Qualys PC/SCAP Auditor

Getting Started Guide

November 15, 2017

Copyright 2011-2017 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

Qualys, Inc.
919 E Hillsdale Blvd
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

Welcome 4

Set Up Policies 6

What do I need to get started? 6
How to import a policy from the library 6
How to create a policy with SCAP 1.2 content 7
How to create a policy with SCAP 1.1/1.0 content 8
How to create a policy with OVAL content 9

Start Scanning 10

What do I need to get started? 10
How to start a scan 10
Tell me about scan results 12
How to verify that authentication worked 13
How to schedule your scans 13

Reporting 14

SCAP Scorecard Report 14
SCAP Policy XML Report 15
SCAP Policy CSV Report 15
Rule Pass/Fail Report 16
Individual Host Report 18
SCAP ARF Report 20

Contact Support 20

Welcome

Welcome to Qualys SCAP Auditor, the cloud-based computing solution for Security Content Automation Protocol (SCAP) compliance. SCAP requires federal agencies to standardize the configuration of computer systems to strengthen IT security. This user guide will walk you through completing your first SCAP scans and creating reports showing your SCAP compliance.

Qualys SCAP Auditor 1.2

Qualys SCAP Auditor 1.2 is a subscription based, Software as a Service solution delivered via Qualys Policy Compliance 8.x and the Qualys Cloud Platform. The SCAP features are versioned independently from other services available via the Qualys portal. Changes to the Qualys SCAP Auditor version number will indicate changes related to SCAP scanning. Qualys SCAP Auditor 1.2 supports USGCB scanning for internal systems on a global scale.

For more information about Qualys SCAP Auditor 1.2, please visit the following site:

https://www.qualys.com/solutions/compliance/scap/

Tell me about availability

The SCAP application must be enabled for your account. Not sure if it's enabled? Go to Help > Account Info and see if there's a SCAP Summary section. If yes, then SCAP is turned on.

You'll also need compliance management permissions. All Managers and Auditors have this permission. For sub-users, a Manager can grant you the "Manage PC module" permission by editing your user account.

SCAP compliance

Compliant with SCAP version 1.2: XCCDF 1.2, OVAL 5.10, CCE 5, CPE 2.3, CVE, and CVSS 2, OCIL 2.0, CCSS 1.0, Asset Identification 1.1, ARF 1.1, TMSAD 1.0

Compliant with SCAP version 1.0/1.1: XCCDF 1.1.4, OVAL 5.3, CCE 5,CPE 2.2, CVE, and CVSS 2

SCAP 1.2 conformance

Our SCAP application conforms with requirements in the SCAP 1.2 specification for the use case compliance checking (with the @use-case attribute in the <ds:data-stream> element set to CONFIGURATION). We are a consumer of SCAP content, meaning we accept existing SCAP source data stream content, process it, and produce valid SCAP result data streams.

SCAP 1.2 certification

Authenticated Configuration Scanner with the CVE option for assessment of Windows 7 (32 and 64 bit) and Red Hat Enterprise Linux (RHEL) 5 Desktop (32 and 64 bit) providing the ability to audit and assess a target system to determine its compliance with USGCB requirements.

Backward compatibility

SCAP Auditor 1.2 provides backward compatibility with SCAP 1.0 for assessment of Windows XP and Windows Vista supporting USGCB and FDCC assessment. We are certified for these capabilities for SCAP 1.0: FDCC Scanner, Authenticated Configuration Scanner, Authenticated Vulnerability and Patch Scanner, and Unauthenticated Vulnerability Scanner.

Additional assessment capabilities

In addition to the SCAP certified assessment capabilities, SCAP Auditor can process SCAP tier III content intended for the following systems: Windows 7 (32 and 64 bit), Windows XP (32 bit), Windows Vista, Windows 2008, Windows 2012, RHEL 5 (32 and 64 bit) and most Linux distributions.

Where can I learn more?

Please refer to "Statement of SCAP Compliance" in the online help. Log in to the Qualys user interface, go to Help > Online Help and use the Search feature to find this help file.

Set Up Policies

We provide pre-defined SCAP policies that are compliant with SCAP requirements 1.0 or 1.2. You can easily import one of these policies from our SCAP Policy Library. All SCAP policies in the library have been validated by the NIST standards. Also you can create a custom policy by uploading your own SCAP or OVAL content.

What do I need to get started?

Compliance hosts in your account

Make sure the hosts you want to check for compliance are defined in your account as Compliance Hosts. Go to PC > Assets > Host Assets and you'll see the compliance hosts (IP addresses) already in your account. You can add compliance hosts (up to the limit for your license) by selecting New > IP Tracked Hosts.

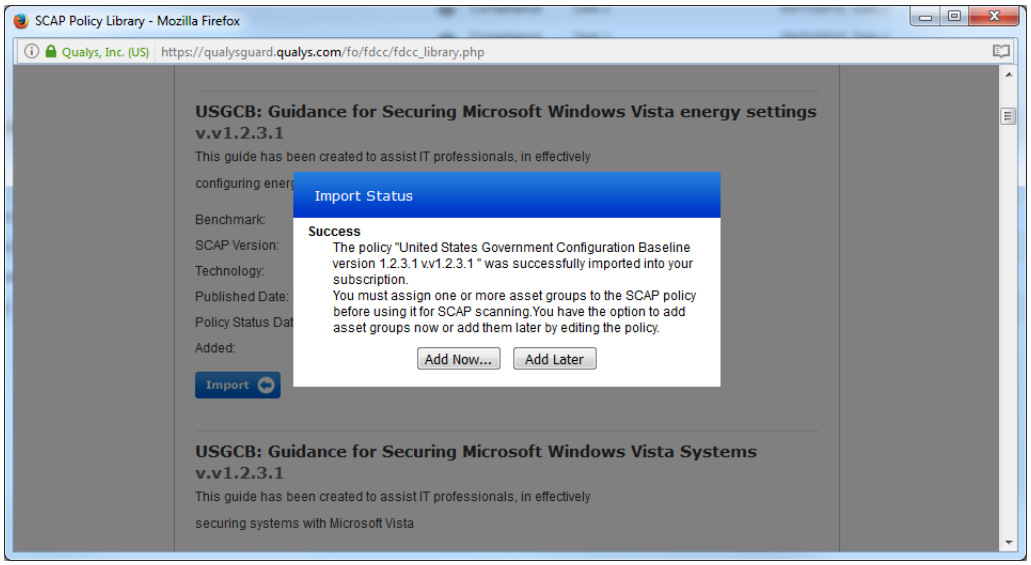
Asset groups with compliance hosts

When you import or create a policy, you'll need to assign asset groups to the policy. The asset groups include the compliance hosts you want to scan against the policy. Go to Assets > Asset Groups > New > Asset Group to add one.

How to import a policy from the library

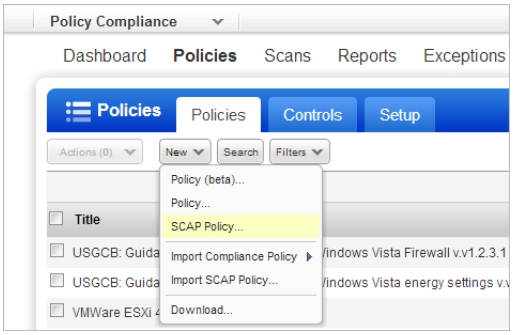
Go to PC > Policies and select New > Import SCAP Policy. Then click the Import button for the SCAP policy you want.

An import status appears like this and we recommend you assign assets now. Be sure to assign asset groups with relevant hosts (for example, add Windows 7 hosts to a Windows 7 policy).

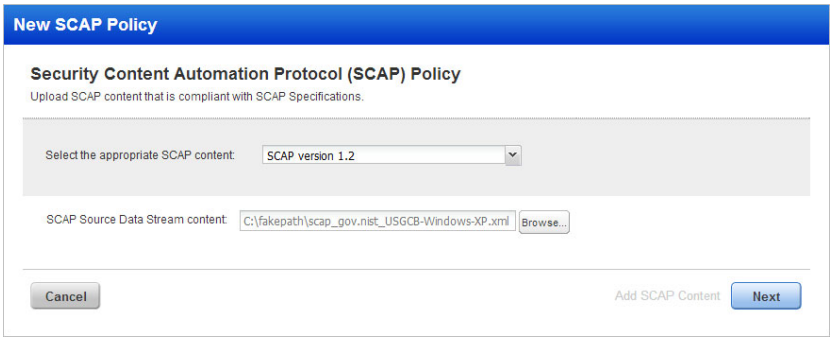


How to create a policy with SCAP 1.2 content

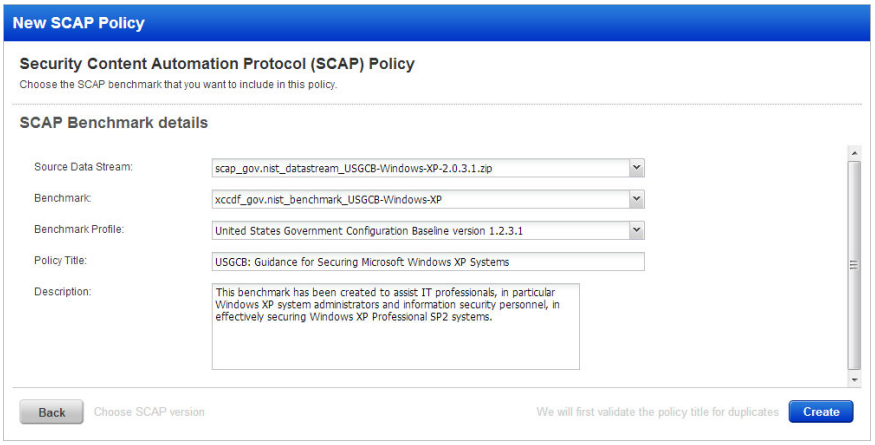
Go to PC > Policies and select New > SCAP Policy.



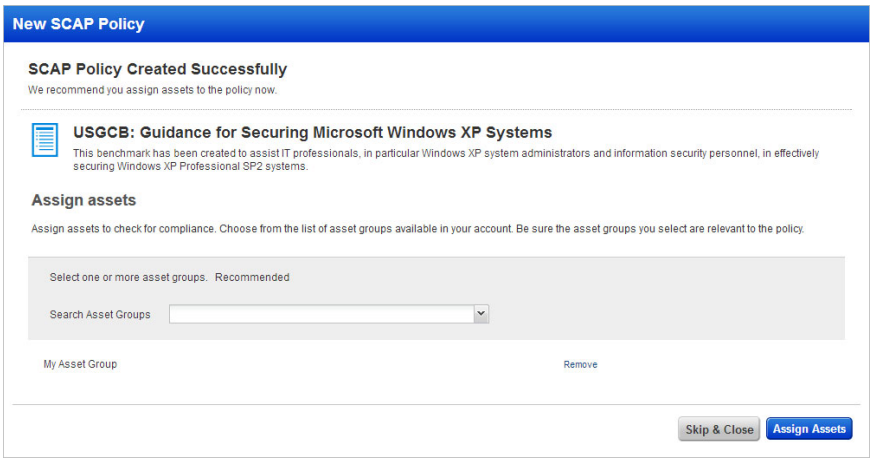
Select the option "SCAP version 1.2" and browse to the data stream collection file. Click Next.



We'll perform schema validation. Any errors will be reported online and must be resolved to continue. Upon successful validation, you'll see SCAP benchmark details. Use the drop-downs to select the source data stream ID, the benchmark ID and the profile title (which corresponds to the profile ID) intended for evaluation. Important - Once you save the policy, you cannot modify these selections. You can, however, create new policies with different selections. Click Create to add the policy to your account.



As stated earlier, you'll need to assign assets to your policy if you want to scan against it. We recommend you do this now. After selecting asset groups click Assign Assets.

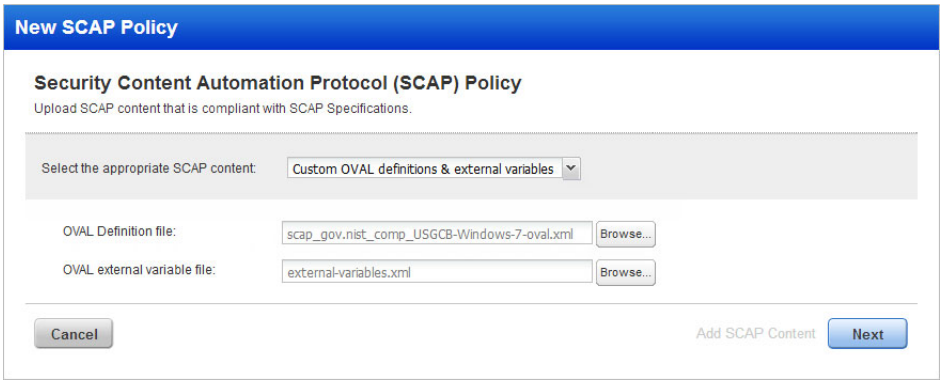


How to create a policy with SCAP 1.1/1.0 content

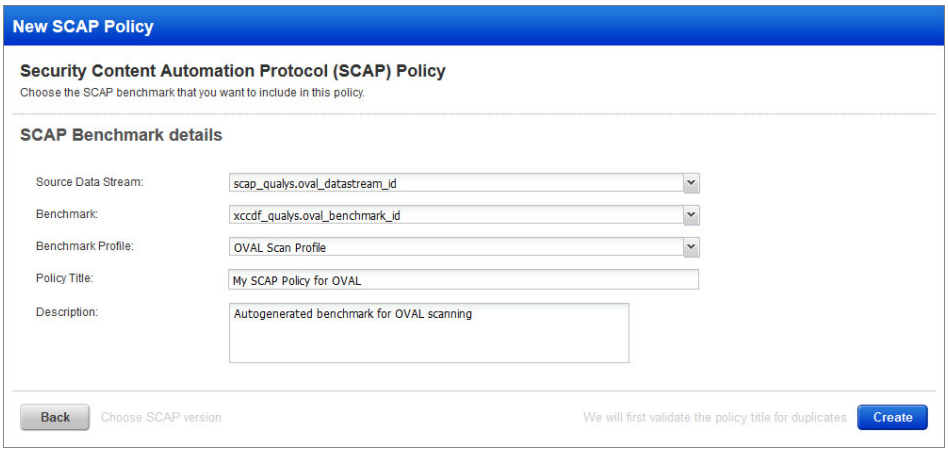
The steps are similar to version 1.2 described above. In this case, you'll select the option "SCAP version 1.1/1.0" in the New SCAP Policy window. Then select the XCCDF content file plus additional data files. Click Next and we'll perform schema validation. Please resolve any content errors reported online. Once you pass schema validation, select a SCAP benchmark - you can customize the details if you want. Click Create to save your new policy. Next assign assets to your policy and you'll be ready to scan.

How to create a policy with OVAL content

To create a SCAP policy with OVAL content, you'll select the option "Custom OVAL definitions & external variables" in the New SCAP Policy window. Then select content to be uploaded - an OVAL definition file and optionally an OVAL external variable file. Click Next.



The benchmark is automatically generated for your policy. The policy will be added to your account with the type OVAL once you click Create.



Next assign assets to your policy and you'll be ready to scan.

Start Scanning

SCAP Scanning analyzes the SCAP compliance of hosts on your network. When you launch SCAP scans, the service safely and accurately measures compliance against a SCAP policy using its Inference-Based Scanning Engine, an adaptive process that intelligently runs only tests applicable to each host scanned.

What do I need to get started?

Scanner Appliance enabled for SCAP scanning

The SCAP option must be enabled on a scanner appliance to support SCAP scanning.

Check the appliance software version - The scanner appliance must be running software version 2.4 or later. You'll find the version number in your account by going to the appliances list (Scans > Appliances) and viewing the appliance info (select the appliance, then select Info from the Quick Actions menu). You can also find the software version in the appliance user interface. On the main menu select VERSION INFO.

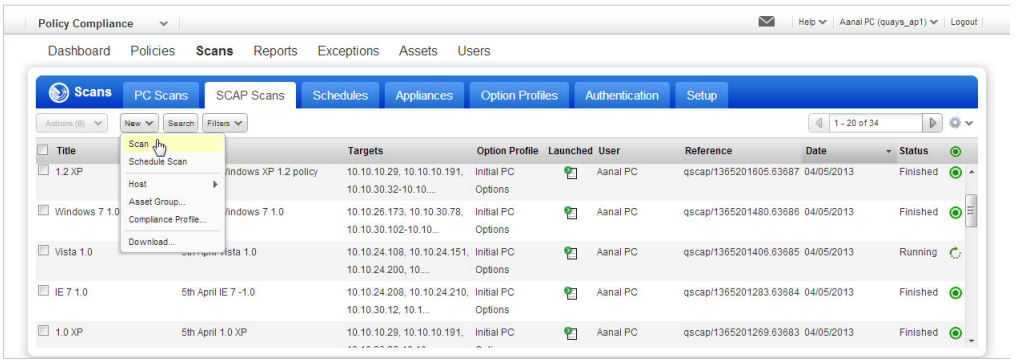
Edit the appliance settings - Go to PC > Scans > Appliances. Edit the appliance you want to use for SCAP scanning. Select the "Enable SCAP" option and then click Save.

Authentication records for your target hosts

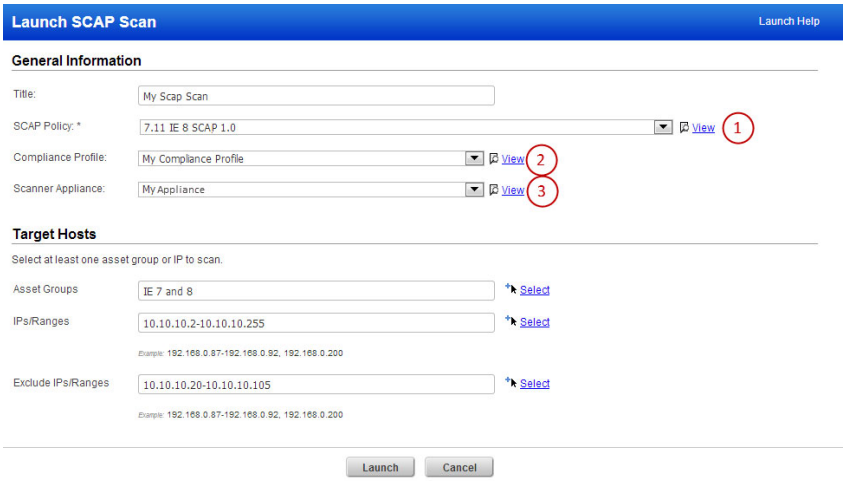
Authentication to hosts is required for SCAP scans using an account with Administrator rights. You'll want to add the credentials to be used for scanning in an authentication record. Go to PC > Scans > Authentication. Select New > Windows Record or New > Unix Record. You'll be prompted to enter your credentials and target hosts. Tip - Click the Launch Help link within the record for help with the settings.

How to start a scan

Go to PC > Scans > SCAP Scans and select New > Scan.



The Launch SCAP Scan wizard appears, prompting you to enter scan settings.



1. Select a SCAP policy to be evaluated by the scan. The menu lists all SCAP policies defined in your account. Click the View link to see the current settings for a selected policy.

2. Select a compliance profile to apply to this SCAP scan. Configuration settings defined in the compliance profile will affect your results. The menu is empty until you (or another user in the subscription) create a compliance profile.

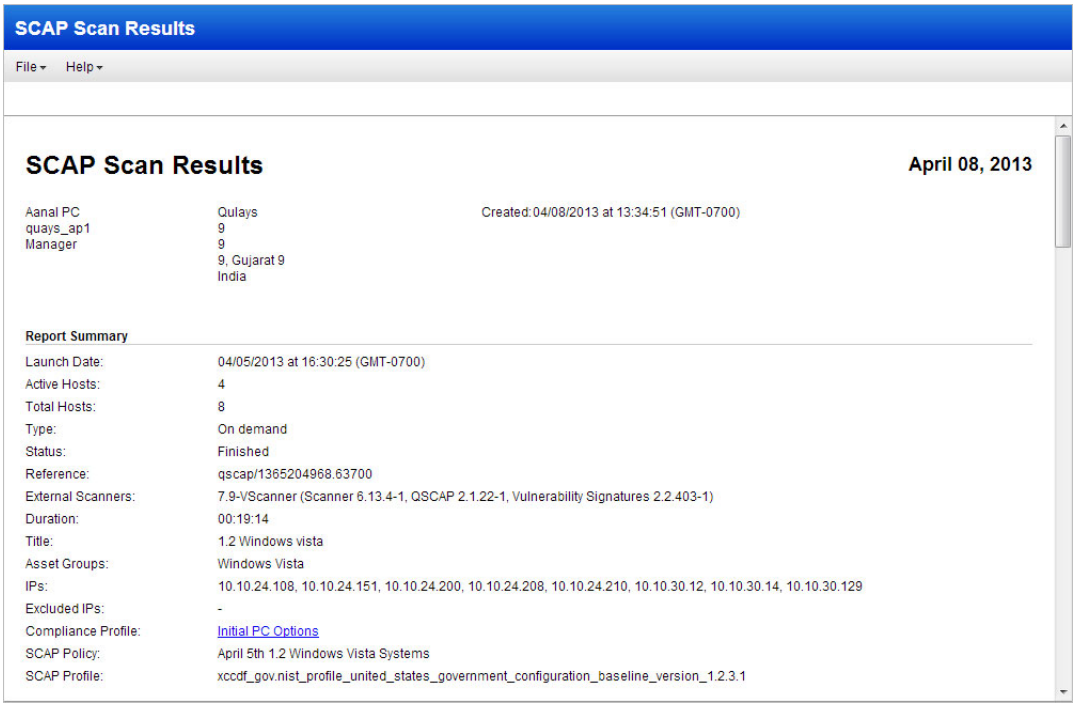
3. Select a scanner appliance that has been enabled for SCAP scanning.

Click the Launch button after entering information.

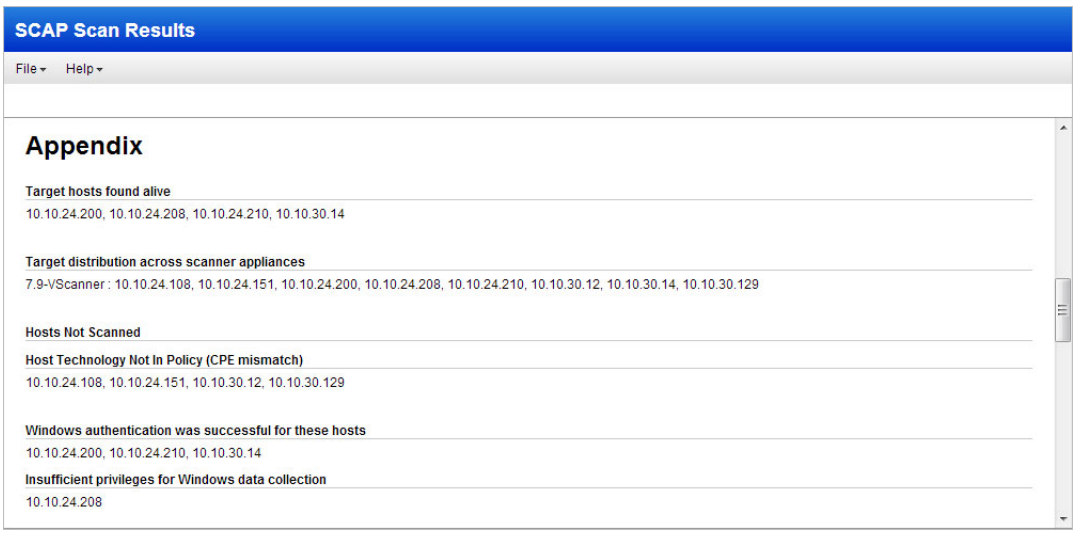
You can track the scan status on the SCAP Scans list. You will receive a scan summary email notification when the scan completes if this notification option is turned on in your account.

Tell me about scan results

Sample SCAP scan results are below.



You'll notice the Appendix includes: Hosts Scanned/Not Scanned, Host Technology Not in Policy (CPE mismatch), Hostname Not Found, Windows authentication was successful/not successful, and compliance profile settings.



Tips:

Once your scan is finished and scan results are processed, you can launch SCAP reports to determine whether hosts are compliant with a SCAP policy. Keep reading to learn how to launch SCAP compliance reports.

Tell me about "No data found". If you run a SCAP scan and it returns the status "Finished" with the message "No data found" it's most likely that authentication was not successful on the target hosts. Be sure to create authentication records for the systems you want to scan. Also check that the credentials in the records are current.

How to verify that authentication worked

We recommend you run the Authentication Report to determine whether authentication was successful for all of the target hosts. Authentication must be successful in order for us to evaluate each host for SCAP compliance. To run this report go to PC > Reports and select New > Compliance Report > Authentication Report.

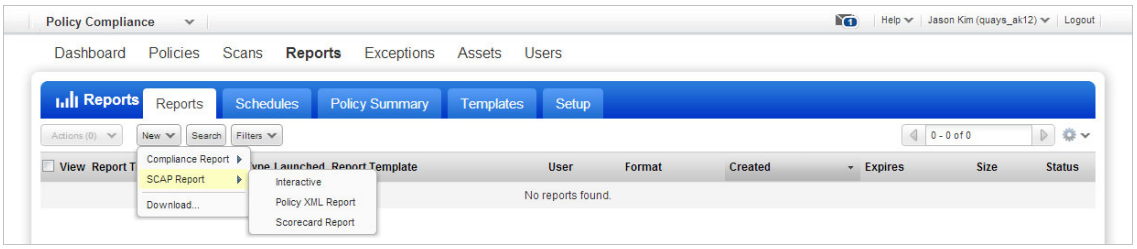
How to schedule your scans

By scheduling scans you'll get SCAP scan results on a regular basis (daily, weekly or monthly) and during a time window convenient for your organization. It's easy to schedule a scan. Just go to PC > Scans > Schedules and select New > Schedule Scan > SCAP.

Reporting

Specialized SCAP compliance reports provide the SCAP status of hosts in your account, based on the most recent SCAP scan results. These reports help you determine whether hosts are compliant with the SCAP policies in your account.

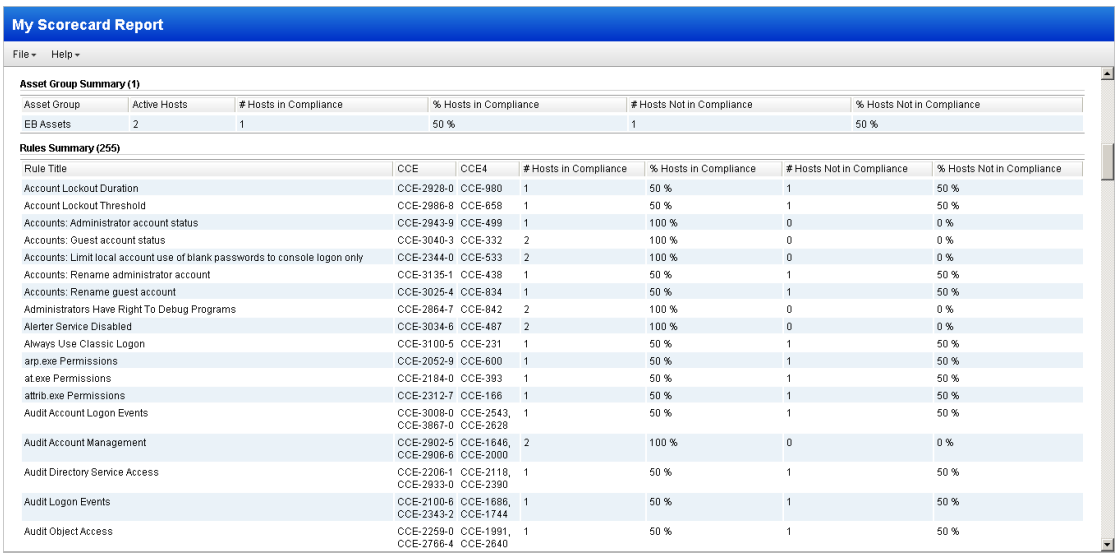
Go to PC > Reports to create new SCAP reports from the New menu (except the SCAP ARF report which is launched from the API). SCAP reports are described below.



SCAP Scorecard Report

The SCAP Scorecard Report gives you a high-level summary of the current SCAP compliance status of a SCAP policy in your account. To run this report go to PC > Reports, select New > SCAP Report > Scorecard Report, select settings and click Run.

Sample SCAP Scorecard Report:



My Scorecard Report

File Help

Asset Group Summary (1)

Asset Group	Active Hosts	# Hosts in Compliance	% Hosts in Compliance	# Hosts Not in Compliance	% Hosts Not in Compliance
EB Assets	2	1	50 %	1	50 %

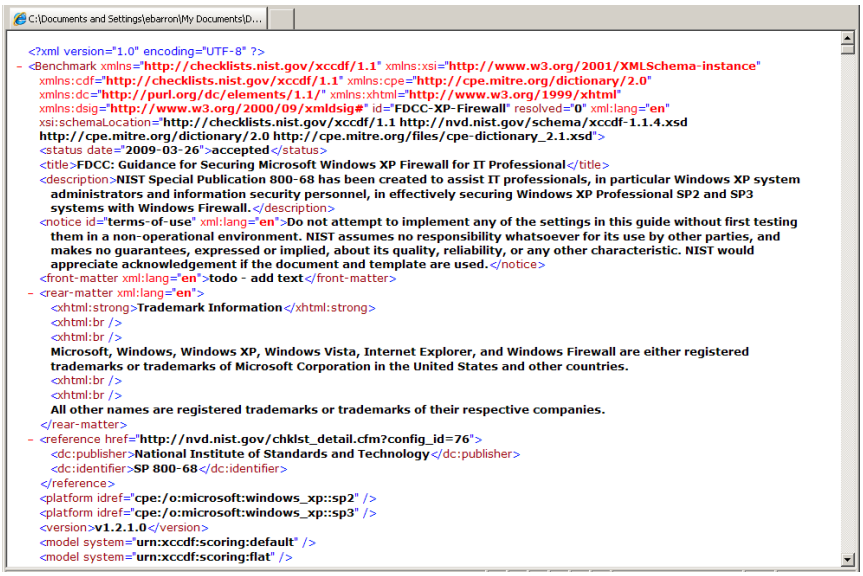
Rules Summary (255)

Rule Title	CCE	CCE4	# Hosts in Compliance	% Hosts in Compliance	# Hosts Not in Compliance	% Hosts Not in Compliance
Account Lockout Duration	CCE-2928-0	CCE-980	1	50 %	1	50 %
Account Lockout Threshold	CCE-2986-8	CCE-658	1	50 %	1	50 %
Accounts: Administrator account status	CCE-2943-9	CCE-499	1	100 %	0	0 %
Accounts: Guest account status	CCE-3040-3	CCE-332	2	100 %	0	0 %
Accounts: Limit local account use of blank passwords to console logon only	CCE-2344-0	CCE-533	2	100 %	0	0 %
Accounts: Rename administrator account	CCE-3135-1	CCE-438	1	50 %	1	50 %
Accounts: Rename guest account	CCE-3025-4	CCE-834	1	50 %	1	50 %
Administrators Have Right To Debug Programs	CCE-2864-7	CCE-842	2	100 %	0	0 %
Alerter Service Disabled	CCE-3034-6	CCE-487	2	100 %	0	0 %
Always Use Classic Logon	CCE-3100-5	CCE-231	1	50 %	1	50 %
arp.exe Permissions	CCE-2052-9	CCE-600	1	50 %	1	50 %
at.exe Permissions	CCE-2184-0	CCE-393	1	50 %	1	50 %
attrib.exe Permissions	CCE-2312-7	CCE-166	1	50 %	1	50 %
Audit Account Logon Events	CCE-3008-0 CCE-3867-0	CCE-2543, CCE-2628	1	50 %	1	50 %
Audit Account Management	CCE-2902-5 CCE-2906-6	CCE-1646, CCE-2000	2	100 %	0	0 %
Audit Directory Service Access	CCE-2206-1 CCE-2933-0	CCE-2118, CCE-2390	1	50 %	1	50 %
Audit Logon Events	CCE-2100-6 CCE-2343-2	CCE-1686, CCE-1744	1	50 %	1	50 %
Audit Object Access	CCE-2259-0 CCE-2766-4	CCE-1991, CCE-2640	1	50 %	1	50 %

SCAP Policy XML Report

The SCAP Policy XML Report determines an organization's compliance with the SCAP mandate for compliance hosts in a selected SCAP policy. To create this report go to PC > Reports and select New > SCAP Report > Policy Report, and choose the XCCDF TestResult (XML) format. Once you click Run we'll create your report and you'll see it in the reports list.

Sample SCAP Policy XML Report:

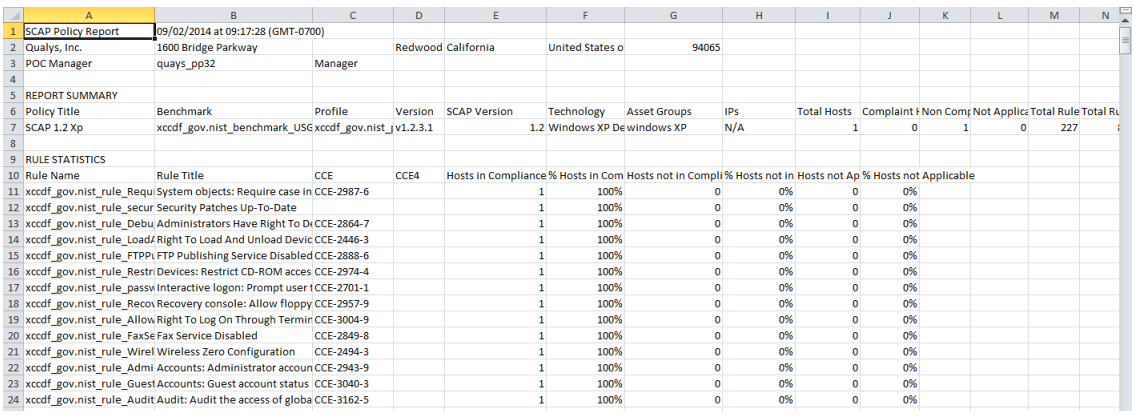


The areas of the XCCDF specification that have been constrained for use with the SCAP profile appear in <TestResult> elements and <rule-result> sub-elements.

SCAP Policy CSV Report

You can also run the SCAP Policy Report in CSV format. This allows you to import the data to external systems or to open the data in spreadsheet format. Simply choose the CSV format when running your report.

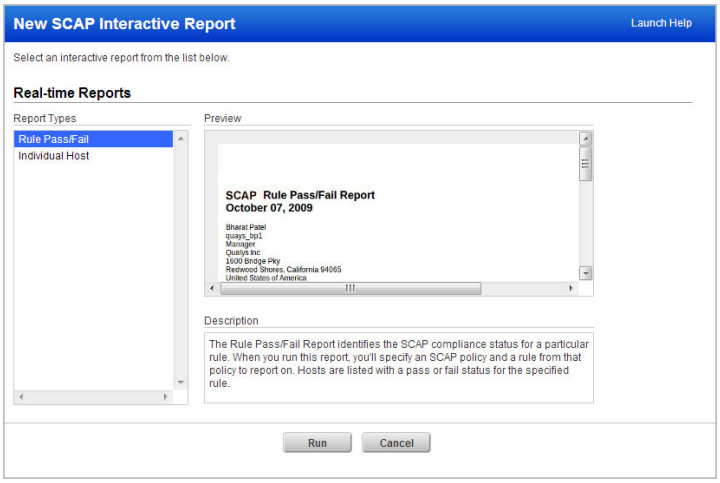
Sample SCAP Policy CSV Report:



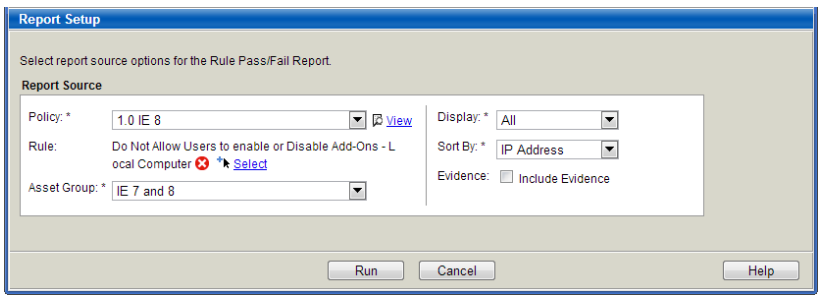
	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	SCAP Policy Report	09/02/2014 at 09:17:28 (GMT-0700)												
2	Qualys, Inc.	1600 Bridge Parkway		Redwood	California	United States o	94065							
3	POC Manager	quays_pp32	Manager											
4														
5	REPORT SUMMARY													
6	Policy Title	Benchmark	Profile	Version	SCAP Version	Technology	Asset Groups	IPs	Total Hosts	Complaint H	Non Comp	Not Applica	Total Rule	Total Ru
7	SCAP 1.2 Xp	xccdf_gov.nist_benchmark_USG	xccdf_gov.nist_p	v1.2.3.1	1.2	Windows XP De	windows XP	N/A	1	0	1	0	227	
8														
9	RULE STATISTICS													
10	Rule Name	Rule Title	CCE	CCE4	Hosts in Compliance	% Hosts in Com	Hosts not in Compli	% Hosts not in	Hosts not Ap	% Hosts not Applicable				
11	xccdf_gov.nist_rule_Requ	System objects: Require case in	CCE-2987-6		1	100%	0	0%	0	0%				
12	xccdf_gov.nist_rule_secur	Security Patches Up-To-Date			1	100%	0	0%	0	0%				
13	xccdf_gov.nist_rule_Debu	Administrators Have Right To D	CCE-2864-7		1	100%	0	0%	0	0%				
14	xccdf_gov.nist_rule_Load/	Right To Load And Unload Devic	CCE-2446-3		1	100%	0	0%	0	0%				
15	xccdf_gov.nist_rule_FTPP(	FTP Publishing Service Disabled	CCE-2888-6		1	100%	0	0%	0	0%				
16	xccdf_gov.nist_rule_Restr	Devices: Restrict CD-ROM acces	CCE-2974-4		1	100%	0	0%	0	0%				
17	xccdf_gov.nist_rule_passw	Interactive logon: Prompt user t	CCE-2701-1		1	100%	0	0%	0	0%				
18	xccdf_gov.nist_rule_Reco	Recovery console: Allow floppy	CCE-2957-9		1	100%	0	0%	0	0%				
19	xccdf_gov.nist_rule_Allow	Right To Log On Through Termir	CCE-3004-9		1	100%	0	0%	0	0%				
20	xccdf_gov.nist_rule_FaxSe	Fax Service Disabled	CCE-2849-8		1	100%	0	0%	0	0%				
21	xccdf_gov.nist_rule_Wirel	Wireless Zero Configuration	CCE-2494-3		1	100%	0	0%	0	0%				
22	xccdf_gov.nist_rule_Admi	Accounts: Administrator accoun	CCE-2943-9		1	100%	0	0%	0	0%				
23	xccdf_gov.nist_rule_Guest	Accounts: Guest account status	CCE-3040-3		1	100%	0	0%	0	0%				
24	xccdf_gov.nist_rule_Audit	Audit: Audit the access of globa	CCE-3162-5		1	100%	0	0%	0	0%				

Rule Pass/Fail Report

The Rule Pass/Fail Report identifies the SCAP compliance status for a particular rule. When you run this report, you'll specify a SCAP policy and a rule from that policy to report on. Go to PC > Reports, select New > SCAP Report > Interactive > Rule Pass/Fail and click Run.



The report setup window prompts you to select report settings. Once you click Run the completed report appears in the same window.



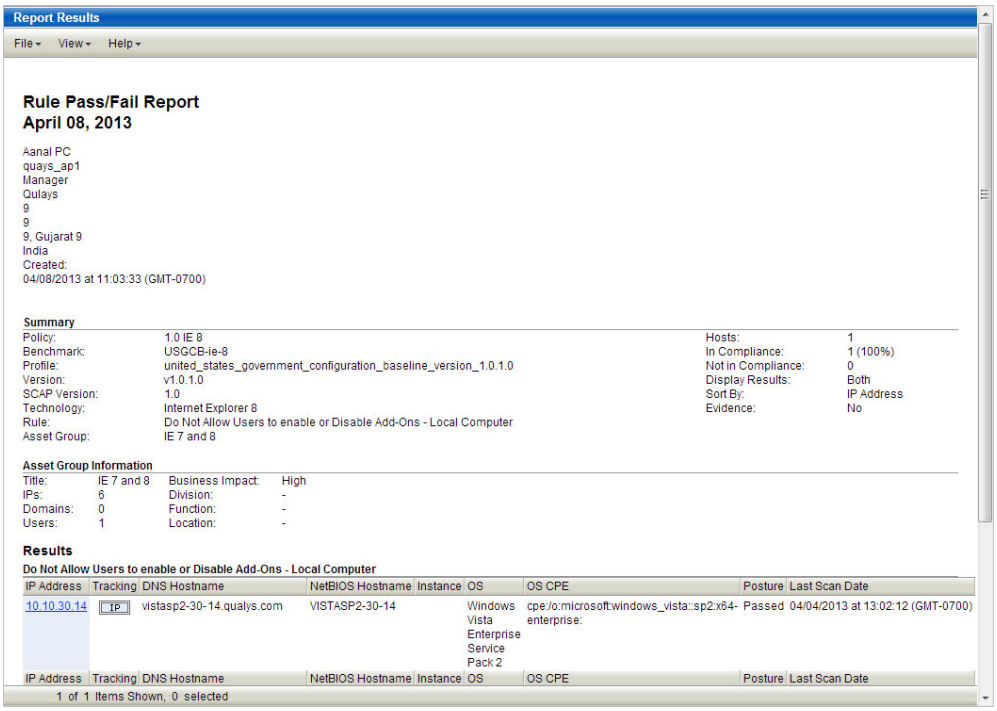
Tips:

Use the Display option to filter the hosts displayed in the report based on posture. You have these options: Passed (Fixed), Failed (includes Error and Unknown) or Ignored (includes Not Applicable, Not Checked, Not Selected and Informational).

You can modify the report settings to change the report output in real-time. Go to View > Setup Pane from within the report. Modify the settings and click Run to update the results.

Interactive reports are not saved to your reports list. You can download and print the report from the File menu within your report.

Sample Rule Pass/Fail Report:



Each host in the report is listed on a separate line with the posture for the selected rule.

How is posture determined?

Our service evaluates the test results for all the nodes (definitions and test sections) according to the rule and determines whether the host satisfied the conditions of the rule.

Passed - The test results for all the nodes satisfied the conditions of the rule.

Failed - In a case where the evidence has a node with the result Error or Unknown, our service will assign the posture Failed since the host did not satisfy the conditions of the rule. If the result is Error, you'll see Failed (Error). If the result is Unknown, you'll see Failed (Unknown).

A rule is ignored if you see one of these postures: Not Applicable, Not Checked, Not Selected or Informational. Not Checked indicates that the rule refers to checks in checking systems other than OVAL. This includes OCIL checks.

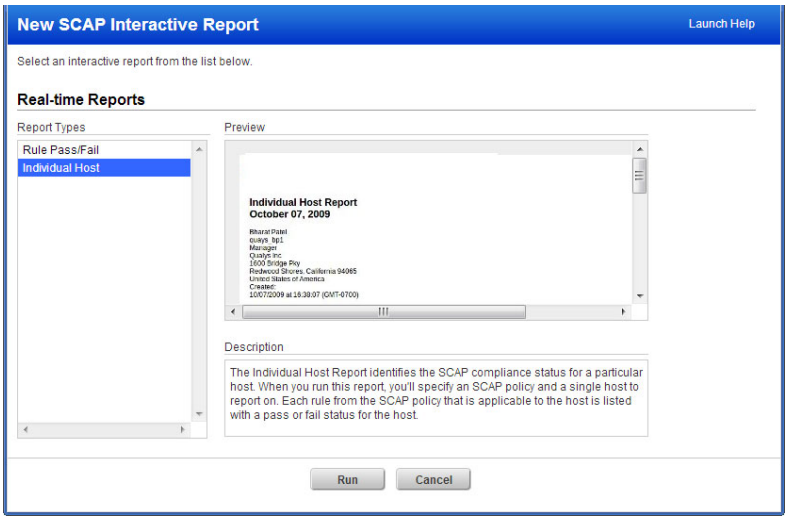
How do I find the Patches Report?

The rule titled "Security Patches Up-To-Date" provides evidence for special patches tested during the most recent SCAP scan of each host in the SCAP policy. These include all patches defined in the "patches" file in the SCAP policy when present. For each host you'll see the patch status. The status Pass indicates the patch was found during the last SCAP scan on the host, and the status Fail (in Red) indicates the patch was not found during the last SCAP scan on the host.

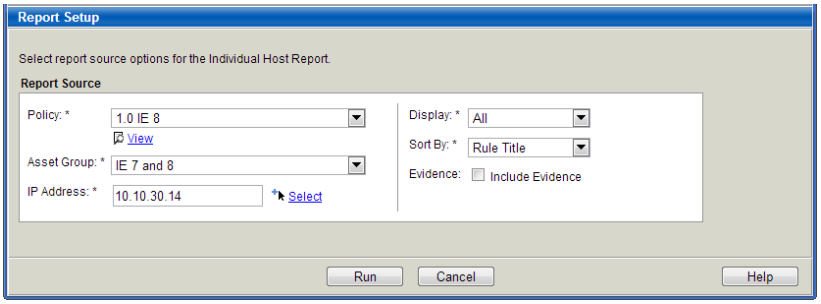
Individual Host Report

The Individual Host Report identifies the SCAP compliance status for a particular host. When you run this report, you'll specify a SCAP policy and a single host to report on.

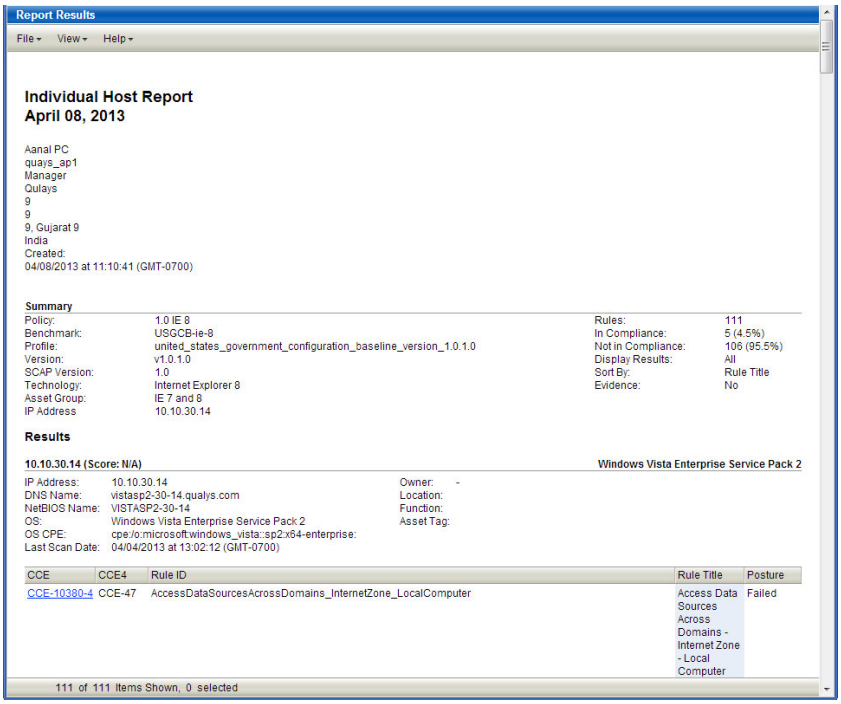
Go to PC > Reports, select New > SCAP Report > Interactive > Individual Host and click Run.



The report setup window prompts you to select report settings.



Sample Individual Host Report:



Each rule from the SCAP policy that is applicable to the host is listed with the posture and posture evidence when included.

Interested in OVAL definitions?

If you ran your report on a policy with custom OVAL definitions, you can go to File > Download to download the OVAL definitions in XML format.

SCAP ARF Report

You can launch a SCAP scan report in Asset Reporting Format (ARF) using our API, a requirement in the SCAP 1.2 specifications from NIST.

How do I launch this report?

Use the SCAP ARF Report API v2 (the resource /api/2.0/fo/compliance/scap/arf/). You'll need to provide the scan ID for a finished SCAP scan and optionally IPs if you want to limit the report to certain IP addresses only.

Not sure how to find the scan ID? You'll see the scan ID when viewing SCAP scan results in the user interface. In the scan results window's title bar you'll see the report URL with its ID number in the "id" parameter, like this:

https://quaysguard.qualys.com/fo/report/fdcc/fdcc_scan_result.php?id=3362251

API Request

Here's a sample API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X POST -d
"scan_id=3362251&ips=10.10.10.1-10.10.10.10"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/scap/arf/"
```

https://qualysapi.qualys.com is the API server URL for US Platform 1. If your account is located on one of our other cloud platforms then you'll want to replace this base URL with the one that is appropriate for your location. For example, for US Platform 2, use https://qualysapi.qg2.apps.qualys.com. For the EU Platform, use https://qualysapi.qualys.eu. If you have an @Customer platform, use a URL like https://qualysapi.<customer_base_url>.

XML Output

The XML output is compliant with the ARF 1.1 Schema. Show me the Schema

Where can I learn more about using the API?

Refer to the API V2 User Guide for a better understanding of API conventions and detailed instructions on using API functions. Get the latest from the Community. Go to the Community

Contact Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access online support information at www.qualys.com/support/.