

# Security Configuration Assessment (SCA)

# **Getting Started Guide**

Security Configuration Assessment (SCA) is a lightweight cloud service which can quickly perform the configuration assessment of the IT assets, and centrally track compliance status of all your assets on basis of the Center for Internet Security (CIS) hardening benchmarks.

It not only helps in continuously improving your configuration posture as per the latest CIS benchmarks but also helps in comparing the configuration posture in terms of various Industry standards like PCI-DSS, HIPAA, NIST and many more.

## Why SCA?

Security configuration setting is an element of a software's security that can be altered through the software itself. For example, an operating system offering access control lists that set the privileges that users have for files, and an application offering a setting to enable or disable the encryption of sensitive data stored by the application. A security configuration vulnerability involves the use of misconfigured security settings that could negatively impact security of the software.

A good security configuration program like SCA would make it difficult for an attacker to exploit such configuration vulnerabilities.

## Add assets to SCA

You can add the assets to SCA to track compliance status on. The host-scanning mechanism for SCA scans remote hosts and also auto discovers instances in case of instance-based technologies.

Go to Assets > Host Assets. From the New menu, select IP Tracked Hosts, DNS Tracked Hosts or NetBIOS Tracked Hosts. The tracking method you choose will be assigned to all of the hosts being added. Review the number of hosts you can add, enter the new IPs/ranges, and click Add.

Qualys. Express					
Security Configu	ration Assess	ment	~		_
Dashboard	Policies	Scans	Reports	Assets	Us
== Assets	Asset Gro	oups	Host Assets	Asset	Searc
Actions (0) 🛛 🗸	New 🗸 Searc	ch Filters	🖌 🗌 🖉 Disp	lay Comment	s
Info Tracking	IP Tracked Hos DNS Tracked H NetBIOS Track	sts Hosts ed Hosts	)		_
□ 🔏	Remove IPs				
□ 🔎	Export All				
□ 🔎	Download				
	10.10.26.10-10	.10.26.255			

Looks like you have assets in VM app. Do you want to add these assets?



Using our revolutionary Qualys Cloud Agent platform you can deploy lightweight cloud agents to continuously assess your infrastructure for security and compliance.

What are the steps Navigate to the Cloud Agent (CA) app and install the Cloud Agent in minutes.

Refer to Qualys Cloud Agent Getting Started Guide.

### Import and Build CIS Policy

Our out of the box CIS policies have controls pre-configured as per recommendations from the CIS and policy controls are optimized for performance, scalability, error handling and default conditions. You can customize values of the CIS checks as per your organization's security policies or even enable/disable certain CIS checks for reporting.

Simply go to Policies > Policies > New > Import CIS Policy. Click on the policy you want and then click Next. Follow the wizard to give your policy a name and click Create. Imported policy is Active by default.



You can choose to show or hide individual controls in reports by activating or inactivating them from the Policy Editor.

Policy E	dito	ог				Turn help	p tips: On   Off	Launch Help
Control	<b>IS</b> erview	1			Search this policy			Y
< >	1	Mana	igemei	nt Plane - Local Authentication, Aut	horization and Accounting (AAA) R	ules		Controls 11
							4 1 - 11 of 11	
	Refe	erence #	CID	Statement	Te	chnologies		
1.1	0	1.1.1	4357	Status of the 'aaa new-model' configuration	command on the device	1	Edit   Ina	activate
1.2	0	1.1.2	4358	Status of the 'aaa authentication login' config	guration command on the device	1	Edit     Ina	ectivate
1.3	ο	1.1.3	4359	Status of the 'aaa authentication enable' cor	figuration command on the device	1	Edit     Ina	ectivate

#### Start collecting configuration data

Scan your hosts to check the compliance of your systems against your CIS policies. Your SCA scans and collects the data as required by the CIS policy, then the Qualys Cloud Platform analyzes and correlates it.

Before you start the scan:

- Add authentication records for your assets (Windows, Unix, etc).
- Use the option profile with recommended settings provided by Qualys (Compliance Profile) or create a new profile and customize the settings.
- Configure a physical scanner or virtual appliance, or scan remotely using Qualys scanner appliances.

It's simple to start your scan. Go to Scans > New > Scan, and tell us which IPs to scan, which scan options to use, and which scanner is right for the job (if you have scanner appliances that is).

Launch Compli	iance Scan Turn help tips: On   Off Launch He
General Informat	ion
Give your scan a name, visible.	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
Title:	Apache Tomcat
Compliance Profile:	Apache Tomcat 7
Scanner Appliance:	Scanner Appliance not available
Choose Target He	osts from
Tell us which hosts (IP	' addresses) you want to scan.
Assets	Tags
Asset Groups	Apache Tomcat 7.0. × × • Select
IPs/Ranges	*N Select
	Example: 192.168.0.87-192.168.0.92, 192.168.0.200
Exclude IPs/Ranges	*k <u>Select</u>
	Example: 192,186.0.87-192,188.0.92, 192,188.0.200
Notification	
Send notification whe	en this scan is finished
	Launch Cancel

#### **Generate Report**

Your SCA report shows you up to date compliance posture against the CIS benchmarks, references to compliance standards (PCI-DSS, HIPAA, NIST and more), Qualys provided control criticality and remediation information.

Go to Reports > Reports > New and select either Authentication Report or Policy Report. Define the format and source of your report and click Run.

You can also quickly generate reports from the scan list or policy list directly. Just choose a scan or policy from your list and click the icon for Run Report in the Generate Report column. 💽 Qualys. Express Security Configuration Assessment Reports Dashboard Policies Scans As III Reports Schedules Reports Templ Search Filters 🗸 Actions (0) 🛛 🗸 New 🗸 Authentication Report View Report Policy Report Ω Policy rep Download... Authentication report

Dashboard Policies Scans Reports Asset	ts Users					
Scans Scans Schedules Appliances	Option Profiles	Authentication Setu	ıp			
Actions (0) V New V Search Fitters V My Scans			4 1 - 20	) of 40	▶ * ◄	
Title •	Targets	Reference	Date	Status	Generate Report	t
Windows 10 20170803	10.10.36.98	compliance/1501796495.57828	08/04/2017	Finished		▶ ^
Windows 10	10.10.24.151, 10.10.36.98, 10.10.36.123, 10.1	compliance/1501798122.57835	08/04/2017	Finished	F	Þ
G Windows 10	10.10.36.98	compliance/1501791783.57821	08/04/2017	Canceled		

	Access Control Requirements			
ub-Category:	ory: Authentication/Passwords			
tal	al			
nai.	3			
issed.	0			
alled.	3			
TOF.	0			
oproved Excep	buons: U			
ending Except	ions: U			
indows Server	2012 R2			
10 10 10 86 /20	12r2dtr-10-86 2012P2DTP-10-86)	Failed		
-	Evaluati	Instance: c on date: 04/15/2017 at 14:36;17 (GMT-070		
OS: Last Scan Date: Tracking Method:	Evaluatis Windows Server 2012 R2 Datacenter 64 bit Edition 04/14/2017 at 13-24-48 (GMT-0700) IP	Instance: o on date: 04/15/2017 at 14:36:17 (GMT-07)		
OS: Last Scan Date: Tracking Method: Asset Tags: Windows 2012	Evaluativ Windows Server 2012 R2 Datacenter 64 bit Edition 04/14/2017 at 13:24:48 (GMT-0700) IP	Instance: c		
OS: Last Scan Date: Tracking Method: Asset Tags: Windows 2012 The following Into Settings/Security	Evaluatis Windows Server 2012 R2 Datacenter 64 bit Edition 04/14/2017 at 13:24:48 (GMT-0700) IP eger value X indicates the current status of the Minimum Password Age' (min_pass_age) wi Settings\Account Policies\Password PolicyMinimum password agesetting for local accounts	Instance: o on date: 04/15/2017 at 14:36:17 (GMT-07) thin the Computer Configuration/Windows		
OS: Last Scan Date: Tracking Method: Asset Tags: Windows 2012 The following Int Settings!Security Expected g	Evaluate Windows Server 2012 R2 Datacenter 64 bit Edition 04/14/2017 at 13:24:48 (GMT-0700) IP eger value X indicates the current status of the "Minimum Password Age" (min_pass_age) wi Settings/Account Policies/Password Policy/Minimum password agesetting for local accounts reater than or equal to	Instance: o on date: 04/15/2017 at 14:36:17 (GMT-07) thin the Computer Configuration/Windows b.		
OS: Last Scan Date: Tracking Method: Asset Tags: Windows 2012 The following lint Settings/Security Expected	Evaluate Windows Server 2012 R2 Datacenter 64 bit Edition 04/14/2017 at 13:24.48 (GMT-0700) IP seper value X indicates the current status of the 'Minimum Password Age' (min_pass_age) with Settings/Account Policies/Password Policy/Minimum password agesetting for local accounts reater than or equal to	Instance: o on date: 04/15/2017 at 14:36:17 (GMT-07) thin the Computer Configuration/Windows		
OS: Last Scan Date: Tracking Method: Asset Tags: Windows 2012 The following Inte Settings/Security Expected g 1 c	Evaluate Windows Server 2012 R2 Datacenter 64 bit Edition 04/14/2017 at 13:24:48 (GMT-0700) IP eger value X indicates the current status of the "Minimum Password Age" (min_pass_age) wi Settings/Account Policies/Password Policy/Minimum password agesetting for local accounts reater than or equal to IR, any of the selected values below: Attituite on found	Instance: o on date: 04/15/2017 at 14:36:17 (GMT-07) thin the Computer Configuration/Windows k		
OS: Last Scan Date: Tracking Method: Asset Tags: Windows 2012 The following Inte Settings1Security Expected 1 1 C	Evaluation  Windows Server 2012 R2 Datacenter 64 bit Edition  04/14/2017 at 13.24.48 (GMT-0700)  IP  seger value X indicates the current status of the 'Minimum Password Age' (min_pass_age) will settings/account Policies/Password Policy/Minimum password agesetting for local accounts  reater than or equal to  R, any of the selected values below:  Attribute not found Unable to retrieve password policy	Instance: o on date: 04/15/2017 at 14:36:17 (GMT-07) thin the Computer Configuration/Windows		

You can remediate the failed controls, per Qualys provided control criticality and the control remediation information.

We also show	compliance m	anning to star	idards like PCL	NIST	HIPPA etc.	in the report
	compliance in	apping to star	idalus like i ci,	TUDI,	1111 1 <i>1</i> 1, ctc.	in the report.

10167 Status of the Syste	em Integrity Protection security policy
Category:	OS Security Settings
Sub-Category:	System Settings (OSI layers 6-7)
Sub-Category:	Payment Card Industry Data Security Standard (PCI-DSS) v3.2 3.2§ 6.6 (For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks). NIST Cyber Security Framework (NIST CSF) 1.0§ PR.DS-6 (Integrity checking mechanisms are used to verify software, firmware, and information integrity). Health Insurance Portability and Accountability (HIPAA) Security Rule 45 CFR Parts 160/164, Subparts A/C: 1996§ 164.312(c)(1) (Integrity). Health Insurance Portability and Accountability (HIPAA) Security Rule 45 CFR Parts 160/164, Subparts A/C: 1996§ 164.312(c)(2) (Mechanism to authenticate electronic protected health information (Addressable)). Health Insurance Portability and Accountability (HIPAA) Security Rule 45 CFR Parts 160/164, Subparts A/C: 1996§ 164.312(c)(2) (Mechanism to authenticate electronic protected health information (Addressable)).
Control references:	Subparts A/C: 1996§ 164.312(e)(2)(i) (Integrity controls (Addressable)). This control is associated with the following documents: 5.18