Qualys®

Policy Compliance

Getting Started Guide

March 30, 2018

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

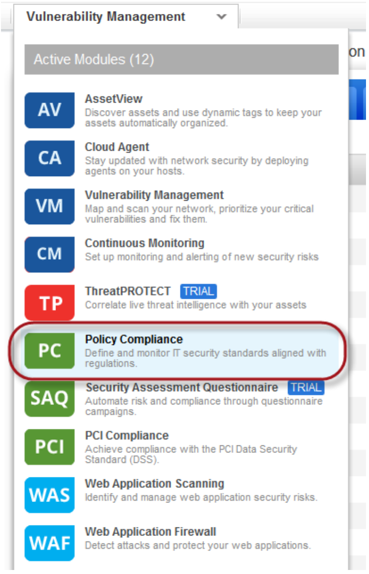
Table of Contents

Get Started

Welcome to Qualys Policy Compliance. We'll help you get started quickly so you can understand the compliance status of your host assets.

Policy Compliance is available in your account only when it is enabled for your subscription. If you would like to enable Policy Compliance for your account, please contact Technical Support or your Technical Account Manager.

Let's take a look now at the user interface. Log into your account and choose Policy Compliance from the application picker.



AV AssetView
Discover assets and use dynamic tags to keep your assets automatically organized.

CA Cloud Agent
Stay updated with network security by deploying agents on your hosts.

VM Vulnerability Management
Map and scan your network, prioritize your critical vulnerabilities and fix them.

CM Continuous Monitoring
Set up monitoring and alerting of new security risks

TP ThreatPROTECT TRIAL
Correlate live threat intelligence with your assets

PC Policy Compliance
Define and monitor IT security standards aligned with regulations.

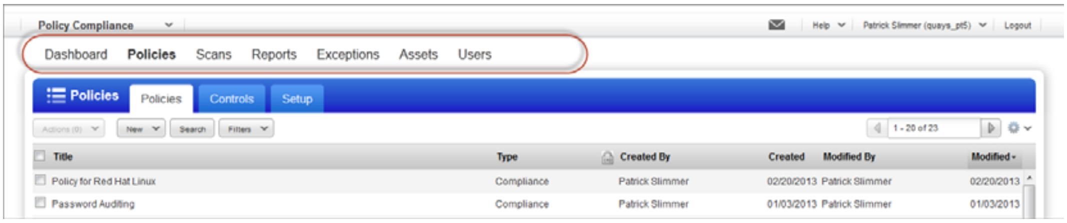
SAQ Security Assessment Questionnaire TRIAL
Automate risk and compliance through questionnaire campaigns.

PCI PCI Compliance
Achieve compliance with the PCI Data Security Standard (DSS).

WAS Web Application Scanning
Identify and manage web application security risks.

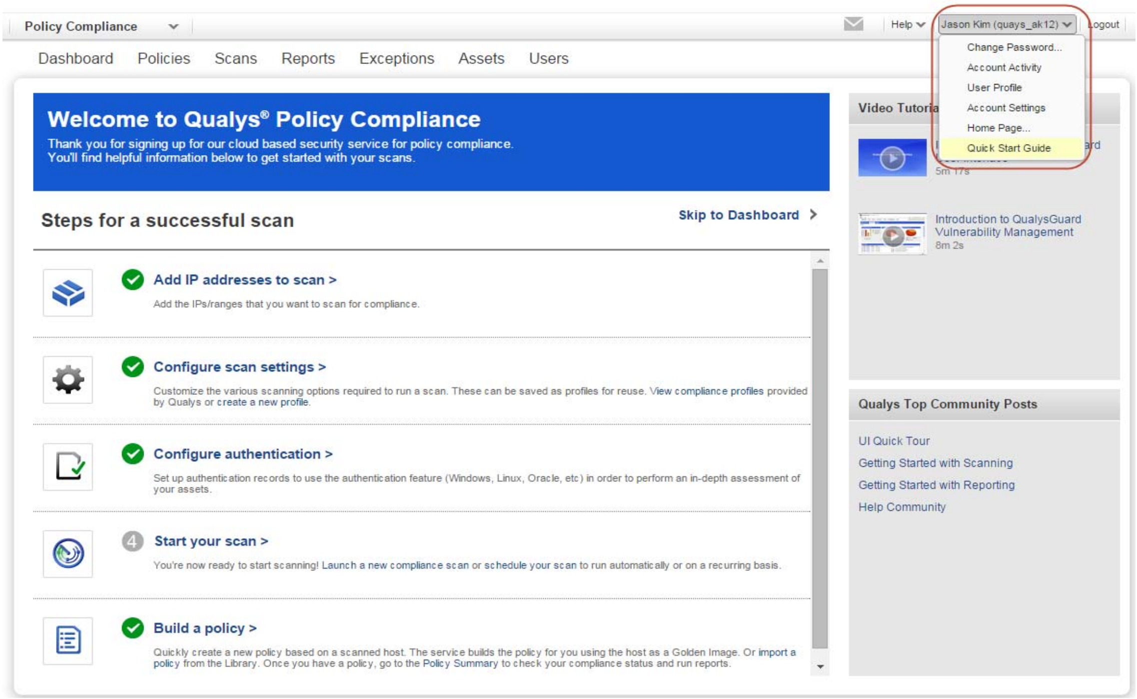
WAF Web Application Firewall
Detect attacks and protect your web applications.

Once in the PC application, you'll see these options along the top menu:



Title	Type	Created By	Created	Modified By	Modified
Policy for Red Hat Linux	Compliance	Patrick Slimmer	02/20/2013	Patrick Slimmer	02/20/2013
Password Auditing	Compliance	Patrick Slimmer	01/03/2013	Patrick Slimmer	01/03/2013

The Policy Compliance Quick Start Guide provides helpful information to get started. Select "Quick Start Guide" below your user name at any time to see this guide.



Welcome to Qualys® Policy Compliance

Thank you for signing up for our cloud based security service for policy compliance. You'll find helpful information below to get started with your scans.

Steps for a successful scan

Add IP addresses to scan >
Add the IPs/ranges that you want to scan for compliance.

Configure scan settings >
Customize the various scanning options required to run a scan. These can be saved as profiles for reuse. View compliance profiles provided by Qualys or create a new profile.

Configure authentication >
Set up authentication records to use the authentication feature (Windows, Linux, Oracle, etc) in order to perform an in-depth assessment of your assets.

4 Start your scan >
You're now ready to start scanning! Launch a new compliance scan or schedule your scan to run automatically or on a recurring basis.

Build a policy >
Quickly create a new policy based on a scanned host. The service builds the policy for you using the host as a Golden Image. Or import a policy from the Library. Once you have a policy, go to the Policy Summary to check your compliance status and run reports.

Introduction to QualysGuard Vulnerability Management
8m 2s

Qualys Top Community Posts

UI Quick Tour
Getting Started with Scanning
Getting Started with Reporting
Help Community

Next we'll walk you through the steps so you can get started with running compliance scans, building policies and creating reports.

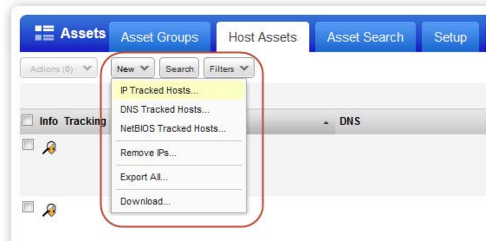
Set Up Assets

You can run compliance scans and create compliance reports on hosts (IP addresses) that have been added to PC.

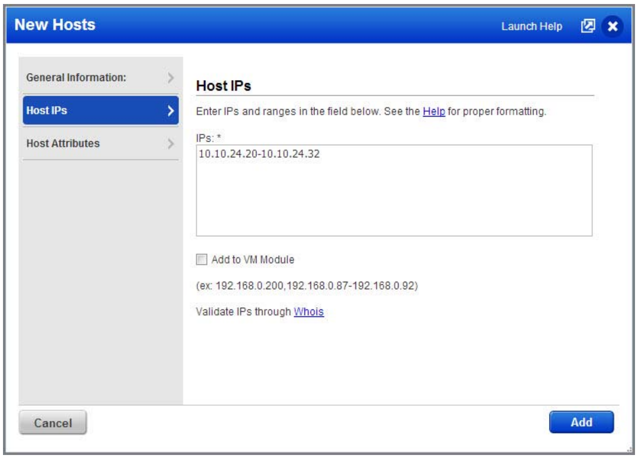
Select Assets on the top menu and then click the Host Assets tab. You'll see the hosts in your PC account.

How do I add new hosts to PC?

When adding new hosts to the subscription, you'll have the option to add the new hosts to PC. Go to New > IP Tracked Hosts (or choose one of the other tracking methods).



In the New Hosts wizard, select Host IPs on the left, enter the IP addresses you want to add and click Add. Then click OK when the confirmation appears.The new hosts will be added to your PC account. If the VM application is enabled in your subscription you can add the new hosts to your VM account by selecting Add to VM Module.



Host IPs

Enter IPs and ranges in the field below. See the Help for proper formatting.

IPs: *
10.10.24.20-10.10.24.32

□ Add to VM Module

(ex: 192.168.0.200,192.168.0.87-192.168.0.92)

Validate IPs through Whois

Start Collecting Compliance Data

Qualys sensors collect compliance data from your assets and beams it up to the Qualys Cloud Platform where it is analyzed and correlated. You can choose to launch scans with scanner appliances and/or install Cloud Agents.

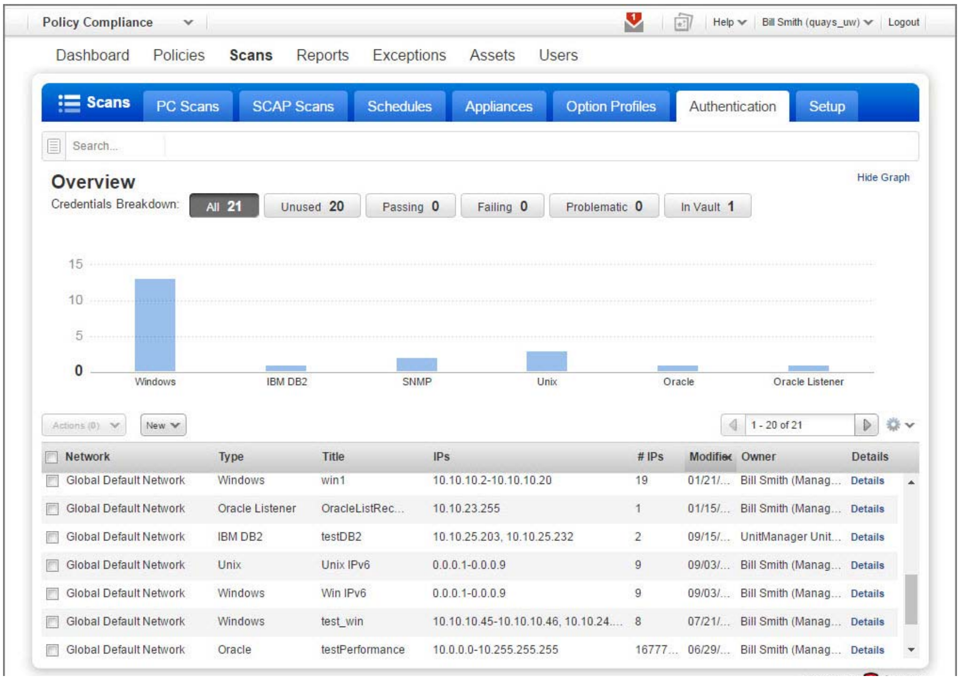
The Scans section is where you manage your compliance scans and your scan configurations.

Configure Authentication

Authentication to hosts is required for compliance scans using our trusted scanning feature. For Windows compliance scanning, an account with Administrator rights is required.

The service performs authentication based on authentication records you define for your target hosts. Each authentication record identifies an authentication type — Windows, Unix, Oracle, Oracle Listener, SNMP, MS SQL Server, Cisco, IBM DB2, VMware, MySQL Server, Sybase, Checkpoint Firewall, PostgreSQL, Tomcat Server, MS IIS, Apache Web Server, IBM WebSphere App Server, Oracle WebLogic Server, and Docker - account login credentials and target IP addresses. Multiple records may be defined. The service uses all the records in your account for compliance scanning.

You'll see the authentication records in your account by going to Scans > Authentication. To add a new record, select the record type from the New menu. The online help describes each record type and setup requirements.

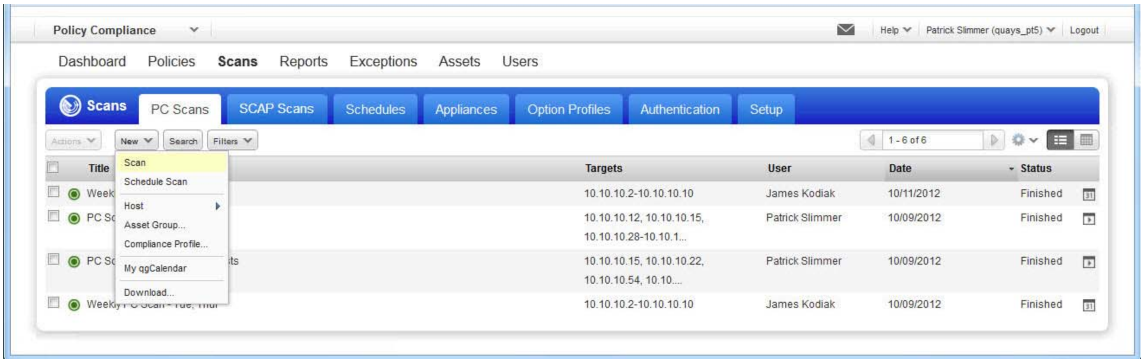


☐ Network	Type	Title	IPs	# IPs	Modified	Owner	Details
☐ Global Default Network	Windows	win1	10.10.10.2-10.10.10.20	19	01/21/...	Bill Smith (Manag...	Details
☐ Global Default Network	Oracle Listener	OracleListRec...	10.10.23.255	1	01/15/...	Bill Smith (Manag...	Details
☐ Global Default Network	IBM DB2	testDB2	10.10.25.203, 10.10.25.232	2	09/15/...	UnitManager Unit...	Details
☐ Global Default Network	Unix	Unix IPv6	0.0.0.1-0.0.0.9	9	09/03/...	Bill Smith (Manag...	Details
☐ Global Default Network	Windows	Win IPv6	0.0.0.1-0.0.0.9	9	09/03/...	Bill Smith (Manag...	Details
☐ Global Default Network	Windows	test_win	10.10.10.45-10.10.10.46, 10.10.24....	8	07/21/...	Bill Smith (Manag...	Details
☐ Global Default Network	Oracle	testPerformance	10.0.0.0-10.255.255.255	16777...	06/29/...	Bill Smith (Manag...	Details

Launch Compliance Scans

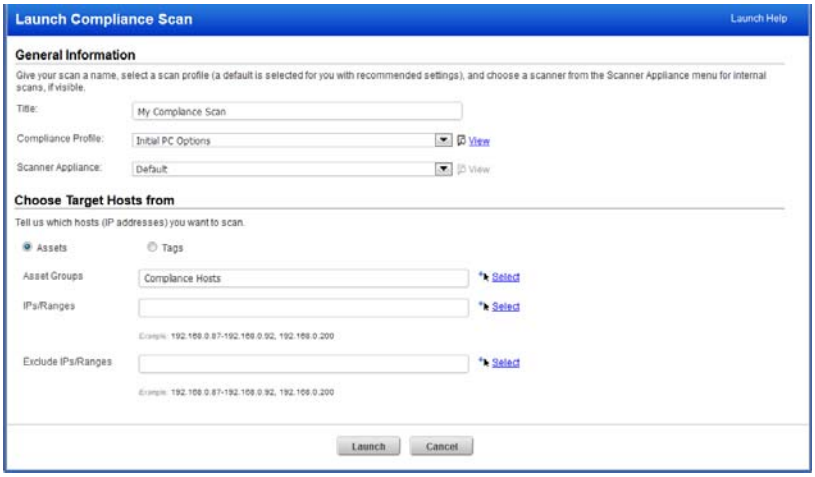
Now you're ready to start scan using scanner appliances. Compliance scans can be launched on demand or scheduled to run at a future date and time.

It's easy. Select Scans from the top menu and click the PC Scans tab. Then go to New > Scan (or Schedule Scan).



Title	Targets	User	Date	Status
Week	10.10.10.2-10.10.10.10	James Kodiak	10/11/2012	Finished
PC Sc	10.10.10.12, 10.10.10.15, 10.10.10.28-10.10.1...	Patrick Slimmer	10/09/2012	Finished
PC Sc ts	10.10.10.15, 10.10.10.22, 10.10.10.54, 10.10....	Patrick Slimmer	10/09/2012	Finished
Weekly PC Scan - Tue, Thur	10.10.10.2-10.10.10.10	James Kodiak	10/09/2012	Finished

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



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: My Compliance Scan

Compliance Profile: Initial PC Options

Scanner Appliance: Default

Choose Target Hosts from

Tell us which hosts (IP addresses) you want to scan.

● Assets ○ Tags

Asset Groups: Compliance Hosts

IPs/Ranges:

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

Exclude IPs/Ranges:

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

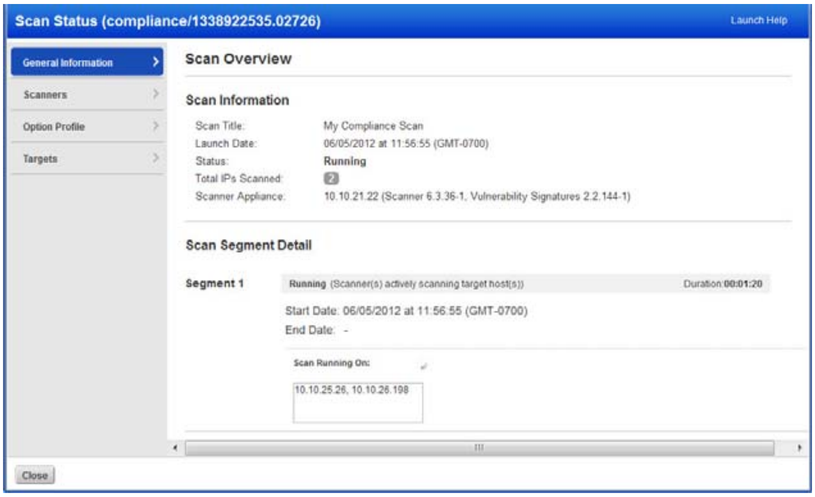
Title — The title helps you identify the scan within the application. The title you enter appears in the scan summary email and the scan results report.

Compliance Profile — This profile contains the various scan settings required to run a compliance scan. We recommend Initial PC Options to get started.

Scanner Appliance — In case your account has scanner appliances, then you can select a scanner option from the menu: External, scanner appliance name, All Scanners in Asset Group, All Scanners in TagSet, Build my list, or Default. You can select one or more scanner appliances for your internal compliance scans. (These same options are available for vulnerability scans.)

Target Hosts — Select the hosts you want to scan. You can enter IPs/ranges and/or asset groups. When Asset Tagging has been added to your account then you also have the option to identify target hosts by selecting asset tags.

After entering information, click the Launch button. The scan status will appear like this:



Scan Status (compliance/1338922535.02726)

Scan Overview

Scan Information

Scan Title: My Compliance Scan
Launch Date: 06/05/2012 at 11:56:55 (GMT-0700)
Status: Running
Total IPs Scanned: 2
Scanner Appliance: 10.10.21.22 (Scanner 6.3.36-1, Vulnerability Signatures 2.2.144-1)

Scan Segment Detail

Segment 1 Running (Scanner(s) actively scanning target host(s)) Duration:00:01:20
Start Date: 06/05/2012 at 11:56:55 (GMT-0700)
End Date: -

Scan Running On:
10.10.25.26, 10.10.26.198

The Scan Status report is updated every 60 seconds until all targeted hosts have been analyzed, allowing you to view results in real time. The scan task runs in the background, so you can safely close the status window and return to it from the scans list.

You can easily track a scan and its status from the scans list. The indicator ◉ appears next to a scan when the scan is finished and the results from the scan have been processed. When results are processed it means posture evaluation for the scanned hosts is updated and the results are available for reporting.

Tips:

No data found — If you run a compliance 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.

Authentication Report — The Authentication Report helps you identify where authentication was successful and where it failed for compliance hosts. For each host, authentication status Passed, Failed or Passed with Insufficient Privileges (Passed*) is provided.

More Information — The online help (Help > Online Help) and the Resources section (Help > Resources) describe trusted scanning setup requirements and best practices. This information details the account requirements for each authentication type.

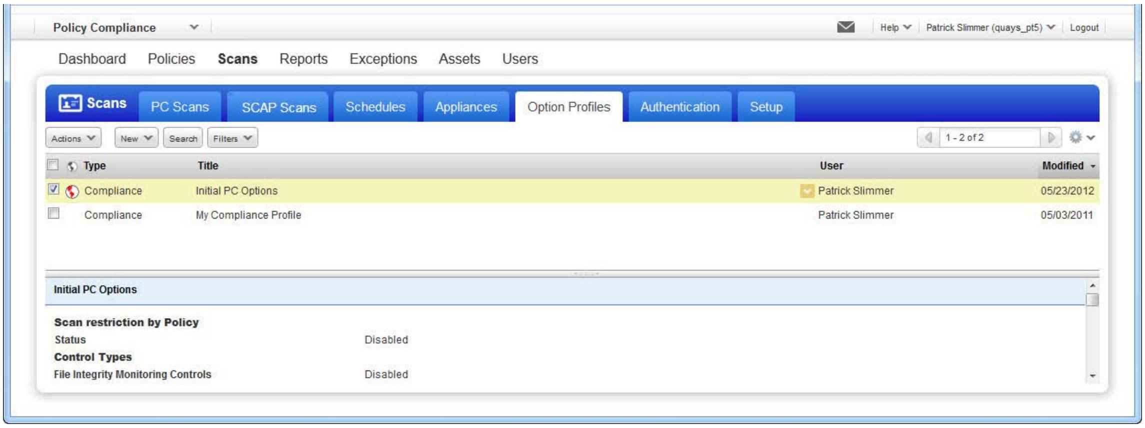
We recommend you schedule scans to run automatically

You can schedule the compliance scan to run at a future date and time, just as you can for vulnerability scans. Select Scans from the top menu and click the Schedules tab. Go to New > Schedule Scan > Compliance.

The New Scheduled Compliance Scan wizard appears where you can add the task. You'll notice the schedule settings are similar to a vulnerability scan schedule, except you enter a compliance profile instead of an option profile.

How to configure scan settings

Compliance profiles contain scan configuration settings that can be fine tuned and saved for future use. To see the compliance profiles in your account, go to Scans > Option Profiles. To add a new compliance profile, go to New > Compliance Profile.



	Type	Title	User	Modified
☑	Compliance	Initial PC Options	Patrick Slimmer	05/23/2012
□	Compliance	My Compliance Profile	Patrick Slimmer	05/03/2011

Initial PC Options

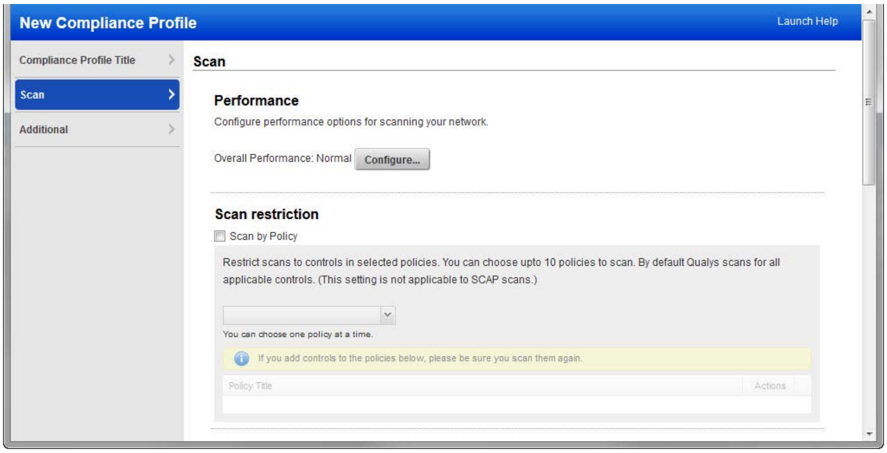
Scan restriction by Policy

Status	Disabled

Control Types

File Integrity Monitoring Controls	Disabled

Below you'll see a sample compliance profile with initial settings provided by the service. The Scan section of the profile includes settings that affect how the service gathers information about target hosts and how the service performs compliance assessment on target hosts.



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 upto 10 policies to scan. By default Qualys scans for all applicable controls. (This setting is not applicable to SCAP scans.)

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

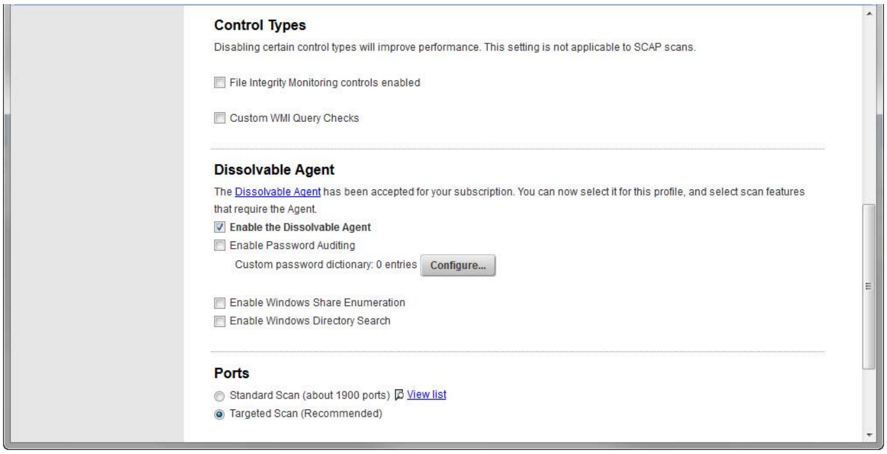
Tell me about scan performance

The performance level selected in the profile determines the number of hosts to scan in parallel, the number of processes to run in parallel against each host, and the delay between groups of packets sent to each host. Click Configure to change the performance level or customize performance settings.

Tell me about scanning controls

The service scans for all controls in all policies unless you choose to restrict scanning to the controls in certain policies (up to 10).

Now scroll down further in your profile to see more scan settings.



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

Dissolvable Agent

The Dissolvable Agent has been accepted for your subscription. You can now select it for this profile, and select scan features that require the Agent.

☑ Enable the Dissolvable Agent
□ Enable Password Auditing
Custom password dictionary: 0 entries Configure...

□ Enable Windows Share Enumeration
□ Enable Windows Directory Search

Ports

○ Standard Scan (about 1900 ports) View list
● Targeted Scan (Recommended)

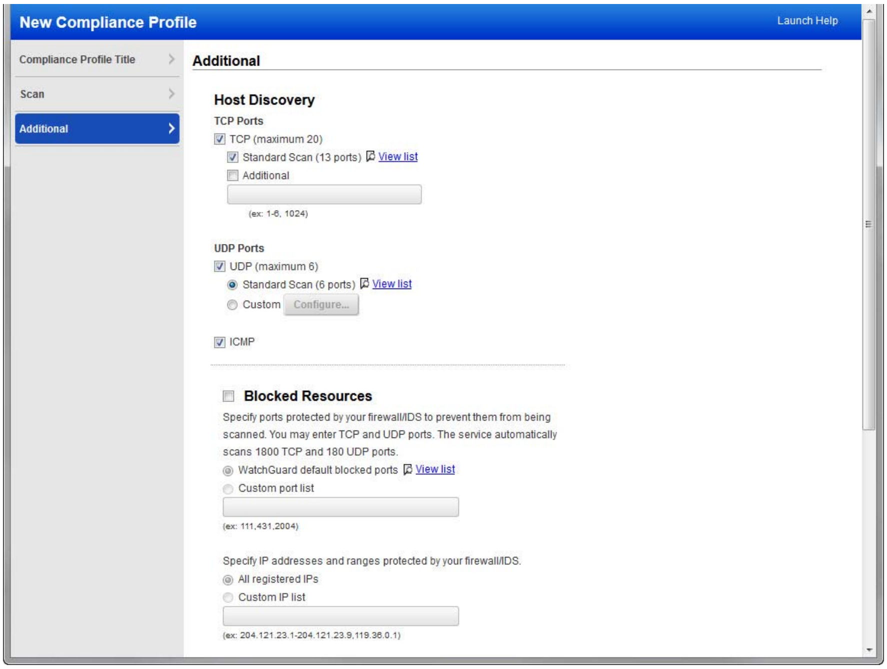
Tell me about additional control types

There are some additional control types you can check during scanning. These are not included in scans by default and require additional steps to set up. For example, to perform file integrity monitoring you must add user defined controls that specify the files you want to track. To scan for password auditing controls, to enumerate Windows shares on your hosts, or to perform a Windows directory search, you must enable the Dissolvable Agent. The online help describes these features in detail.

Which ports are scanned?

When “Standard Scan” is selected, all ports in the standard ports list are scanned (about 1900 ports) in addition to any custom ports specified in Unix authentication records. You can click the “View list” link to see the standard ports list. When “Targeted Scan” is selected, the service targets the scan to a smaller set of ports. This is the recommended setting, and it is the initial setting for a new compliance profile.

Click the Additional tab in your profile for configuration settings that affect how the service performs host discovery and how the service interacts with your firewall/IDS configuration. The initial settings are best practice in most cases.



Additional

Host Discovery

TCP Ports

☑ TCP (maximum 20)

☑ Standard Scan (13 ports) View list

□ Additional

(ex: 1-6, 1024)

UDP Ports

☑ UDP (maximum 6)

● Standard Scan (6 ports) View list

○ Custom Configure...

☑ ICMP

□ Blocked Resources

Specify ports protected by your firewall/IDS to prevent them from being scanned. You may enter TCP and UDP ports. The service automatically scans 1800 TCP and 180 UDP ports.

● WatchGuard default blocked ports View list

○ Custom port list

(ex: 111,431,2004)

Specify IP addresses and ranges protected by your firewall/IDS.

● All registered IPs

○ Custom IP list

(ex: 204.121.23.1-204.121.23.9,119.36.0.1)

What is host discovery?

This is the first phase of a scan when the service sends probes to attempt to discover whether the hosts in the scan target are alive and running.

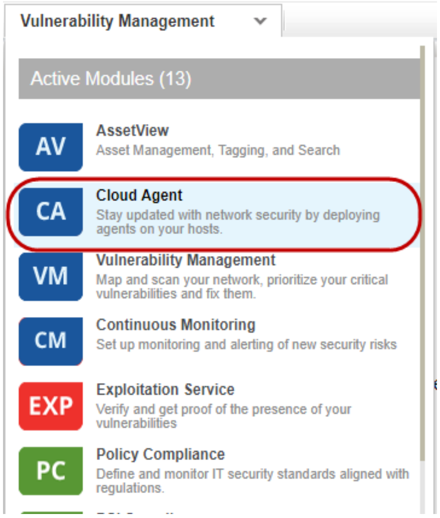
Important: By changing the default settings the service may not detect all live hosts and hosts that go undetected cannot be analyzed for compliance. These settings should only be customized under special circumstances. For example, you might want to add ports that are not included in the Standard port list, remove probes that will trigger your firewall/IDS, or only discover live hosts that respond to an ICMP ping.

Install Cloud Agents

Qualys Cloud Agent is our revolutionary platform that supports security assessments in real time, without the need to schedule scan windows and manage credentials for scanning. You can choose to install cloud agents instead of scanner appliances for continuous compliance data collection. These lightweight agents can be installed anywhere - any host such as a laptop, desktop, server or virtual machine - in minutes.

All agent installations are managed in Qualys Cloud Agent. We'll help you create activate keys, download and install agents, and activate your agents for Policy Compliance (PC).

Log into your account and choose Cloud Agent from the application picker.



AV AssetView
Asset Management, Tagging, and Search

CA Cloud Agent
Stay updated with network security by deploying agents on your hosts.

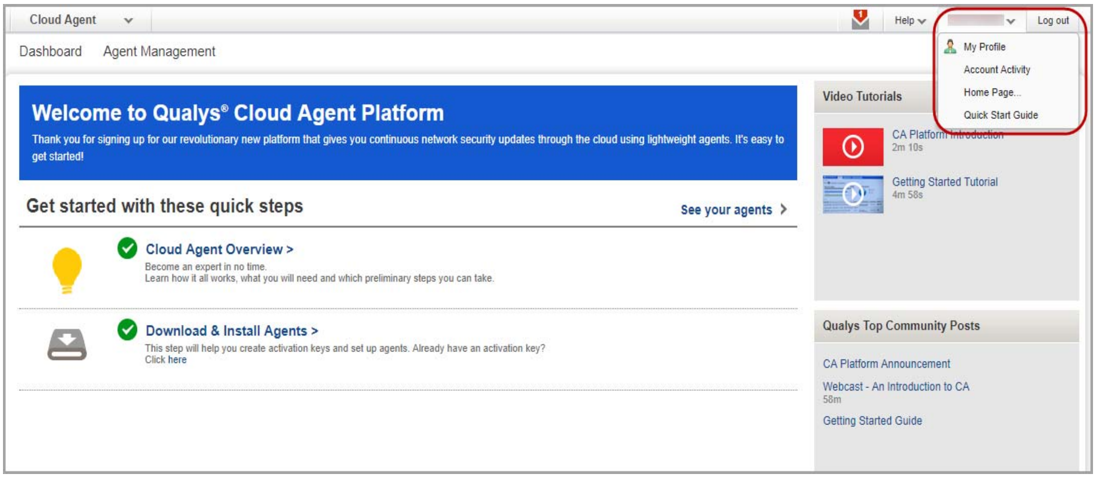
VM Vulnerability Management
Map and scan your network, prioritize your critical vulnerabilities and fix them.

CM Continuous Monitoring
Set up monitoring and alerting of new security risks

EXP Exploitation Service
Verify and get proof of the presence of your vulnerabilities

PC Policy Compliance
Define and monitor IT security standards aligned with regulations.

The Cloud Agent Platform Quick Start Guide provides helpful information to get started. Select "Quick Start Guide" below your user name at any time to see this guide. You'll find helpful links to Cloud Agent free training and user guides.



Welcome to Qualys® Cloud Agent Platform

Thank you for signing up for our revolutionary new platform that gives you continuous network security updates through the cloud using lightweight agents. It's easy to get started!

Get started with these quick steps

Cloud Agent Overview >
Become an expert in no time.
Learn how it all works, what you will need and which preliminary steps you can take.

Download & Install Agents >
This step will help you create activation keys and set up agents. Already have an activation key?
Click here

Qualys Top Community Posts
CA Platform Announcement
Webcast - An Introduction to CA
58m
Getting Started Guide

Define Policies

Create a compliance policy based on your organization's compliance needs, and assign relevant assets to the policy. You can easily import policies directly to your account from our Compliance Policy Library. The library includes policies that are based on popular compliance frameworks, including SOX, HIPAA, CoBIT and more. You can also import a compliance policy from an XML file. The XML file may be one that was exported from your account or one that was shared with you by another security professional.

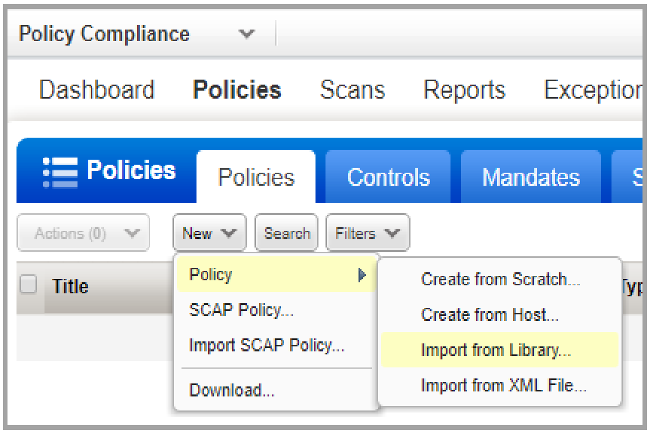
The policy imported policy appears in your policies list where you can assign assets to the policy and customize the policy settings.

By default, we'll only import the service-provided controls in the policy. Choose "Create user defined controls" to also import UDCs.

Once the compliance policy is in place, you can apply the policy to saved compliance scan results to identify whether hosts are meeting compliance requirements. The next few sections will guide you through the process of creating your first policy.

Creating your first policy

Go to PC > Policies > New > Policy.



Get started using any of these methods:

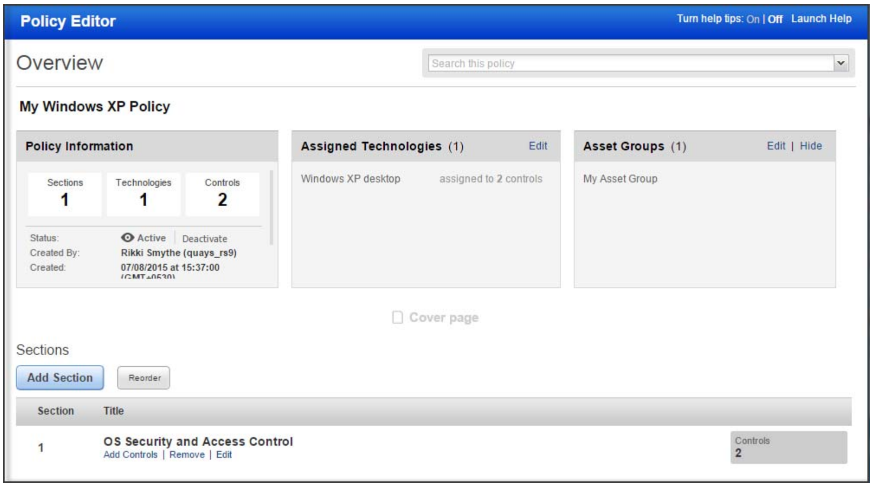
Import from Library — We provide many policies in our Library, including CIS-certified policies. Find the policy you want, click on it and then click Next to import it to your account.

Create from scratch — Follow the wizard to select policy technologies, assign assets to the policy, and give your policy a name. When the Policy Editor appears you can add controls to your policy and set control values.

Create from host — You'll select a host that has already been scanned for compliance, give your policy a name, and click Create. We'll build the policy for you based on the latest compliance findings for the host. We'll add controls to the policy and organize them into sections.

Import from XML file — Follow the wizard to choose the XML file you want to import and give your policy a name.

Here's a sample policy for the Windows XP technology.



Policy Editor — Turn help tips: On | Off Launch Help

Overview — Search this policy

My Windows XP Policy

Policy Information

Sections	Technologies	Controls
1	1	2

Status: Active | Deactivate
Created By: Rikki Smythe (quays_rs9)
Created: 07/08/2015 at 15:37:00 (GMT+0530)

Assigned Technologies (1) Edit
Windows XP desktop — assigned to 2 controls

Asset Groups (1) Edit | Hide
My Asset Group

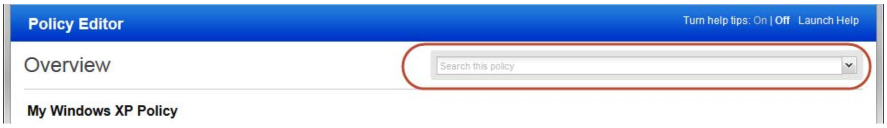
□ Cover page

Sections
Add Section | Reorder

Section	Title	
1	OS Security and Access Control Add Controls | Remove | Edit	Controls 2

Can I search the policy?

Yes. Use the search feature in the top, right corner to jump directly to any section or control in the policy. Search by keyword or control ID.



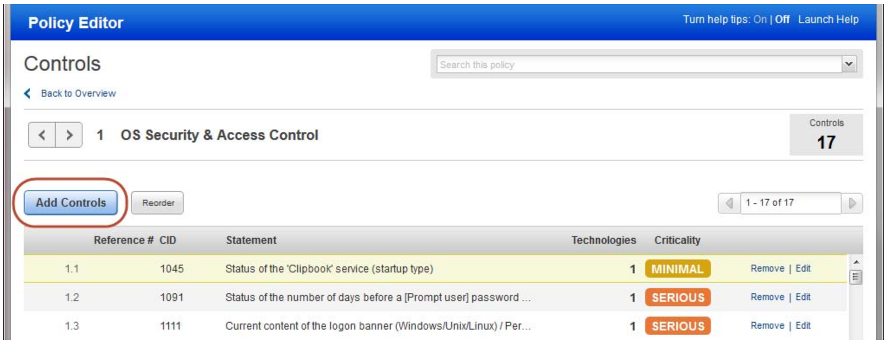
Policy Editor — Turn help tips: On | Off Launch Help

Overview — Search this policy

My Windows XP Policy

How do I add controls to a section?

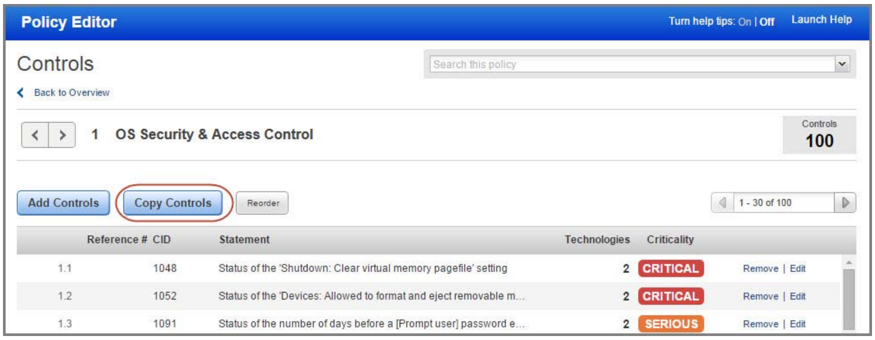
Drill-down into a section from the home page (double-click on the section), and then click the Add Controls button to search for and add controls to the section. Note that you can only select controls that have not already been added to the policy, and the controls must be applicable to the global technologies list set for the policy.



Reference #	CID	Statement	Technologies	Criticality	
1.1	1045	Status of the 'Clipbook' service (startup type)	1	MINIMAL	Remove | Edit
1.2	1091	Status of the number of days before a [Prompt user] password ...	1	SERIOUS	Remove | Edit
1.3	1111	Current content of the logon banner (Windows/Unix/Linux) / Per...	1	SERIOUS	Remove | Edit

How do I copy control settings?

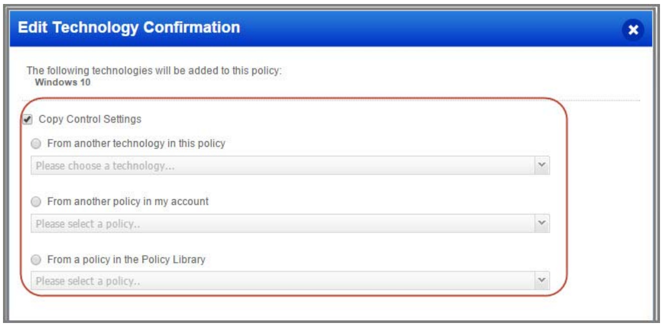
Save time by copying controls along-with their settings already defined in another policy. Click Copy Controls in a new section or existing section in your policy. Tell us which policy has the controls you're looking for. Select the controls you want to copy, and click Copy.



Reference #	CID	Statement	Technologies	Criticality	
1.1	1048	Status of the 'Shutdown: Clear virtual memory pagefile' setting	2	CRITICAL	Remove | Edit
1.2	1052	Status of the 'Devices: Allowed to format and eject removable m...	2	CRITICAL	Remove | Edit
1.3	1091	Status of the number of days before a [Prompt user] password e...	2	SERIOUS	Remove | Edit

Similarly, when you add a new technology to your policy, you can copy control settings from another technology in the same policy, another policy in your account or a policy in the Library.

For example, let's say you're adding Windows 10 to your policy and you choose to copy settings from another technology like Windows 8. We will apply settings from all applicable Windows 8 controls to Windows 10 controls.



The following technologies will be added to this policy:
Windows 10

☑ Copy Control Settings

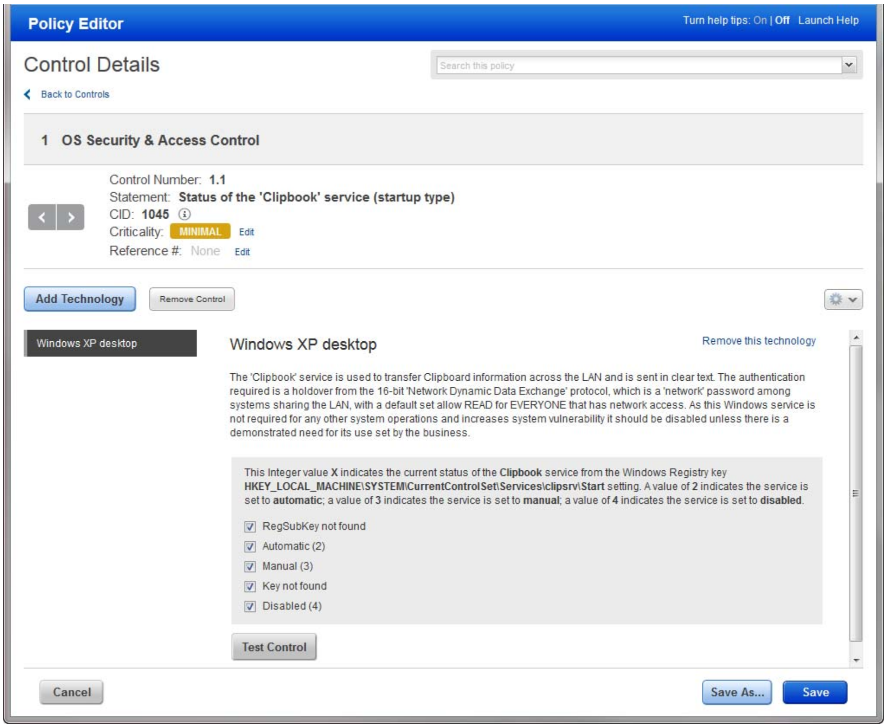
○ From another technology in this policy
Please choose a technology...

○ From another policy in my account
Please select a policy..

○ From a policy in the Policy Library
Please select a policy..

How do I edit control details?

Drill-down into a section from the home page (double-click on the section), and then double-click on any control (or click Edit) to see control details. From here you can change the control value for any technology, add/remove technologies for the control, and add an external reference number. Use the left and right arrows to quickly scroll through the controls in the section.



1 OS Security & Access Control

Control Number: **1.1**
Statement: **Status of the 'Clipbook' service (startup type)**
CID: **1045**
Criticality: MINIMAL Edit
Reference #: None Edit

Windows XP desktop

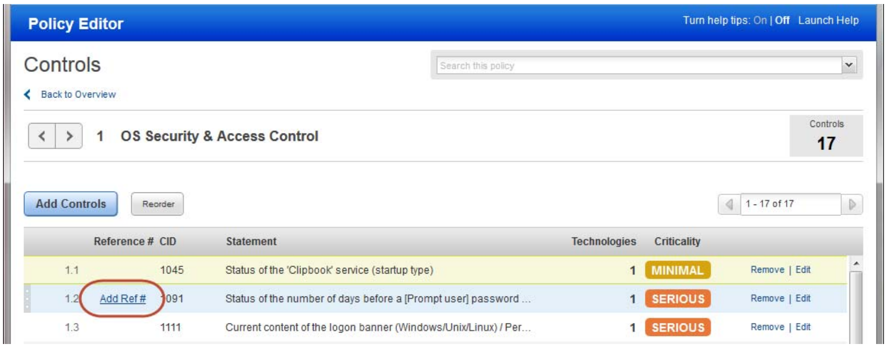
The 'Clipbook' service is used to transfer Clipboard information across the LAN and is sent in clear text. The authentication required is a holdover from the 16-bit 'Network Dynamic Data Exchange' protocol, which is a 'network' password among systems sharing the LAN, with a default set allow READ for EVERYONE that has network access. As this Windows service is not required for any other system operations and increases system vulnerability it should be disabled unless there is a demonstrated need for its use set by the business.

This Integer value **X** indicates the current status of the **Clipbook** service from the Windows Registry key **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\clipsrv\Start** setting. A value of **2** indicates the service is set to **automatic**; a value of **3** indicates the service is set to **manual**; a value of **4** indicates the service is set to **disabled**.

☑ RegSubKey not found
☑ Automatic (2)
☑ Manual (3)
☑ Key not found
☑ Disabled (4)

How do I add a control reference?

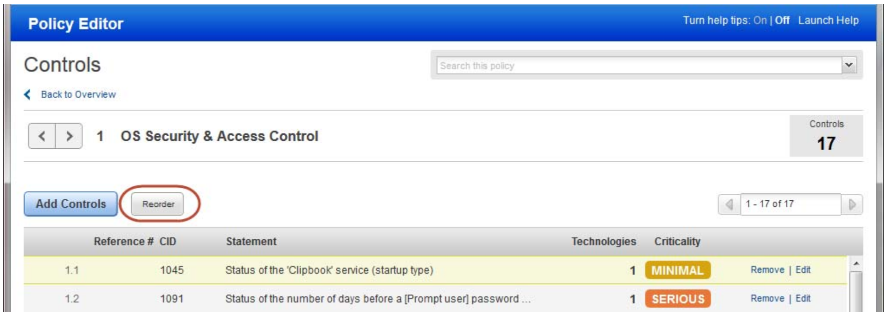
You can add a reference to any control by either clicking the Add Ref # link from the list of controls or clicking Edit next to Reference # in the Control Details. The text you enter will appear in your policy reports under Control References. Note that Managers and Auditors can still add references (documents, URLs and text) by editing a control from the controls data list (go to PC > Policies > Controls).



Reference #	CID	Statement	Technologies	Criticality	
1.1	1045	Status of the 'Clipbook' service (startup type)	1	MINIMAL	Remove | Edit
1.2 Add Ref #	1091	Status of the number of days before a [Prompt user] password ...	1	SERIOUS	Remove | Edit
1.3	1111	Current content of the logon banner (Windows/Unix/Linux) / Per...	1	SERIOUS	Remove | Edit

How do I reorder controls?

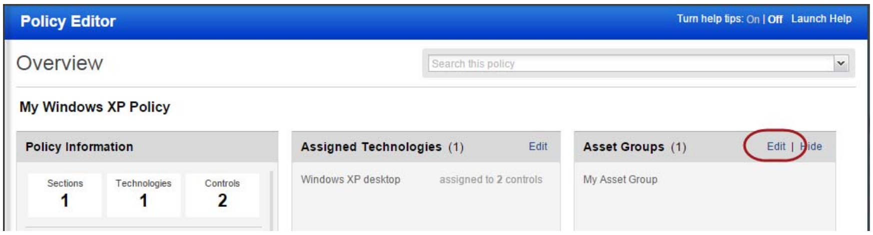
From the controls list, you can reorder controls using these methods: 1) Click the Reorder button and then type over any control number. This is an easy way to move controls from one section to another, for example change control 2.1 to 1.1 to move it from section 2 to section 1. 2) Simply drag and drop a control to a new position. Click the far left edge of the control row to move it.



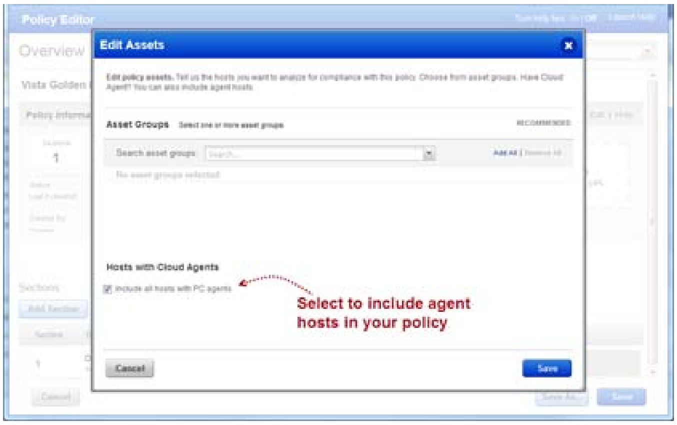
Reference #	CID	Statement	Technologies	Criticality	
1.1	1045	Status of the 'Clipbook' service (startup type)	1	MINIMAL	Remove | Edit
1.2	1091	Status of the number of days before a [Prompt user] password ...	1	SERIOUS	Remove | Edit

Can I change the policy assets?

Yes. Click Edit next to Asset Groups and add asset groups or asset tags that contain the hosts you want to test for compliance.



Do you have PC Agent? You'll also see the option to include agent hosts in the policy. Select the check box "Include all hosts with PC agents". All hosts in your PC Agent license will be included.


Policy Editor
Overview
Edit Assets
Edit policy assets. Tell us the hosts you want to analyze for compliance with this policy. Choose from asset groups. Have Cloud Agent? You can also include agent hosts.
Asset Groups Select one or more asset groups
RECOMMENDED
Search asset groups
Search...
Add All | Remove All
No asset groups selected
Hosts with Cloud Agents
☑ Include all hosts with PC agents
Select to include agent hosts in your policy
Cancel
Save

When you run policy reports, you'll be able to identify the agent hosts in the policy by looking for the tracking method AGENT.

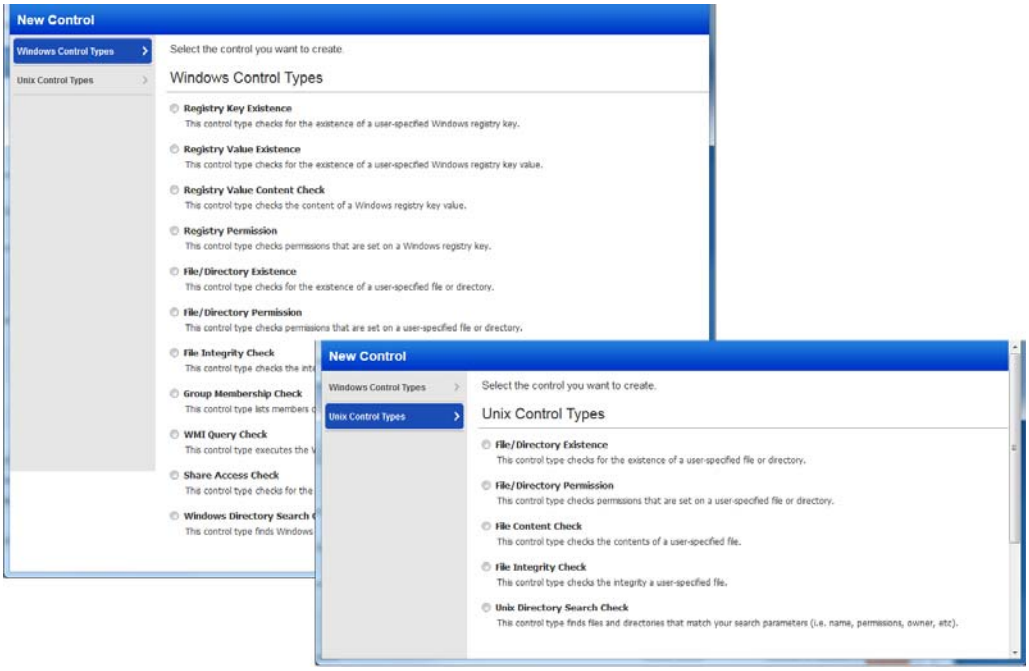
Add User Defined Controls

Managers and Auditors have the option to add user-defined custom controls to the subscription making them available for compliance scanning and reporting. The service supports custom controls for both Windows and Unix platforms.

When defining a custom control, you must 1) provide general information for the control like a control statement and category, 2) specify the scan parameters that define the data point check to be performed by the scanning engine, and 3) identify the technologies that the control applies to and set the default expected value for each technology.

To add a custom control:

1. Select Policies from the top menu, and then click the Controls tab.
2. Go to New > Control.
3. In the New Control window, select Windows Control Types or Unix Control Types.



New Control

Windows Control Types >
Unix Control Types >

Select the control you want to create

Windows Control Types

○ **Registry Key Existence**
This control type checks for tha axistence of a user-specfied Windows registry key.

○ **Registry Value Existence**
This control type checks for the existence of a user-specfied Windows registry key value.

○ **Registry Value Content Check**
This control type checks the content of a Windows registry key value.

○ **Registry Permission**
This control type checks permissions that are set on a Windows registry key.

○ **File/Directory Existence**
This control type checks for the existence of a user-specfied file or directory.

○ **File/Directory Permission**
This control type checks permissions that are set on a user-specfied file or directory.

○ **File Integrity Check**
This control type checks the int

○ **Group Membership Check**
This control type lists members c

○ **WMI Query Check**
This control type executes the V

○ **Share Access Check**
This control type checks for the

○ **Windows Directory Search C**
This control type finds Windows

New Control

Windows Control Types >
Unix Control Types >

Select the control you want to create.

Unix Control Types

○ **File/Directory Existence**
This control type checks for the existence of a user-specfied file or directory.

○ **File/Directory Permission**
This control type checks permissions that are set on a user-specfied file or directory.

○ **File Content Check**
This control type checks the contents of a user-specfied file.

○ **File Integrity Check**
This control type checks the integrity a user-specfied file.

○ **Unix Directory Search Check**
This control type finds files and directories that match your search parameters (i.e. name, permissions, owner, etc).

4 Identify the type of control you want to create, and select it.

5 Provide details in the following sections: General Information, Scan Parameters, Control Technologies and References. (See the online help for complete information.)

6 Click Create to save the new control.

Once saved, the custom control appears in the controls list with the service-provided controls. The service automatically assigns the new custom control a unique CID (Control ID) starting at 100000. Subsequent CIDs are incremented by one — 100001, 100002, 100003, etc. The new control is automatically included in all future compliance scans and may be added to policies.

Sample Control: Unix File Content Check

A Unix File Content Check control checks the contents of a user-specified file on a Unix system.

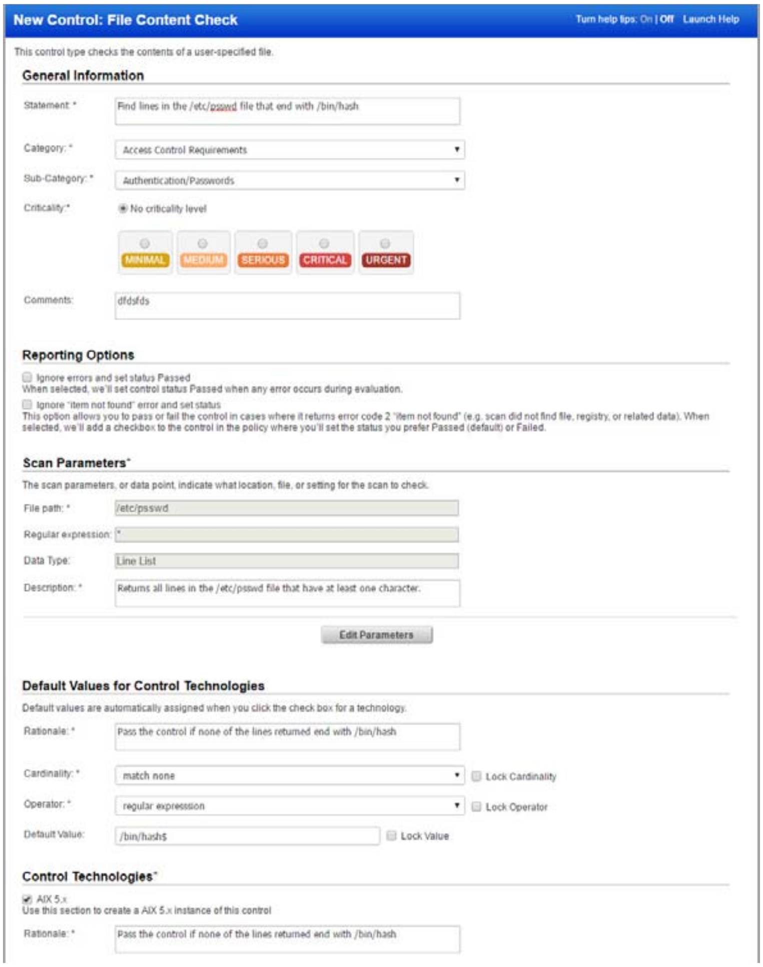
A Unix File Content Check control includes 2 regular expressions. The first regular expression is entered in the Scan Parameters section and is used to filter results on the target file/directory at the time of the scan. The second regular expression is entered in the Control Technologies section and is used to perform the pass/fail evaluation of the returned results.

You can define default values to apply to all control technologies. When you select a technology the default values are automatically assigned to the technology. You can lock the default values if you don't want users to change them in the policy editor.

Example:

This sample control can be used to find lines in the /etc/passwd file that end with /bin/bash.

The settings in the Scan Parameters section instruct the scanning engine to first return all lines in the /etc/passwd file that have at least one character. The settings in the Control Technologies section instruct the scanning engine to pass the control if none of the lines end with /bin/bash. If at least one line in the file ends with /bin/bash then the control will fail.



New Control: File Content Check
Turn help tips: On | Off Launch Help

This control type checks the contents of a user-specified file.

General Information

Statement: * Find lines in the /etc/pswd file that end with /bin/hash

Category: * Access Control Requirements ▾

Sub-Category: * Authentication/Passwords ▾

Criticality:* ● No criticality level

○ MINIMAL ○ MEDIUM ○ SERIOUS ○ CRITICAL ○ URGENT

Comments: dfdsfds

Reporting Options

□ Ignore errors and set status Passed
When selected, we'll set control status Passed when any error occurs during evaluation.

□ Ignore "item not found" error and set status
This option allows you to pass or fail the control in cases where it returns error code 2 "item not found" (e.g. scan did not find file, registry, or related data). When selected, we'll add a checkbox to the control in the policy where you'll set the status you prefer Passed (default) or Failed.

Scan Parameters*

The scan parameters, or data point, indicate what location, file, or setting for the scan to check.

File path: * /etc/psswd

Regular expression: *

Data Type: Line List

Description: * Returns all lines in the /etc/psswd file that have at least one character.

Default Values for Control Technologies

Default values are automatically assigned when you click the check box for a technology.

Rationale: * Pass the control if none of the lines returned end with /bin/hash

Cardinality: * match none ▾ □ Lock Cardinality

Operator: * regular expresssion ▾ □ Lock Operator

Default Value: /bin/hash$ □ Lock Value

Control Technologies*

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

Rationale: * Pass the control if none of the lines returned end with /bin/hash

Sample Control: Windows Registry Permission

A Windows Registry Permission control checks permissions that are set on a Windows registry key for different user groups and individual users.

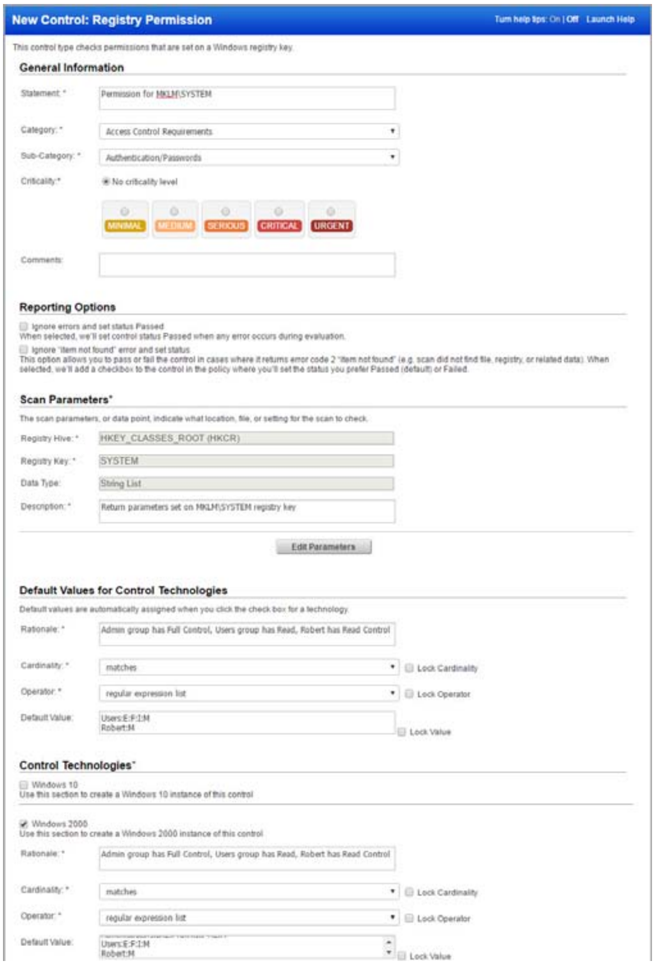
To maximize space, the Policy Compliance application assigns each permission a letter (A,B,C,D,...) and displays the letter instead of the full permission name. You must use the same mapping when setting the default expected value for the control. (See "Registry Permissions" in the online help for a table that maps each permission to the letter it represents.)

You can define default values to apply to all control technologies. When you select a technology the default values are automatically assigned to the technology. You can lock the default values if you don't want users to change them in the policy editor.

Example:

This sample control checks that the registry key HKLM\SYSTEM has the following permissions:

The Administrators group has Full Control permission (D:E:F:G:H:I:J:K:L:M)
The Users group has Read permission (E:F:I:M)
A user named Robert has Read Control permission (M)



New Control: Registry Permission

This control type checks permissions that are set on a Windows registry key.

General Information

Statement: * Permission for MKLM\SYSTEM

Category: * Access Control Requirements

Sub-Category: * Authentication/Passwords

Criticality:* ● No criticality level

○ MINIMAL ○ MEDIUM ○ SERIOUS ○ CRITICAL ○ URGENT

Comments:

Reporting Options

□ Ignore errors and set status Passed
When selected, we'll set control status Passed when any error occurs during evaluation.

□ Ignore "item not found" error and set status
This option allows you to pass or fail the control in cases where it returns error code 2 "item not found" (e.g. scan did not find file, registry, or related data). When selected, we'll add a checkbox to the control in the policy where you'll set the status you prefer Passed (default) or Failed.

Scan Parameters*

The scan parameters, or data point, indicate what location, file, or setting for the scan to check.

Registry Hive: * HKEY_CLASSES_ROOT (HKCR)

Registry Key: * SYSTEM

Data Type: String List

Description: * Return parameters set on MKLM\SYSTEM registry key

Default Values for Control Technologies

Default values are automatically assigned when you click the check box for a technology.

Rationale: * Admin group has Full Control, Users group has Read, Robert has Read Control

Cardinality: * matches □ Lock Cardinality

Operator: * regular expression list □ Lock Operator

Default Value: Users:E:F:I:M
Robert:M □ Lock Value

Control Technologies*

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

☑ Windows 2000
Use this section to create a Windows 2000 instance of this control

Rationale: * Admin group has Full Control, Users group has Read, Robert has Read Control

Cardinality: * matches □ Lock Cardinality

Operator: * regular expression list □ Lock Operator

Default Value: Users:E:F:I:M
Robert:M □ Lock Value

Import and Export User Defined Controls

Manager and Auditor users have the option to import and export user defined controls in XML format. Other users can export user defined controls if they have the "Manage compliance" permission; these users do not have permission to import controls.

Tip: The schema ImportableControl.xsd is used to import and export user defined controls. For a description of this schema, go to PC > Policies > Controls and then select Help > Online Help. Under "Custom Controls XML" select "Tell me about control XML".

Export User Defined Controls

To export user defined controls:

1. Go to PC > Policies > Controls.
2. Use the check boxes to select user defined controls you'd like to export.
3. Select Actions > Export.

The selected controls will be saved in an XML file named “control_export_yyyymmdd.xml” using the schema ImportableControl.xsd. A maximum of 500 controls can be exported.

Import User Defined Controls

To import user defined controls:

1. Create user defined control(s) using the schema ImportableControl.xsd.
2. Go to PC > Policies > Controls.
3. Select New > Import from XML file and select the XML file with your user defined controls.

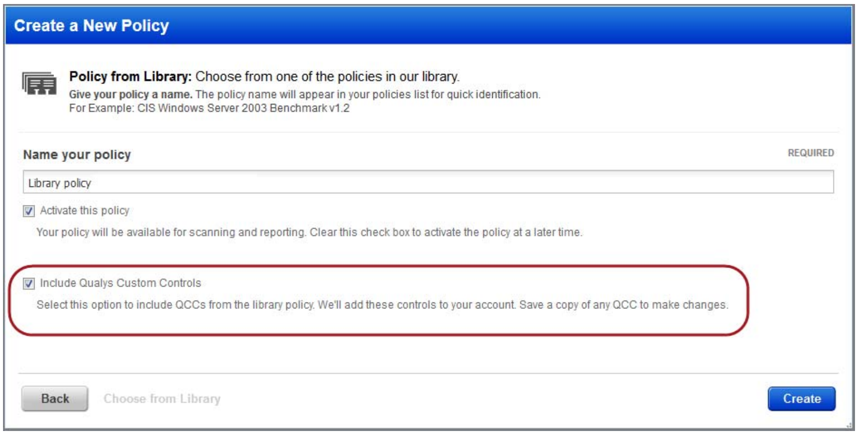
Note: If a control exists in your account with the same scan parameters as control(s) being imported, the service assigns the DESCRIPTION parameter of the existing control to the DESCRIPTION parameter of all imported controls with the same scan parameters.

Qualys Custom Controls in Library Policies

Library policies provided by Qualys may include a 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 (UDC). Once added to your account you can copy any QCC to make your own UDC that you can customize the controls to meet your needs.

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. Simply uncheck the option if you don’t want the QCCs to be imported.



Create a New Policy

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 REQUIRED

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.

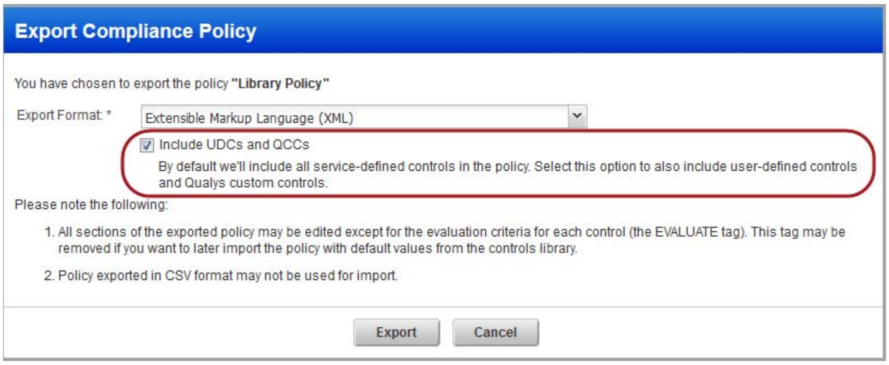
☑ Include Qualys Custom Controls
Select this option to include QCCs from the library policy. We'll add these controls to your account. Save a copy of any QCC to make changes.

The QCCs added from the policy appear on your controls list. The Type column shows QCC for each Qualys Custom Control.

You can make a copy of any QCC to create a UDC that you can customize to meet your exact needs. Just choose Copy from the Quick Actions menu and then confirm the action. The new UDC appears on the controls list where you can edit it.

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

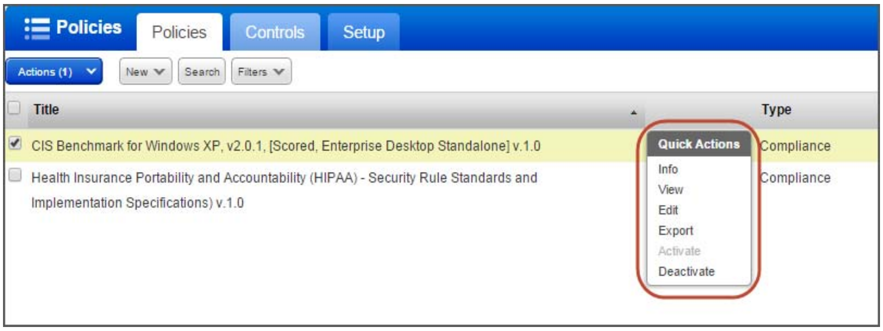
By default we'll include all service-defined controls in the policy. Select this option to also include user-defined controls and Qualys custom controls.

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.

Manage Your Policies

Go to PC > Policies to see all the policies in your subscription. From here you can view and edit policies, export policies, and change the policy status (active/inactive).



	Title	Type
☑	CIS Benchmark for Windows XP, v2.0.1, [Scored, Enterprise Desktop Standalone] v.1.0	Compliance
□	Health Insurance Portability and Accountability (HIPAA) - Security Rule Standards and Implementation Specifications) v.1.0	Compliance

How do I export a policy?

Choose Export from the Quick Actions menu and select a format (CSV or XML). You can include user-defined controls (UDCs) along with the service-provided controls when you export a policy from your account to CSV or XML. Exporting a policy lets you quickly and easily share it or compare it with other policies you may have.

How do I import a policy?

You can import a policy from an XML file including user-defined controls (UDCs) or directly from the Compliance Policy Library. Once a policy is imported, you can customize the policy to suit your needs (unless it is locked). Just go to New > Policy, select either Import from XML File or Import from Library and we'll walk you through the steps.

How do I lock a policy?

You can lock a policy so that you can restrict other users from updating it. Simply, navigate to Policies > Policies and select the policy you want to lock. Select Lock from the Quick Actions menu. You can use the Actions menu to lock multiple policies in one go. Similarly, you can unlock a locked policy. Policies must be unlocked to enable editing.

Tell me about locked policies

Locked policies may be imported for certification purposes. For example, the service provides locked policies for testing compliance against specific CIS benchmarks. These policies have been reviewed and certified by CIS (the Center for Internet Security). You can import a CIS-certified policy from the library into your account, assign relevant assets to the policy and then use the policy to certify that you are meeting all requirements outlined in the CIS benchmark.

Tell me about policy status

Every policy in your account will either be active or inactive . Inactive policies will not be scanned or reported on. You can make a policy inactive by simply choosing Deactivate from the Quick Actions menu. (Then you can activate it later by choosing Activate.)

Why make a policy inactive? You may want to hide a new policy while you're working on it and then publish it at a later time. Or let's say a policy has become out of date and you want to edit the policy before republishing it. In such cases you mark the policy inactive and make the required changes. Then activate it when you're done.

How do I evaluate policy?

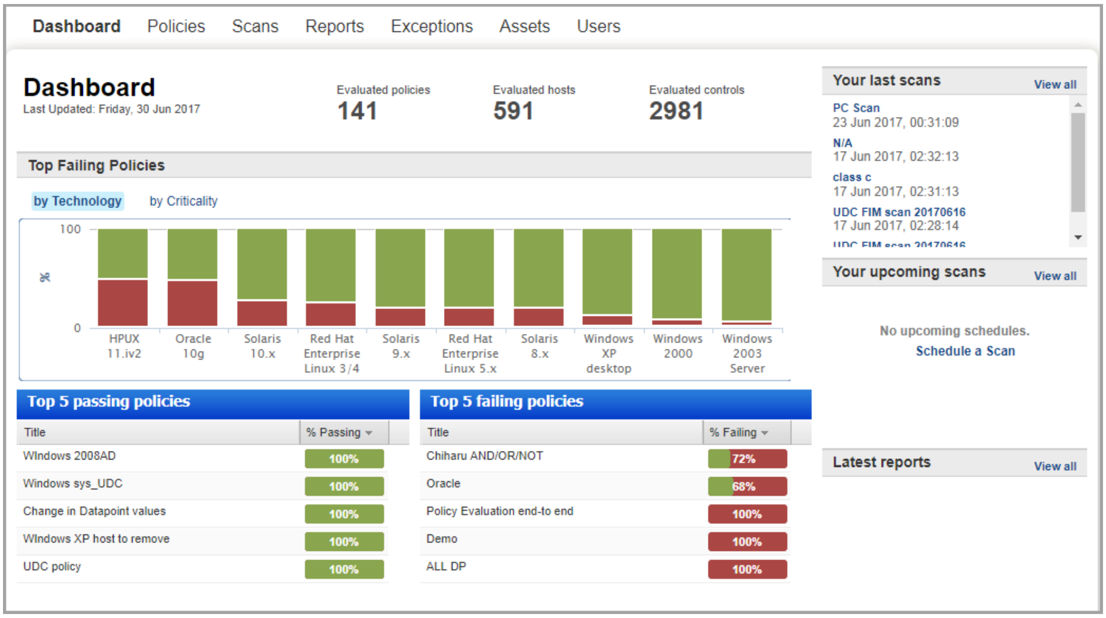
Policies are evaluated when new scan results are processed for the hosts in your policy. You can also start policy evaluation when saving changes to a policy or anytime from the policies data list. Simply select the Evaluate Now check box before you click Save in the Policy Editor or from the policy data list, select any policy and choose Evaluate from the Quick Actions menu. To evaluate multiple policies at one go, select the policies and choose Evaluate from the Actions menu above the list.

Reporting Overview

A policy compliance dashboard and specialized policy compliance reports provide compliance status information for the hosts in your account, based on the results returned from the most recent compliance scans. These reports help you determine whether hosts are compliant with the policies in your account.

Dashboard

The policy compliance dashboard provides a summary of your overall compliance status across all policies in your account. It displays the top failing policies broken down by technology or by criticality so you can prioritize your compliance efforts. From the dashboard, you can drill-down into a policy summary report for any policy listed, make changes to upcoming schedules, view compliance reports and more. To view the dashboard, select Dashboard on the top menu.



Dashboard
Last Updated: Friday, 30 Jun 2017

Evaluated policies	Evaluated hosts	Evaluated controls
141	591	2981

Your last scans

PC Scan
23 Jun 2017, 00:31:09

N/A
17 Jun 2017, 02:32:13

class c
17 Jun 2017, 02:31:13

UDC FIM scan 20170616
17 Jun 2017, 02:28:14

UDC FIM scan 20170616

Your upcoming scans

No upcoming schedules.

Top 5 passing policies

Title	% Passing
WIndows 2008AD	100%
Windows sys_UDC	100%
Change in Datapoint values	100%
WIndows XP host to remove	100%
UDC policy	100%

Top 5 failing policies

Title	% Failing
Chiharu AND/OR/NOT	72%
Oracle	68%
Policy Evaluation end-to end	100%
Demo	100%
ALL DP	100%

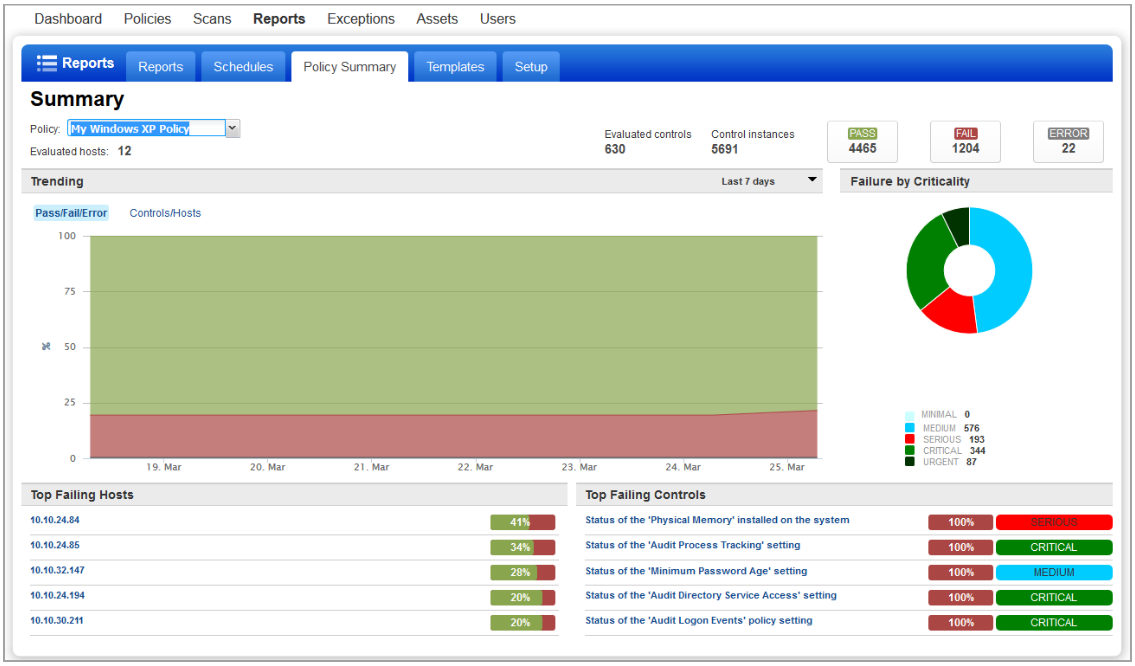
You can also view all your Policy Compliance Summary for an asset in the Compliance tab of Asset View. You can see the compliance policies each asset is associated with and how the policies are doing in terms of secure configuration controls on each asset.

Simply navigate to AssetView > Assets tab, select an asset and click View Asset Details. Locate the Compliance tab to view a detailed compliance summary for that asset.

Policy Summary

The Policy Summary provides a one-page summary of your compliance status for a specific policy in your account. You can view the Policy Summary from the Reports section (Reports > Policy Summary) or link to it from the PC Dashboard (double-click any policy title under Top 5 passing policies or Top 5 failing policies).

At the top of the page, select the policy you're interested in from the Policy menu. When you link to this page from the Dashboard the policy is selected for you. You can change the policy selection at any time to report on a different policy in your account. You can also change the trend duration selection. Your selection determines the number of days (7-90) included in the trend graphs. Note that trend graphs may show aggregate data when a longer time frame is selected.



Summary

Policy: My Windows XP Policy
Evaluated hosts: 12

Evaluated controls 630
Control instances 5691
PASS 4465
FAIL 1204
ERROR 22

Trending
Last 7 days

Failure by Criticality

⬜	MINIMAL	0
🟦	MEDIUM	576
🟥	SERIOUS	193
🟩	CRITICAL	344
⬛	URGENT	87

Top Failing Hosts

10.10.24.84	41%
10.10.24.85	34%
10.10.32.147	28%
10.10.24.194	20%
10.10.30.211	20%

Top Failing Controls

Status of the 'Physical Memory' installed on the system	100%	SERIOUS
Status of the 'Audit Process Tracking' setting	100%	CRITICAL
Status of the 'Minimum Password Age' setting	100%	MEDIUM
Status of the 'Audit Directory Service Access' setting	100%	CRITICAL
Status of the 'Audit Logon Events' policy setting	100%	CRITICAL

Did you know?

You can run interactive compliance reports directly from the Policy Summary.

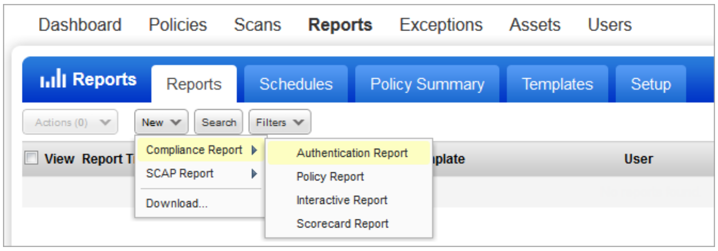
Select the IP address for any host listed under "Top Failing Hosts" to run the Individual Host Compliance Report for the selected host/policy.

Select the control title for any control listed under "Top Failing Controls" to run the Control Pass/Fail Report for the selected control/policy.

Policy Compliance Reports

All policy compliance reports are based on the most recent compliance scan for each host. There are template based reports and interactive reports. Once generated, template based reports are saved to your reports list. Interactive reports are not saved.

To create a new compliance report, select Reports from the top menu, click the Reports tab and select the report you want to run from the New menu.

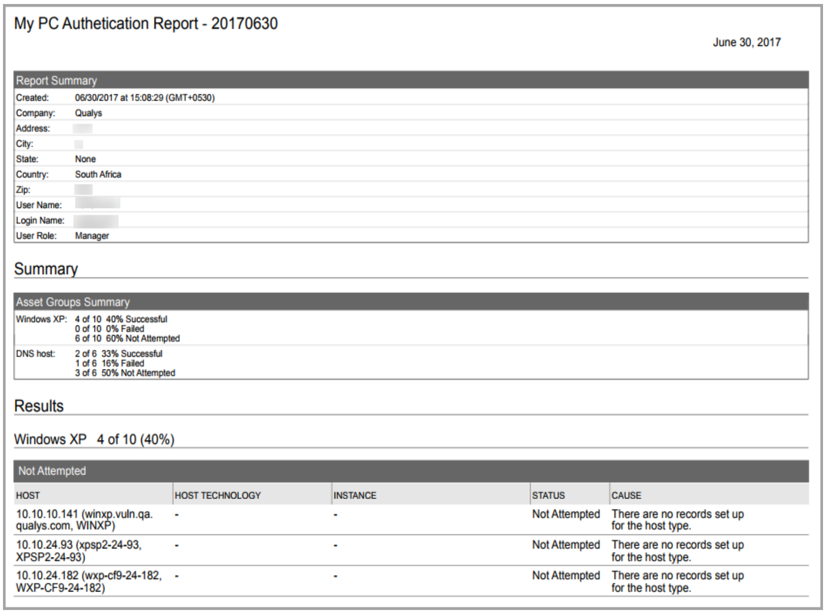


Authentication Report

The Authentication Report indicates whether authentication was successful for scanned hosts. If authentication to a host is not successful, then no controls can be evaluated for the host and no compliance data can be collected for the host. If authentication to a host is successful, then the host can be evaluated for compliance. The Authentication Report uses a hidden report template provided by the service. This template cannot be viewed from the report templates list.

To run the Authentication Report, go to New > Compliance Report > Authentication Report. Select a report format, report source (certain business units or asset groups), and choose whether to display the Summary and/or Details section. Click Run.

Sample Authentication Report:



My PC Authetication Report - 20170630

June 30, 2017

Report Summary	
Created:	06/30/2017 at 15:08:29 (GMT+0530)
Company:	Qualys
Address:	[redacted]
City:	[redacted]
State:	None
Country:	South Africa
Zip:	[redacted]
User Name:	[redacted]
Login Name:	[redacted]
User Role:	Manager

Summary

Asset Groups Summary	
Windows XP:	4 of 10 40% Successful 0 of 10 0% Failed 6 of 10 60% Not Attempted
DNS host:	2 of 6 33% Successful 1 of 6 16% Failed 3 of 6 50% Not Attempted

Results

Windows XP 4 of 10 (40%)

Not Attempted

HOST	HOST TECHNOLOGY	INSTANCE	STATUS	CAUSE
10.10.10.141 (winxp.vuln.qa.qualys.com, WINXP)	-	-	Not Attempted	There are no records set up for the host type.
10.10.24.93 (xpsp2-24-93, XPSP2-24-93)	-	-	Not Attempted	There are no records set up for the host type.
10.10.24.182 (wxp-cf9-24-182, WXP-CF9-24-182)	-	-	Not Attempted	There are no records set up for the host type.

Policy Report

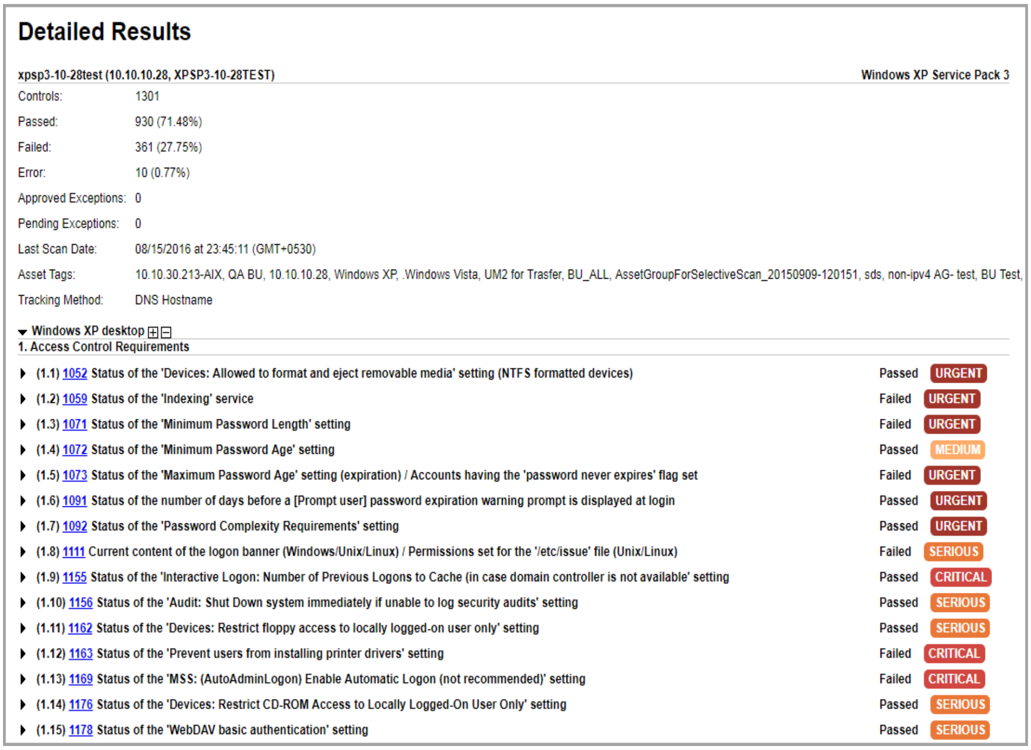
The Policy Report provides compliance status and trend information for a specific policy.

The Policy Report requires a policy report template. The template settings determine the layout and organization of your report, the trend duration for trend graphs, and the list of frameworks that may appear in the report. The service provides the “Policy Report Template” to help you get started. You can use this template as is or customize the settings.

To run the Policy Report, select New > Compliance Report > Policy Report. In the New Policy Report wizard specify your policy report template in the Report Template field. Choose the policy you want to report on. Under Asset Groups you have the option to run the report on all asset groups in the policy or to select specific asset groups in the policy. Click Run.

Sample Policy Report:

This sample shows the Detailed Results section of a Policy Report. The report lists hosts relevant to the policy with the controls tested on each host and the passed/failed status for each control. For each control, you can expand details to see the expected value as defined in the policy and the actual value returned when the host was last scanned.



Detailed Results

xpsp3-10-28test (10.10.10.28, XPSP3-10-28TEST) Windows XP Service Pack 3

Controls:	1301
Passed:	930 (71.48%)
Failed:	361 (27.75%)
Error:	10 (0.77%)
Approved Exceptions:	0
Pending Exceptions:	0
Last Scan Date:	08/15/2016 at 23:45:11 (GMT+0530)
Asset Tags:	10.10.30.213-AIX, QA BU, 10.10.10.28, Windows XP, .Windows Vista, UM2 for Trasfer, BU_ALL, AssetGroupForSelectiveScan_20150909-120151, sds, non-ipv4 AG- test, BU Test,
Tracking Method:	DNS Hostname

▾ Windows XP desktop ⊞⊟

1. Access Control Requirements

▸ (1.1) 1052 Status of the 'Devices: Allowed to format and eject removable media' setting (NTFS formatted devices)	Passed	URGENT
▸ (1.2) 1059 Status of the 'Indexing' service	Failed	URGENT
▸ (1.3) 1071 Status of the 'Minimum Password Length' setting	Failed	URGENT
▸ (1.4) 1072 Status of the 'Minimum Password Age' setting	Passed	MEDIUM
▸ (1.5) 1073 Status of the 'Maximum Password Age' setting (expiration) / Accounts having the 'password never expires' flag set	Failed	URGENT
▸ (1.6) 1091 Status of the number of days before a [Prompt user] password expiration warning prompt is displayed at login	Passed	URGENT
▸ (1.7) 1092 Status of the 'Password Complexity Requirements' setting	Passed	URGENT
▸ (1.8) 1111 Current content of the logon banner (Windows/Unix/Linux) / Permissions set for the '/etc/issue' file (Unix/Linux)	Failed	SERIOUS
▸ (1.9) 1155 Status of the 'Interactive Logon: Number of Previous Logons to Cache (in case domain controller is not available' setting	Passed	CRITICAL
▸ (1.10) 1156 Status of the 'Audit: Shut Down system immediately if unable to log security audits' setting	Passed	SERIOUS
▸ (1.11) 1162 Status of the 'Devices: Restrict floppy access to locally logged-on user only' setting	Passed	SERIOUS
▸ (1.12) 1163 Status of the 'Prevent users from installing printer drivers' setting	Failed	CRITICAL
▸ (1.13) 1169 Status of the 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' setting	Failed	CRITICAL
▸ (1.14) 1176 Status of the 'Devices: Restrict CD-ROM Access to Locally Logged-On User Only' setting	Passed	SERIOUS
▸ (1.15) 1178 Status of the 'WebDAV basic authentication' setting	Passed	SERIOUS

Mandate Based Reports

The Mandate Based Report helps you view the compliance posture of the organization in terms of the underlying Security baseline against selected Mandates. You get a harmonized report on one or more compliance policies and mandates.

You can choose any mandates/standards you want 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 their selected policies.

The Mandate Based Report requires a Mandate template. The template settings identify the sections you want to include in the report.

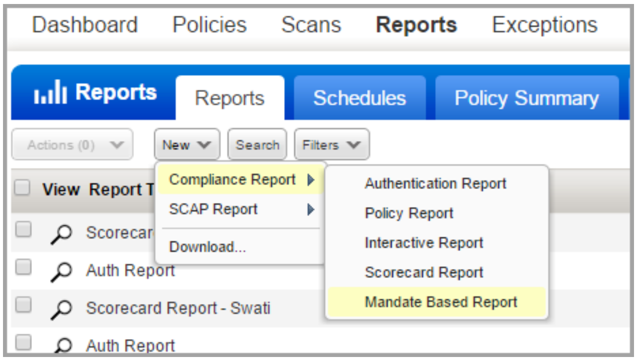
To create a custom Mandate Based Template, go to Reports > Templates and select Mandate Template and configure the report template settings.

You can group the report in two ways:

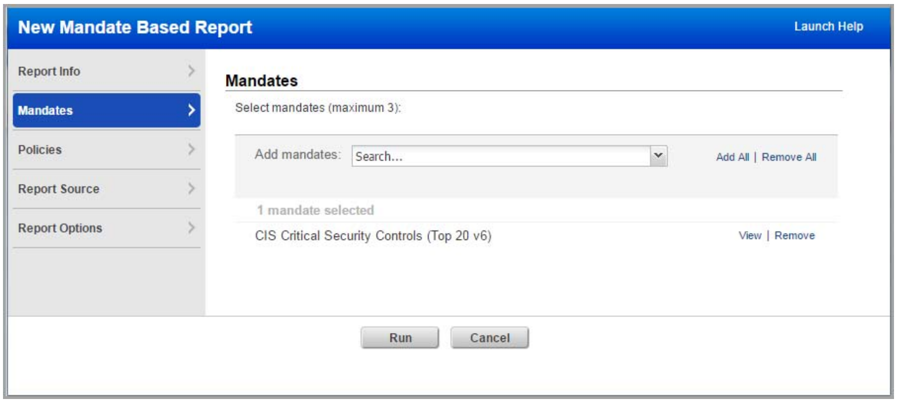
Group by Mandates: generates the report so that information is grouped to flow as per the selected mandates. This works great when you are generating a report for a single mandate.

Group by Control Objectives: harmonizes the overlapping requirements of the mandates and that mandate related control objectives. The information in the generated report is grouped to flow as per the control objectives. This grouping works best when you are generating a report for multiple mandates.

To run the Mandate Based Report, click the Reports tab and select New > Compliance Report and select Mandate Based Report.



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



Mandates

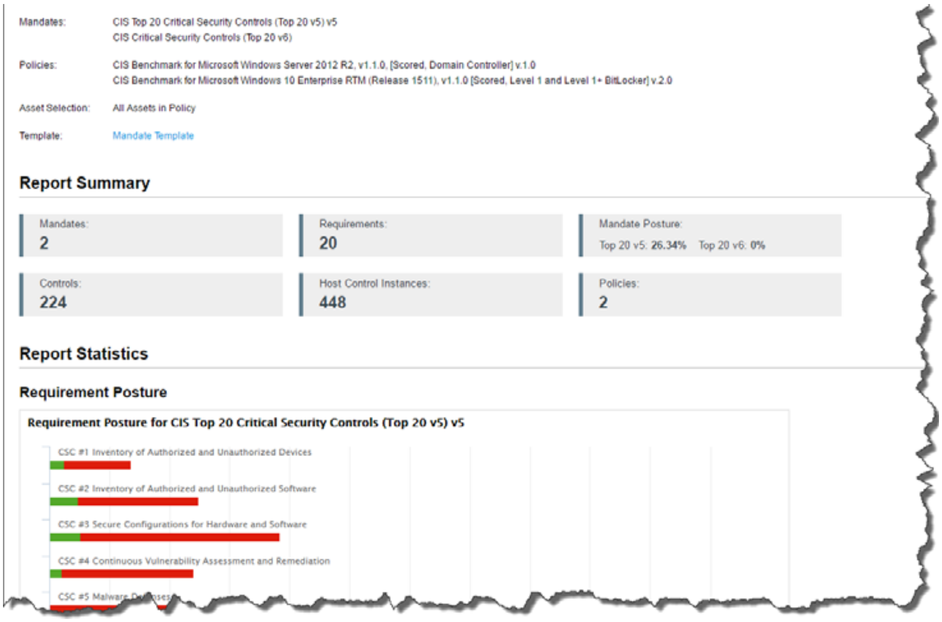
Select mandates (maximum 3):

Add mandates: Search...

1 mandate selected

CIS Critical Security Controls (Top 20 v6)

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



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

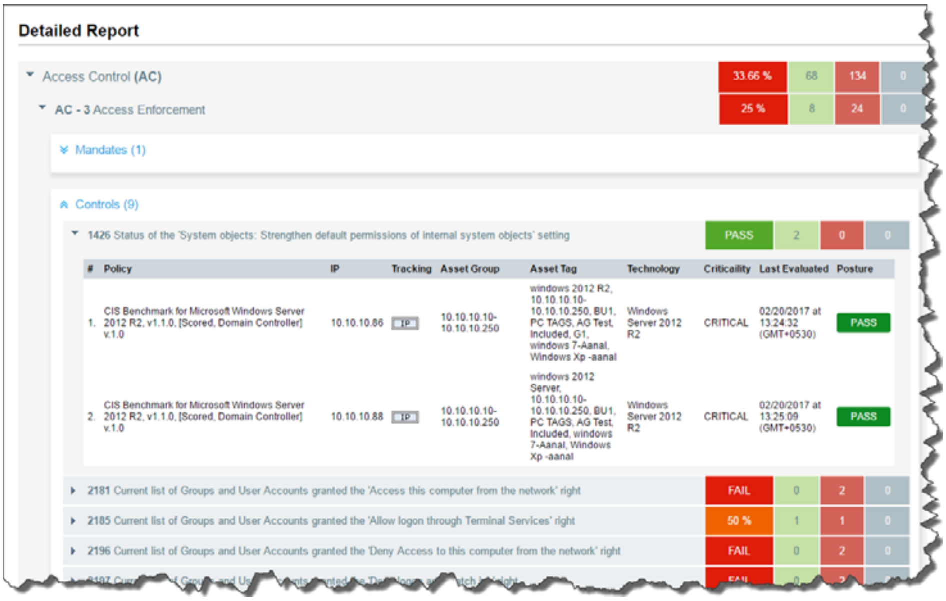
Report Statistics

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

In the Detailed Report section of the report, you can view and drill down to view posture of the control objectives.



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	Criticality	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

Compliance Scorecard Report

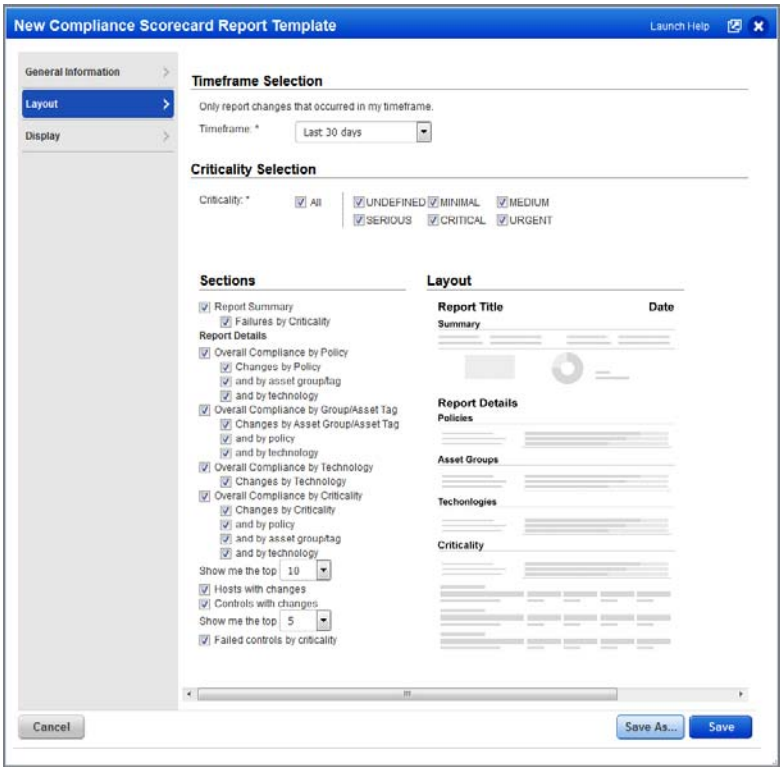
The Compliance Scorecard Report allows you to:

- Report on multiple policies in a single report (up to 20 policies)
- Report your compliance score across selected policies for specific environments (up to 10 asset groups or asset tags)
- View compliance status by policy, by asset group/tag, by technology and by criticality
- Include a breakdown of compliance status changes over a period of time
- Get a list of the top hosts and controls that changed during your selected timeframe

The Scorecard Report requires a scorecard report template. The template settings identify the sections you want to include in the report and the timeframe you want to report on (from the last 1 day to the last 90 days). The service provides a global “Compliance Scorecard Report” template to help you get started. You can use this template as is or customize the settings.

Here’s a look at the compliance scorecard report template.

You’ll notice that there are multiple ways you can report on your compliance data – by policy, by asset group/asset tag, by technology and by criticality. For each section, you can include the current compliance status plus details about compliance status changes.



New Compliance Scorecard Report Template

Timeframe Selection

Only report changes that occurred in my timeframe.

Timeframe: * Last 30 days

Criticality Selection

Criticality: * ☑ All | ☑ UNDEFINED ☑ MINIMAL ☑ MEDIUM ☑ SERIOUS ☑ CRITICAL ☑ URGENT

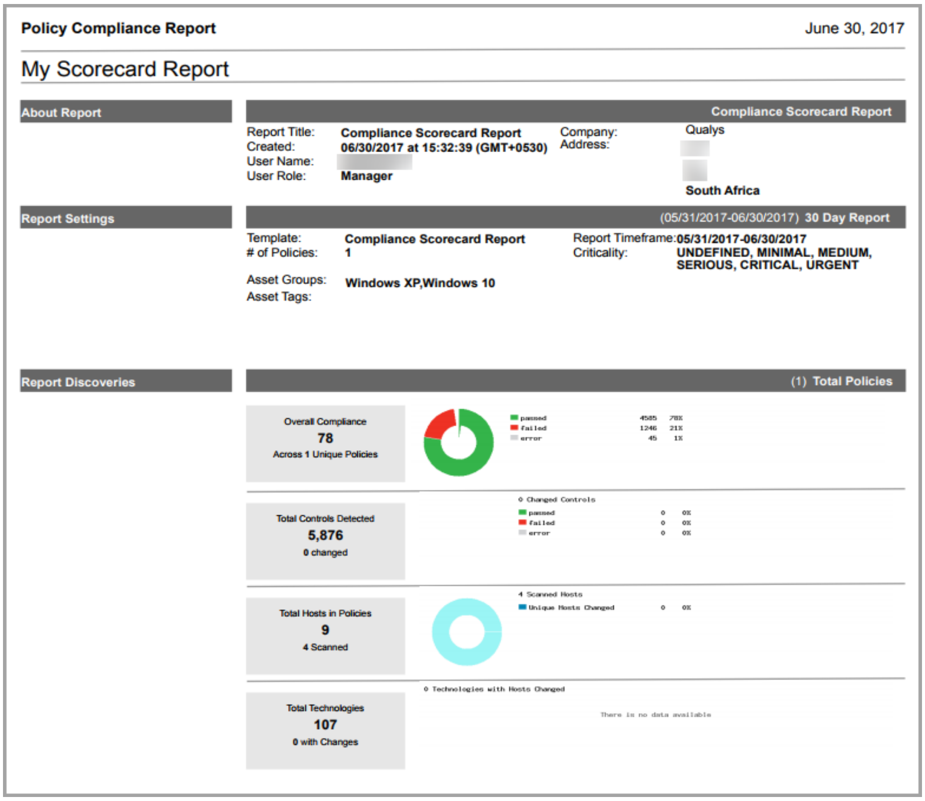
Sections

- ☑ Report Summary
  - ☑ Failures by Criticality
- Report Details
- ☑ Overall Compliance by Policy
  - ☑ Changes by Policy
  - ☑ and by asset group/tag
  - ☑ and by technology
- ☑ Overall Compliance by Group/Asset Tag
  - ☑ Changes by Asset Group/Asset Tag
  - ☑ and by policy
  - ☑ and by technology
- ☑ Overall Compliance by Technology
  - ☑ Changes by Technology
- ☑ Overall Compliance by Criticality
  - ☑ Changes by Criticality
  - ☑ and by policy
  - ☑ and by asset group/tag
  - ☑ and by technology
- Show me the top 10
- ☑ Hosts with changes
- ☑ Controls with changes
- Show me the top 5
- ☑ Failed controls by criticality

To run the Scorecard Report, select New > Compliance Report > Scorecard Report. Choose a template and format. Then select up to 20 policies and up to 10 asset groups or asset tags for your report. Your report will only include compliance evaluation data for hosts that match at least one of the selected policies and at least one of the selected asset groups. Click Run.

Sample Scorecard Report:

Here’s a look at the summary section of the scorecard report. You can quickly see your overall compliance score across the selected policies, the number of control instances with changes, the number of hosts with changes, the number of technologies with hosts that changed, and more.



Policy Compliance Report June 30, 2017

My Scorecard Report

About Report — **Compliance Scorecard Report**

Report Title: **Compliance Scorecard Report**
Created: **06/30/2017 at 15:32:39 (GMT+0530)**
User Name: [redacted]
User Role: **Manager**

Company: Qualys
Address: [redacted]
South Africa

Report Settings — (05/31/2017-06/30/2017) **30 Day Report**

Template: **Compliance Scorecard Report**
# of Policies: **1**

Asset Groups: **Windows XP,Windows 10**
Asset Tags:

Report Timeframe: **05/31/2017-06/30/2017**
Criticality: **UNDEFINED, MINIMAL, MEDIUM, SERIOUS, CRITICAL, URGENT**

Report Discoveries — (1) **Total Policies**

Overall Compliance
78
Across 1 Unique Policies

```
🟩 passed     4585   78%
🟥 failed     1246   21%
▨ error        45    1%
```

Total Controls Detected
5,876
0 changed

```
0 Changed Controls
🟩 passed      0   0%
🟥 failed      0   0%
▨ error        0   0%
```

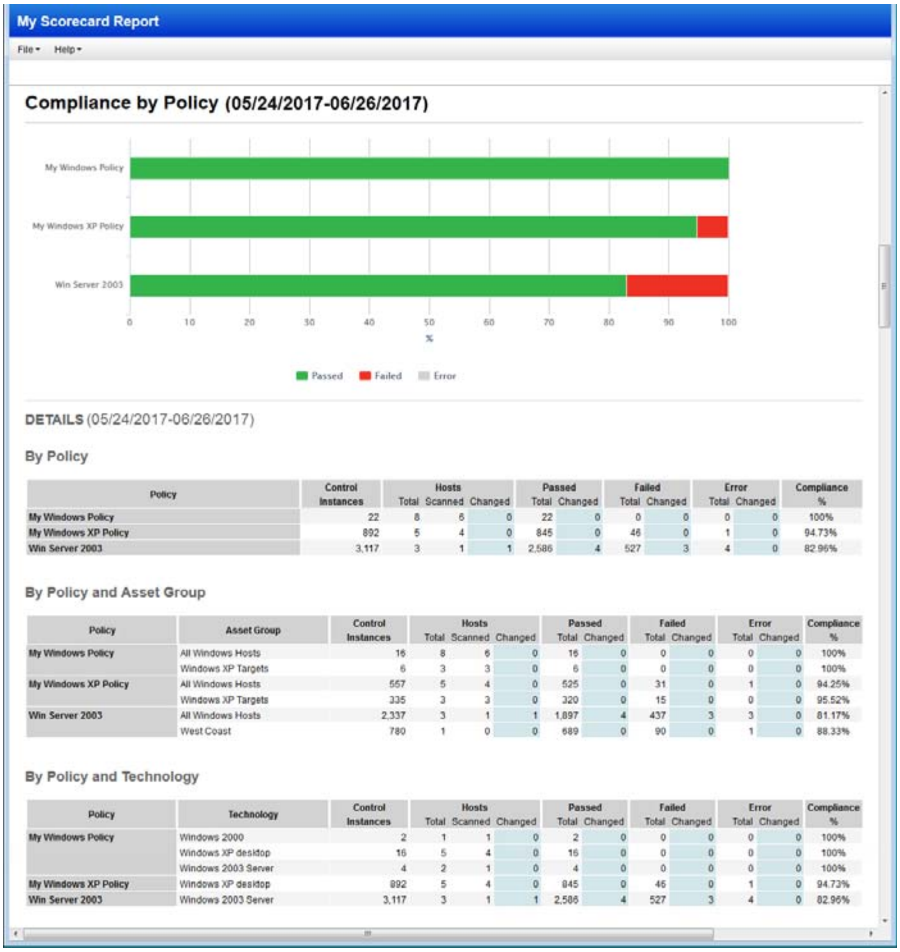
Total Hosts in Policies
9
4 Scanned

```
4 Scanned Hosts
🟦 Unique Hosts Changed   0   0%
```

Total Technologies
107
0 with Changes

```
0 Technologies with Hosts Changed
There is no data available
```

Here’s an example of the compliance by policy section where you get your current compliance status for each policy with the number of passed and failed control instances, plus the detailed changes for each policy.



Compliance by Policy (05/24/2017-06/26/2017)

DETAILS (05/24/2017-06/26/2017)

By Policy

Policy	Control Instances	Hosts			Passed		Failed		Error		Compliance %
		Total	Scanned	Changed	Total	Changed	Total	Changed	Total	Changed	
My Windows Policy	22	8	6	0	22	0	0	0	0	0	100%
My Windows XP Policy	892	5	4	0	845	0	46	0	1	0	94.73%
Win Server 2003	3,117	3	1	1	2,586	4	527	3	4	0	82.96%

By Policy and Asset Group

Policy	Asset Group	Control Instances	Hosts			Passed		Failed		Error		Compliance %
			Total	Scanned	Changed	Total	Changed	Total	Changed	Total	Changed	
My Windows Policy	All Windows Hosts	16	8	6	0	16	0	0	0	0	0	100%
	Windows XP Targets	6	3	3	0	6	0	0	0	0	0	100%
My Windows XP Policy	All Windows Hosts	557	5	4	0	525	0	31	0	1	0	94.25%
	Windows XP Targets	335	3	3	0	320	0	15	0	0	0	95.52%
Win Server 2003	All Windows Hosts	2,337	3	1	1	1,897	4	437	3	3	0	81.17%
	West Coast	780	1	0	0	689	0	90	0	1	0	88.33%

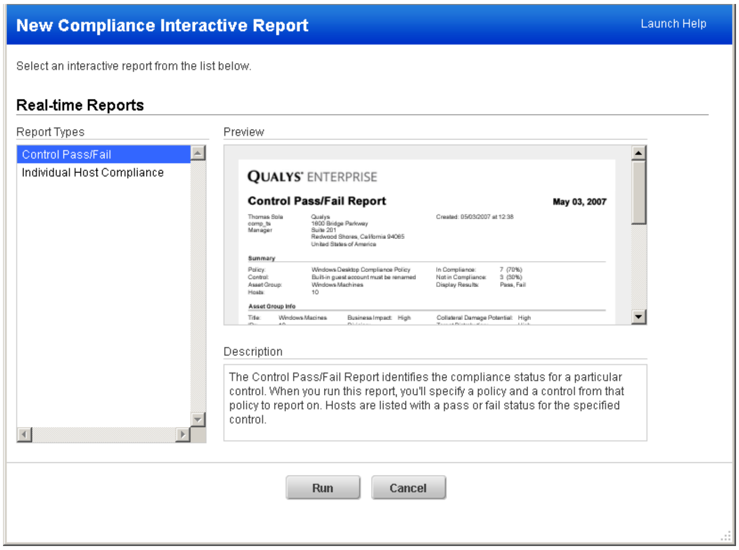
By Policy and Technology

Policy	Technology	Control Instances	Hosts			Passed		Failed		Error		Compliance %
			Total	Scanned	Changed	Total	Changed	Total	Changed	Total	Changed	
My Windows Policy	Windows 2000	2	1	1	0	2	0	0	0	0	0	100%
	Windows XP desktop	16	5	4	0	16	0	0	0	0	0	100%
	Windows 2003 Server	4	2	1	0	4	0	0	0	0	0	100%
My Windows XP Policy	Windows XP desktop	892	5	4	0	845	0	46	0	1	0	94.73%
Win Server 2003	Windows 2003 Server	3,117	3	1	1	2,586	4	527	3	4	0	82.96%

Control Pass/Fail Report

The Control Pass/Fail Report identifies the pass/fail status for a specific control. When running this report, identify the policy and control you want to report on. Hosts included in the report are listed with a pass or fail status for the specified control.

To run the Control Pass/Fail Report, click the Reports tab and select New > Compliance Report > Interactive report and then select Control Pass/Fail and click Run.



New Compliance Interactive Report

Select an interactive report from the list below.

Real-time Reports

Report Types: Control Pass/Fail (selected), Individual Host Compliance

Preview:

QUALYS ENTERPRISE

Control Pass/Fail Report — **May 03, 2007**

Thomas Sola, comp_ts, Manager — Qualys, 1600 Bridge Parkway, Suite 201, Redwood Shores, California 94065, United States of America — Created: 05/03/2007 at 12:38

Summary

Policy:	Windows Desktop Compliance Policy	In Compliance:	7 (70%)
Control:	Built-in guest account must be renamed	Not in Compliance:	3 (30%)
Asset Group:	Windows Machines	Display Results:	Pass, Fail
Hosts:	10		

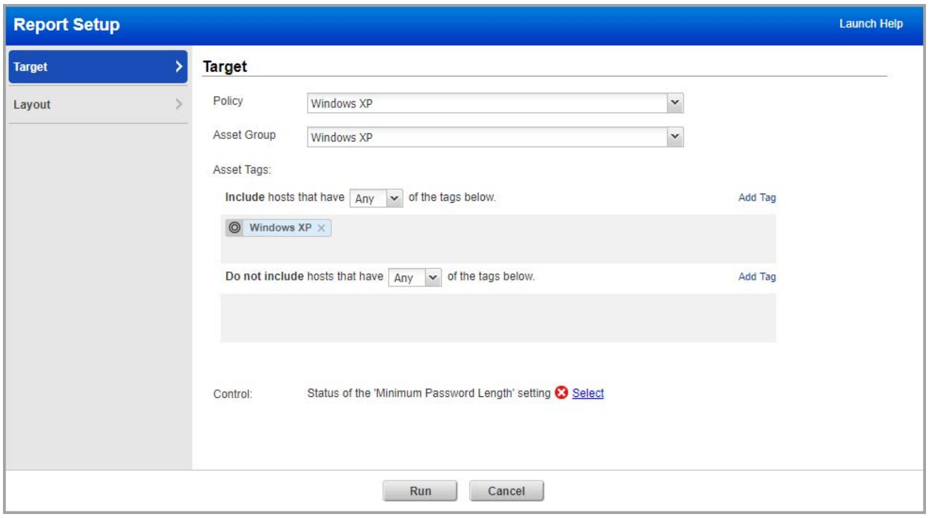
Asset Group Info

Title: Windows Macines — Business Impact: High — Collateral Damage Potential: High

Description:

The Control Pass/Fail Report identifies the compliance status for a particular control. When you run this report, you'll specify a policy and a control from that policy to report on. Hosts are listed with a pass or fail status for the specified control.

The report setup wizard prompts you to select report settings.



Report Setup

Target

Policy: Windows XP

Asset Group: Windows XP

Asset Tags:

Include hosts that have Any of the tags below.

Windows XP

Do not include hosts that have Any of the tags below.

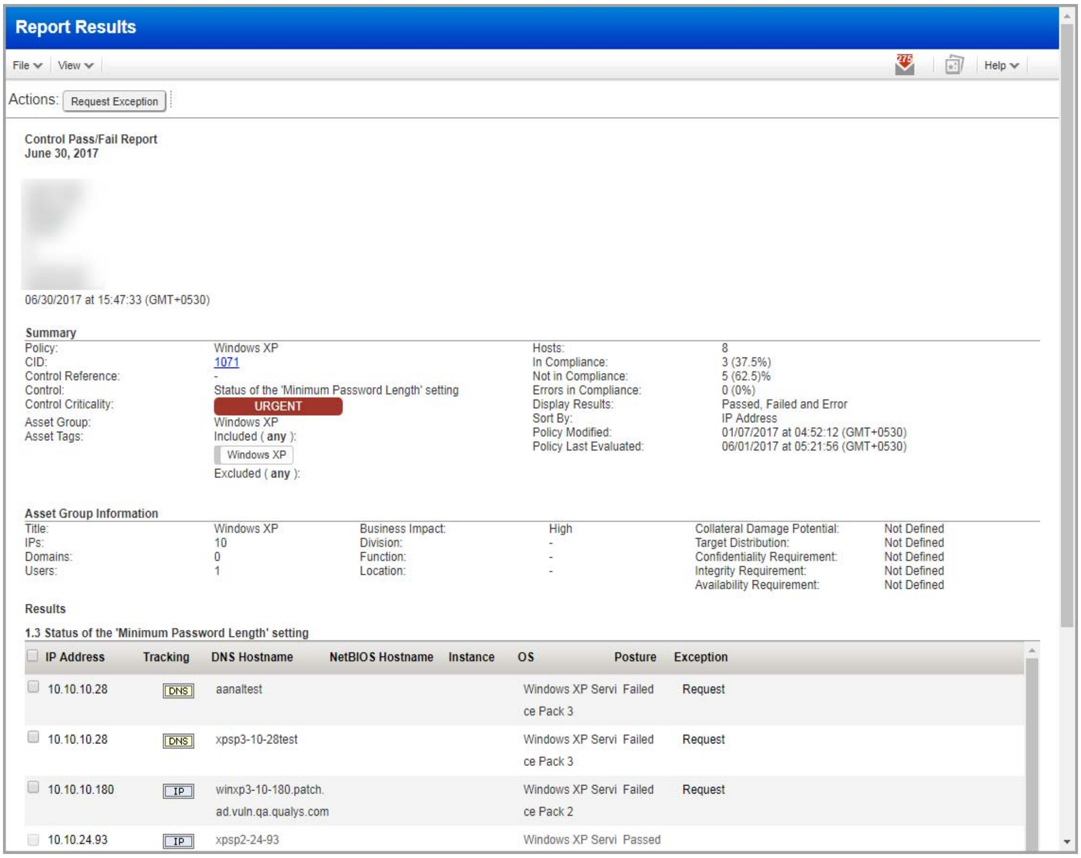
Control: Status of the 'Minimum Password Length' setting

1. Select a policy in your account and a control within that policy.
2. Select an asset group that is assigned to the policy (this option is available to Managers and Auditors) to report on.

3. Click Run to start report generation.

The completed report appears in the same window. Note that this report is dynamically generated and it is not saved on your reports list.

Sample Control Pass/Fail Report:



Control Pass/Fail Report
June 30, 2017

06/30/2017 at 15:47:33 (GMT+0530)

Summary

Policy:	Windows XP	Hosts:	8
CID:	1071	In Compliance:	3 (37.5%)
Control Reference:	-	Not in Compliance:	5 (62.5)%
Control:	Status of the 'Minimum Password Length' setting	Errors in Compliance:	0 (0%)
Control Criticality:	URGENT	Display Results:	Passed, Failed and Error
Asset Group:	Windows XP	Sort By:	IP Address

Asset Tags:	Included (**any**):
	Windows XP
	Excluded (**any**):
		Policy Modified:	01/07/2017 at 04:52:12 (GMT+0530)

		Policy Last Evaluated:	06/01/2017 at 05:21:56 (GMT+0530)

Asset Group Information

Title:	Windows XP	Business Impact:	High	Collateral Damage Potential:	Not Defined
IPs:	10	Division:	-	Target Distribution:	Not Defined
Domains:	0	Function:	-	Confidentiality Requirement:	Not Defined
Users:	1	Location:	-	Integrity Requirement:	Not Defined
				Availability Requirement:	Not Defined

Results

1.3 Status of the 'Minimum Password Length' setting

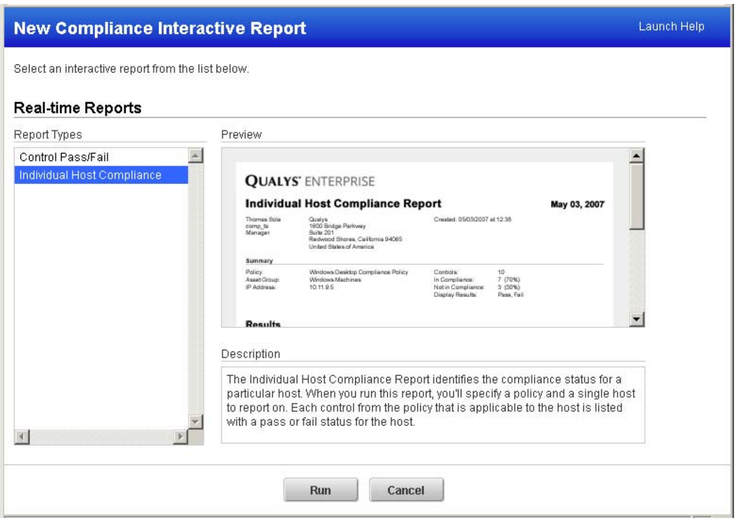
□	IP Address	Tracking	DNS Hostname	NetBIOS Hostname	Instance	OS	Posture	Exception
□	10.10.10.28	DNS	aanaltest			Windows XP Service Pack 3	Failed	Request
□	10.10.10.28	DNS	xpsp3-10-28test			Windows XP Service Pack 3	Failed	Request
□	10.10.10.180	IP	winxp3-10-180.patch.ad.vuln.qa.qualys.com			Windows XP Service Pack 2	Failed	Request
□	10.10.24.93	IP	xpsp2-24-93			Windows XP Servi	Passed	

The Posture column identifies the status for the control on each host. Passed indicates that the expected value defined in the policy for the control matches the actual value returned during the last compliance scan on the host. Failed indicates that the expected value defined in the policy for the control does not match the actual value returned during the last compliance scan on the host. Passed^{E} indicates that the host is exempt from the control. This means that an exception was requested and accepted for the control on the host.

Individual Host Compliance Report

The Individual Host Compliance Report identifies the compliance status for a specific host. When running this report, identify the policy and host you want to report on. Each control from the policy that is applicable to the host is listed with a pass or fail status.

To run the Individual Host Compliance Report, click the Reports tab and select New > Compliance Report > Interactive report and then select Individual Host Compliance.



Select an interactive report from the list below.

Real-time Reports

Report Types

- Control Pass/Fail
- Individual Host Compliance

Preview

QUALYS ENTERPRISE

Individual Host Compliance Report **May 03, 2007**

Thomas Sola
comp_ts
Manager

Qualys
1600 Bridge Parkway
Suite 201
Redwood Shores, California 94065
United States of America

Created: 05/03/2007 at 12:38

Summary

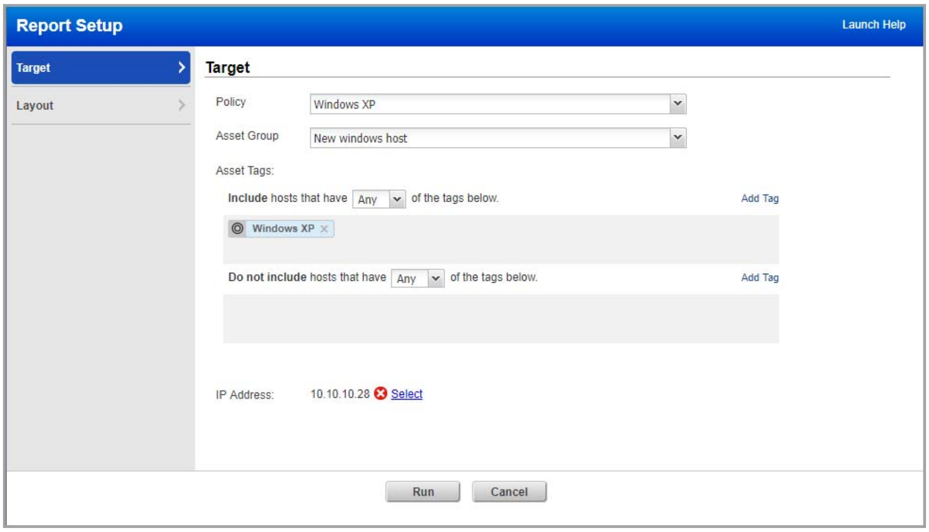
Policy:	Windows Desktop Compliance Policy	Controls:	10
Asset Group:	Windows Machines	In Compliance:	7 (70%)
IP Address:	10.11.9.5	Not in Compliance:	3 (30%)
		Display Results:	Pass, Fail

Results

Description

The Individual Host Compliance Report identifies the compliance status for a particular host. When you run this report, you'll specify a policy and a single host to report on. Each control from the policy that is applicable to the host is listed with a pass or fail status for the host.

The report setup wizard prompts you to select report settings.



Target

Policy: Windows XP

Asset Group: New windows host

Asset Tags:

Include hosts that have Any of the tags below. Add Tag

Windows XP ×

Do not include hosts that have Any of the tags below. Add Tag

IP Address: 10.10.10.28 Select

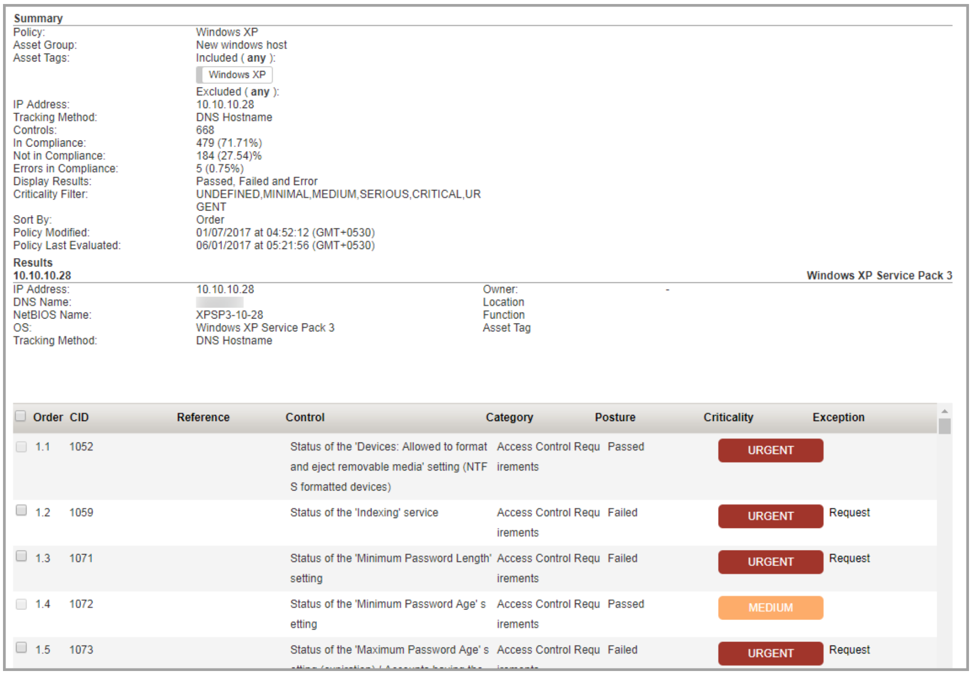
1. Select a policy in your account.
2. Select an asset group that is assigned to the policy (this option is available to Managers and Auditors), and then click the Select link to select a host (IP address) to report on.

3 Tell us whether you want to show controls that passed for the host, that failed for the host, or both. You can also filter the report by criticality levels.

4 For Sort by, specify how you want hosts to be sorted. You may select one of these options: Order (the order of the controls in the policy), Control, Category, Posture, Exception (status).

5 Click Run to start the report generation.

Sample Individual Host Compliance Report:



Summary

Policy:	Windows XP
Asset Group:	New windows host

Asset Tags:	Included (**any**):
	Windows XP
	Excluded (**any**):

IP Address:	10.10.10.28
Tracking Method:	DNS Hostname
Controls:	668
In Compliance:	479 (71.71%)
Not in Compliance:	184 (27.54)%
Errors in Compliance:	5 (0.75%)
Display Results:	Passed, Failed and Error
Criticality Filter:	UNDEFINED,MINIMAL,MEDIUM,SERIOUS,CRITICAL,URGENT
Sort By:	Order
Policy Modified:	01/07/2017 at 04:52:12 (GMT+0530)
Policy Last Evaluated:	06/01/2017 at 05:21:56 (GMT+0530)

Results

10.10.10.28 **Windows XP Service Pack 3**

IP Address:	10.10.10.28	Owner:	-
DNS Name:	[redacted]	Location	
NetBIOS Name:	XPSP3-10-28	Function	
OS:	Windows XP Service Pack 3	Asset Tag	
Tracking Method:	DNS Hostname		

□	Order	CID	Reference	Control	Category	Posture	Criticality	Exception
□	1.1	1052		Status of the 'Devices: Allowed to format and eject removable media' setting (NTFS formatted devices)	Access Control Requirements	Passed	URGENT	
□	1.2	1059		Status of the 'Indexing' service	Access Control Requirements	Failed	URGENT	Request
□	1.3	1071		Status of the 'Minimum Password Length' setting	Access Control Requirements	Failed	URGENT	Request
□	1.4	1072		Status of the 'Minimum Password Age' setting	Access Control Requirements	Passed	MEDIUM	
□	1.5	1073		Status of the 'Maximum Password Age' s	Access Control Requ	Failed	URGENT	Request

In the Results section, click on a control in the list to display scan results for the control on the host. The Expected value is the value as defined in the policy. The Actual value represents the compliance data retrieved from the most recent compliance scan. The service compares the actual value to the expected value to determine the compliance status.

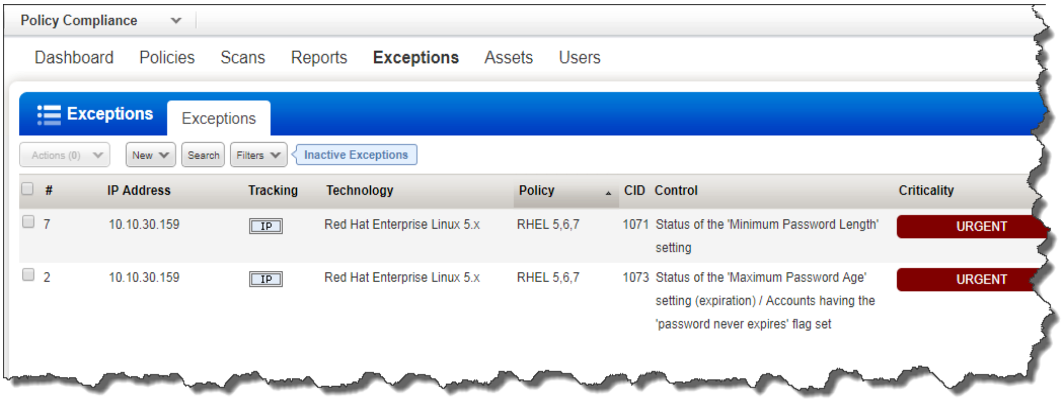
Managing exceptions

Users may request exceptions for some hosts/controls in a selected policy to support a business need. For example a compliance policy may have a control that states the service FTP is not allowed on a server, however there may be a business requirement to exempt one or more hosts from this particular control in the policy. Users submit exceptions for one or more hosts/controls in a policy that failed compliance. When approved, compliance reports do not fail compliance for the hosts/controls in the exception request for a period of time defined in the request.

The exceptions workflow allows all users to submit and view exception requests and their status. Managers and Auditors can approve exception requests; Unit Managers may approve requests submitted by users in their business unit when this privileges is granted in their user account. User actions on exceptions are logged in the exception history.

You request exceptions from these interactive reports: Control Pass/Fail Report and Individual Host Compliance Report. In the report results, simply identify the control/host that needs an exception and select the check box next to each control/host that you want to include in the request and then click the Request Exception button at the top of the report.

See all exceptions on your hosts in the Exceptions tab. Select Info from the Quick Actions menu for any exception to view complete details, including the related policy, control and technology, plus the expected control value as defined in the policy and the actual value returned during the compliance scan. You can also view a history log for the exception.



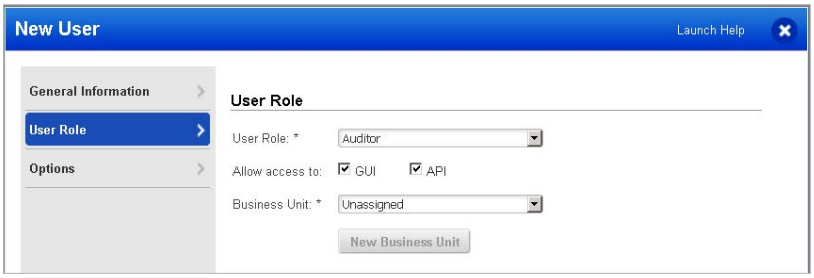
□	#	IP Address	Tracking	Technology	Policy	CID	Control	Criticality
□	7	10.10.30.159	IP	Red Hat Enterprise Linux 5.x	RHEL 5,6,7	1071	Status of the 'Minimum Password Length' setting	URGENT
□	2	10.10.30.159	IP	Red Hat Enterprise Linux 5.x	RHEL 5,6,7	1073	Status of the 'Maximum Password Age' setting (expiration) / Accounts having the 'password never expires' flag set	URGENT

Tips and Tricks

Add Auditor Users

Create users with the Auditor user role to perform compliance management tasks. Auditors can create and manage compliance policies for the subscription, generate reports on compliance data and manage exception requests. Auditors are automatically part of the Unassigned business unit and have permission to all compliance hosts defined for the subscription. Note that Auditors only have visibility into compliance data (not vulnerability data). Auditors cannot perform any vulnerability management functions.

To add an Auditor, select New > User above the user list. Using the wizard, provide general information such as user name and address. continue to the User Role section and select Auditor from the User Role menu.



User Role

User Role: * Auditor

Allow access to: ☑ GUI ☑ API

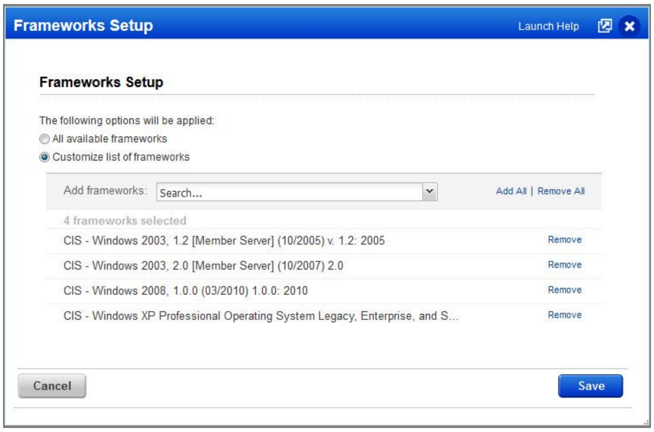
Business Unit: * Unassigned

The first time the Auditor logs in they will see the Quick Start with links to compliance management features. An Auditor can create asset groups including compliance hosts, create a policy, create policy report templates and run compliance reports.

Customize Frameworks for the Subscription

When you view technical control information the details include a list of frameworks, standards and regulations that the control maps to. Manager users have the option to customize the list to only display selected frameworks. This setting is made at the subscription level and affects the list of frameworks displayed to all users in technical control details and in PC reports. By customizing the list to only select frameworks, you can reduce the size of your reports.

To customize the frameworks list, go to Policies, click the Setup tab, and then select Frameworks. Select the option “Customize list of frameworks” and then select the frameworks you want to display in the subscription. Additionally, any user with compliance management privileges can customize the list of frameworks in their compliance policy reports. This setting is made in the policy report template.



Frameworks Setup

The following options will be applied:

○ All available frameworks
● Customize list of frameworks

Add frameworks: Search...

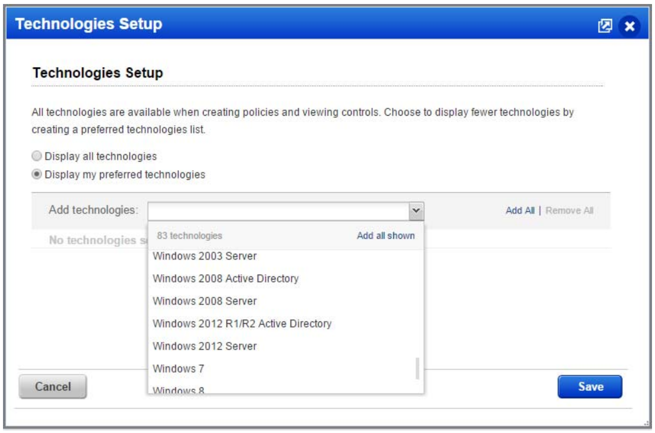
4 frameworks selected

CIS - Windows 2003, 1.2 [Member Server] (10/2005) v. 1.2: 2005	Remove
CIS - Windows 2003, 2.0 [Member Server] (10/2007) 2.0	Remove
CIS - Windows 2008, 1.0.0 (03/2010) 1.0.0: 2010	Remove
CIS - Windows XP Professional Operating System Legacy, Enterprise, and S...	Remove

Customize Technologies for the Subscription

You can hide the technologies that you do not use on a regular basis. By hiding these technologies, Manager users ensure that you no longer need to go through the whole list of all the available technologies to select the ones you want. This is especially useful while searching controls by technologies. Only the controls related to the preferred technologies are displayed and are available for search.

To customize the technologies list, go to Policies, click the Setup tab, and then select Technologies. Create a list of preferred technologies that should be displayed. For example, let's say you're interested only in Windows. You add all the Windows technologies to your preferred list. All other technologies like Unix, Sybase, Solaris, etc will be hidden.



Technologies Setup

All technologies are available when creating policies and viewing controls. Choose to display fewer technologies by creating a preferred technologies list.

○ Display all technologies
● Display my preferred technologies

Add technologies:

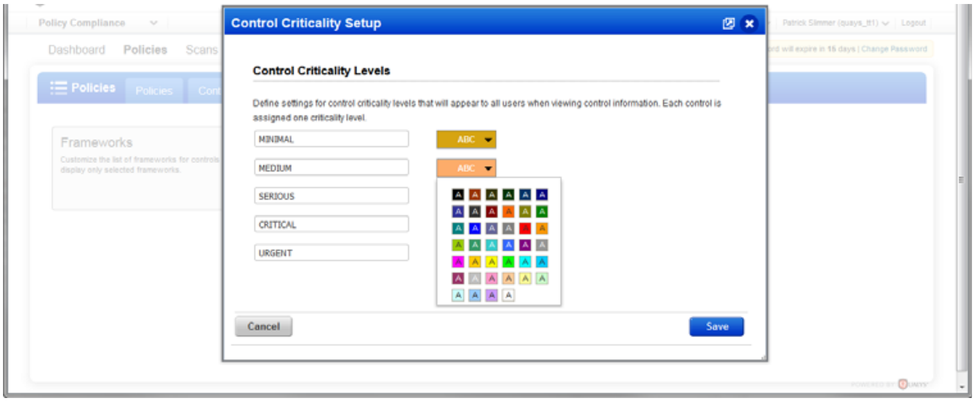
No technologies s

83 technologies

Windows 2003 Server
Windows 2008 Active Directory
Windows 2008 Server
Windows 2012 R1/R2 Active Directory
Windows 2012 Server
Windows 7
Windows 8

Review & Customize Control Criticality

Control Criticality provides ratings for controls, including the ability to customize ratings at the control level and at the policy level. Criticality appears in control details – in the controls list, in your policies and reports. We've defined 5 criticality levels ranging from Minimal to Urgent. You can rename these levels and change their colors if you want (go to PC > Policies > Setup and select Control Criticality Levels).


Policy Compliance
Dashboard
Policies
Scans
Policies
Policies
Cont
Frameworks
Customize the list of frameworks for controls
display only selected frameworks.
Patrick Slimmer (quays_tt1)
Logout
rd will expire in 15 days | Change Password
Control Criticality Setup
ABC
ABC
A
Cancel
Save

Control Criticality Levels

Define settings for control criticality levels that will appear to all users when viewing control information. Each control is assigned one criticality level.

MINIMAL
MEDIUM
SERIOUS
CRITICAL
URGENT

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/.