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.

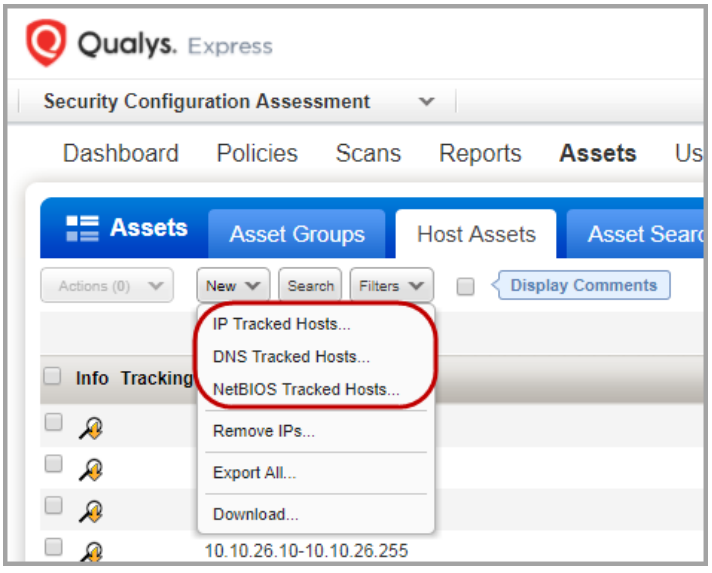
Why SCA?

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.

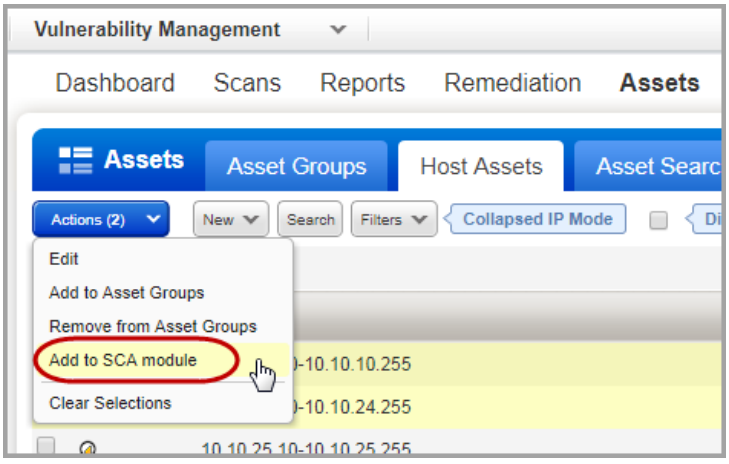
Add assets to SCA

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.



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



Simply, go to VM > Host Assets and select the assets you want to add to SCA.

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

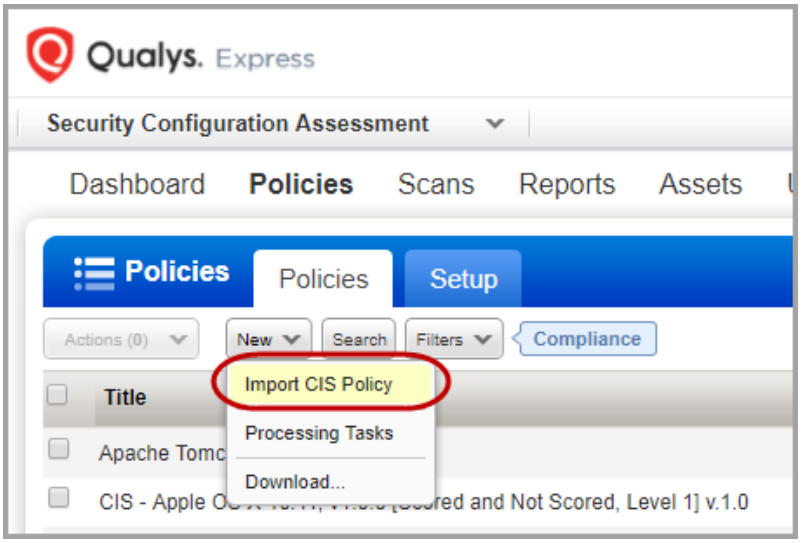
What are the steps Navigate to the Cloud Agent (CA) app and install the Cloud Agent in minutes.

Refer to Qualys Cloud Agent Getting Started Guide.

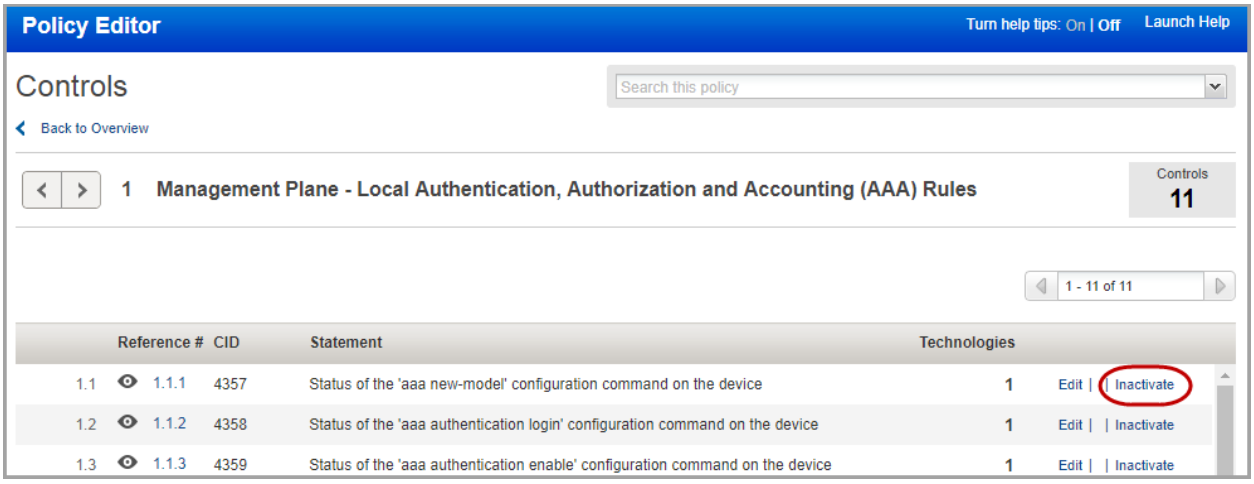
Import and Build CIS Policy

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.



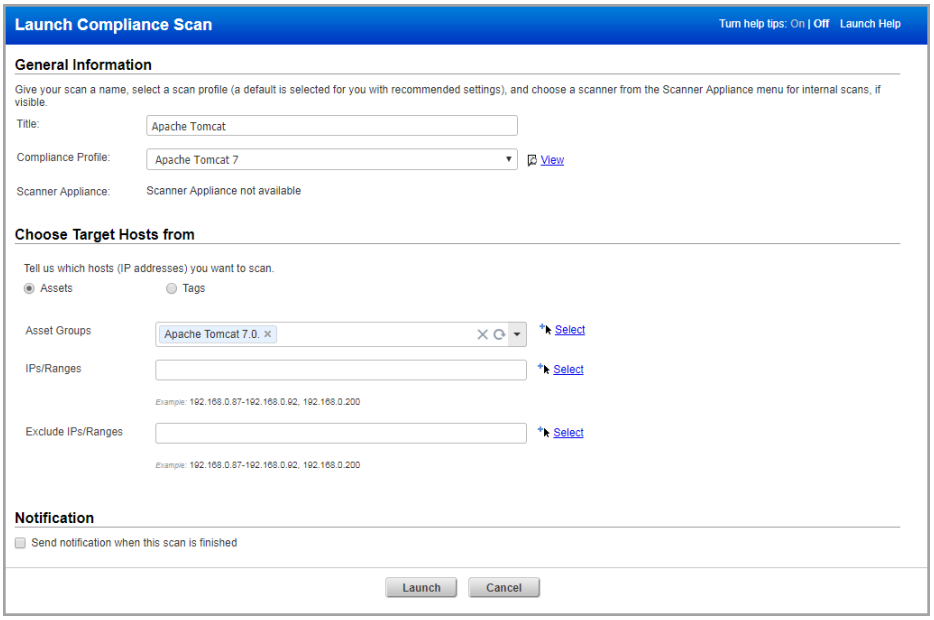
Start collecting configuration data

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).

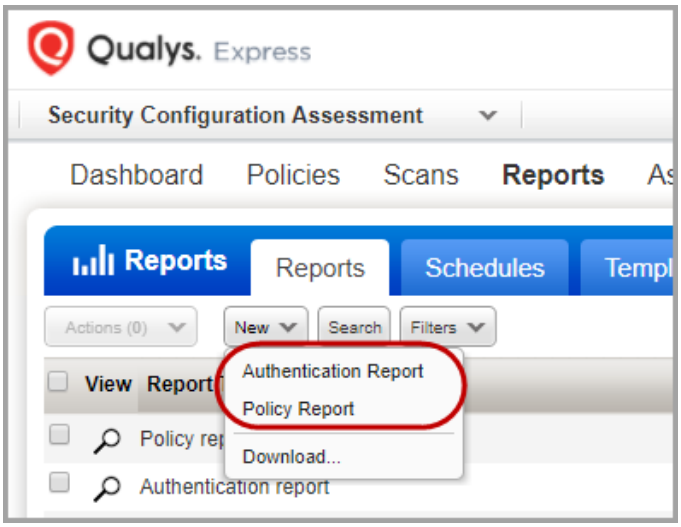


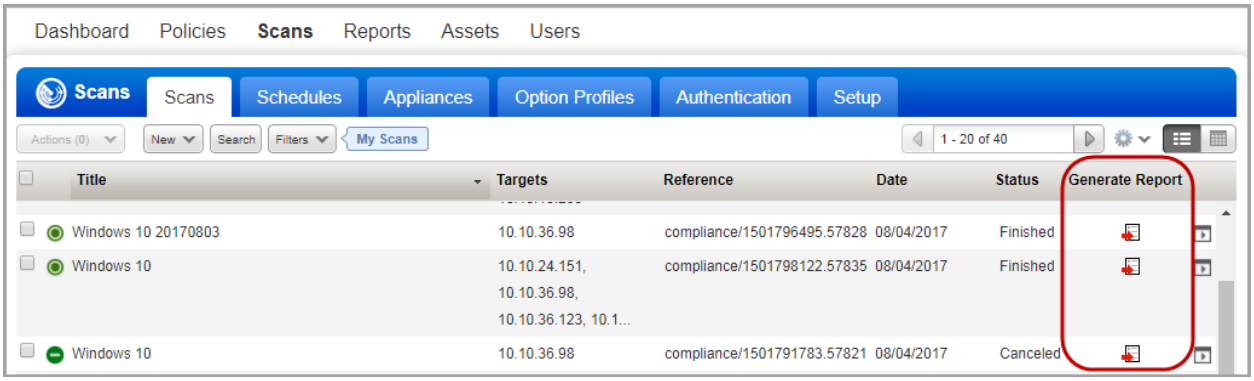
Generate Report

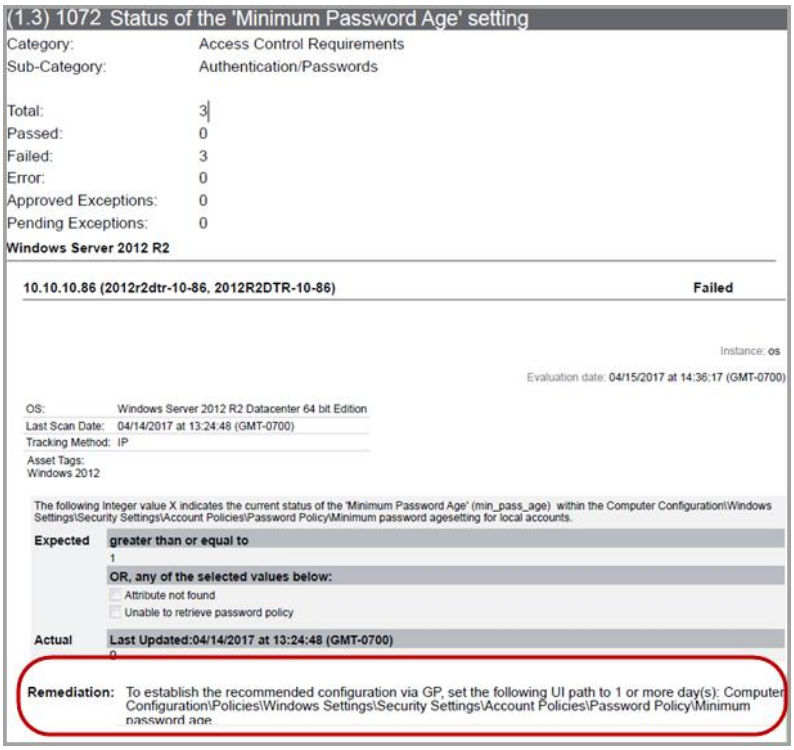
Your SCA report shows you up to date compliance posture against the CIS benchmarks, references to compliance standards (PCI-DSS, HIPAA, NIST and more), Qualys provided control criticality and remediation information.

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.

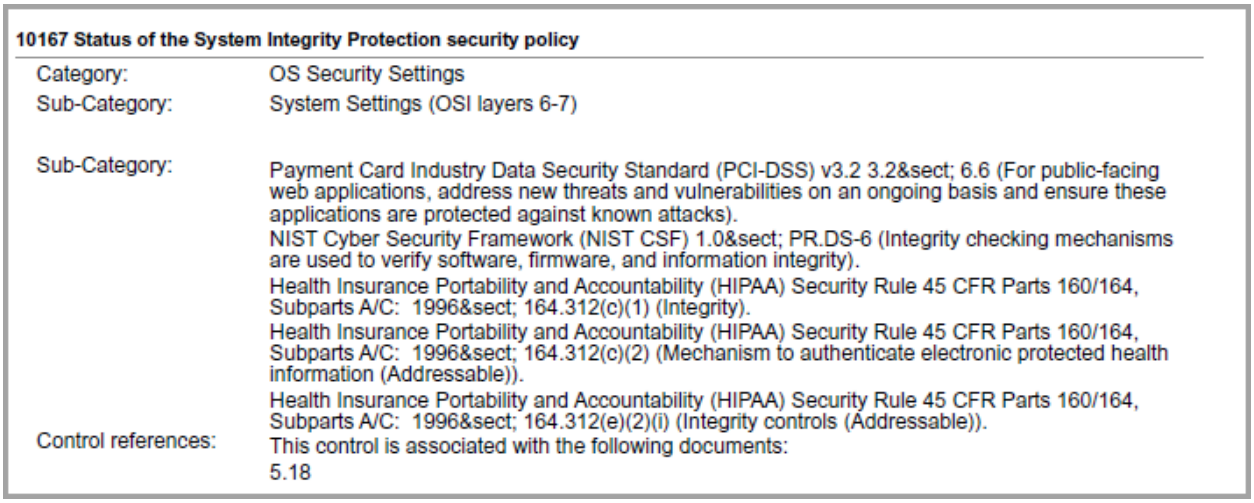






You can remediate the failed controls, per Qualys provided control criticality and the control remediation information.

We also show compliance mapping to standards like PCI, NIST, HIPPA, etc. in the report.



10167 Status of the System 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(e)(2)(i) (Integrity controls (Addressable)).
Control references:	This control is associated with the following documents: 5.18