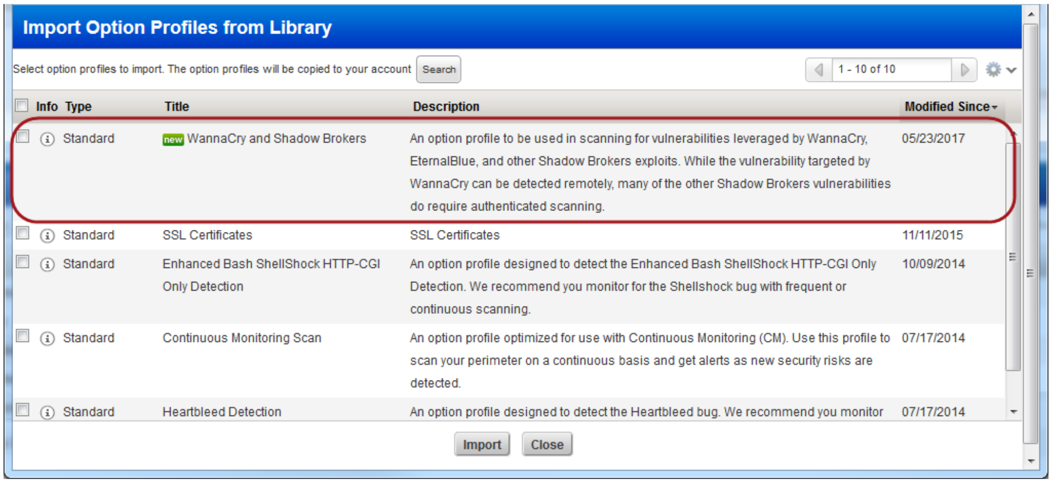
new **WannaCry and Shadow Brokers**
An option profile to be used in scanning for vulnerabilities leveraged by WannaCry, EternalBlue, and other Shadow Brokers exploits. While the vulnerability targeted by WannaCry can be detected remotely, many of the other Shadow Brokers vulnerabilities do require authenticated scanning.

SSL Certificates
SSL Certificates

Enhanced Bash ShellShock HTTP-CGI Only Detection
An option profile designed to detect the Enhanced Bash ShellShock HTTP-CGI Only Detection. We recommend you monitor for the Shellshock bug with frequent or continuous scanning.

Continuous Monitoring Scan

Optionally, go to Scans > Option Profiles > New > Import from Library.



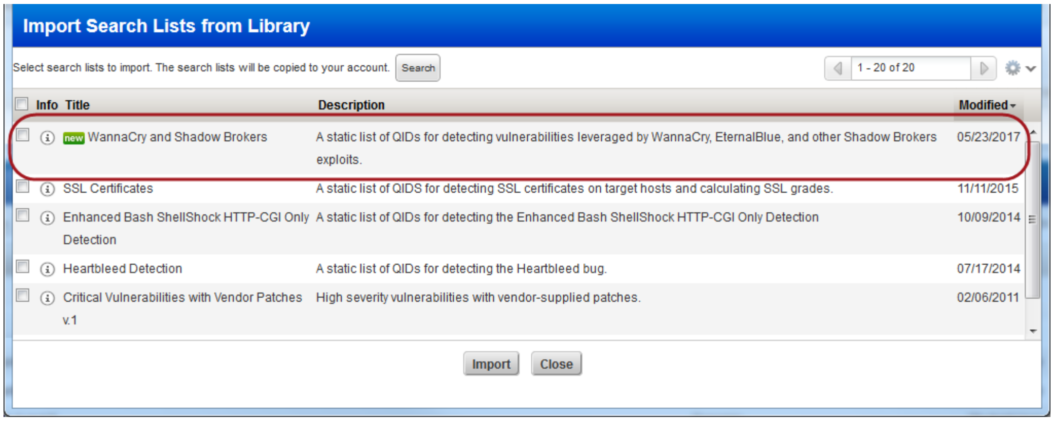
Import Option Profiles from Library

Select option profiles to import. The option profiles will be copied to your account

Info	Type	Title	Description	Modified Since
□ ⓘ	Standard	new WannaCry and Shadow Brokers	An option profile to be used in scanning for vulnerabilities leveraged by WannaCry, EternalBlue, and other Shadow Brokers exploits. While the vulnerability targeted by WannaCry can be detected remotely, many of the other Shadow Brokers vulnerabilities do require authenticated scanning.	05/23/2017
□ ⓘ	Standard	SSL Certificates	SSL Certificates	11/11/2015
□ ⓘ	Standard	Enhanced Bash ShellShock HTTP-CGI Only Detection	An option profile designed to detect the Enhanced Bash ShellShock HTTP-CGI Only Detection. We recommend you monitor for the Shellshock bug with frequent or continuous scanning.	10/09/2014
□ ⓘ	Standard	Continuous Monitoring Scan	An option profile optimized for use with Continuous Monitoring (CM). Use this profile to scan your perimeter on a continuous basis and get alerts as new security risks are detected.	07/17/2014
□ ⓘ	Standard	Heartbleed Detection	An option profile designed to detect the Heartbleed bug. We recommend you monitor	07/17/2014

Import Search Lists from our Library

Import the WannaCry and Shadow Brokers search list for use in your own custom option profiles or in report templates. Go to Scans > Search Lists > New > Import from Library.



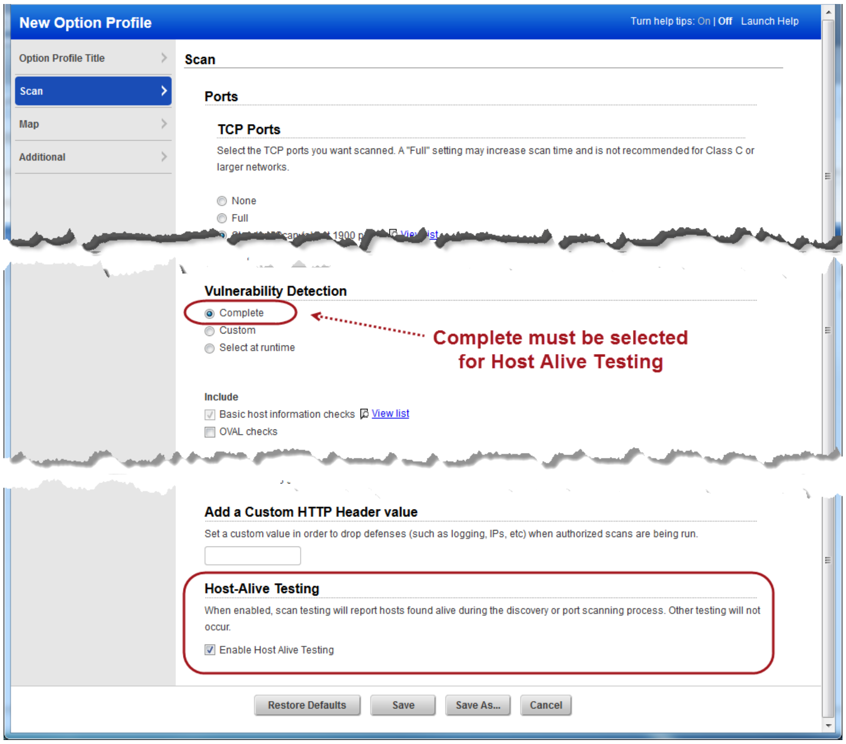
Select search lists to import. The search lists will be copied to your account.

□	Info	Title	Description	Modified
□	ⓘ	new WannaCry and Shadow Brokers	A static list of QIDs for detecting vulnerabilities leveraged by WannaCry, EternalBlue, and other Shadow Brokers exploits.	05/23/2017
□	ⓘ	SSL Certificates	A static list of QIDS for detecting SSL certificates on target hosts and calculating SSL grades.	11/11/2015
□	ⓘ	Enhanced Bash ShellShock HTTP-CGI Only Detection	A static list of QIDs for detecting the Enhanced Bash ShellShock HTTP-CGI Only Detection	10/09/2014
□	ⓘ	Heartbleed Detection	A static list of QIDs for detecting the Heartbleed bug.	07/17/2014
□	ⓘ	Critical Vulnerabilities with Vendor Patches v.1	High severity vulnerabilities with vendor-supplied patches.	02/06/2011

Host Alive Testing Option

A new scan option allows you to launch a quick scan to determine which of your target hosts are alive without also performing other scan tests. To run a host alive test, choose Enable Host Alive Testing in your scan option profile and run a vulnerability scan with this profile.

Ready to get started? In your option profile, scroll to the bottom of the Scan tab to select the new option Enable Host Alive Testing.



Scan

Ports

TCP Ports

Select the TCP ports you want scanned. A "Full" setting may increase scan time and is not recommended for Class C or larger networks.

○ None
○ Full

Vulnerability Detection

● Complete
○ Custom
○ Select at runtime

Complete must be selected for Host Alive Testing

Include

☑ Basic host information checks View list
☐ OVAL checks

Add a Custom HTTP Header value

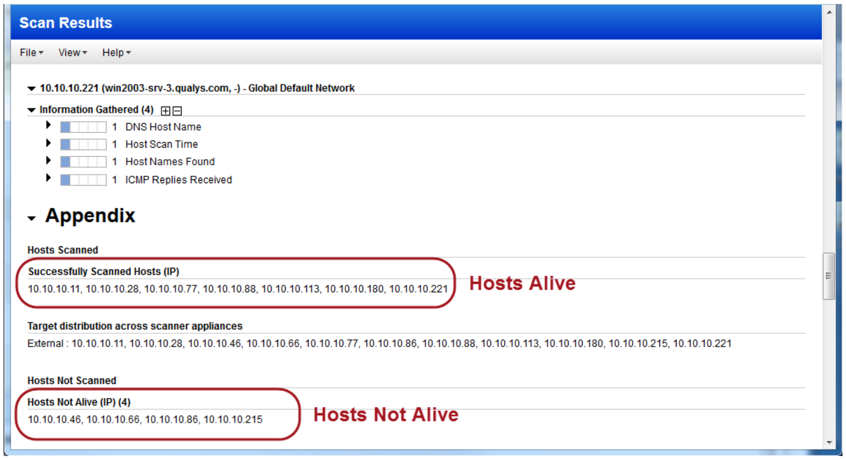
Set a custom value in order to drop defenses (such as logging, IPs, etc) when authorized scans are being run.

Host-Alive Testing

When enabled, scan testing will report hosts found alive during the discovery or port scanning process. Other testing will not occur.

☑ Enable Host Alive Testing

Note – This option can only be selected in a profile with Complete Vulnerability Detection.



10.10.10.221 (win2003-srv-3.qualys.com, -) - Global Default Network

Information Gathered (4)

- 1 DNS Host Name
- 1 Host Scan Time
- 1 Host Names Found
- 1 ICMP Replies Received

Appendix

Hosts Scanned

Successfully Scanned Hosts (IP)

10.10.10.11, 10.10.10.28, 10.10.10.77, 10.10.10.88, 10.10.10.113, 10.10.10.180, 10.10.10.221

Hosts Alive

Target distribution across scanner appliances

External : 10.10.10.11, 10.10.10.28, 10.10.10.46, 10.10.10.66, 10.10.10.77, 10.10.10.86, 10.10.10.88, 10.10.10.113, 10.10.10.180, 10.10.10.215, 10.10.10.221

Hosts Not Scanned

Hosts Not Alive (IP) (4)

10.10.10.46, 10.10.10.66, 10.10.10.86, 10.10.10.215

Hosts Not Alive

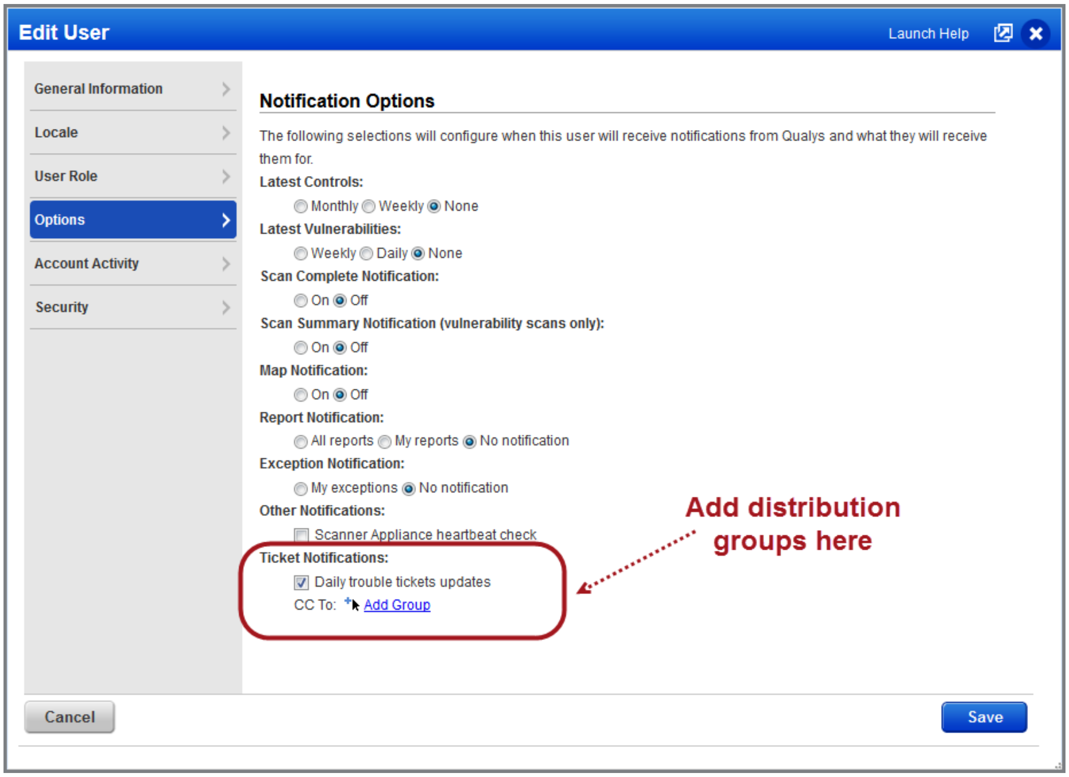
In your Scan Results report, you may see some Information Gathered QIDs reported for the target hosts found alive like in the sample report on the left.

Host that are alive are listed under Successfully Scanned Hosts in the Appendix.

Hosts that are not found alive during the scan are listed under Hosts Not Alive.

New CC Option for Ticket Notifications

Now when you enable the Daily Trouble Ticket Updates notification (in your user profile) you’ll see the option to add distribution groups. Email addresses in your selected distribution groups will be CC-ed on your Daily Trouble Ticket Updates notification emails.



Notification Options

The following selections will configure when this user will receive notifications from Qualys and what they will receive them for.

Latest Controls:
○ Monthly ○ Weekly ● None

Latest Vulnerabilities:
○ Weekly ○ Daily ● None

Scan Complete Notification:
○ On ● Off

Scan Summary Notification (vulnerability scans only):
○ On ● Off

Map Notification:
○ On ● Off

Report Notification:
○ All reports ○ My reports ● No notification

Exception Notification:
○ My exceptions ● No notification

Other Notifications:
□ Scanner Appliance heartbeat check

Ticket Notifications:
☑ Daily trouble tickets updates
CC To: Add Group

Add distribution groups here

Good to Know

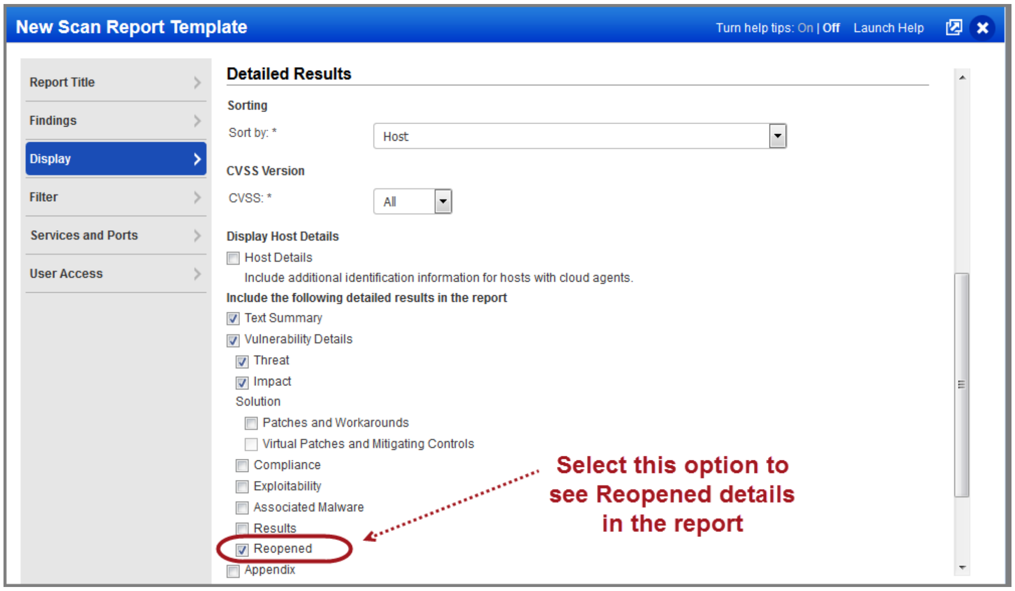
- Only the first 100 email addresses in your selected distribution groups will be sent notifications. If you select groups with more than 100 email addresses notifications will be sent only to the first 100 email addresses.

- If your selected distribution groups have BCC email addresses defined, we’ll consider BCC email addresses as CC addresses; this means BCC users will be sent Daily Trouble Ticket Updates notifications.

Show Reopened Info in Scan Reports

We've added a new report template option that allows you to include reopened information in your host based scan reports, including the date/time a vulnerability was first reopened, date/time the vulnerability was last reopened, and the number of times the vulnerability was reopened. A vulnerability is reopened when it was verified as fixed by the previous scan and is detected by a new scan.

In your scan report template, go to the Display tab and choose Reopened under Vulnerability Details.



Detailed Results

Sorting

Sort by: * Host

CVSS Version

CVSS: * All

Display Host Details

☐ Host Details

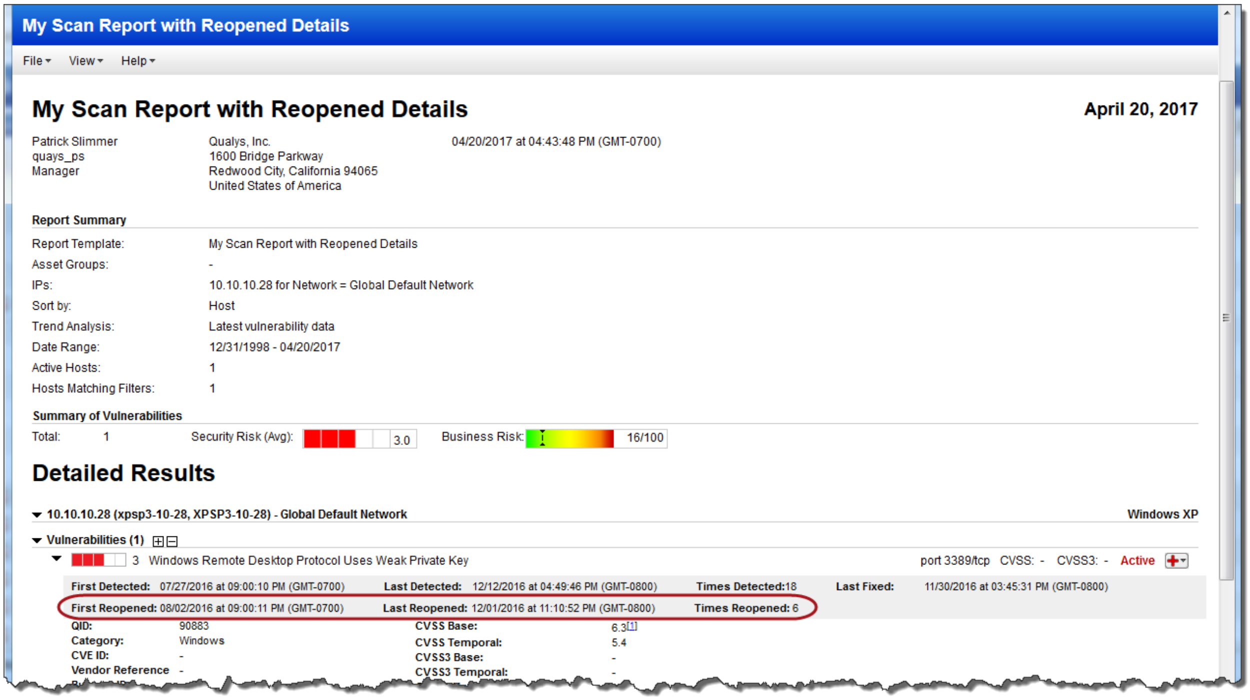
Include additional identification information for hosts with cloud agents.

Include the following detailed results in the report

☑ Text Summary
☑ Vulnerability Details
☑ Threat
☑ Impact
Solution
☐ Patches and Workarounds
☐ Virtual Patches and Mitigating Controls
☐ Compliance
☐ Exploitability
☐ Associated Malware
☐ Results
☑ Reopened
☐ Appendix

Select this option to see Reopened details in the report

In this sample HTML report you'll see that QID 90883 has been reopened 6 times. It was first reopened on August 2, 2016 and last reopened on December 1, 2016.



My Scan Report with Reopened Details April 20, 2017

Patrick Slimmer
quays_ps
Manager

Qualys, Inc.
1600 Bridge Parkway
Redwood City, California 94065
United States of America

04/20/2017 at 04:43:48 PM (GMT-0700)

Report Summary

Report Template:	My Scan Report with Reopened Details
Asset Groups:	-
IPs:	10.10.10.28 for Network = Global Default Network
Sort by:	Host
Trend Analysis:	Latest vulnerability data
Date Range:	12/31/1998 - 04/20/2017
Active Hosts:	1
Hosts Matching Filters:	1

Summary of Vulnerabilities

Total: 1 Security Risk (Avg): 3.0 Business Risk: 16/100

Detailed Results

10.10.10.28 (xpsp3-10-28, XPSP3-10-28) - Global Default Network Windows XP

Vulnerabilities (1)

3 Windows Remote Desktop Protocol Uses Weak Private Key port 3389/tcp CVSS: - CVSS3: - Active

First Detected: 07/27/2016 at 09:00:10 PM (GMT-0700) **Last Detected:** 12/12/2016 at 04:49:46 PM (GMT-0800) **Times Detected:**18 **Last Fixed:** 11/30/2016 at 03:45:31 PM (GMT-0800)

First Reopened: 08/02/2016 at 09:00:11 PM (GMT-0700) **Last Reopened:** 12/01/2016 at 11:10:52 PM (GMT-0800) **Times Reopened:** 6

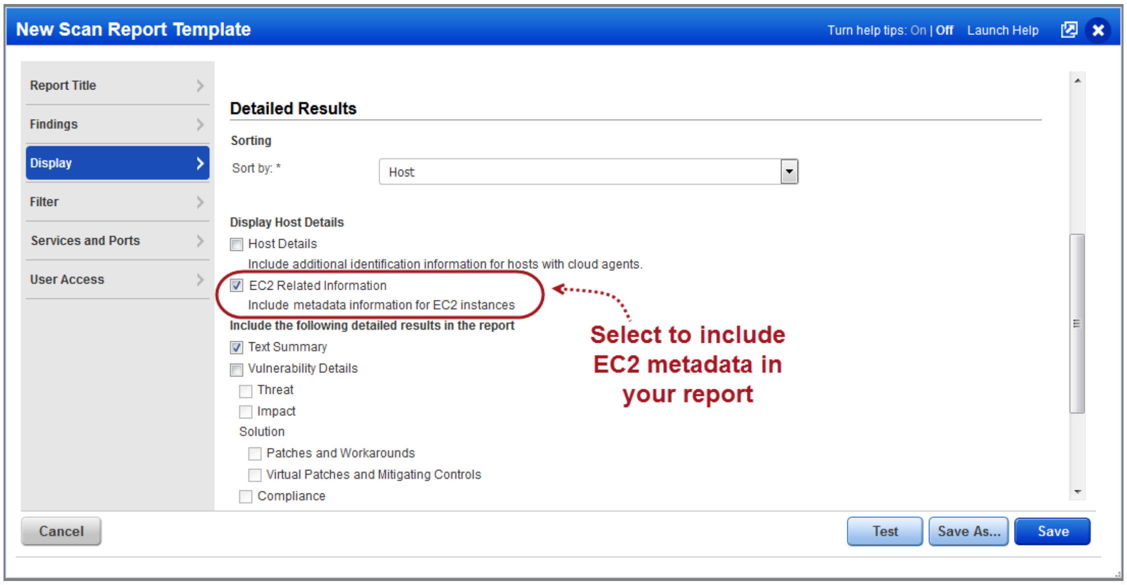
QID:	90883	**CVSS Base:**	6.3[1]
Category:	Windows	**CVSS Temporal:**	5.4
CVE ID:	-	**CVSS3 Base:**	-
Vendor Reference	-	**CVSS3 Temporal:**	-

Show EC2 Asset Info in Scan Reports

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

We've added a new report template option that allows you to include metadata information in your scan reports for your EC2 instances, including the public and private DNS name, image ID, VPC ID, instance state and instance type.

In your scan report template, go to the Display tab and choose EC2 Related Information. You must also select these options: 1) Host Based Findings (on the Findings tab) and Sort by Host (on the Display tab).



Detailed Results

Sorting

Sort by: * Host

Display Host Details

☐ Host Details

Include additional identification information for hosts with cloud agents.

☑ EC2 Related Information

Include metadata information for EC2 instances

Include the following detailed results in the report

☑ Text Summary

☐ Vulnerability Details

☐ Threat

☐ Impact

Solution

☐ Patches and Workarounds

☐ Virtual Patches and Mitigating Controls

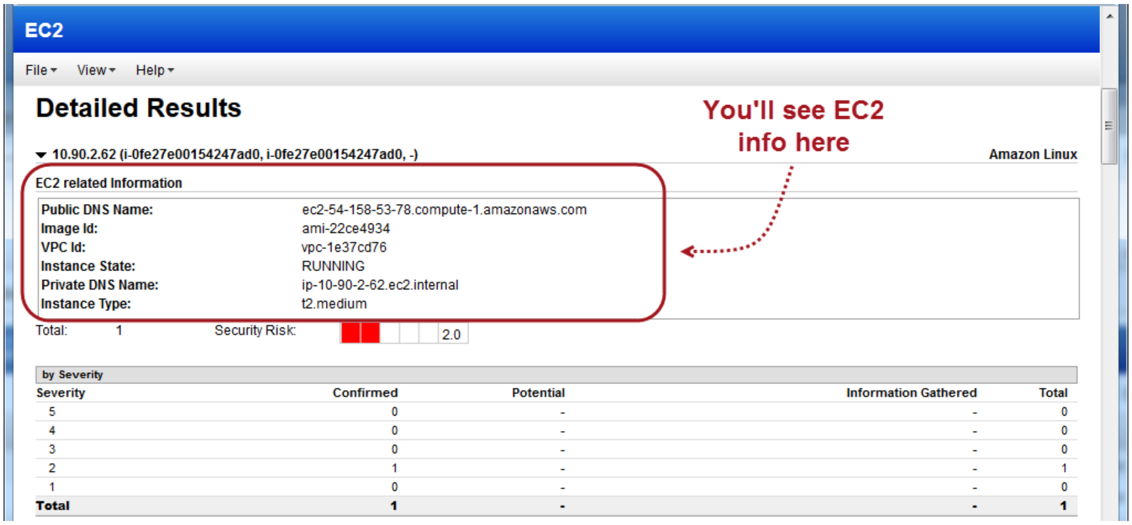
☐ Compliance

Select to include EC2 metadata in your report

Don't see this option? It only appears in accounts with EC2 Scanning enabled.

Sample HTML Report

EC2 related information appears in the report for each EC2 instance.



Detailed Results

You'll see EC2 info here

▼ 10.90.2.62 (i-0fe27e00154247ad0, i-0fe27e00154247ad0, -) Amazon Linux

EC2 related Information

Public DNS Name:	ec2-54-158-53-78.compute-1.amazonaws.com
Image Id:	ami-22ce4934
VPC Id:	vpc-1e37cd76
Instance State:	RUNNING
Private DNS Name:	ip-10-90-2-62.ec2.internal
Instance Type:	t2.medium

Total: 1 Security Risk: 2.0

by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	0	-	-	0
4	0	-	-	0
3	0	-	-	0
2	1	-	-	1
1	0	-	-	0
Total	**1**	**-**	**-**	**1**

Sample CSV Report

You’ll see new columns in the CSV output (in bold). These columns only appear in the output when EC2 Related Information is selected in the report template.

"IP","DNS","EC2 Instance ID","NetBIOS",**"Public Hostname","Image ID","VPC ID","Instance State","Private Hostname","Instance Type"**,"Tracking Method","OS","IP Status","QID","Title","Vuln Status","Type","Severity","Port","Protocol","FQDN","SSL","First Detected","Last Detected","Times Detected","Date Last Fixed","CVE ID","Vendor Reference","Bugtraq ID","Threat","PCI Vuln","Ticket State","Instance","Category"
"10.90.2.62","i-0fe27e00154247ad0","i-0fe27e00154247ad0",,"ec2-54-158-53-78.compute-1.amazonaws.com","ami-22ce4934","vpc-1e37cd76","RUNNING","ip-10-90-2-62.ec2.internal","t2.medium","EC2","Amazon Linux","host scanned, found vuln","11","Hidden RPC Services","Active","Vuln","2",,,,,"04/26/2017 23:12:04","04/28/2017 12:42:38","7",,,,,"The Portmapper/Rpcbind listens on port 111 and stores an updated list of registered RPC services running on the server (RPC name, version and port number). It acts as a ""gateway"" for clients wanting to connect to any RPC daemon.
...

Scan Report in XML Format - Ability to Exclude Glossary data

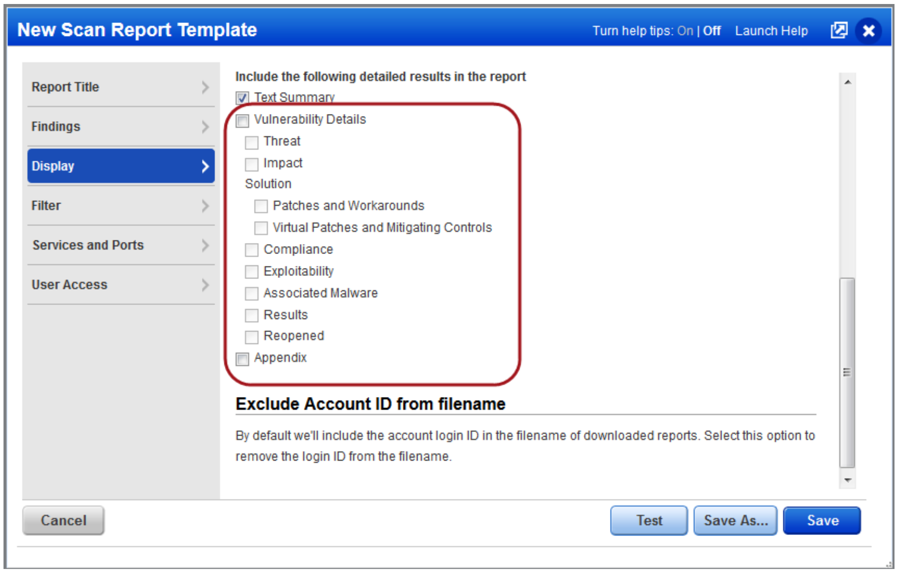
This update applies to the Scan Report in XML format only. Previously the <GLOSSARY> tag was always included in the scan report XML format regardless of template sub option settings under Vulnerability Details (e.g. Threat, Impact, Solution - Patches and Workarounds, etc). Now you can exclude the <GLOSSARY> tag and this will reduce the size of your reports.

What are the changes?

- the <GLOSSARY> tag will be excluded from the XML format if none of the “Vulnerability Details” sub options are selected

- the <GLOSSARY> tag will be included in the XML format if any one of the “Vulnerability Details” sub options is selected

- the Scan Report DTD (asset_data_report.dtd) was updated - see the *Qualys API Release Notes* for info



Include the following detailed results in the report

☑ Text Summary
☐ Vulnerability Details
☐ Threat
☐ Impact
Solution
☐ Patches and Workarounds
☐ Virtual Patches and Mitigating Controls
☐ Compliance
☐ Exploitability
☐ Associated Malware
☐ Results
☐ Reopened
☐ Appendix

Exclude Account ID from filename

By default we'll include the account login ID in the filename of downloaded reports. Select this option to remove the login ID from the filename.

Ticketbleed Vulnerability gets F Grade from Qualys SSL Labs

With this release servers found vulnerable to the Ticketbleed vulnerability get an F Grade from SSL Labs, when the SSL Labs feature is enabled for your subscription. This helps you easily identify servers vulnerable to Ticketbleed (CVE-2016-924).

Ticketbleed Vulnerability

QID: 370302
Title: F5 BIG-IP ASM Session Tickets Information Disclosure Vulnerability (Ticketbleed) (K05121675)
CVE ID: CVE-2016-924

Tell me about SSL Labs

SSL Labs is integrated with Qualys VM to provide grades for your certificates. This is intended to help you identify and prioritize certificates with SSL configuration issues. When enabled you'll see a letter grade (A-F) for each certificate in your certificates list. Grades are updated automatically each time new vulnerability scan results are processed for your hosts.

Learn more about Qualys SSL Labs
https://www.ssllabs.com/

Qualys Policy Compliance (PC)

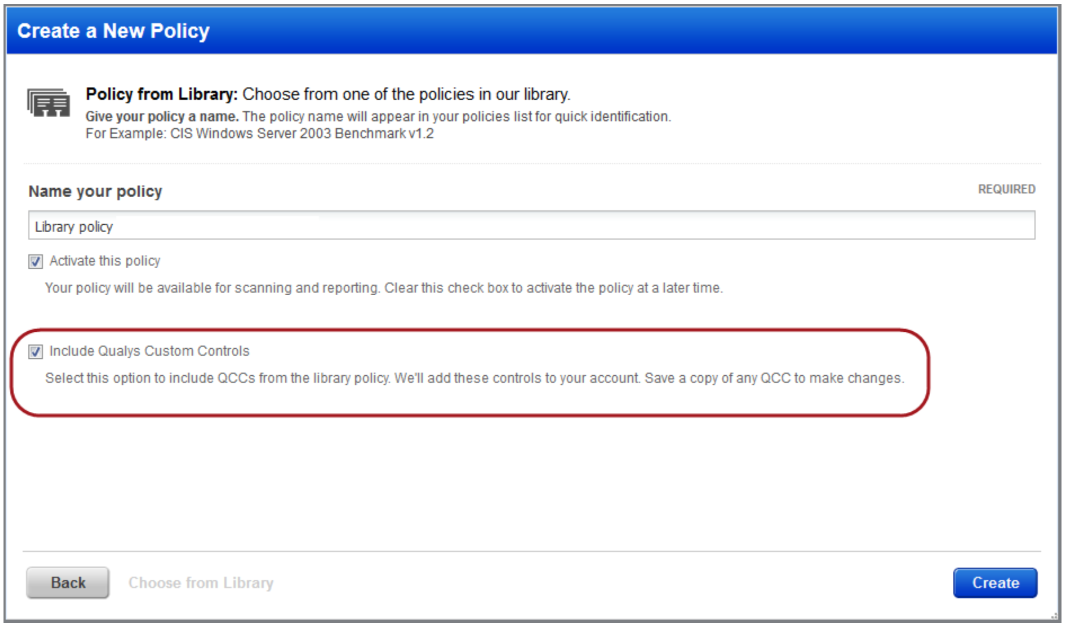
Introducing Qualys Custom Controls in Library Policies

Library policies provided by Qualys may now include a new control type called Qualys Custom Control (QCC). With this new control type we can quickly provide to users new controls that are similar to user-defined controls. Once added to your account you can copy any QCC to make your own UDC that you can customize to meet your needs.

> Note - In order for us to ensure that we don't add duplicate controls to your list when importing the same library policy multiple times these controls get an internal UDC ID assigned. You'll see the UDC ID when you export a QCC from your account, and when you export a library policy that includes a QCC from your account. See the *Qualys 8.10 API Release Notes* to learn more.

Import a Policy from the Library

Go to Policies > New > Policy > Import from Library. Choose a policy and click Next. If the selected policy includes QCCs you'll see the option "Include Qualys Custom Controls". This option is selected by default and is recommended. Click Create to import the policy and the add the QCCs. Don't want the QCCs? No problem. Simply uncheck the option.



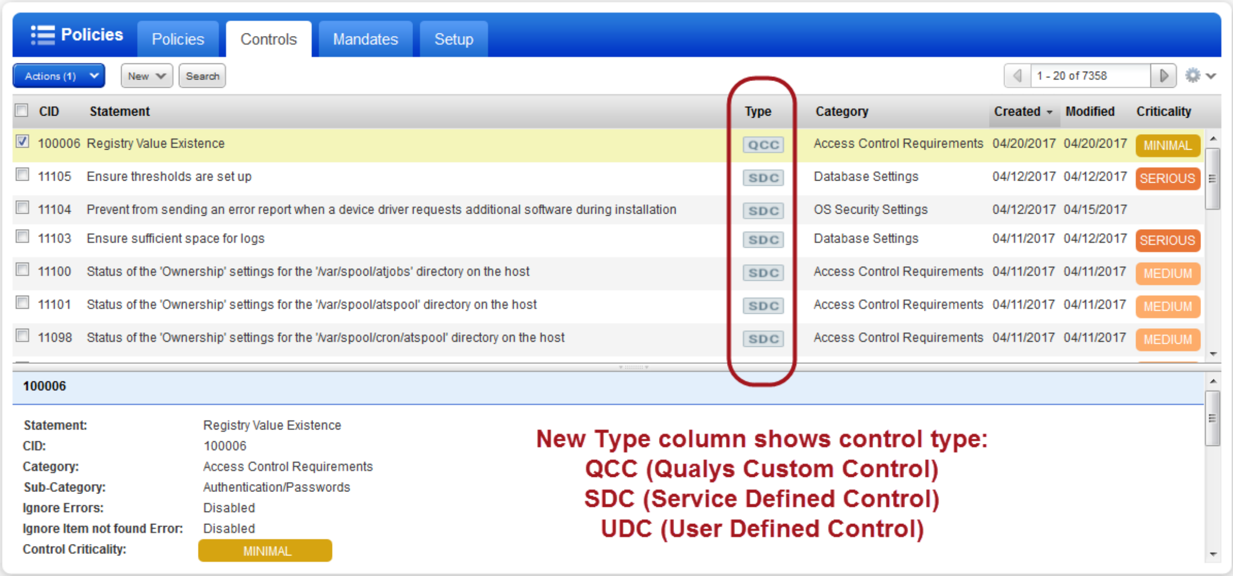
Policy from Library: Choose from one of the policies in our library.
Give your policy a name. The policy name will appear in your policies list for quick identification.
For Example: CIS Windows Server 2003 Benchmark v1.2

Name your policy: Library policy

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

☑ Include Qualys Custom Controls
Select this option to include QCCs from the library policy. We'll add these controls to your account. Save a copy of any QCC to make changes.

You'll have the chance to add asset groups to the policy and save it. Then the policy will appear on your policies list. The QCCs added from the policy appear on your controls list. A new Type column shows QCC for each Qualys Custom Control.



☐	CID	Statement	Type	Category	Created	Modified	Criticality
☑	100006	Registry Value Existence	QCC	Access Control Requirements	04/20/2017	04/20/2017	MINIMAL
☐	11105	Ensure thresholds are set up	SDC	Database Settings	04/12/2017	04/12/2017	SERIOUS
☐	11104	Prevent from sending an error report when a device driver requests additional software during installation	SDC	OS Security Settings	04/12/2017	04/15/2017	
☐	11103	Ensure sufficient space for logs	SDC	Database Settings	04/11/2017	04/12/2017	SERIOUS
☐	11100	Status of the 'Ownership' settings for the '/var/spool/atjobs' directory on the host	SDC	Access Control Requirements	04/11/2017	04/11/2017	MEDIUM
☐	11101	Status of the 'Ownership' settings for the '/var/spool/atspool' directory on the host	SDC	Access Control Requirements	04/11/2017	04/11/2017	MEDIUM
☐	11098	Status of the 'Ownership' settings for the '/var/spool/cron/atspool' directory on the host	SDC	Access Control Requirements	04/11/2017	04/11/2017	MEDIUM

100006

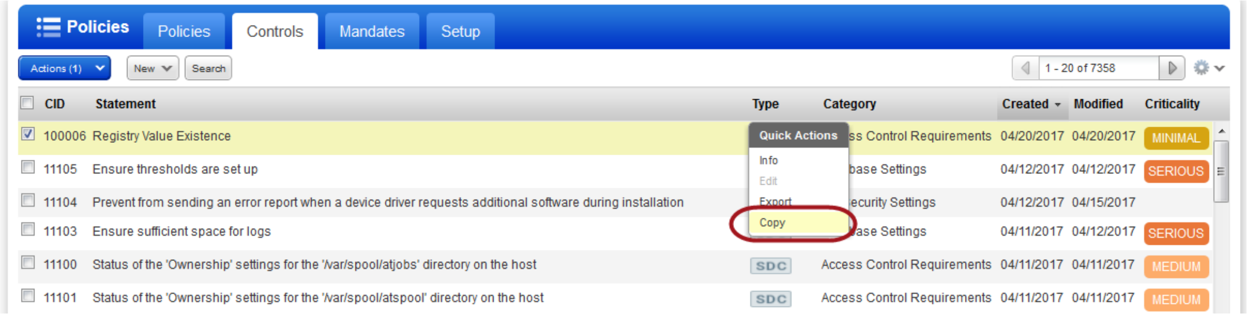
Statement:	Registry Value Existence
CID:	100006
Category:	Access Control Requirements
Sub-Category:	Authentication/Passwords
Ignore Errors:	Disabled
Ignore Item not found Error:	Disabled
Control Criticality:	MINIMAL

New Type column shows control type:
QCC (Qualys Custom Control)
SDC (Service Defined Control)
UDC (User Defined Control)

Good to Know - A QCC cannot be edited (except to change criticality) or deleted. Like service-defined controls, Qualys may update QCCs in subsequent releases to provide new technology support, updates to values, etc. This will not have any impact to the QCCs added to policies.

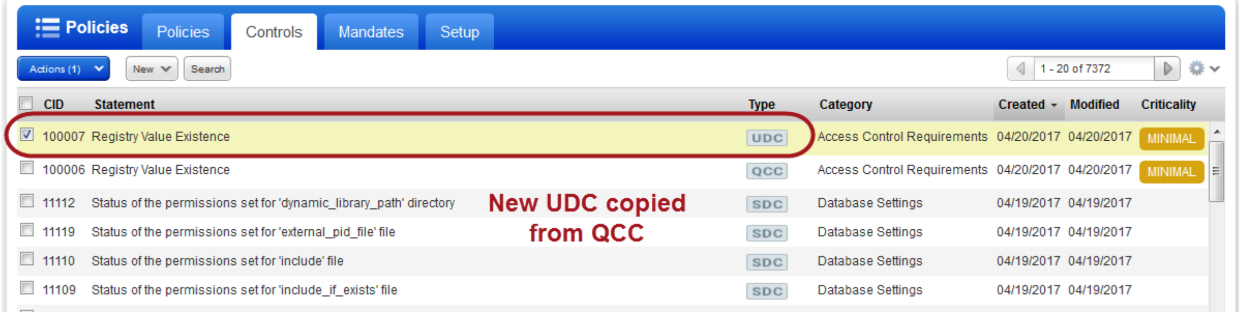
Copy a QCC to create a UDC

You can make a copy of any QCC to create a UDC that you can customize to meet your exact needs. It's easy to do – just choose Copy from the Quick Actions menu and then confirm the action.



☐	CID	Statement	Type	Category	Created	Modified	Criticality
☑	100006	Registry Value Existence		ss Control Requirements	04/20/2017	04/20/2017	MINIMAL
☐	11105	Ensure thresholds are set up		base Settings	04/12/2017	04/12/2017	SERIOUS
☐	11104	Prevent from sending an error report when a device driver requests additional software during installation		ecurity Settings	04/12/2017	04/15/2017	
☐	11103	Ensure sufficient space for logs		ase Settings	04/11/2017	04/12/2017	SERIOUS
☐	11100	Status of the 'Ownership' settings for the '/var/spool/atjobs' directory on the host	SDC	Access Control Requirements	04/11/2017	04/11/2017	MEDIUM
☐	11101	Status of the 'Ownership' settings for the '/var/spool/atspool' directory on the host	SDC	Access Control Requirements	04/11/2017	04/11/2017	MEDIUM

The new UDC will appear on the controls list where you can edit it.

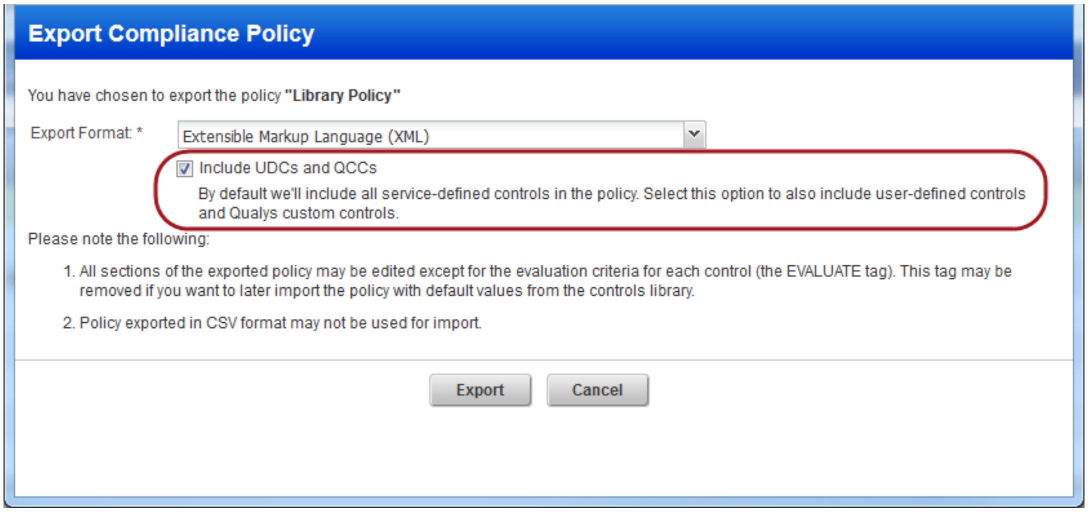


☐	CID	Statement	Type	Category	Created	Modified	Criticality
☑	100007	Registry Value Existence	UDC	Access Control Requirements	04/20/2017	04/20/2017	MINIMAL
☐	100006	Registry Value Existence	QCC	Access Control Requirements	04/20/2017	04/20/2017	MINIMAL
☐	11112	Status of the permissions set for 'dynamic_library_path' directory	SDC	Database Settings	04/19/2017	04/19/2017	
☐	11119	Status of the permissions set for 'external_pid_file' file	SDC	Database Settings	04/19/2017	04/19/2017	
☐	11110	Status of the permissions set for 'include' file	SDC	Database Settings	04/19/2017	04/19/2017	
☐	11109	Status of the permissions set for 'include_if_exists' file	SDC	Database Settings	04/19/2017	04/19/2017	

New UDC copied from QCC

Export a Policy with QCCs

When you export a policy you will now see the option Include UDCs and QCCs. By default we include all service-defined controls in the policy. Select this option to also include user-defined controls and Qualys custom controls in the policy.



Export Compliance Policy

You have chosen to export the policy **"Library Policy"**

Export Format: * Extensible Markup Language (XML)

☑ Include UDCs and QCCs

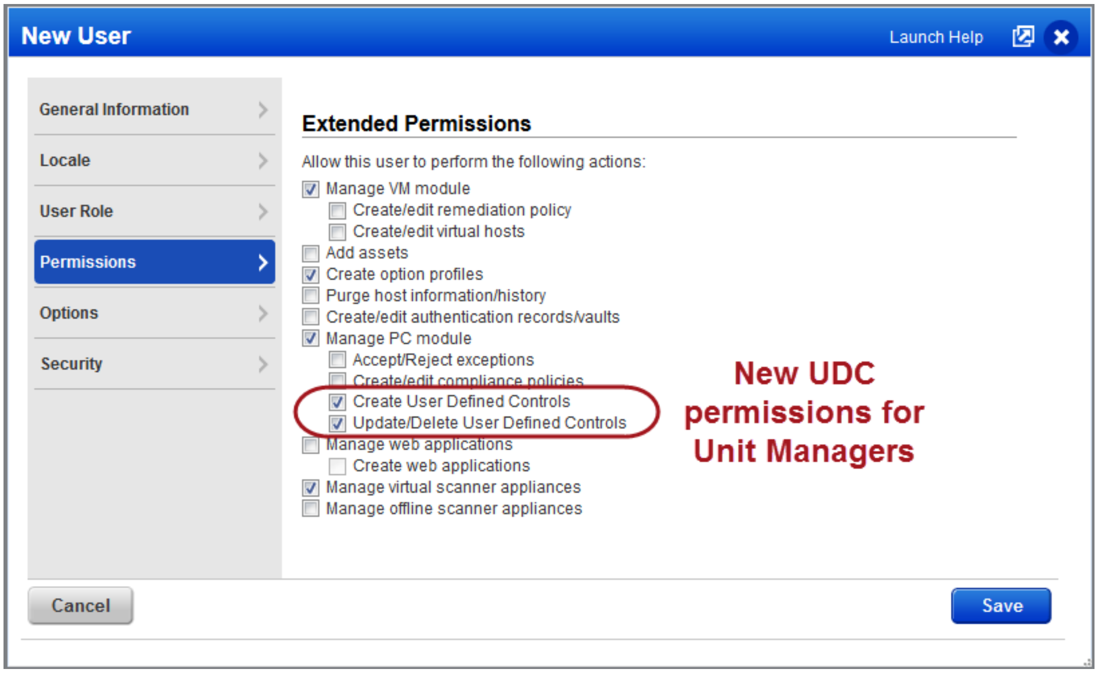
By default we'll include all service-defined controls in the policy. Select this option to also include user-defined controls and Qualys custom controls.

Please note the following:

1. All sections of the exported policy may be edited except for the evaluation criteria for each control (the EVALUATE tag). This tag may be removed if you want to later import the policy with default values from the controls library.
2. Policy exported in CSV format may not be used for import.

New UDC Permissions for Unit Managers

Now Unit Managers may be granted permission to create, update and delete User Defined Controls (UDCs). When creating or editing a Unit Manager account, go to the Permissions tab and choose Manage PC module. Then give the user one or both of these new permissions: Create User Defined Controls and Update/Delete User Defined Controls.



New User

Extended Permissions

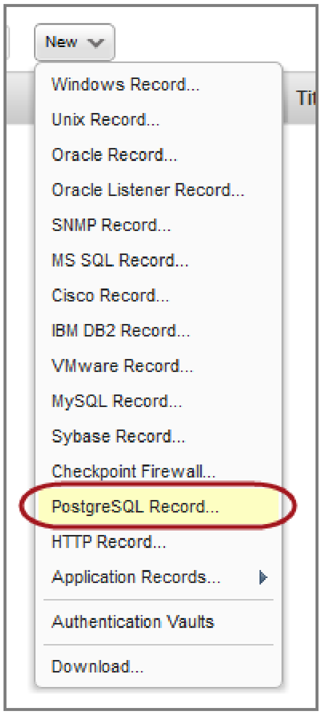
Allow this user to perform the following actions:

- ☑ Manage VM module
  - ☐ Create/edit remediation policy
  - ☐ Create/edit virtual hosts
- ☐ Add assets
- ☑ Create option profiles
- ☐ Purge host information/history
- ☐ Create/edit authentication records/vaults
- ☑ Manage PC module
  - ☐ Accept/Reject exceptions
  - ☐ Create/edit compliance policies
  - ☑ Create User Defined Controls
  - ☑ Update/Delete User Defined Controls
- ☐ Manage web applications
  - ☐ Create web applications
- ☑ Manage virtual scanner appliances
- ☐ Manage offline scanner appliances

New UDC permissions for Unit Managers

New Support for PostgreSQL Authentication

We now support compliance scans for PostgreSQL database instances running on Unix hosts. You'll need to create a new PostgreSQL authentication record. Unix authentication is required so you'll also need a Unix record for the host running the PostgreSQL database.



Which technologies are supported?

PostgreSQL 9.x

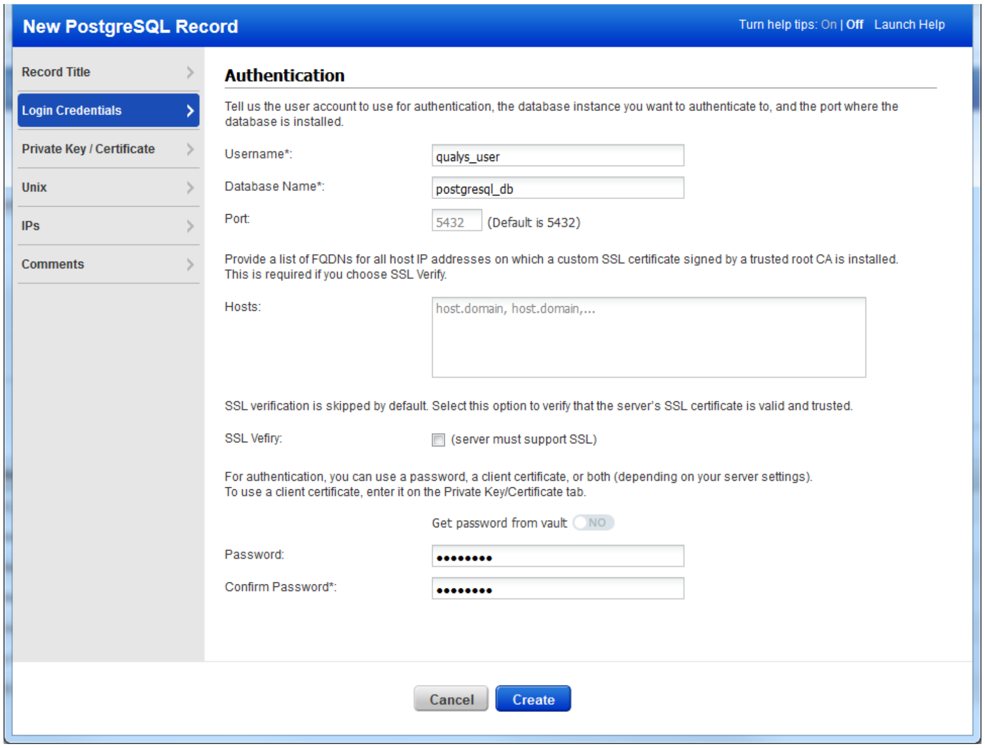
How do I get started?

Go to Scans > Authentication, and choose New > PostgreSQL Record (as shown on the right). This authentication type is supported for compliance scans only.

Your PostgreSQL Record

Tell us the user account to be used for authentication, the database instance to authenticate to, and the port where the database is installed.

The authentication method you use depends on your server settings.
You can provide:
- a password (enter it on the Login Credentials tab or get it from a vault),
- a client certificate (enter it on the Private Key / Certificate tab),
- a password AND client certificate (enter values on both tabs).



Authentication

Tell us the user account to use for authentication, the database instance you want to authenticate to, and the port where the database is installed.

Username*: qualys_user

Database Name*: postgresql_db

Port: 5432 (Default is 5432)

Provide a list of FQDNs for all host IP addresses on which a custom SSL certificate signed by a trusted root CA is installed. This is required if you choose SSL Verify.

Hosts: host.domain, host.domain,...

SSL verification is skipped by default. Select this option to verify that the server's SSL certificate is valid and trusted.

SSL Vefiry: ☐ (server must support SSL)

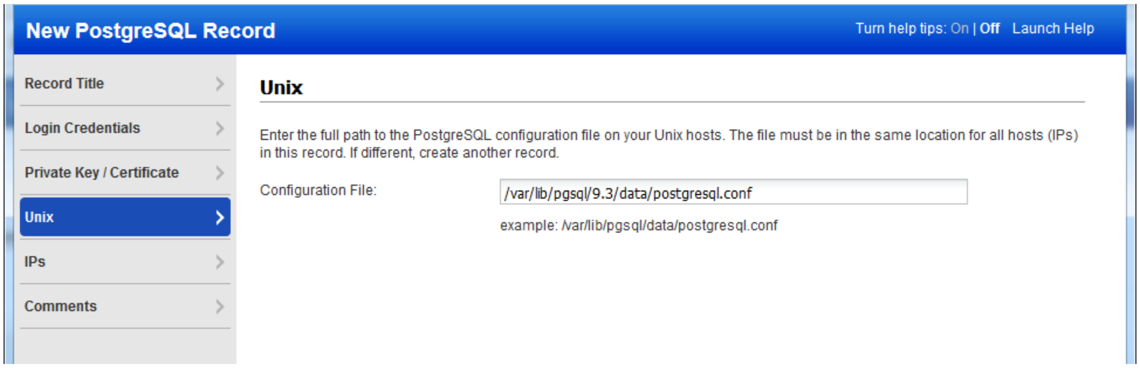
For authentication, you can use a password, a client certificate, or both (depending on your server settings).
To use a client certificate, enter it on the Private Key/Certificate tab.

Get password from vault NO

Password: ••••••••

Confirm Password*: ••••••••

On the Unix tab, tell us the full path to the PostgreSQL configuration file on your Unix hosts (IP addresses). The file must be in the same location on all IPs in this record (listed on the IPs tab).



Unix

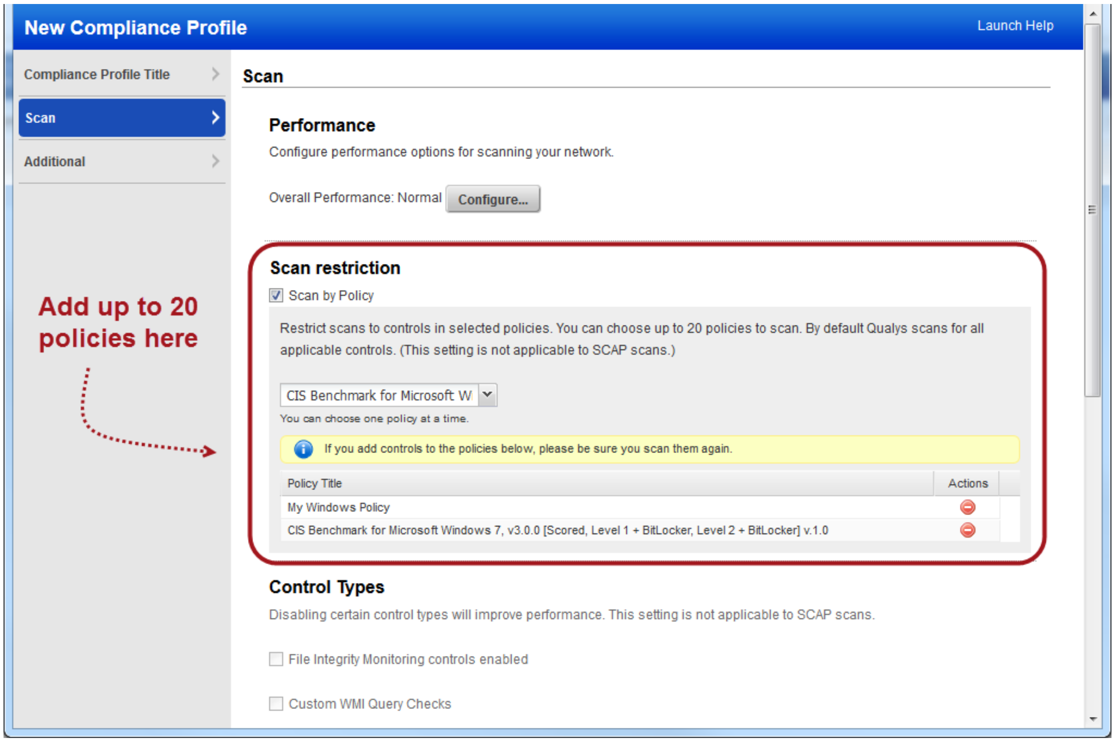
Enter the full path to the PostgreSQL configuration file on your Unix hosts. The file must be in the same location for all hosts (IPs) in this record. If different, create another record.

Configuration File: /var/lib/pgsql/9.3/data/postgresql.conf

example: /var/lib/pgsql/data/postgresql.conf

Increased Scan by Policy Limit

When using the Scan by Policy feature you can now choose up to 20 policies in the compliance option profile. This limit was increased from 10 policies.



Scan

Performance

Configure performance options for scanning your network.

Overall Performance: Normal Configure...

Scan restriction

☑ Scan by Policy

Restrict scans to controls in selected policies. You can choose up to 20 policies to scan. By default Qualys scans for all applicable controls. (This setting is not applicable to SCAP scans.)

CIS Benchmark for Microsoft W

You can choose one policy at a time.

If you add controls to the policies below, please be sure you scan them again.

Policy Title	Actions
My Windows Policy	⊖
CIS Benchmark for Microsoft Windows 7, v3.0.0 [Scored, Level 1 + BitLocker, Level 2 + BitLocker] v.1.0	⊖

Control Types

Disabling certain control types will improve performance. This setting is not applicable to SCAP scans.

□ File Integrity Monitoring controls enabled

□ Custom WMI Query Checks

Generate Mandate Based Reports to View Compliance Posture

You can now view the compliance posture of the organization in terms of the underlying Security baseline against selected mandates by simply launching a mandate based report. You can use mandate based report templates to create harmonized reports on one or more compliance policies and mandates.

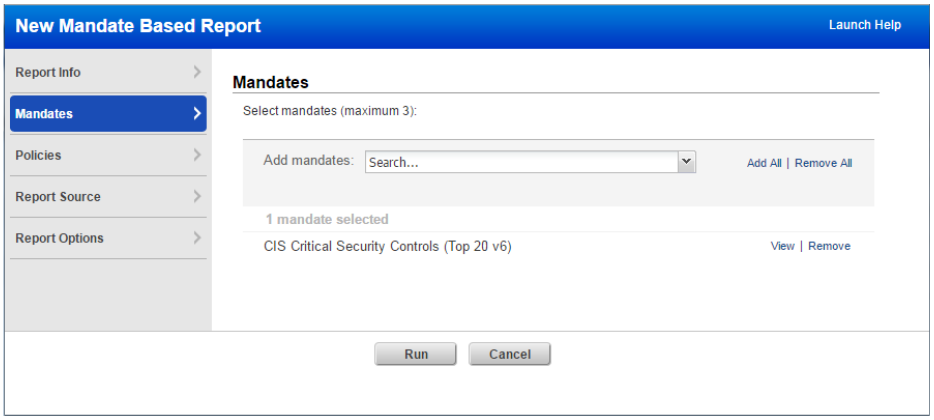
Choose any mandates/standards you have to comply with (or even the sub-requirements from multiple mandates to create a Union of the total requirements) and get a view of compliance posture in terms of the selected policies. We have provided you with a set of pre-defined mandates which you can use to generate mandate based reports. View list of these pre-defined mandates in the Policies > Mandates tab.

To generate a mandate based report:

First you need to create a custom mandate based template. Just go to Reports > Templates > Mandate Template and configure settings.

Then, navigate to Reports > New > Compliance Report > Mandate Based Report.

Add mandates, select policies and choose assets you want to get information from, in your report.



Mandates

Select mandates (maximum 3):

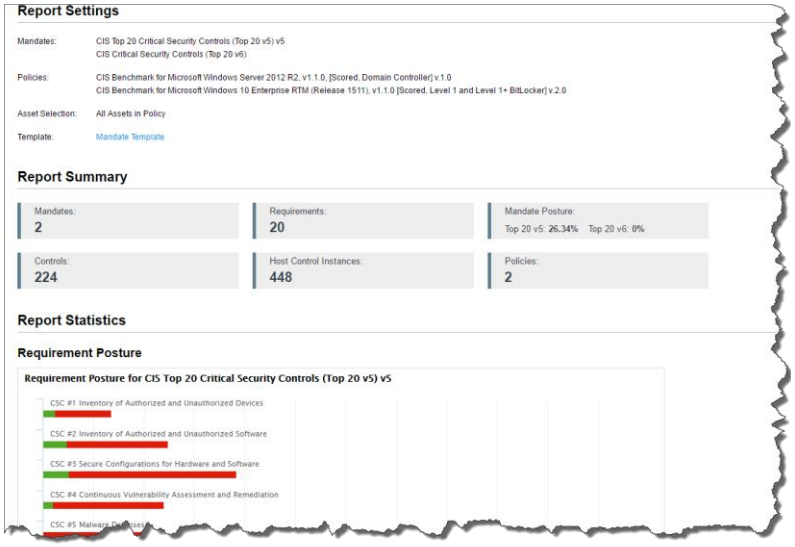
Add mandates: Search...

Add All | Remove All

1 mandate selected

CIS Critical Security Controls (Top 20 v6) View | Remove

Depending on what you select in the report layout while creating the custom mandate based template, a report is generated.



Report Settings

Mandates:	CIS Top 20 Critical Security Controls (Top 20 v5) v5 CIS Critical Security Controls (Top 20 v6)
Policies:	CIS Benchmark for Microsoft Windows Server 2012 R2, v1.1.0, [Scored, Domain Controller] v.1.0 CIS Benchmark for Microsoft Windows 10 Enterprise RTM (Release 1511), v1.1.0 [Scored, Level 1 and Level 1+ BitLocker] v.2.0
Asset Selection:	All Assets in Policy
Template:	Mandate Template

Report Summary

Mandates: 2

Requirements: 20

Mandate Posture: Top 20 v5: 26.34% Top 20 v6: 0%

Controls: 224

Host Control Instances: 448

Policies: 2

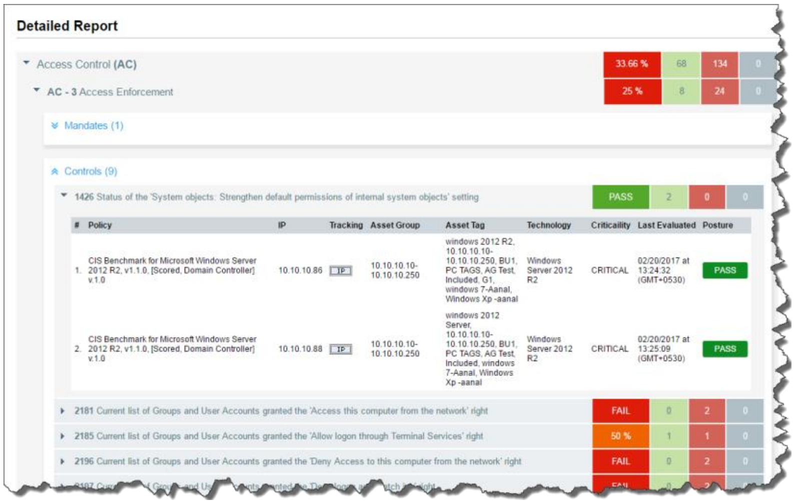
Report Statistics

Requirement Posture

Requirement Posture for CIS Top 20 Critical Security Controls (Top 20 v5) v5

CSC #1 Inventory of Authorized and Unauthorized Devices
CSC #2 Inventory of Authorized and Unauthorized Software
CSC #3 Secure Configurations for Hardware and Software
CSC #4 Continuous Vulnerability Assessment and Remediation
CSC #5 Malware Defenses

View selected mandates and policies and their detailed posture.



Detailed Report

- Access Control **(AC)** — 33.66 % | 68 | 134 | 0
  - **AC - 3** Access Enforcement — 25 % | 8 | 24 | 0
    - Mandates (1)
    - Controls (9)
      - **1426** Status of the 'System objects: Strengthen default permissions of internal system objects' setting — PASS | 2 | 0 | 0

#	Policy	IP	Tracking	Asset Group	Asset Tag	Technology	Criticaility	Last Evaluated	Posture
1.	CIS Benchmark for Microsoft Windows Server 2012 R2, v1.1.0, [Scored, Domain Controller] v.1.0	10.10.10.86	IP	10.10.10.10-10.10.10.250	windows 2012 R2, 10.10.10.10-10.10.10.250, BU1, PC TAGS, AG Test, Included, G1, windows 7-Aanal, Windows Xp -aanal	Windows Server 2012 R2	CRITICAL	02/20/2017 at 13:24:32 (GMT+0530)	PASS
2.	CIS Benchmark for Microsoft Windows Server 2012 R2, v1.1.0, [Scored, Domain Controller] v.1.0	10.10.10.88	IP	10.10.10.10-10.10.10.250	windows 2012 Server, 10.10.10.10-10.10.10.250, BU1, PC TAGS, AG Test, Included, windows 7-Aanal, Windows Xp -aanal	Windows Server 2012 R2	CRITICAL	02/20/2017 at 13:25:09 (GMT+0530)	PASS

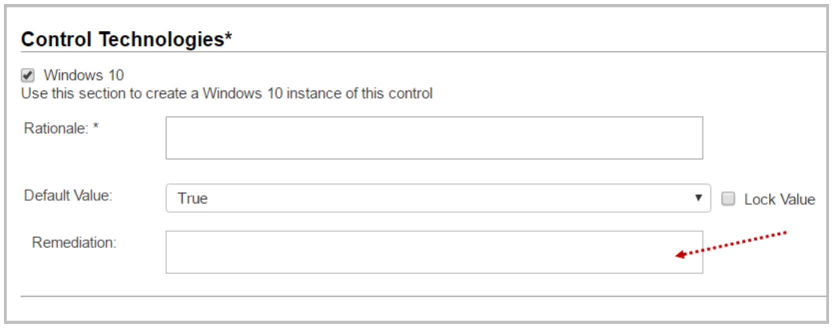
- **2181** Current list of Groups and User Accounts granted the 'Access this computer from the network' right — FAIL | 0 | 2 | 0
- **2185** Current list of Groups and User Accounts granted the 'Allow logon through Terminal Services' right — 50 % | 1 | 1 | 0
- **2196** Current list of Groups and User Accounts granted the 'Deny Access to this computer from the network' right — FAIL | 0 | 2 | 0

In the Detailed Report section of the report, you can drill down to view the posture for each control objective.

View Remediation Information in Reports

You can now include the remediation information for control technologies in compliance reports. For system defined controls, the reports display the remediation information set by Qualys. For user defined controls, the remediation information that you set for each control technology is displayed in the reports. If no remediation information is set/available, the reports will display N/A.

For user defined controls, the remediation information should be first added to the control technology. Go to Policy > Controls, and then edit an existing control or create a new control.



Control Technologies*

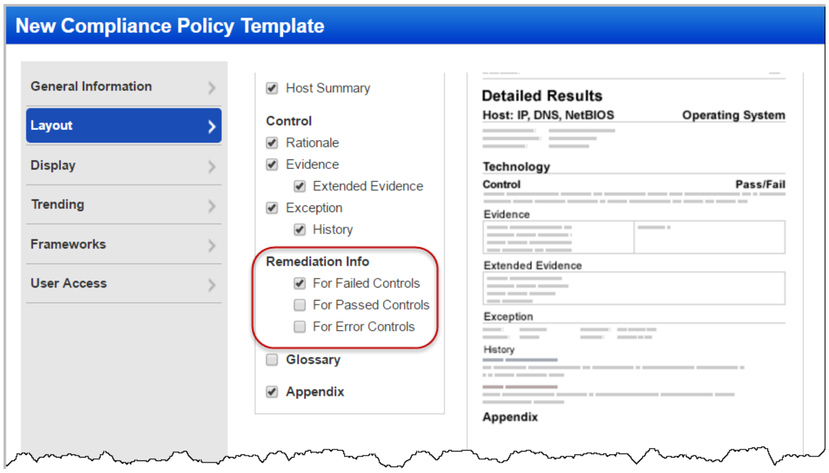
☑ Windows 10
Use this section to create a Windows 10 instance of this control

Rationale: *

Default Value: True ▾ ☐ Lock Value

Remediation:

Under the Control Technologies section, select a control, and then enter the remediation information.



New Compliance Policy Template

- General Information
- **Layout**
- Display
- Trending
- Frameworks
- User Access

☑ Host Summary

Control
☑ Rationale
☑ Evidence
☑ Extended Evidence
☑ Exception
☑ History

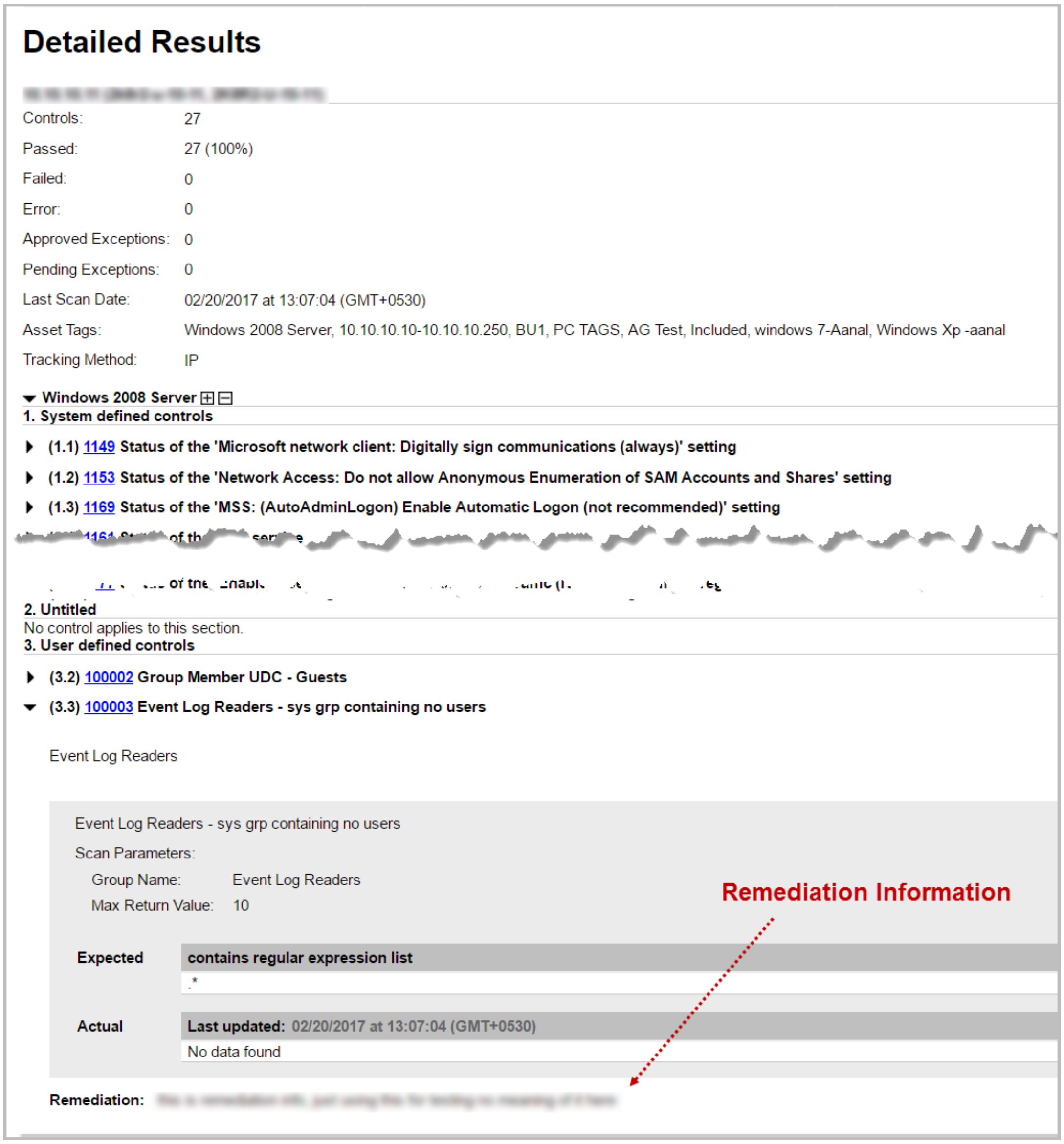
Remediation Info
☑ For Failed Controls
☐ For Passed Controls
☐ For Error Controls

☐ Glossary

☑ Appendix

To show remediation information in reports, go to Reports > Templates, and then edit an existing template or create a new template. On the Layout tab, select the respective check boxes to show remediation information in the reports.

You can then view the remediation information in reports generated using that report template.



Detailed Results

[redacted]

Controls:	27
Passed:	27 (100%)
Failed:	0
Error:	0
Approved Exceptions:	0
Pending Exceptions:	0
Last Scan Date:	02/20/2017 at 13:07:04 (GMT+0530)
Asset Tags:	Windows 2008 Server, 10.10.10.10-10.10.10.250, BU1, PC TAGS, AG Test, Included, windows 7-Aanal, Windows Xp -aanal
Tracking Method:	IP

Windows 2008 Server ⊞ ⊟

1. System defined controls

- **(1.1) 1149 Status of the 'Microsoft network client: Digitally sign communications (always)' setting**
- **(1.2) 1153 Status of the 'Network Access: Do not allow Anonymous Enumeration of SAM Accounts and Shares' setting**
- **(1.3) 1169 Status of the 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' setting**
- **1161 [illegible] of th[illegible] ser[illegible]e**
- **[illegible] of the [illegible]**

2. Untitled

No control applies to this section.

3. User defined controls

- **(3.2) 100002 Group Member UDC - Guests**
- **(3.3) 100003 Event Log Readers - sys grp containing no users**

Event Log Readers

Event Log Readers - sys grp containing no users

Scan Parameters:

Group Name:	Event Log Readers
Max Return Value:	10

Remediation Information

Expected	**contains regular expression list**
	.*
Actual	**Last updated: 02/20/2017 at 13:07:04 (GMT+0530)**
	No data found

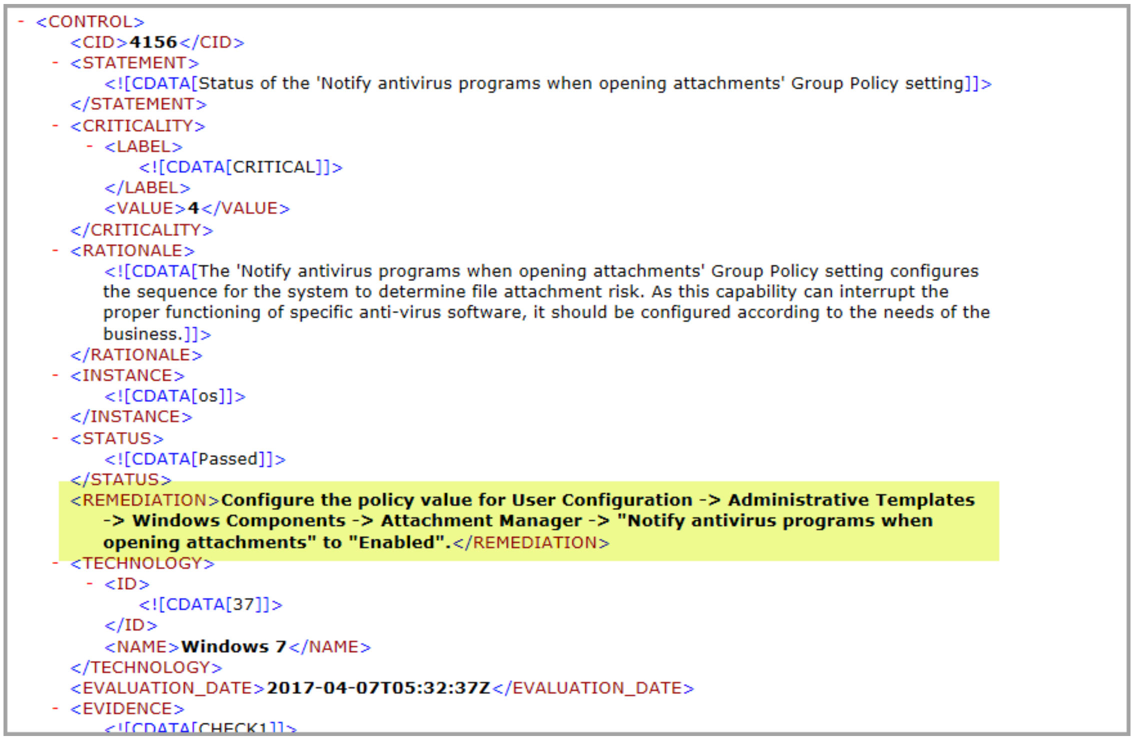
Remediation: [redacted]

Remediation Information in CSV and XML Formats

Policy compliance reports now display Remediation information in the CSV and XML report formats.

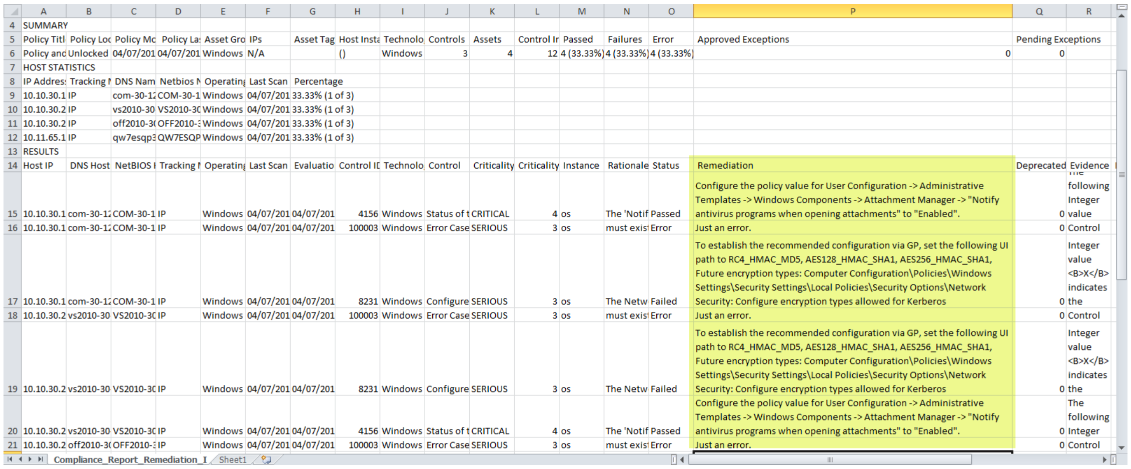
Simply download a policy report in CSV or XML format and you'll see the information under REMEDIATION tag (XML) or Remediation column (CSV).

Sample XML



```
- <CONTROL>
     <CID>4156</CID>
   - <STATEMENT>
        <![CDATA[Status of the 'Notify antivirus programs when opening attachments' Group Policy setting]]>
     </STATEMENT>
   - <CRITICALITY>
      - <LABEL>
           <![CDATA[CRITICAL]]>
        </LABEL>
        <VALUE>4</VALUE>
     </CRITICALITY>
   - <RATIONALE>
        <![CDATA[The 'Notify antivirus programs when opening attachments' Group Policy setting configures
        the sequence for the system to determine file attachment risk. As this capability can interrupt the
        proper functioning of specific anti-virus software, it should be configured according to the needs of the
        business.]]>
     </RATIONALE>
   - <INSTANCE>
        <![CDATA[os]]>
     </INSTANCE>
   - <STATUS>
        <![CDATA[Passed]]>
     </STATUS>
     <REMEDIATION>Configure the policy value for User Configuration -> Administrative Templates
        -> Windows Components -> Attachment Manager -> "Notify antivirus programs when
        opening attachments" to "Enabled".</REMEDIATION>
   - <TECHNOLOGY>
      - <ID>
           <![CDATA[37]]>
        </ID>
        <NAME>Windows 7</NAME>
     </TECHNOLOGY>
     <EVALUATION_DATE>2017-04-07T05:32:37Z</EVALUATION_DATE>
   - <EVIDENCE>
        <![CDATA[CHECK1]]>
```

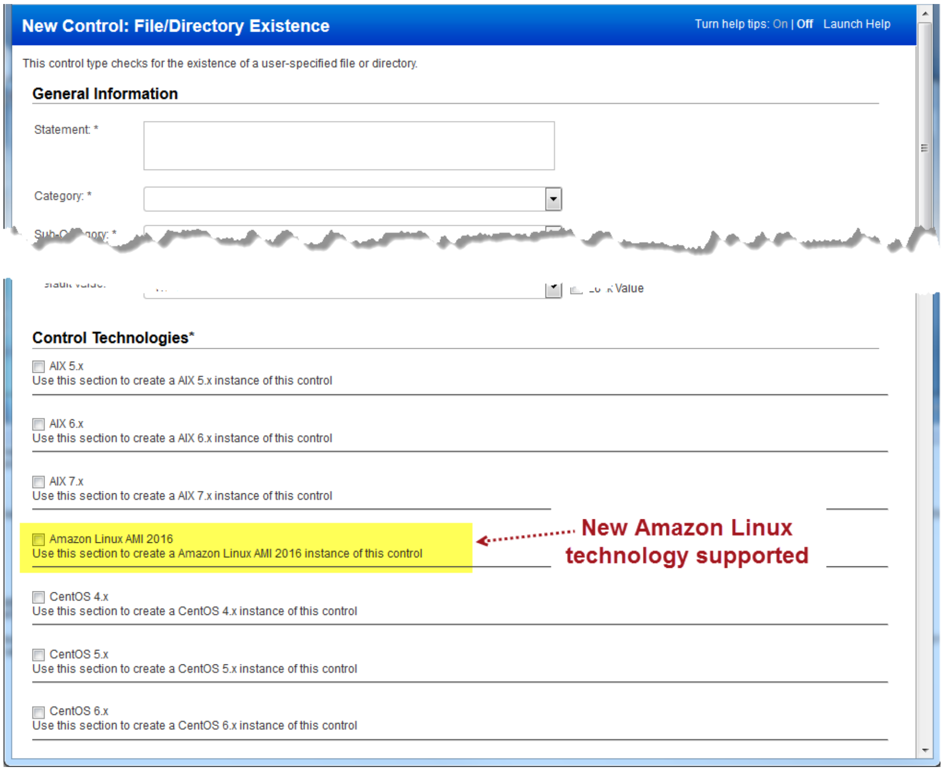
Sample CSV



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
4	SUMMARY																	
5	Policy Titl	Policy Loc	Policy Mc	Policy La:	Asset Gro	IPs	Asset Tag	Host Insta	Technolo	Controls	Assets	Control Ir	Passed	Failures	Error	Approved Exceptions	Pending Exceptions	
6	Policy and	Unlocked	04/07/201	04/07/201	Windows	N/A		()	Windows	3	4	12	4 (33.33%)	4 (33.33%)	4 (33.33%)	0	0	
7	HOST STATISTICS																	
8	IP Addres:	Tracking I	DNS Nam	Netbios N	Operating	Last Scan	Percentage											
9	10.10.30.1	IP	com-30-12	COM-30-1	Windows	04/07/201	33.33% (1 of 3)											
10	10.10.30.2	IP	vs2010-30	VS2010-30	Windows	04/07/201	33.33% (1 of 3)											
11	10.10.30.2	IP	off2010-30	OFF2010-3	Windows	04/07/201	33.33% (1 of 3)											
12	10.11.65.1	IP	qw7esqp3	QW7ESQP	Windows	04/07/201	33.33% (1 of 3)											
13	RESULTS																	
14	Host IP	DNS Host	NetBIOS I	Tracking I	Operating	Last Scan	Evaluatio	Control ID	Technolo	Control	Criticality	Criticality	Instance	Rationale	Status	Remediation	Deprecated	Evidence
15	10.10.30.1	com-30-12	COM-30-1	IP	Windows	04/07/201	04/07/201	4156	Windows	Status of t	CRITICAL	4	os	The 'Notif	Passed	Configure the policy value for User Configuration -> Administrative Templates -> Windows Components -> Attachment Manager -> "Notify antivirus programs when opening attachments" to "Enabled".	0	The following Integer value
16	10.10.30.1	com-30-12	COM-30-1	IP	Windows	04/07/201	04/07/201	100003	Windows	Error Case	SERIOUS	3	os	must exist	Error	Just an error.	0	Control
17	10.10.30.1	com-30-12	COM-30-1	IP	Windows	04/07/201	04/07/201	8231	Windows	Configure	SERIOUS	3	os	The Netw	Failed	To establish the recommended configuration via GP, set the following UI path to RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network Security: Configure encryption types allowed for Kerberos	0	Integer value <B>X</B> indicates the
18	10.10.30.2	vs2010-30	VS2010-30	IP	Windows	04/07/201	04/07/201	100003	Windows	Error Case	SERIOUS	3	os	must exist	Error	Just an error.	0	Control
19	10.10.30.2	vs2010-30	VS2010-30	IP	Windows	04/07/201	04/07/201	8231	Windows	Configure	SERIOUS	3	os	The Netw	Failed	To establish the recommended configuration via GP, set the following UI path to RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network Security: Configure encryption types allowed for Kerberos	0	Integer value <B>X</B> indicates the
20	10.10.30.2	vs2010-30	VS2010-30	IP	Windows	04/07/201	04/07/201	4156	Windows	Status of t	CRITICAL	4	os	The 'Notif	Passed	Configure the policy value for User Configuration -> Administrative Templates -> Windows Components -> Attachment Manager -> "Notify antivirus programs when opening attachments" to "Enabled".	0	The following Integer
21	10.10.30.2	off2010-30	OFF2010-3	IP	Windows	04/07/201	04/07/201	100003	Windows	Error Case	SERIOUS	3	os	must exist	Error	Just an error.	0	Control

Amazon Linux AMI 2016 Technology Supported for Unix UDCs

Want to create a UDC for Amazon Linux AMI 2016? Go to Policies > Controls > New > Control, and select any of the Unix control types. Scroll down to the Control Technologies section to provide a rationale statement and expected value for each technology you're interested in.



This control type checks for the existence of a user-specified file or directory.

General Information

Statement: *

Category: *

Sub-Category: *

□ Value

Control Technologies*

□ AIX 5.x
Use this section to create a AIX 5.x instance of this control

□ AIX 6.x
Use this section to create a AIX 6.x instance of this control

□ AIX 7.x
Use this section to create a AIX 7.x instance of this control

□ Amazon Linux AMI 2016
Use this section to create a Amazon Linux AMI 2016 instance of this control

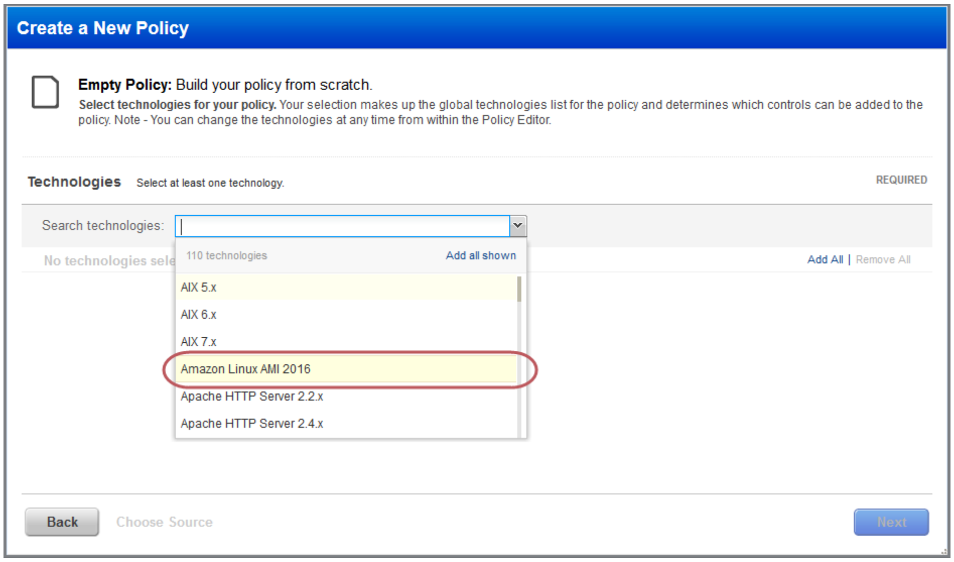
New Amazon Linux technology supported

□ CentOS 4.x
Use this section to create a CentOS 4.x instance of this control

□ CentOS 5.x
Use this section to create a CentOS 5.x instance of this control

□ CentOS 6.x
Use this section to create a CentOS 6.x instance of this control

You'll also see Amazon Linux AMI 2016 in the technologies list when creating a new policy.



Empty Policy: Build your policy from scratch.
Select technologies for your policy. Your selection makes up the global technologies list for the policy and determines which controls can be added to the policy. Note - You can change the technologies at any time from within the Policy Editor.

Technologies Select at least one technology. REQUIRED

Search technologies:

No technologies sele

110 technologies

AIX 5.x
AIX 6.x
AIX 7.x
Amazon Linux AMI 2016
Apache HTTP Server 2.2.x
Apache HTTP Server 2.4.x

Issues Addressed

- Host Based Scan Reports in CSV format - Fixed an issue where we were not properly parsing and displaying the port, protocol and instance information for vulnerabilities detected on Oracle instances. Now this information appears correctly.
- Host Based Scan Reports in CSV format - Fixed an issue where we didn't calculate and display the CVSS v3 score when the report target did not include asset groups.
- Host Based Scan Reports in CSV format - Fixed an issue where we were displaying HTML code for special characters in the Exploit, Malware and Vendor columns (such as &quot; instead of ").
- Host Based Scan Reports in CSV format - Fixed an issue where we incorrectly displayed a value of "0" instead of a blank value for the CVSS v3 score when the CVSS Temporal and Base scores were not available.
- Patch Report - The issue of broken patch links in the patch report is now fixed. The hyperlinks are now removed and the patch links are no more clickable in the PDF.
- Patch Scorecard Report will no longer display the "Asset Tags" label as this report cannot be filtered by tags.
- Policy Report - The Asset Tag radio button is now only enabled after the user selects a policy for the report.
- Policy Report - Instance information is now displayed accurately in all policy report formats.
- Policy Report - OS details and technology information is now displayed accurately for the selected target.
- Asset Search Report in PDF format - Fixed an issue where the Appendix section was missing in PDF format. The Appendix section includes details about QIDs included in the asset search.
- We have fixed multiple filter related issues to eliminate discrepancies in the vulnerability count in PDF and XML reports. Now, the count of vulnerabilities is in sync for PDF and XML reports.
- A scheduled scan report with the "Exclude account login ID from filename" option selected in the report template is now working as expected.
- The Ticket State field is now displayed appropriately in all report formats for Host Based Scan Reports and is not displayed in Scan Based Scan Reports.
- The scan date is now displayed accurately in reports and scan results.
- The tracking method is now displayed for all types of reports including XML reports.
- VM scan result retains the existing OS value in the case where a scan returns a null, empty or unknown OS value.
- In PDF scan results with too many QIDs for a custom selected QID scan, the data is now neatly represented without any overlap at the end pages of the results.
- Previously, when there are no scanner appliances in your account, "Launch EC2 Vulnerability Scan" displayed Asset Group and IP fields which are not relevant for EC2 scans. This is fixed, and now the appropriate fields for including/excluding hosts are displayed.
- Previously, an "internal error" was displayed when the EC2 scan was launched with all terminated instances. This is fixed, and now the proper message is displayed "Empty target - all instances have Terminated status" and the scan is not launched.

- The Activity Log now displays a log entry when an EC2 scheduled scan with a tag having all terminated instances is not launched.
- Previously, the VM Scan list did not load completely for a Unit Manager with EC2 scan, and the user would see the message “Please wait for a moment while we process your request” constantly. This is now fixed, and the VM scan list now loads successfully.
- Users can now successfully create tags from the Asset Search tab when tracking method is selected as Agent and EC2.
- Appropriate messages to guide the user are now displayed when the Launch Vulnerability Scan Preview takes a long time to display a list of hosts resolved from asset tags targeted for the scan. An appropriate message is also displayed in case the request times out and the list of targeted hosts doesn’t load.
- When you create a new Docker authentication record, if you choose “Do not show this message again” check box, the alert box should not displayed henceforth.
- Authentication records which don’t have IPs assigned to them and are purely based on Domains shall show IPs in the data list when you click the “Details” link on the Authentication tab.
- Fixed an issue where you couldn’t change the Latest Controls email notification option for sub-users (Unit Managers, Scanners, Readers) from Monthly to Weekly or None.
- You can now enable Other Notifications for a Remediation user. If the notifications are enabled, the Remediation user now receives the notifications.
- Fixed an issue where an automated email notification was sent with a blank subject line. The email was sent because the report template for a scheduled report was not found. The subject line was blank only in cases where the notification option was not enabled for the scheduled report. If enabled we used the subject line provided in the notification settings.
- We have now removed the Network option from IPv6 mapping.
- IPv6 addresses can now be successfully added using CSV file.
- Removal of default scanner from an asset group does not display an error now. If you have to remove the default scanner, among other scanner appliances that are added, the newly added scanner is marked as the default scanner appliance. Also, you can now save an asset group without any default scanner assigned.
- Previously, the VM > Assets > Applications data downloaded as CSV would show incorrect data against the column headers. This is fixed, and now the CSV displays correct data against each column header.
- The Remove IP link on the Details page of Authentication now functions correctly.
- Previously, a Manager was able to see the scans launched by a Unit Manager, however the Unit Manager could not see those scans. This is fixed, and now the Unit Manager can see the list of scans launched.
- Previously, searching the VM Scan list for target IP address was taking more time than expected, and displayed the message “Please wait for a moment while we process your request” constantly. This is fixed, and the search results now appear faster than before.
- The VM Scan list now loads faster than before for a non-manager account.
- Improved performance when loading the Business Unit Information page and when loading and saving the Edit Business Unit page.

- Changed the screen text for Assets > Setup > Host Attributes since custom host attribute names only appear in Host Information.
- For Enterprise users, the Change Password window will now appear first and then after re-login the Customer Notice to enable the New Data Security Model window will appear.
- Unsupported browsers now display the following text “The browser you are using is not supported. Some critical security features are not available for your browser version”.
- Now when you get details of a scheduled scan through the API, the response does not truncate the tag names.
- If you filter assets by using tracking_method=IP in API request when all your assets are tracked by IPs, the tracking method for all assets now correctly displays as IP.
- The Subscription API now exports only the Excluded IP’s History which is in the Excluded IPs table.
- We have updated the API User Guide (v2) with more examples on Creating Unix records with Private Keys.
- Updated the online help for Cisco authentication. Added to the list of commands that the user account provided for authentication must be able to run.
- Updated the Cisco authentication help to clarify that the “enable” password is only supported for compliance scans.