



**Qualys®**

## **QSC 2021 Configuration Assessment & Response**

**Lab Tutorial Supplement**

# Table of Contents

<b>Policy Compliance Assets</b> .....	<b>3</b>
<b>Scannable Host Assets</b> .....	<b>3</b>
<b>Agent Host Assets</b> .....	<b>4</b>
<b>Control Library</b> .....	<b>6</b>
<b>User Defined Controls</b> .....	<b>6</b>
File Content Check UDC.....	6
File Integrity Check UDC.....	7
Registry Value Content Check UDC.....	9
WMI Query Check UDC.....	10
<b>Compliance Scanning</b> .....	<b>11</b>
<b>Agent Scans</b> .....	<b>11</b>
Agent Middleware Technologies Discovered.....	12
<b>Scanner Appliance Scans</b> .....	<b>13</b>
Compliance Profile.....	13
Launch Compliance Scan.....	16
Scan Results.....	17
<b>Policy Scope</b> .....	<b>18</b>
<b>Asset Groups</b> .....	<b>18</b>
<b>Asset Tags</b> .....	<b>19</b>
<b>Policy Scope</b> .....	<b>19</b>
<b>Create Policy</b> .....	<b>20</b>
<b>Import Policy from Library</b> .....	<b>21</b>
<b>Create Empty Policy</b> .....	<b>23</b>
<b>Cardinality</b> .....	<b>25</b>
contains.....	27
does not contain.....	28
matches.....	29
is contained in.....	30
intersect.....	31
<b>Compliance Reports</b> .....	<b>32</b>
<b>Authentication Report</b> .....	<b>32</b>
<b>Policy Report</b> .....	<b>33</b>
<b>Interactive Reports</b> .....	<b>35</b>
Requesting Exceptions.....	35
Working With Exception Requests.....	39
The Auditor Role.....	39
<b>Policy Compliance Certification Exam</b> .....	<b>41</b>
<b>Course Survey and Trial Account</b> .....	<b>43</b>

# Policy Compliance Assets

Qualys Policy Compliance (PC) and Security Configuration Assessment (SCA) perform automated compliance assessments on IT systems throughout your network or enterprise architecture.

**Navigate to the following URL to view the “Policy Compliance Assets” tutorial:**



LAB 1 - <https://ior.ad/7RDL>

## Scannable Host Assets

Host assets can be added to your Policy Compliance subscription by adding their IP addresses into the list of “scannable” assets.

**Add IPs to Subscription** Launch Help

**General Information** > **Subscription IPs**  
**Subscription IPs** >  
**Host Attributes** >

**Subscription IPs**

Enter IPs and ranges in the field below. See the [Help](#) for proper formatting.

Network:  
You can choose any network. New IPs will be available to all networks, regardless of your selection. Custom host attributes will be applied only to the selected network.

**It is your responsibility to verify that you have permission to scan all IPs submitted.**

IPs: \*

64.41.200.243-64.41.200.251

(ex: 192.168.0.200,192.168.0.87-192.168.0.92, fe80::250:56ff:fe90:aaa0, fe80::250:56ff:fe90:aaa1)  
Validate IPs through [Whois](#)

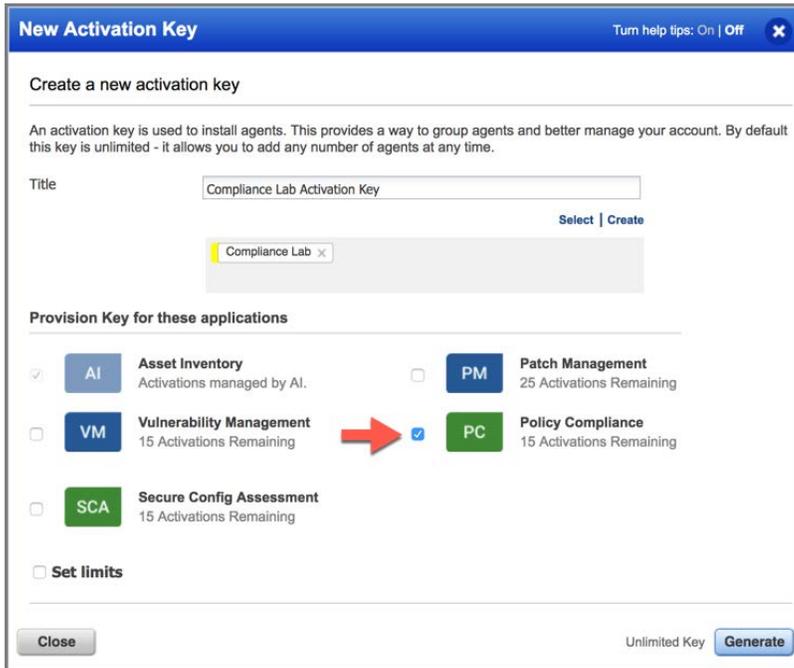
**Add To:**

**VM** Vulnerability Management Unlimited  
 **PC** Policy Compliance Unlimited  
 **SCA** Security Configuration Assessment 99724  
 **CERT** CertView 99923

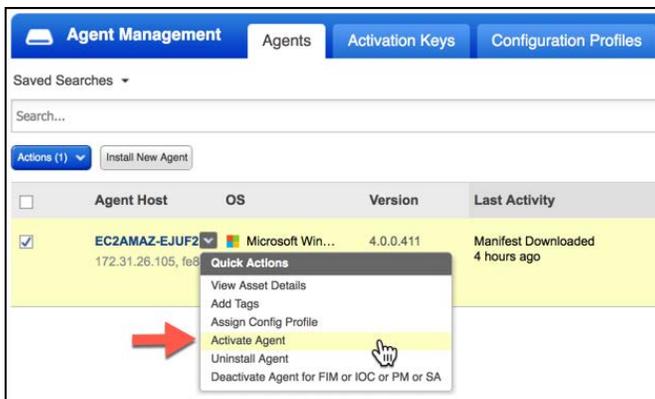
After entering one or more IP addresses, select the PC application module or the Security Configuration Assessment (SCA) module.

# Agent Host Assets

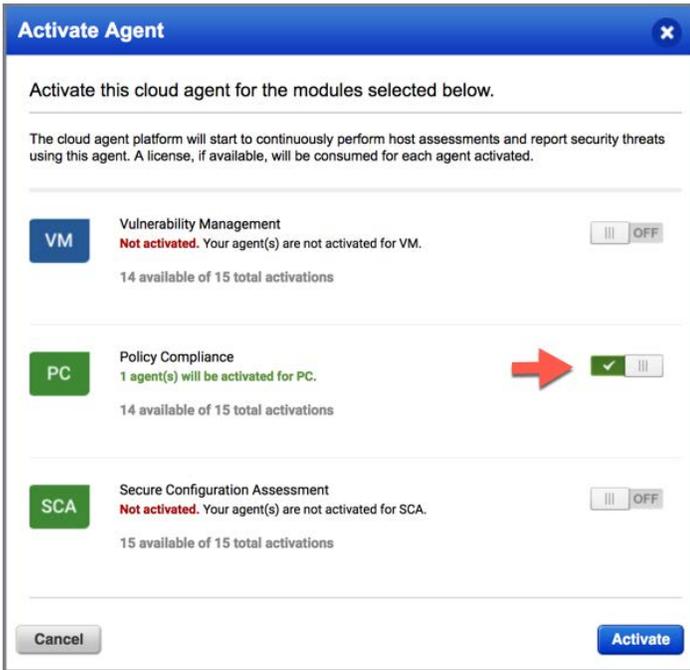
Host assets can also be added to your Policy Compliance subscription by installing one or more Qualys Cloud Agents (with the PC or SCA module enabled) on targeted host assets.



Alternatively, you can activate the PC or SCA module after Cloud Agent has been installed.



From the Qualys Cloud Agent application, open the “Quick Actions” menu for any host and select the “Activate Agent” option.



Toggle the PC or SCA switch to the "ON" position and click the "Activate" button. Agents can be activated in bulk, using the Cloud Agent Application Program Interface (API).

# Control Library

The Control Library contains thousands of technical controls, which form the building blocks for all policies. Each control has its own unique Control ID (CID).

Types of Controls



**System Defined Control (SDC)** - These are controls provided by Qualys.



**User Defined Control (UDC)** - These are custom controls that users create.

The Control Library contains System Defined Controls (provided by Qualys), which are designed around various regulatory requirements, standards, frameworks, benchmarks and best practices.

You can also add your own “custom” User Defined Controls (UDCs) to the Control Library

## User Defined Controls

User Defined Controls (UDCs) extend the coverage already provided by System Defined Controls (SDCs). UDCs created and customized by an end user, are automatically added to the Control Library. You can create any number of custom UDCs, to meet the specific needs of your organization.

### File Content Check UDC

Much useful configuration data can still be found within text-based files (especially on Unix and Linux systems). The “File Content Check” control type, allows you to enumerate the contents of a text-based file.

**Navigate to the following URL to view the “File Content Check UDC” tutorial:**



LAB 2 - <https://ior.ad/7S4L>

The objective in this example, is to ensure that remote access (via SSH) is disabled for the ‘root’ user account. The Scan Parameters specify the targeted datapoint or configuration setting this control will evaluate.

Scan Parameters*	
The scan parameters, or data point, indicate what location, file, or setting for the scan to check.	
File path	/etc/ssh/sshd_config
Regular expression	^\s*[^#]
Data Type:	Line List
Description: *	List uncommented lines in sshd_config.

In this example, only uncommented lines (`^\s*[^#]`) within file ‘/etc/ssh/sshd\_config’ will be collected.

When the uncommented lines from file 'sshd\_config' are listed, they are then compared to this control's "Default Value."

Default Values for Control Technologies	
Default values are automatically assigned when you click the check box for a technology.	
Rationale: *	<input type="text" value="Fail any host that permits the 'root' account to login remotely."/>
Cardinality: *	<input type="text" value="match none"/>
Operator: *	<input type="text" value="regular expression"/>
Default Value:	<input type="text" value="^\s*PermitRootLogin\s*yes\$"/> <input type="checkbox"/> Lock Value

The cardinality setting of "match none," will ensure host assets FAIL this control test, if any of the lines in 'sshd\_config' contain the setting that allows the 'root' account to login remotely (i.e., ^\s\*PermitRootLogin\s\*yes\$).

Once the Default Value has been configured, it must then be assigned to specific OS and/or software technologies.

## File Integrity Check UDC

Integrity checks can help you to identify when updates or changes are made to critical or sensitive files or directories. Qualys Policy Compliance provides integrity check UDCs for Windows and Linux hosts. In this lab tutorial, you'll create a User Defined Control (UDC) to perform a file integrity check on a UNIX host.

**Navigate to the following URL to view the "File Integrity Check UDC" tutorial:**

**PLAY** → LAB 3 - <https://ior.ad/7S4Q>

The objective in this example, is to collect the hash value for file 'etc/hosts' to determine if the file has been modified or changed. The Scan Parameters specify the targeted datapoint or configuration setting this control will evaluate.

Scan Parameters*	
The scan parameters, or data point, indicate what location, file, or setting for the scan to check.	
File path	/etc/hosts
Hash Type	SHA-256
Data Type:	String
Description: *	<input type="text" value="Has the /etc/hosts file been changed or modified?"/>

In this example, an SHA-256 hash of file '/etc/hosts' is collected and then compared to this control's "Default Value."

When configuring the Default Value, you have the option to manually enter the file's present hash value or you can have it automatically collected by a Qualys scanner or agent.

### Default Values for Control Technologies

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

Rationale: \*

Operator: \*

Default Value:   Lock Value

Use scan data as expected value

Choose this option if you want to calculate Pass/Fail status for this control by comparing scan data from the previous scan and the latest scan.

This option is used in conjunction with the option "Auto Update expected value".  
For network scans this option is set in the option profile.  
For cloud agent scans this is set under Agent Scan Options for this control.

Select the "Use scan data as expected value" check box (above), to automatically collect and update the hash value of the targeted file, using compliance scan results.

### Agent Scan Options

Auto Update Expected Value

When enabled, we'll update this control's expected value with the actual value collected from each cloud agent scan.  
You must also enable "Use scan data as expected value" in this control (under Control Technologies).  
To create reports reflecting results for each agent scan, schedule your compliance reports to run in between the scan interval defined for your agents.

When the "Use scan data as expected value" option is used with Qualys agent hosts, the "Agent Scan Options" within the UDC (above), should be configured to "Auto Update Expected Value."

### Edit Compliance Profile

Compliance Profile Title > Scan

Scan >

System Authentication >

Additional >

#### Integrity Monitoring

This setting applies to file and directory integrity checks configured with "Use scan data as expected value".  
When enabled, we'll update the control expected value used for posture evaluation with the actual value returned by the scan.

Auto Update expected value

For Qualys scanners, this same option is configurable, under Integrity Monitoring, within the "Scan" section of a Compliance Profile.

## Registry Value Content Check UDC

The Windows System Registry contains a wealth of information that can be used to validate thousands of compliance and auditing objectives. Registry Value Content Checks permit you to validate or verify the content of any registry value.

**Navigate to the following URL to view the “Registry Value Content Check UDC” tutorial:**

**PLAY**

LAB 4 - <https://ior.ad/7S4N>

The objective in this example, is to ensure remote access is disabled on targeted Windows hosts. The Scan Parameters specify the Registry Value this control will evaluate.

Scan Parameters*	
The scan parameters, or data point, indicate what location, file, or setting for the scan to check.	
Registry Hive	HKEY_LOCAL_MACHINE (HKLM)
Registry Key	SYSTEM\CurrentControlSet\Services\TermService
NAME	Start
Data Type:	Integer
Description: *	<input (rdp)."="" for="" service="" start-up"="" terminal="" type="text" value=""/>

In this example, the system “start-up” value (Registry Value = Start) is collected for Windows Terminal Service and then compared to this control’s “Default Value.”

Default Values for Control Technologies	
Default values are automatically assigned when you click the check box for a technology.	
Rationale: *	<input type="text" value="Verify Terminal Service (RDP) is Disabled."/>
Operator: *	<input type="text" value="equal to"/> ▼
Default Value:	<input type="text" value="4"/> <input type="checkbox"/> Lock Value

A “Startup” value of “4” specifies that Terminal Service is disabled:

- 2 = Automatic
- 3 = Manual
- 4 = Disabled

To meet the objective of this control, hosts with a value of four (4) will receive a PASS result.

## WMI Query Check UDC

This User Defined Control (UDC) will use a WMI Query to enumerate the running processes on a Windows host. This list can then be evaluated to identify the absence of REQUIRED applications, and/or the presence of PROHIBITED applications.

**Navigate to the following URL to view the “WMI Query Check UDC” tutorial:**



LAB 5 - <https://ior.ad/7S4K>

The objective in this example, is to identify the presence of prohibited or suspicious applications that may be running on a host. The Scan Parameters specify the targeted datapoint or configuration setting this control will evaluate.

Scan Parameters*	
The scan parameters, or data point, indicate what location, file, or setting for the scan to check.	
Namespace	Root\Cimv2
Query	SELECT Name FROM Win32_Process
Data Type:	String List
Description: *	List All Running Processes

The query in this example will return the list of running process names, from targeted Windows hosts, which are then compared to the list of “prohibited” applications.

Default Values for Control Technologies	
Default values are automatically assigned when you click the check box for a technology.	
Rationale: *	Identify prohibited or suspicious software applications.
Cardinality: *	does not contain
Operator: *	string list
Default Value:	wireshark.exe zenmap.exe

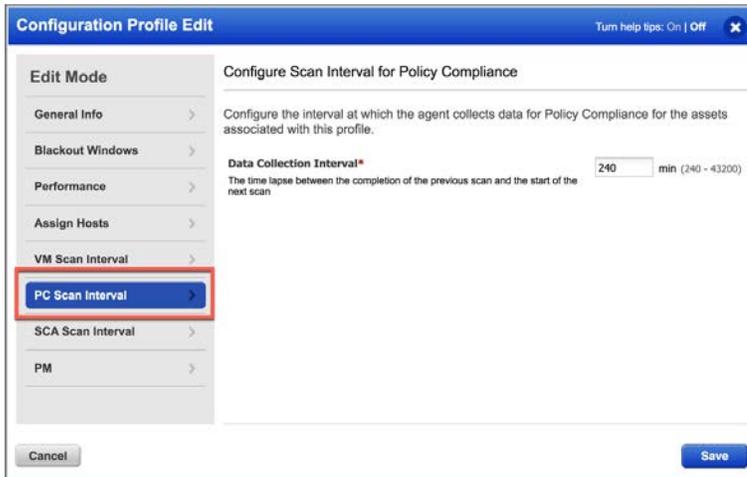
If any of the “prohibited” applications are found to be running on a target host, this control test will produce a FAIL result. The “does not contain” cardinality is required here, to achieve this outcome.

# Compliance Scanning

Whether performed by a Qualys scanner or agent, compliance scans collect data points (defined *in the Qualys Control Library*) from host assets in your account. When new controls are added to the library, additional scans are required to collect their associated data points.

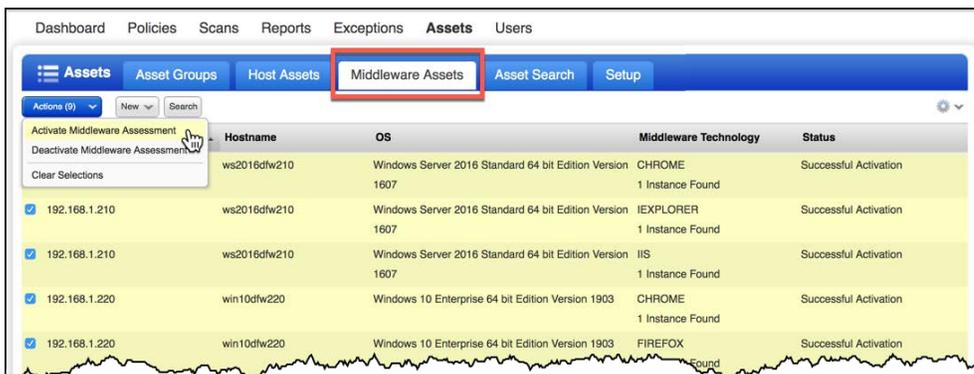
## Agent Scans

Qualys Cloud Agent compliance scans, are automatically performed at configurable intervals.



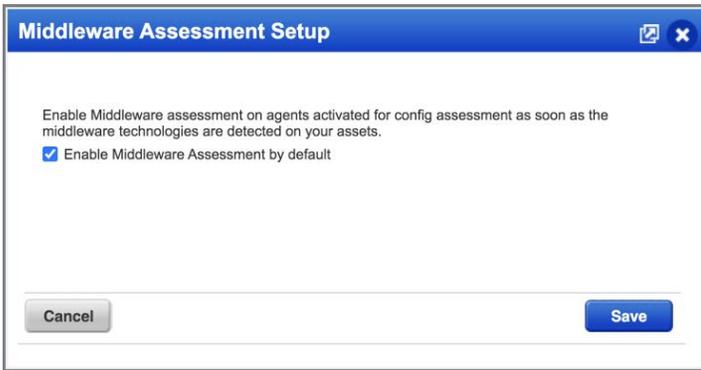
You can customize the “Data Collection Interval” from every four hours, to every 30 days.

From the “Middleware Assets” tab (within the Policy Compliance application) use the “Actions” button to “Activate Middleware Assessment” (for selected host assets).



This will add the Middleware technology manifest to selected agent hosts.

Alternatively, enable Middleware Assessments for all agent hosts in your PC or SCA subscription.



From the PC/SCA application, navigate to: Assets > Setup > Middleware Assessment.

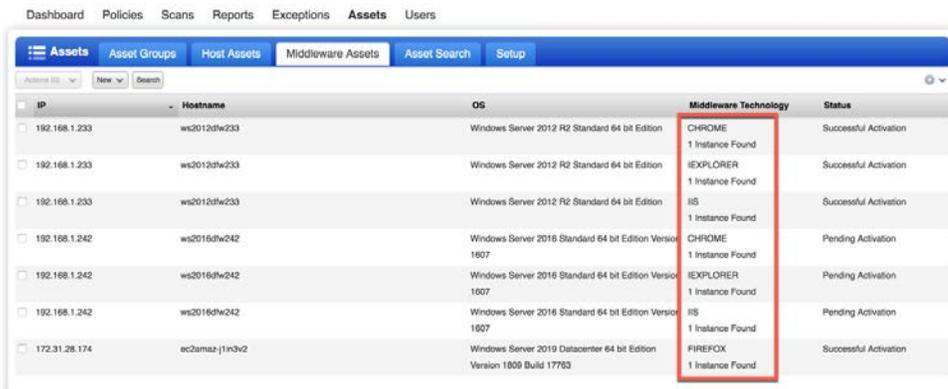
Presently, Qualys Cloud Agent supports the following Linux and Windows middleware technologies.

Linux Agent 2.8.x RHEL/OEL/CentOS/Ubuntu/Amazon Linux	Windows Agent 4.0.x All Windows flavors
Apache Tomcat 7, 8, 9	Apache Tomcat 7, 8, 9
Pivotal tc Server 3.x	MS IIS 7, 8, 10
vFabric tc Server 2.9.x	Internet Explorer 9, 10, 11
Docker 1.x, Docker CE/EE	Microsoft Office (Access, Excel, Outlook, PowerPoint, Word) 2013, 2016, 2019

**Middleware** includes software that provides common services and capabilities to applications outside of what's offered by the operating system.

## Agent Middleware Technologies Discovered

Middleware technology instances discovered during Qualys Cloud Agent scans, are displayed under the "Middleware Assets" tab, within the PC/SCA application.



You can "Activate Middleware Assessments" for individual hosts or all PC/SCA agent hosts.

# Scanner Appliance Scans

To complete a compliance scan, using a Qualys Scanner Appliance, you must provide:

1. Host authentication credentials (via Qualys Authentication Record)
2. Your scanning options and preferences (via Qualys Compliance Profile)

## Compliance Profile

A Compliance Profile contains your scanning options and is a required component of every compliance scan.

**Navigate to the following URL to view the “Compliance Profile” tutorial:**



LAB 6 - <https://ior.ad/7SdX>

## Scan by Policy

By default, a Qualys scanner will attempt to collect all data points that have been defined within the Control Library (depending; of course, on the host technologies targeted by the scan).

**Scan restriction**

Scan by Policy

Restrict scans to controls in selected policies. You can choose up to 20 policies to scan. By default Qualys scans for all applicable controls.

NIST 800-53 Rev 4 for Linux v.3.

You can choose one policy at a time.

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

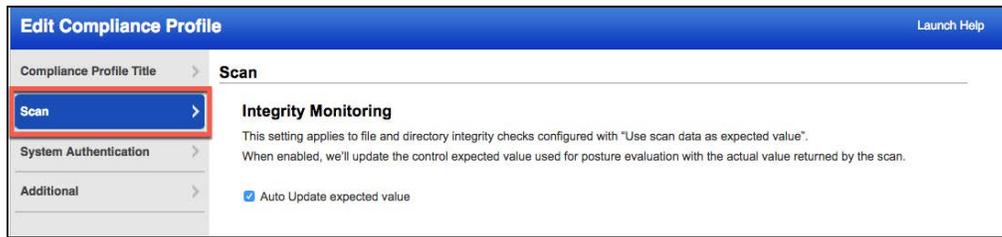
Policy Title	Actions
CIS Benchmark for CentOS Linux 6, v2.1.0 [Scored, Level 1 and Level 2] v.4.0	
NIST 800-53 Rev 4 for Linux v.3.0	

The “Scan by Policy” option allows you to restrict your compliance scans to focus exclusively on data points contained within the policies you specify.

The "Scan by Policy" option is required for compliance scans performed within the Qualys Security Configuration Assessment (SCA) application.

## Integrity Monitoring

The "File Integrity Check" control type you created earlier, is configured to "Use scan data as expected value."

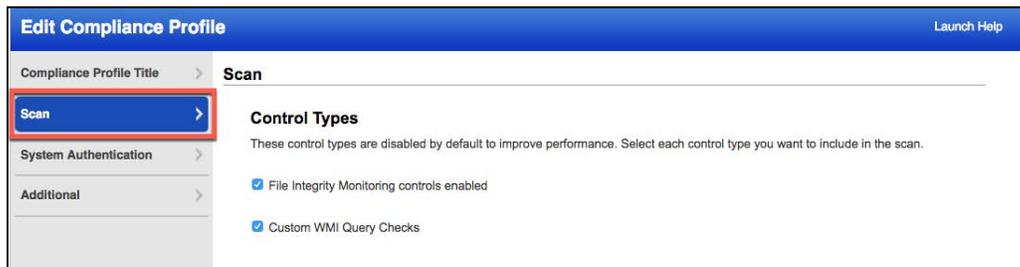


To ensure this works successfully, select the check box to "**Auto Update expected value,**" here in the "Scan" section of the Compliance profile.

This same option (Auto Update expected value), was configured for AGENT host assets, within the "File Integrity Check" UDC (see Lab Tutorial: "File Integrity Check UDC").

## Control Types

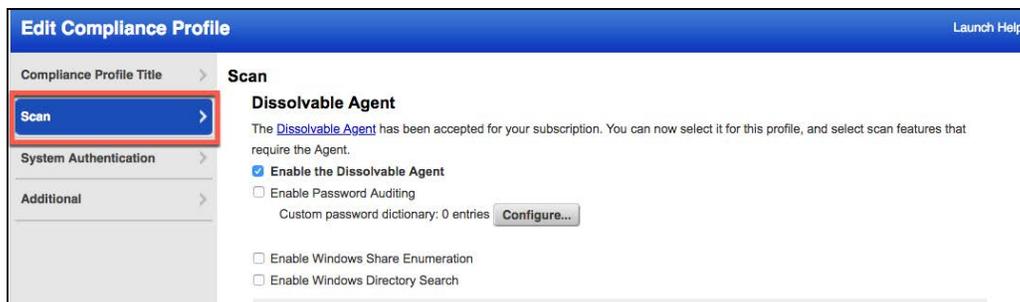
To improve scan performance, both Integrity Monitoring and WMI Query Check control types are disabled (by default), and must be explicitly selected within each Compliance Profile.



- **Integrity Monitoring** – Enable to collect the hash values needed to perform integrity checks on both Unix and Windows systems.
- **WMI Query Checks** – Enable to perform WMI queries on Windows systems.

## Dissolvable Agent

The "Dissolvable Agent" works exclusively with Windows hosts and helps to collect compliance data, especially when the Windows Remote Registry Service is unavailable.



Optionally, you can enable Password Auditing, Windows Share Enumeration, or Windows Directory Searches, once the Dissolvable Agent has been accepted and enabled.

- **Password Auditing** – Perform password auditing tests to identify user accounts with: empty passwords (CID 3893), passwords equal to the user name (CID 3894), or passwords found in your own custom password dictionary (CID 3895).
- **Windows Share Enumeration** - Find Windows shares that are readable by everyone and report the number of files for each share on each host (Control ID 4528) and whether the files are writable. This is good for identifying groups of files that may need tighter access control.
- **Windows Directory Search** - Select this option to include one or more Windows Directory Search UDCs in the scan, that search for files/directories using many criteria such as file name, user accounts, and specific user access permissions.

At scan time, Dissolvable Agent is installed on Windows devices to collect data, and once the scan is finished it is completely removed from target systems.

For more Compliance Profile details, enroll in the “Policy Compliance Strategies & Best Practices Self-Paced Training” course ([qualys.com/learning](https://qualys.com/learning)).

## Launch Compliance Scan

Before launching or scheduling a compliance scan, ensure you have the correct scanning options defined in a Compliance Profile and that you have created Authentication Records for the host assets you intend to target.

**Navigate to the following URL to view the “Compliance Scan” tutorial:**

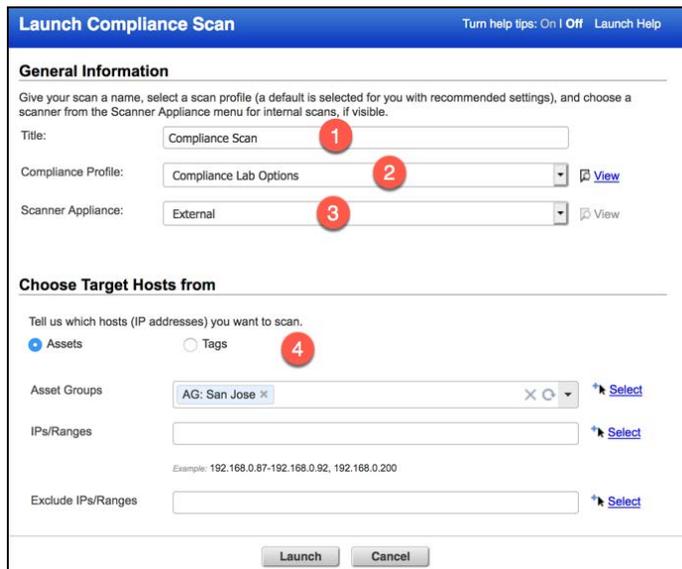


To be successful, compliance scans must be performed in “authenticated” mode. If a Qualys scanner fails to authenticate to a host, it will not attempt to collect its compliance data and will simply move to the next host target.



Type	Title	IPs	# IPs	Owner	Template Reco Details
Unix	Root Delegation via 'sudo'	64.41.200.243-64.41.200.245, 64.41.200.250	4	trann3z92 PM (Manager)	Details
Windows	Domain Admin		0	trann3z92 PM (Manager)	Details

To view authentication results (from scans already completed), just click the “Details” link at the right-side of any Authentication Record. Alternatively, you can view authentication results by creating an Authentication Report.



**Launch Compliance Scan** Turn help tips: On | Off Launch Help

**General Information**

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

Title:  1

Compliance Profile:  2 [View](#)

Scanner Appliance:  3 [View](#)

**Choose Target Hosts from**

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

Assets  Tags 4

Asset Groups:  [Select](#)

IPs/Ranges:  [Select](#)

Exclude IPs/Ranges:  [Select](#)

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

When launching a compliance scan, you must provide: 1) Title, 2) Compliance Profile, 3) Scanner Appliance, and 4) Target Hosts.

When choosing a target host, select from: Asset Groups, Asset Tags, or IPs.

**Choose Target Hosts from**

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

Assets
  Tags

**Use IP Network Range Tags For Include**

Choose from tags defined with IP address rules. This will allow you to scan the entire IP range(s) in each selected tag.

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

AG: San Jose x

**Use IP Network Range Tags For Exclude**

Choose from tags defined with IP address rules. This will allow you to exclude the entire IP range(s) in each selected tag.

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

(no tags selected)

Launch Cancel

You can monitor the status of any compliance scan, from the “PC Scans” tab. All scans are initially queued, before they begin running. **Note: scans can only collect data points for controls already in the Controls Library.**

## Scan Results

When a compliance scan is finished, any “Authentication Issues” encountered during the scan will be included in the scan results.

! **Authentication issues found!** View impacted IP(s)

**1 host** returned insufficient privileges for compliance data collection.

**Hosts with Insufficient Privilege (Showing 1 of 1)**

DNS	IP	NetBIOS	Instance	Cause
demo16	64.41.200.246	DEMO16	os	Insufficient privileges

Application technologies found on the host are also listed in the scan results.

**Application technologies found based on OS-level authentication**

**Google Chrome was found for these hosts**

Google Chrome (Windows)

64.41.200.247

**Internet Explorer was found for these hosts**

Internet Explorer 10

64.41.200.249

Internet Explorer 11

64.41.200.248, 64.41.200.251

**Mozilla Firefox was found for these hosts**

Mozilla Firefox (Windows)

64.41.200.247

# Policy Scope

Any policy you create or import, must identify the host assets it will audit; this is known as the Policy Scope. Both Asset Groups and Asset Tags are used to define the “scope” of a policy.

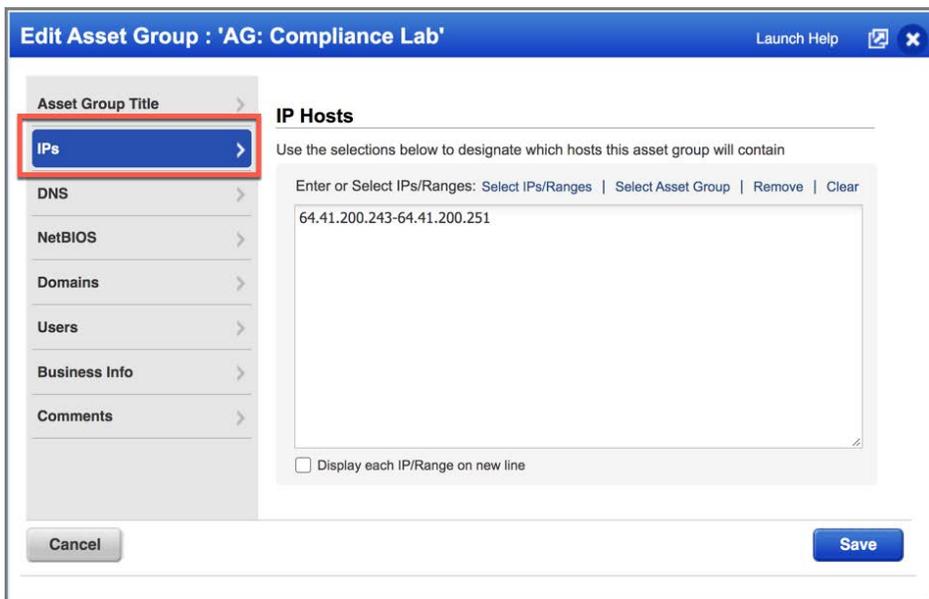
This tutorial, creates an Asset Group containing the Training Lab IPs and then identifies its matching Asset Tag that is automatically generated.

**Navigate to the following URL to view the “Asset Groups & Tags” tutorial:**



## Asset Groups

Asset Groups allow you to group host assets within your Qualys Account. Simply create a new Asset Group and manually add IP address members. A single IP address can be a member of multiple Asset Groups.

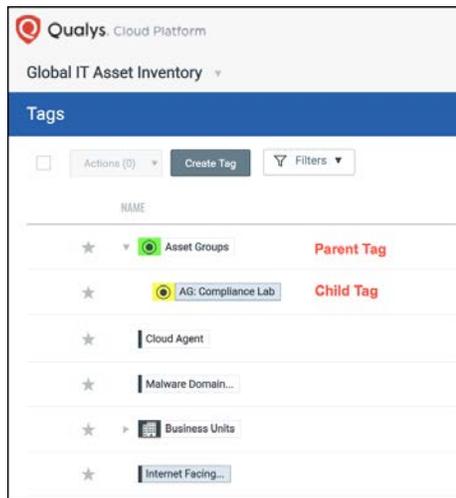


Optionally, Asset Group members can also be added by their DNS or NetBIOS names.

To help distinguish Asset Groups from Asset Tags with similar names, the Asset Group “Title” commonly begins with the “AG:” prefix (e.g., AG: Compliance Lab).

# Asset Tags

The Qualys platform will automatically create a matching Asset Tag for each Asset Group you add to your account. All matching Asset Tags are initially placed under the “Asset Groups” hierarchy (Parent Tag above).



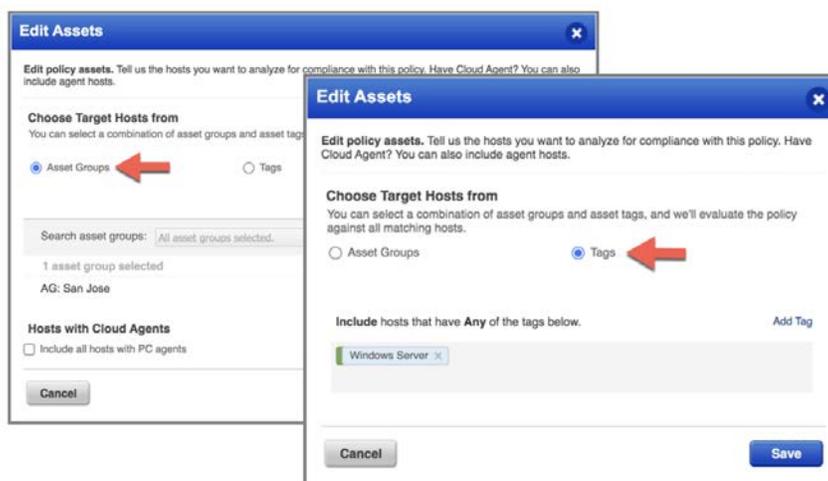
**Static Tags** – Are assigned manually to host assets and are commonly used as the starting point of an Asset Tag Hierarchy.

**Dynamic Tags** - Host assignment is determined by an Asset Tag Rule Engine and dynamically changes with updates to a host.

**Asset Tag Hierarchy** - Tags are typically nested, creating various parent/child relationships. A child tag should represent a subset of its parent tag.

# Policy Scope

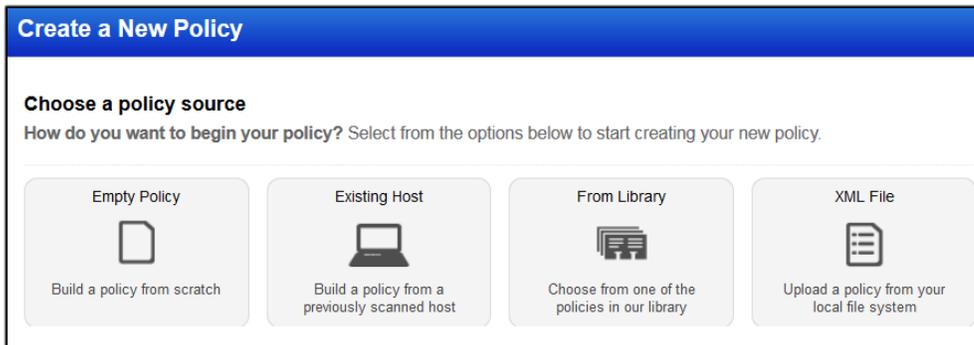
The Asset Groups and Asset Tags within your account, will serve to define the “scope” of the policies you create.



When building Asset Groups and Tags, keep in mind the host assets you will assess for compliance.

# Create Policy

A Qualys Policy contains controls that reflect the requirements of security frameworks, regulations, standards, mandates, benchmarks and your own internal security policies. The Qualys Policy Compliance applications offers multiple ways to create a policy:



- Empty Policy – Build a policy from scratch.
- Existing Host – Build a policy from a previously scanned host.
- From Library – Choose from one of the policies in the Qualys Policy Library.
- XML File – Upload a policy from your local file system.

Regardless of which method you choose, all policies must contain three basic components: 1) technologies, 2) controls, and 3) host assets.

## Required Policy Components

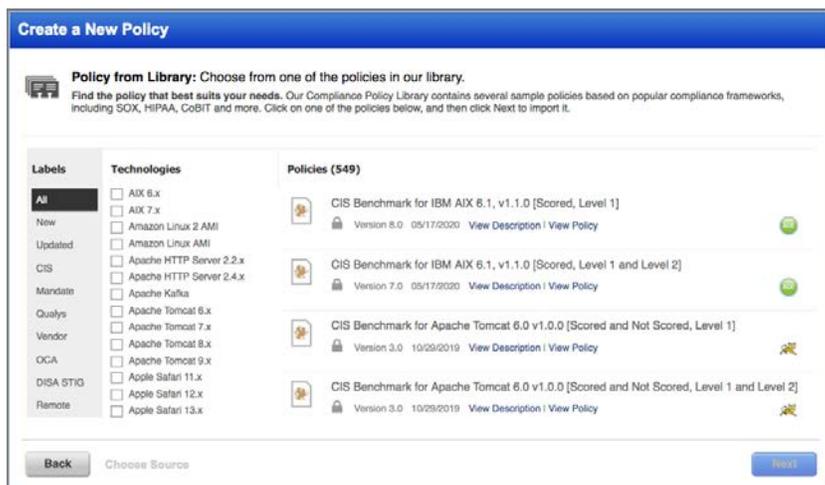
The following components are required for all Policies you create:



1. All policies must have one or more technologies:
  - Operating System
  - Service/Application
2. Add SDCs and/or UDCs to a policy, from the Control Library or other policies.
3. Add hosts to a policy to define its scope:
  - Asset Groups
  - Asset Tags

# Import Policy from Library

The Policy Library contains hundreds of compliance policies, designed to meet the objectives of popular mandates, frameworks, regulations, standards, and benchmarks.



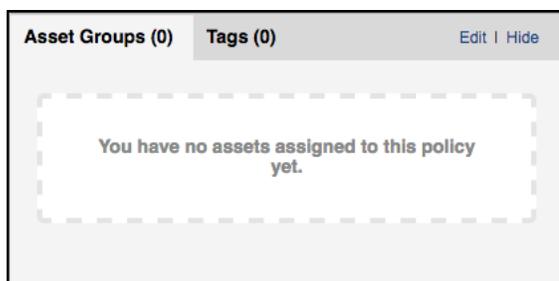
Navigate to the following URL to view the “Import Policy From Library” tutorial:



## Add Assets

After importing a policy from the library, the policy technologies and controls are automatically added. Before saving an imported policy, you will need to add host assets.

The “scope” of a policy, defines the host assets that will be audited by the policy.



You can add assets to a policy using Asset Groups or Asset Tags.

**Edit Assets**

Edit policy assets. Tell us the hosts you want to analyze for compliance with this policy. Have Cloud Agent? You can also include agent hosts.

**Choose Target Hosts from**  
You can select a combination of asset groups and asset tags, and we'll evaluate the policy against all matching hosts.

Asset Groups  Tags

Search asset groups: All asset groups selected. Add All | Remove All

1 asset group selected  
AG: San Jose View | Remove

**Hosts with Cloud Agents**

Include all hosts with PC agents

Cancel Save

By default, Asset Groups do not include Cloud Agent hosts. The check box to “Include all hosts with PC agents,” allows you to include agent hosts, when Asset Groups are used to define the scope.

Asset Tags; on the other hand, support both "scannable" as well as "agent" host assets, by default.

**Sections**

Section	Title	Controls
1	Account Policies	9
2	Local Policies	106
3	System Services	45
4	Windows Firewall With Advanced Security	26
5	Advanced Audit Policy Configuration	28

Cancel Evaluate now Save As... Save

The "Evaluate now" option, will evaluate all controls in a policy (against current scan results) when the policy is saved.

The Policy Compliance application has many out-of-box policies (below) for OCA asset technologies.

**Create a New Policy**

**Policy from Library:** Choose from one of the policies in our library.  
Find the policy that best suits your needs. Our Compliance Policy Library contains several sample policies based on popular compliance frameworks, including SOX, HIPAA, CoBIT and more. Click on one of the policies below, and then click Next to import it.

**Labels**

- All
- New
- Updated
- CiS
- Mandate
- Qualys
- Vendor
- DISA STIG
- Remediation

**Technologies**

- ArubaOS 6.x
- Brocade Fabric 7.x
- Brocade Fabric 8.x
- Cisco FTD 6.x
- Cisco WLC 8.x
- Comware 5
- Comware 7
- Data Domain OS 5.x
- FireEye CMS 7.x
- FireEye CMS 8.x
- HP Printers
- HP Safeguard
- HPE 3PAR OS 3.x

**Policies (15)**

- Security Configuration and Compliance Policy for Cisco FTD 6.x (OCA)  
Version 1.0 01/13/2020 View Description | View Policy
- Security Configuration and Compliance Policy for Cisco WLC 8.x (OCA)  
Version 1.0 01/13/2020 View Description | View Policy
- Security Configuration and Compliance Policy for Brocade Fabric 7.x (OCA)  
Version 1.0 07/23/2019 View Description | View Policy
- Security Configuration and Compliance Policy for Brocade Fabric 8.x (OCA)  
Version 1.0 07/23/2019 View Description | View Policy

Back Choose Source Next

TIP: Use the OCA Asset Tag to define the “scope” of an OCA policy.

# Create Empty Policy

In this exercise, you will create a 'blank' policy, and manually add all policy components (i.e., technologies, assets, and controls).

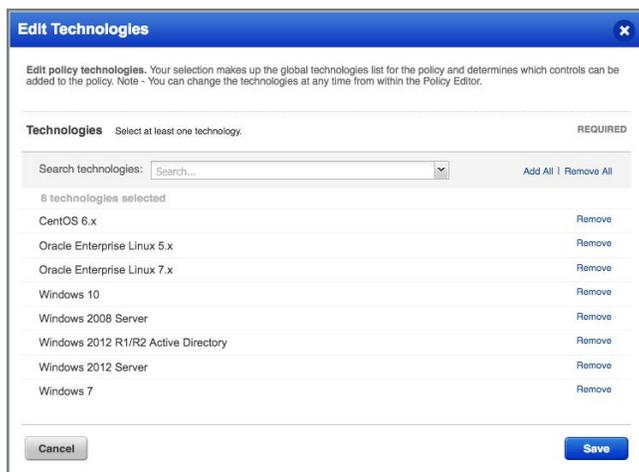
**Navigate to the following URL to view the "Create Empty Policy" tutorial:**



LAB 10 - <https://ior.ad/7Shz>

## Add Technologies

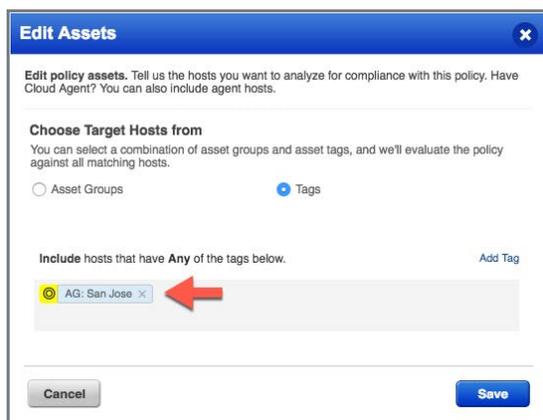
Before you can create an empty policy, you must first select one or more technologies.



Although our lab tutorial combines both Unix and Windows technologies together in the same policy, some prefer (for simplicity) to keep them separate.

## Add Assets

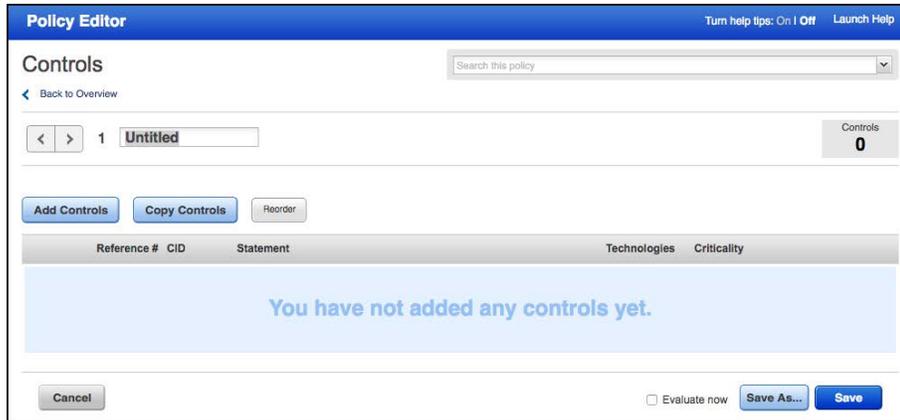
The "AG: San Jose" asset group (created in the second lab tutorial) spans all of the Unix and Windows technologies in this policy.



The "AG: San Jose" Asset Tag was automatically created, when the "AG: San Jose" Asset Group was added to your account.

## Add Controls

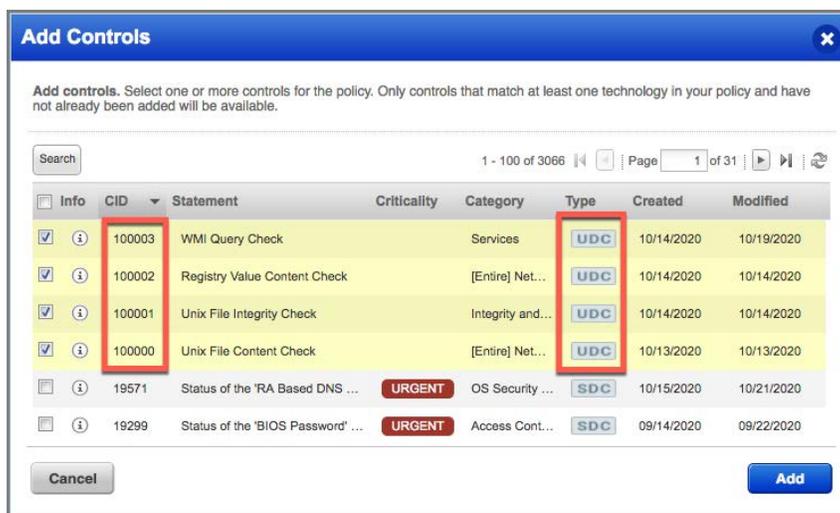
Initially the Policy Editor displays a blank policy. Controls have yet to be added.



Controls are added to one or more sections, using either the “Add Controls” or “Copy Controls” buttons.

- Add Controls – add controls from the control library.
- Copy Controls – copy controls from another policy.

Controls added from the Control Library, often need adjustments or tuning. Copying controls from another policy, has the advantage of any previous adjustments or tuning you have already made.



When attempting to add User Defined Controls (UDCs) to a policy, look for CID numbers starting at 100,000.

# Cardinality

Many of the User Defined Control types in the Qualys Policy Compliance application use the "String List" or "Regular Expression List" data types, creating a scenario where, a list of values (Y) specified in the control, are compared to another list of values (X) collected from a target host.

The cardinality setting determines how list "X" is compared to List "Y," to reach the appropriate PASS/FAIL outcome.

CARDINALITY	YOU ARE COMPLIANT WHEN
contains	X contains all of Y
does not contain	X does not contain any of Y
matches	All strings in X match all strings in Y (any order)
intersect	Any string in X matches any strings in Y
is contained in	All strings in X are contained in Y

- X (Actual) = List of values returned by a scan or agent.
- Y (Expected) = List of values defined by a control.

The WMI Query Check UDC (created in an earlier lab tutorial) is designed to identify host assets running prohibited software, by comparing a list of "prohibited" software applications, to the list of running processes collected from a targeted host.

Identify prohibited or suspicious software applications.

List the names of running processes.

does not contain | string list | wireshark.exe  
zennmap.exe

Please enter the IP address you want to test this control against and click Evaluate.

IP Address: 64.41.200.248 | View IPs | Evaluate

Control result: **PASS** The expected value does match the configuration gathered from the target. You may change both the target and the expected value and click Evaluate again.

**Actual**  
List the names of running processes.  
Last updated: 10/15/2020 at 07:43:57 PM (GMT-0500)

'System Idle Process'
'System'
'Registry'
'smss.exe'
'csrss.exe'

In the lab tutorial example, the "does not contain" cardinality produces the intended outcome; hosts will PASS, only if they are NOT running "prohibited" software applications.

Changing the cardinality setting from “does not contain” to “contains,” produces a FAIL outcome (as expected). The “contains” cardinality would be more appropriate in a “required” software control.

Identify prohibited or suspicious software applications.

List the names of running processes.

contains string list wireshark.exe  
zennmap.exe

Please enter the IP address you want to test this control against and click Evaluate.

IP Address: 64.41.200.248 View IPs Evaluate

Control result: **FAIL** The expected value does not match the configuration gathered from the target. You may change both the target and the expected value and click Evaluate again.

**Actual**  
List the names of running processes.  
Last updated: 10/15/2020 at 07:43:57 PM (GMT-0500)

'System Idle Process'
'System'
'Registry'
'smss.exe'
'csrss.exe'

You can experiment with different cardinality settings, expected values, and even IP addresses, while adjusting and tuning a control. Just continue to click the “Evaluate” button to see how your changes impact the PASS/FAIL results.

The test and evaluate capabilities built into the Policy Editor, help to demonstrate one advantage of having compliance scan data available, prior to building any policy.

List the names of running processes.

does not contain string list wireshark.exe  
zennmap.exe

Please enter the IP address you want to test this control against and click Evaluate.

IP Address: 64.41.200.248 View IPs Evaluate

Control result: **PASS** The expected value does match the configuration gathered from the target. You may change both the target and the expected value and click Evaluate again.

**Actual**  
List the names of running processes.  
Last updated: 10/15/2020 at 07:43:57 PM (GMT-0500)

'System Idle Process'
'System'
'Registry'
'smss.exe'
'csrss.exe'

You can adjust a controls cardinality, data type, expected list of values, and IP address when testing and evaluating controls against real host assets (in your account). This part of the tuning process commonly performed when adding controls to any policy.

Any adjustment you make in the Policy Editor will not impact the Default Values (within the Control Library); what happens in the policy stays in the policy.

The testing and evaluation tools in the policy editor require scan data to function properly.

# contains

The “contains” cardinality operator is ideal for defining a “Required Software List”.

**1.1 - Current list of 'Required software applications installed' [64.41.200.249]**  
Passed  
**CRITICAL**  
Evaluation date: 01/06/2020 at 01:00:42 (GMT+0530)

The installation of the correct primary user applications, such as the 'Microsoft Office Suite' and other supporting software, are critical to the proper use of the system. While a single rogue application can bring the entire process to a halt, the applications installed on the system should match those specified as approved.

The following List String value(s) X indicate the current list of installed applications (registered with the OS) on the system as defined within the registry key checked is HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall.

**Expected**  
**Y =** contains regular expression list  
WinPcap  
Wireshark  
**OR any of the selected values below:**  
 No software found  
 Key not found

**Actual**  
The following List String value(s) X indicate the current list of installed applications (registered with the OS) on the system as defined within the HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall registry key. NOTE: For 64-bit versions, the registry key checked is HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall.  
Last updated: 01/05/2020 at 21:02:59 (GMT+0530)

WinPcap 4.1.3.4.1.0.2980  
Wireshark 2.6.1 64-bit-2.6.1  
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148:9.0.30729.4148  
Microsoft Visual C++ 2017 Redistributable (x64) - 14.12.25810:14.12.25810.0  
Microsoft Visual C++ 2017 x64 Additional Runtime - 14.12.25810:14.12.25810  
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.4148:9.0.30729.4148

X =

As long as a host has **ALL** required software applications installed, it will pass.

**1.1 - Current list of 'Required software applications installed' [64.41.200.249]**  
Failed  
**CRITICAL**  
Evaluation date: 01/06/2020 at 01:00:42 (GMT+0530)

The installation of the correct primary user applications, such as the 'Microsoft Office Suite' and other supporting software, are critical to the proper use of the system. While a single rogue application can bring the entire process to a halt, the applications installed on the system should match those specified as approved.

The following List String value(s) X indicate the current list of installed applications (registered with the OS) on the system as defined within the registry key checked is HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall.

**Expected**  
**Y =** contains regular expression list  
WinPcap  
Wireshark  
**OR any of the selected values below:**  
 No software found  
 Key not found

**Actual**  
The following List String value(s) X indicate the current list of installed applications (registered with the OS) on the system as defined within the HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall registry key. NOTE: For 64-bit versions, the registry key checked is HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall.  
Last updated: 01/05/2020 at 21:02:59 (GMT+0530)

WinPcap 4.1.3.4.1.0.2980  
Microsoft Visual C++ 2017 x64 Minimum Runtime - 14.12.25810:14.12.25810  
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148:9.0.30729.4148  
Microsoft Visual C++ 2017 Redistributable (x64) - 14.12.25810:14.12.25810.0  
Microsoft Visual C++ 2017 x64 Additional Runtime - 14.12.25810:14.12.25810  
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.4148:9.0.30729.4148  
VMware Tools:9.4.0.1280544

X =

If any required software element is missing, the host will fail.

# does not contain

The “does not contain” cardinality operator is useful if you want to identify the presence of prohibited software or services.

**1.1 - Current list of 'Prohibited software applications installed' [54.41.200.249]**

Passed  
**CRITICAL**  
Evaluation date: 02/04/2020 at 02:20:54 PM (GMT+0530)

The installation of unauthorized, incorrect, or rogue applications can interfere with user workflow and delay the timely completion of company projects. As a result, systems, unauthorized, incorrect versions or rogue applications installed on any system should be identified and removed as appropriate to the needs of the business.

The following List String value(s) X indicate the current list of installed applications (registered with the OS) on the system as defined within the rule. The registry key checked is HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall.

**Expected** **does not contain regular expression list**

**Y =**

- Wireshark
- Nagios
- Solarwinds

**OR any of the selected values below:**

- No software found
- Key not found

**Actual** **Last updated:** 01/05/2020 at 21:02:59 (GMT+0530)

**X =**

- Apple Application Support (32-bit):3.1.3
- Apple Mobile Device Support:3.1.1.3
- Apple Software Update:2.1.3.127
- Bonjour:3.0.0.10
- Google Chrome:63.0.3239.132
- Google Update Helper:1.3.33.7
- iTunes:12.1.2.27
- LimePro 2.0.5.6046:2.0.5.6046
- Microsoft .NET Framework 1.1.1.1.4322
- Microsoft Antimalware:2.0.6212.2

As long as a host does not contain any of the listed software applications, it will produce a PASS.

**1.1 - Current list of 'Prohibited software applications installed' [54.41.200.249]**

Failed  
**CRITICAL**  
Evaluation date: 02/04/2020 at 02:20:54 PM (GMT+0530)

The installation of unauthorized, incorrect, or rogue applications can interfere with user workflow and delay the timely completion of company projects. As a result, systems, unauthorized, incorrect versions or rogue applications installed on any system should be identified and removed as appropriate to the needs of the business.

The following List String value(s) X indicate the current list of installed applications (registered with the OS) on the system as defined within the rule. The registry key checked is HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall.

**Expected** **does not contain regular expression list**

**Y =**

- Wireshark
- Nagios
- Solarwinds

**OR any of the selected values below:**

- No software found
- Key not found

**Actual** **Last updated:** 12/10/2019 at 11:44:40 PM (GMT+0530)

**X =**

- Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.4148:9.0.30729.4148
- Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148:9.0.30729.4148
- Microsoft Visual C++ 2017 Redistributable (x64) - 14.12.25810:14.12.25810.0
- Microsoft Visual C++ 2017 x64 Additional Runtime - 14.12.25810:14.12.25810
- Microsoft Visual C++ 2017 x64 Minimum Runtime - 14.12.25810:14.12.25810
- VMware Tools:3.4.0.1280544
- WinPcap 4.1.3.4.1.0.2980
- Wireshark 2.6.1 64-bit:2.6.1

If any prohibited item is found, the host will FAIL.

## matches

The “matches” cardinality operator determines if one list matches another.

**1.8 - Windows Group Membership Check-Custom Policy with UDCs [64.41.200.249]**

Passed  
Evaluation date: 01/09/2020 at 15:42:18 (GMT+0530)

Windows Group Membership Check

Who are the members of the "Administrators" local group?

Expected **matches regular expression list**

Administrator
engrdlab
Domain Controllers
Enterprise Admins
Domain Admins
qscanner

Y =

Actual **Last updated: 01/07/2020 at 20:31:05 (GMT+0530)**

TRNAdministrator
TRNengrdlab
TRNDomain Controllers
TRNEnterprise Admins
TRNDomain Admins
TRNqscanner

X =

The list of actual values must match the list of expected values (independent of their order), to receive a PASS.

**1.8 - Windows Group Membership Check-Custom Policy with UDCs [64.41.200.246]**

Failed  
Evaluation date: 01/09/2020 at 15:42:18 (GMT+0530)

Windows Group Membership Check

Who are the members of the "Administrators" local group?

Expected **matches regular expression list**

Administrator
Domain Admins
qscanner
engrdlab
Domain Controllers
Enterprise Admins

Y =

Actual **Last updated: 01/07/2020 at 20:31:05 (GMT+0530)**

WIN2008R2\Administrator
WIN2008R2\qscanner
TRNDomain Admins

X =

If the number of items in the list of actual values is greater than or less than the number of items in the list of expected values, a FAIL condition occurs.

## is contained in

The “is contained in” cardinality operator determines if all items in the list of actual values are contained in the list of expected values. All items in the list of actual values must also be in the list of expected values, to produce a PASS.

1.13 - Current list of Groups and User Accounts granted the 'Access this computer from the network' right [64.41.200.246]

Passed

**CRITICAL**

Evaluation date: 01/06/2020 at 01:00:42 (GMT+0530)

The 'Access this computer from the network' right allows a User to interact with remote Windows systems. By Windows default, all users with a mix of folder/file permissions on the networked systems, certain files and/or other confidential information resources, such as print queues, network login--these Users can potentially access file servers with non-NTFS file systems, which only enforce folder-level access.) As the KB 823659, this right should be limited as appropriate to the needs of the business. CAUTION: If the 'Everyone group is being removed, shall be blocked from accessing remote hosts.

The following List String value(s) X indicate the current User Accounts defined within the Access this computer from the network policy:

Expected	is contained in regular expression list
Y =	Administrators
	Backup Operators
	OR any of the selected values below:
	<input checked="" type="checkbox"/> Right not assigned

Actual	Last updated: 12/10/2019 at 11:44:40 PM (GMT+0530)
X =	BUILTIN\Administrators

Notice that a PASS is still produced, if the number of items in the list of actual values is less than the number of items in the list of expected values.

1.13 - Current list of Groups and User Accounts granted the 'Access this computer from the network' right [64.41.200.246]

Failed

**CRITICAL**

Evaluation date: 02/04/2020 at 02:20:54 PM (GMT+0530)

The 'Access this computer from the network' right allows a User to interact with remote Windows systems. By Windows default, all users with a mix of folder/file permissions on the networked systems, certain files and/or other confidential information resources, such as print queues, network login--these Users can potentially access file servers with non-NTFS file systems, which only enforce folder-level access.) As the KB 823659, this right should be limited as appropriate to the needs of the business. CAUTION: If the 'Everyone group is being removed, shall be blocked from accessing remote hosts.

The following List String value(s) X indicate the current User Accounts defined within the Access this computer from the network policy:

Expected	is contained in regular expression list
Y =	Administrators
	Backup Operators
	OR any of the selected values below:
	<input checked="" type="checkbox"/> Right not assigned

Actual	Last updated: 12/10/2019 at 11:44:40 PM (GMT+0530)
X =	BUILTIN\Administrators
	BUILTIN\Backup Operators
	BUILTIN\Power Users
	BUILTIN\Users

If any item in the list of actual values is not within the list of expected values, a FAIL result is produced.

# intersect

If you wanted to identify a list of “Optional Software” the “intersects” cardinality operator can be used.

**1.1 - Current list of 'Required software applications installed' [64.41.200.249]**

Passed

**CRITICAL**

Evaluation date: 01/06/2020 at 14:18:30 (GMT+0530)

The installation of the correct primary user applications, such as the 'Microsoft Office Suite' and other supporting software, are critical to the proper user work while a single rogue application can bring the entire process to a halt, the applications installed on the system should match those specified as appropriate

The following List String value(s) X indicate the current list of installed applications (registered with the OS) on the system as defined within the HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall.

**Expected**

**Y =**

**Intersect regular expression list**

- Wreshark
- Nagios
- Solarwinds

**OR any of the selected values below:**

- No software found
- Key not found

**Actual**

**X =**

**Last updated:** 01/05/2020 at 21:02:59 (GMT+0530)

- Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.4148;9.0.30729.4148
- Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148;9.0.30729.4148
- Microsoft Visual C++ 2017 Redistributable (x64) - 14.12.25810;14.12.25810.0
- Microsoft Visual C++ 2017 x64 Additional Runtime - 14.12.25810;14.12.25810
- Microsoft Visual C++ 2017 x64 Minimum Runtime - 14.12.25810;14.12.25810
- VMware Tools:3.4.6.1200544
- Wreshark 2.6.1 64-bit:2.6.1

If any of the required software element is present, the host will pass.

# Compliance Reports

## Authentication Report

Authentication is a requirement for performing compliance scans; therefore, it is important to monitor the success and failure of authentication attempts made by your Qualys Scanner Appliance.

An Authentication Report will help you identify failed authentication attempts and other conditions that could result in the failure to collect compliance data.

The illustration below, depicts an Authentication Report taken from our Training Lab environment.

Asset Tags Summary				
Included ( any ):	10 of 10	100% Successful		
AG: San Jose	0 of 10	0% Failed		
Excluded ( any ):	0 of 10	0% Not Attempted		
<b>▼ Results</b>				
▼ Selected Asset Tags: 10 of 10 (100%)				
▼ Unix/Cisco/Checkpoint Firewall				
Host	Host Technology	Instance	Status	Cause
64.41.200.243 (demo13.s02.sjc01.qualys.com, -)	CentOS 6.x		Passed	-
64.41.200.244 (demo14.s02.sjc01.qualys.com, -)	Oracle Enterprise Linux 5.x		Passed	-
64.41.200.245 (demo15.s02.sjc01.qualys.com, -)	Oracle Enterprise Linux 7.x		Passed	-
64.41.200.250 (demo20.s02.sjc01.qualys.com, -)	CentOS 6.x		Passed	-
Host	Host Technology	Instance	Status	Cause
▼ Windows				
Host	Host Technology	Instance	Status	Cause
64.41.200.246 (win2008r2.trn.qualys.com, WIN2008R2)	Windows 2008 Server		Passed	-
64.41.200.247 (trn-win7.trn.qualys.com, TRN-WIN7)	Windows 7		Passed	-
64.41.200.248 (trn-win10-pro.trn.qualys.com, TRN-WIN10-PRO)	Windows 10		Passed	-
64.41.200.249 (trn-win2012-dc.trn.qualys.com, TRN-WIN2012-DC)	Windows 2012 R1/R2 Active Directory	Active Directory 2012	Passed	-
64.41.200.249 (trn-win2012-dc.trn.qualys.com, TRN-WIN2012-DC)	Windows 2012 Server		Passed	-
64.41.200.251 (trn-win10.trn.qualys.com, TRN-WIN10)	Windows 10		Passed	-
Host	Host Technology	Instance	Status	Cause

Authentication attempts by the Qualys Scanner Appliance, have been successful for all lab targets. The following is a list of all possible authentication outcomes:

**Passed** – Authentication was successful.

**Insufficient Privileges** – Authentication was successful, but the Qualys scanning account was not able to access data needed to perform one or more compliance assessment tests.

Host	Host Technology	Instance	Status	Cause
64.41.200.246 (demo16, DEMO16)	Windows 2008 Server		Passed	Insufficient privileges
64.41.200.247 (trn-win7.trn.qualys.com, TRN-WIN7)	-		Failed	Unable to complete Windows login for host=64.41.200.247, user=qscanner, domain=trn.qualys.com, ntstatus=c000005e

**Failed** – Authentication was not successful.

**Not Attempted** – An authentication record was not found for a targeted host, and therefore authentication was not attempted.

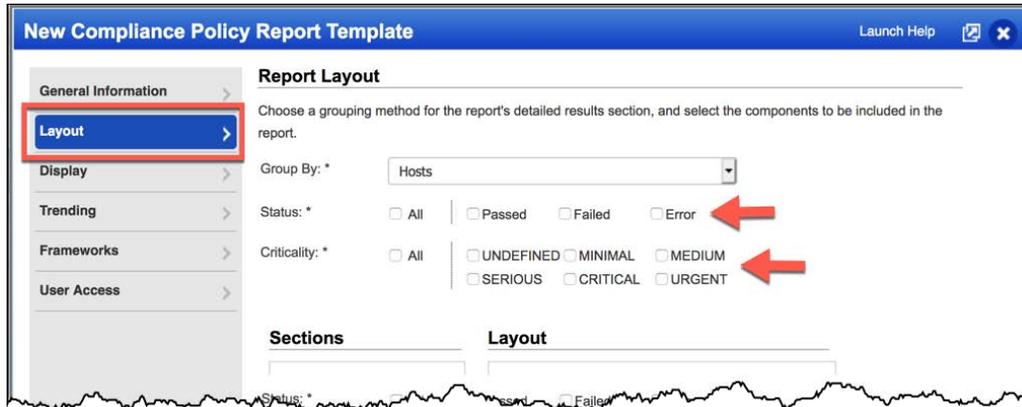
Host	Host Technology	Instance	Status	Cause
64.41.200.244 (demo14.s02.sjc01.qualys.com, -)	-		Not Attempted	Host has no authentication information associated with it
Host	Host Technology	Instance	Status	Cause

A status of “Not Attempted” typically identifies host IPs that do not have a corresponding authentication record.

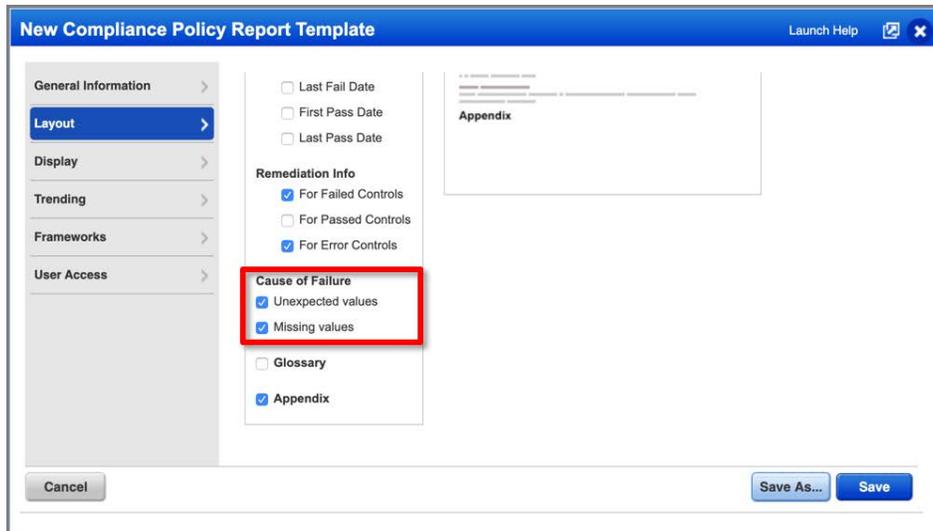
Qualys recommends using root and Administrator equivalent accounts for all compliance scans.

## Policy Report

The “Layout” section of a Policy Report Template provides some useful report filtering options.



You can create reports that only display “Failed” controls and focus the report on the most critical controls.

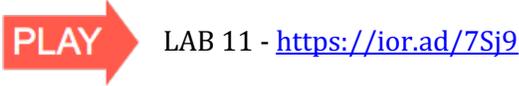


The “Cause of Failure” options will help to highlight required values that are missing or unexpected.

# Create Policy Report

A Policy Report focuses on the controls of a single policy and may contain one or more hosts or technologies, within the policy scope. The evidence included for each control, helps one to understand the reason for any PASS or FAIL outcome.

**Navigate to the following URL to view the “Create Policy Report” tutorial:**



Once a specific policy has been selected, only host assets defined within the Policy Scope will be included in a Policy Report. Additional filtering options include:

- **All Assets in policy** - Include all assets defined within the policy scope.
- **Select Asset Groups in policy** – Include assets from one or more specific Asset Groups.
- **Select IPs in policy** – Include one or more IP addresses.
- **Single Instance** – Include one or more technology instances
- **Select Asset Tags** – Include assets labeled with one or more specific Asset Tags.

A distinguishing characteristic of the Policy Report is the evidence that impacts each PASS/FAIL result.

File name	Setting	Value
/etc/ssh/sshd_config	PermitRootLogin	yes

This is the type of information needed by systems administrators and operational teams to correct a configuration error or any other type of failed requirement.

# Interactive Reports

When a host fails to meet a control requirement, one option involves correcting the condition that led to the failure. However, if a compensating control has been deployed to address the problem, another option involves requesting an exception for the failed control. The Policy Compliance Application provides Interactive Reports for requesting and managing exceptions:

- **Control Pass/Fail Report**
- **Individual Host Compliance Report**

## Requesting Exceptions

*Navigate to the following URL to view the “Interactive Report” tutorial:*



LAB 12 - <https://ior.ad/7Sqv>

To request an exception for a failed control, you have the option of running one of two interactive reports. Interactive reports have very short lives; they are not saved (like other reports) under the “Reports” tab.

**New Compliance Interactive Report** Launch Help

Select an interactive report from the list below.

**Real-time Reports**

Report Types

- Control Pass/Fail**
- Individual Host Compliance

Preview

**QUALYS GUARD**

**Control Pass/Fail/Error Report**

Thomas Soto      Quincy      Created: 05/03/2007 at 12:38  
Systems Manager      1000 Bridge Parkway  
Suite 201  
Redwood Shores, California 94065  
United States of America

**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	Errors in Compliance:	3 (30%)
Hosts:	10	Display Results:	Pass, Fail, Error

**Asset Group Info**

Title:	Windows Machines	Business Impact:	High	Collateral Damage Potential:	High
--------	------------------	------------------	------	------------------------------	------

**Description**

The Control Pass/Fail/Error 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, fail or error status for the specified control.

An interactive report will remain running, until you have successfully completed one or more exception requests. Interactive reports that are closed are not saved, but can easily be recreated.

The “Individual Host Compliance” report (below) displays all control test outcomes for a single host.

Report Setup Launch Help

**Target**

Layout >

Policy: CIS Benchmark for Microsoft Windows 10 Enterprise (Release 1803), v1

Asset Group: Select an item

Asset Tags:

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

Window 10

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

IP Address: 64.41.200.248 ✘ [Select](#)

Run Cancel

Once a policy and assets have been selected, an individual host IP address (from the policy scope) must be specified.

The “Control Pass/Fail” report (below) displays the results or outcomes for a single control, on one or more host assets.

Report Setup Launch Help

**Target**

Layout >

Policy: CIS Benchmark for Microsoft Windows 10 Enterprise (Release 1803), v1

Asset Group: Select an item

Asset Tags:

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

Window 10

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

Control: Status of the 'Minimum Password Length' setting ✘ [Select](#)

Run Cancel

Once the policy and assets have been selected, an individual Control ID (from the policies list of controls) must be specified.

In most cases, you will request exceptions for failed controls. Alternatively, you have the option to filter controls by their “Criticality.”

Order	CID	Reference	Control	Category	Posture	Criticality	Exception
<input type="checkbox"/>	1.1	1318	1.1.1 Status of the 'Enforce password history' setting	Access Control Requir	Failed	URGENT	<a href="#">Request</a>
<input type="checkbox"/>	1.2	3376	1.1.2 Status of the 'Maximum Password Age' setting (expiration)	Access Control Requir	Failed	URGENT	<a href="#">Request</a>
<input type="checkbox"/>	1.3	1072	1.1.3 Status of the 'Minimum Password Age' setting	Access Control Requir	Failed	URGENT	<a href="#">Request</a>
<input type="checkbox"/>	1.4	1071	1.1.4 Status of the 'Minimum Password Length' setting	Access Control Requir	Failed	CRITICAL	<a href="#">Request</a>
<input type="checkbox"/>	1.5	1092	1.1.5 Status of the 'Password Complexity Requir	Access Control Requir	Failed	URGENT	<a href="#">Request</a>

Notice the “Exception” column (on the right-side). The “Request” links allow you to request an exception, for the controls that are listed.

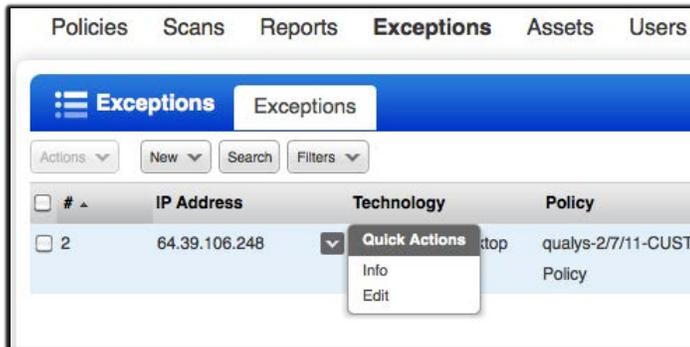
By default, exception requests will be assigned to an “Auditor” account. Optionally, exception requests can be assigned to a “Manager” account. The examples in this lab tutorial use the “Auditor” account. The “Comments” field is required.

<input type="checkbox"/>	Order CID	Reference	Control	Category	Posture	Criticality	Exception
<input type="checkbox"/>	1.1 1318	1.1.1	Status of the 'Enforce password history' setting	Access Control Requirements	Passed	URGENT	Approved
<input type="checkbox"/>	1.2 3376	1.1.2	Status of the 'Maximum Password Age' setting (expiration)	Access Control Requirements	Failed	URGENT	Expired
<input type="checkbox"/>	1.3 1072	1.1.3	Status of the 'Minimum Password Age' setting	Access Control Requirements	Failed	URGENT	Expired
<input type="checkbox"/>	1.4 1071	1.1.4	Status of the 'Minimum Password Length' setting	Access Control Requirements	Failed	URGENT	Expired
<input type="checkbox"/>	1.5 1092	1.1.5	Status of the 'Password Complexity Requirements' setting	Access Control Requirements	Failed	URGENT	Pending
<input type="checkbox"/>	1.6 2484	1.1.6	Status of the 'Store passwords using reversible encryption' setting	Access Control Requirements	Passed	URGENT	
<input type="checkbox"/>	1.7 2341	1.2.1	Status of the 'Account Lockout Duration' setting (invalid login attempts)	Access Control Requirements	Passed	URGENT	

The values displayed in the “Exception” as well as the “Posture” columns will change, as selected controls go through the exception handling process. Auditors have the option of assigning expiration dates to approved exceptions. If the control is failing (at the time of its expiration date), “Expired” will be displayed in the “Exception” column.

## Working With Exception Requests

When editing exception requests, an Auditor must determine the impact of allowing a failed control/host to be exempted from a policy. It is common for some type of compensating control to be implemented, as justification or cause for approval.



When granting any exception, Auditors should always take into account, the regulations, standards, and mandates that impact your organization or business.

**Navigate to the following URL to view the “Working With Exception Requests” tutorial:**

**PLAY** → LAB 13 - <https://ior.ad/7Sr0>

## The Auditor Role

The role of Auditor was created primarily to approve or reject exceptions requested for failing hosts. To properly fulfill this role an auditor should be familiar with your organizations security policies, governing regulations, as well as security frameworks.

In addition to approving/rejecting exceptions, auditors can:

- Create and edit policies
- Generate reports
- Add new controls to the Control Library

Additional Auditor Characteristics:

- Auditors cannot be added to a Business Unit.
- Auditors cannot run compliance scans.
- Auditors have access to all hosts in your Policy Compliance subscription (and cannot be restricted to a single Asset Group).
- Auditors only have visibility into compliance data (not vulnerability data).
- Other user roles cannot be changed to the role of Auditor.

Although a “Manager” account can also be used to approve exception requests, the examples in this lab tutorial use the “Auditor” account.

**Edit Exception:** Turn help tips: On | Off Launch Help

**Details**

Action: Approved

End Date: 03/31/2021

Reassign: \* Qualys Auditor (Auditor: trann3qe25)

Comments: \*  
Training Lab hosts are granted an exception for 90-days

Reopen exception on change of evidence  
This applies only if the exception is approved. Reopen this exception if a future scan returns a value that is different than the current value, and the control is still failing (or error).

Cancel Save

An Exception can be reassigned, approved or rejected. An approved exception can be set to expire on a specific date. Approved exception requests will be noted in the next interactive report. If an exception request is rejected, it will keep its failed status.

The option to “Reopen exception on change of evidence,” will reopen an “approved” exception, if a future scan returns a value that is different than the current value, and the control is still failing.

# Policy Compliance Certification Exam

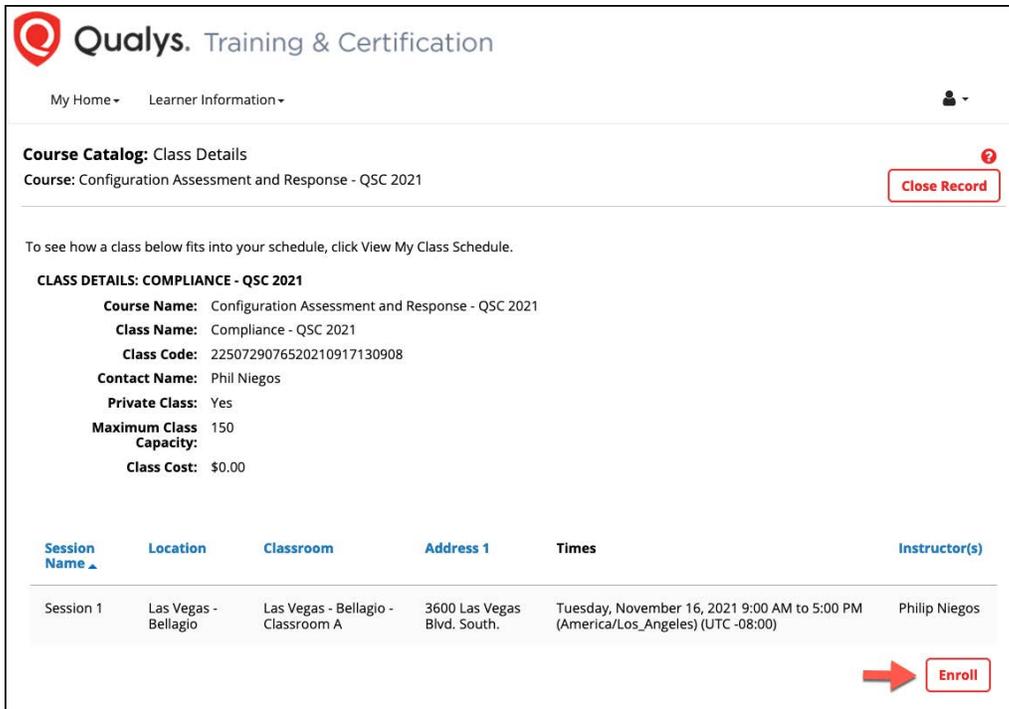
Participants in this training course have the option to take the Policy Compliance Certification Exam. This exam is provided through our Learning Management System ([qualys.com/learning](https://qualys.com/learning)). To take the exam, candidates will need a “learner” account.



If you would like to take the exam, but do not already have a “learner” account, click the “Request a new account” link (above), from the “Qualys Training & Certification” login page ([qualys.com/learning](https://qualys.com/learning)).

Once you have created a “learner” account (and for those who already have an account), click the following link to access the “QSC 2021 Configuration Assessment & Response” course page:

<https://gml.geolearning.com/geonext/qualys/scheduledclassdetails4enroll.geo?id=22511237828>



**CLASS DETAILS: COMPLIANCE - QSC 2021**

**Course Name:** Configuration Assessment and Response - QSC 2021  
**Class Name:** Compliance - QSC 2021  
**Class Code:** 2250729076520210917130908  
**Contact Name:** Phil Niegos  
**Private Class:** Yes  
**Maximum Class Capacity:** 150  
**Class Cost:** \$0.00

Session Name	Location	Classroom	Address 1	Times	Instructor(s)
Session 1	Las Vegas - Bellagio	Las Vegas - Bellagio - Classroom A	3600 Las Vegas Blvd. South.	Tuesday, November 16, 2021 9:00 AM to 5:00 PM (America/Los_Angeles) (UTC -08:00)	Philip Niegos

From the course page, click the “Enroll” button (lower-right corner).

After successfully completing the course enrollment, click the “Launch” button, for the Qualys Policy Compliance Exam.

Qualys. Training & Certification

My Home - Learner Information -

Configuration Assessment and Response - QSC 2021 Close Record

Class Name	Date	Classroom	Instructor(s)
Compliance - QSC 2021	Tuesday, November 16, 2021 9:00 AM to 5:00 PM (America/Los_Angeles) (UTC -08:00)	Las Vegas - Bellagio - Classroom A	Philip Niegos

To access a learning activity, select the activity name and click Launch or Open.

Activity Name	Type	Score	Progress	Time Taken	Attempts	Action
QSC 2021 Configuration Assessment & Response Lab Supplement	pdf	N/A	N/A	N/A	0	Open
QSC 2021 Configuration Assessment & Response Slides	pdf	N/A	N/A	N/A	0	Open
Qualys Policy Compliance Exam	Actual Test	N/A	Not Attempted	N/A		Launch

Each candidate is provided five attempts to pass the exam. You may use the course presentation slides and lab tutorial supplement to help you answer the exam questions. You may also use any of the resources within the Qualys UI (such as the “Help” menu) and resources found on the Qualys Community (community.qualys.com) to answer exam questions.

Qualys. Training & Certification

My Home - Learner Information -

Qualys Vulnerability Management Detection & Response - QSC 2020 Close Record

Progress: Completed Status: Enrolled Required: No Duration: 6 hours

Print Certificate

Class Name	Date	Instructor(s)
VMDR - QSC 2020	Tuesday, November 17, 2020 9:00 AM to 4:00 PM (America/Los_Angeles) (UTC -08:00)	Philip Niegos

To access a learning activity, select the activity name and click Launch or Open.

Activity Name	Type	Score	Progress	Last Accessed	Action
QSC20 VMDR Lab Tutorial Supplement	pdf	N/A	N/A	N/A	Open
QSC20 VMDR Presentation Slides	pdf	N/A	N/A	N/A	Open
Qualys Vulnerability Management Detection & Response (VMDR) Exam	Actual Test	100%	Passed	11/3/2020 7:38:14 PM	Launch

With a passing score of 75% (or greater), click the “Print Certificate” button to download and print your course exam certificate.

# Course Survey and Trial Account

Please let us know what you think about the “QSC 2021 Configuration Assessment & Response” training course.

Survey - <https://forms.office.com/r/rsy0Aja6Xz>

Would you like a trial account to practice and experiment with the lessons and topics provided in this course?

Link to Trial - <https://www.qualys.com/free-trial/>