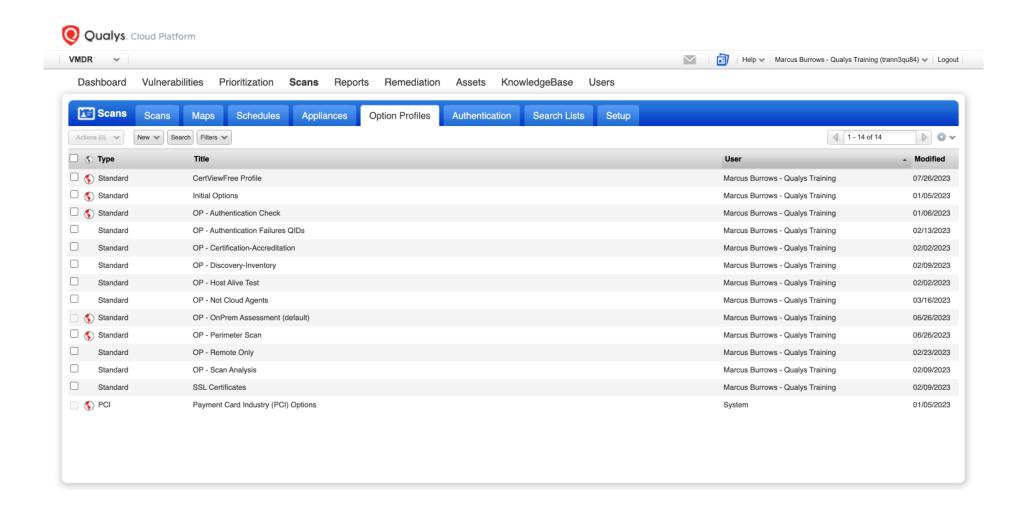
creating an Scan Option Profile for Vulnerability Assessment

An option profile includes scan settings. You need to choose an option profile each time you start or schedule a scan. In this lab, you will create an Option Profile for on-premises assessments. Click anywhere to continue.

Jan 3, 2024 1 of 34

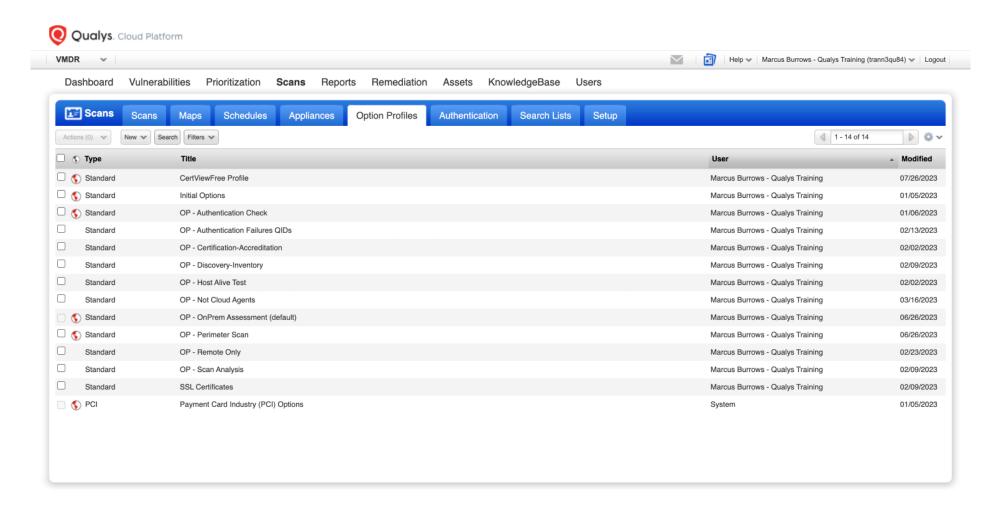


Creating an Scan Option Profile for Vulnerability Assessment



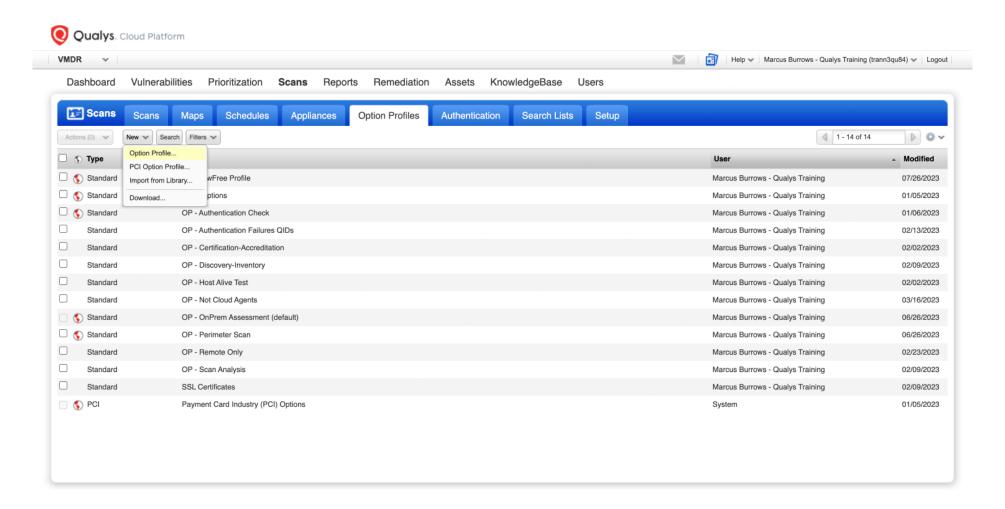
Jan 3, 2024 2 of 34

On the Option Profiles tab, click the New button.



Jan 3, 2024 3 of 34

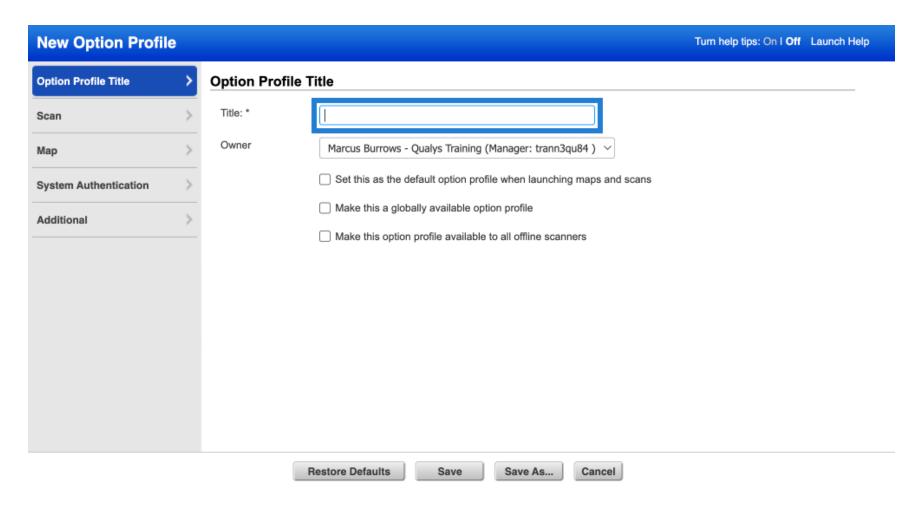
Click Option Profile...



Jan 3, 2024 4 of 34

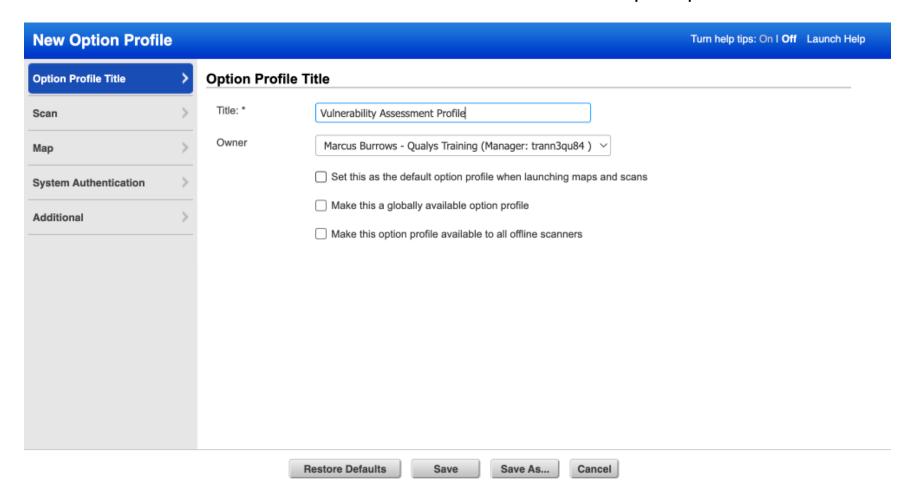
real Creating an Scan Option Profile for Vulnerability Assessment

As the name for the new profile, type Vulnerability Assessment Profile



Jan 3, 2024 5 of 34

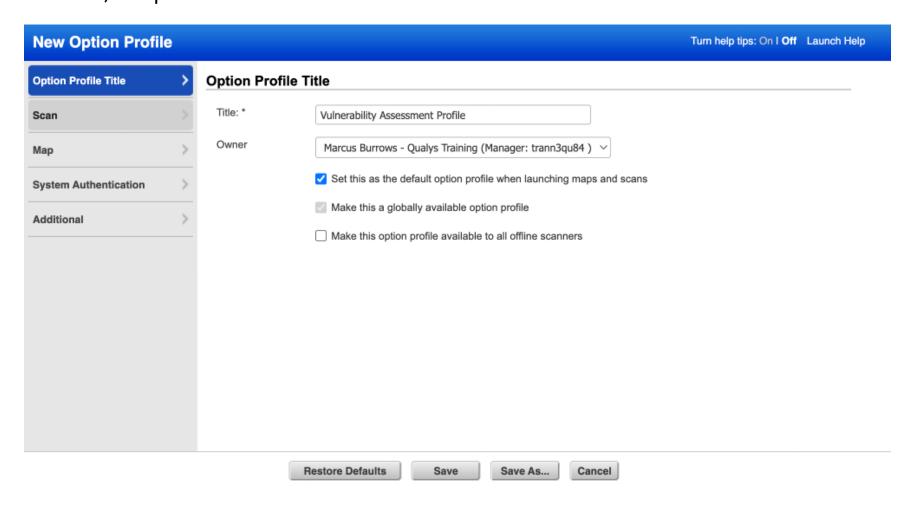
During this lab, you will configure the recommended settings for on-premises vulnerability i assessments. Click the checkbox next to "Set this as the default option profile".



Jan 3, 2024 6 of 34

creating an Scan Option Profile for Vulnerability Assessment

Note that the setting "Make this a globally available option profile" has been selected automatically. As the default, this profile will be available to other users. Click the Scan tab.



Jan 3, 2024 7 of 34

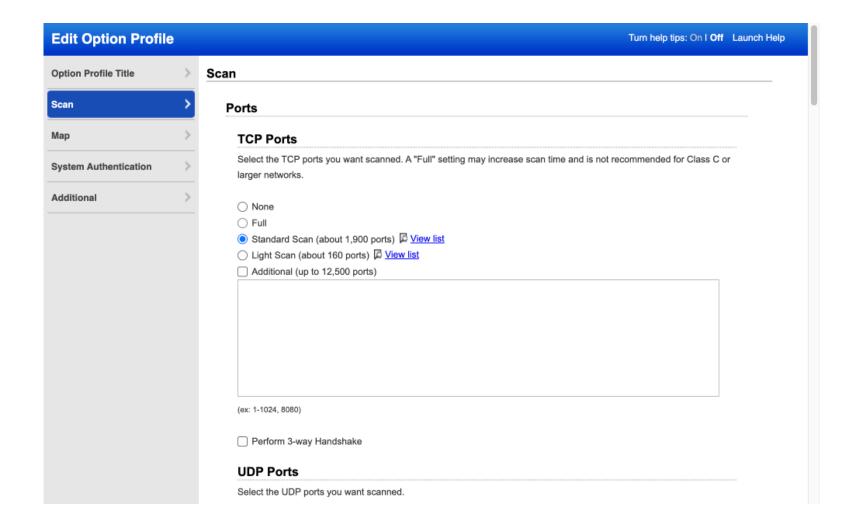
riorad Creating an Scan Option Profile for Vulnerability Assessment

Here, ports are specified for fingerprinting and discovery of services. Standard Scan is recommended to manage performance and scan time. Additional ports can be added if required. Click on the scroll bar on the right.

Jan 3, 2024 8 of 34



Creating an Scan Option Profile for Vulnerability Assessment



Jan 3, 2024 9 of 34

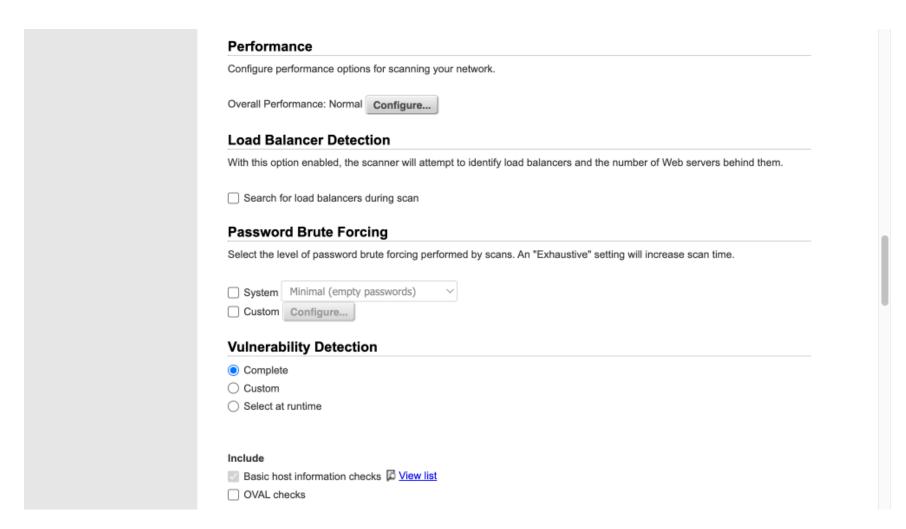
Standard Scan is also recommended for UDP ports. Again, click on the scrollbar to scroll down.

Select the UDP ports you want scanned.
○ None
○ Full
Standard Scan (about 180 ports)
○ Light Scan (about 30 ports)
Additional (up to 20,500 ports)
(ex: 1-1024, 8080) Authoritative Ontion for light scans
Authoritative Option for light scans
Authoritative Option for light scans This option changes the processing of scan data so that vulnerability status (New, Active, Reopened, Fixed) is updated for
Authoritative Option for light scans This option changes the processing of scan data so that vulnerability status (New, Active, Reopened, Fixed) is updated for all vulnerabilities on target hosts, not just vulnerabilities on scanned ports. You can choose this option only for light port
Authoritative Option for light scans This option changes the processing of scan data so that vulnerability status (New, Active, Reopened, Fixed) is updated for all vulnerabilities on target hosts, not just vulnerabilities on scanned ports. You can choose this option only for light port scans or those where None + Additional Ports are configured. Learn about authoritative scans
Authoritative Option for light scans This option changes the processing of scan data so that vulnerability status (New, Active, Reopened, Fixed) is updated for all vulnerabilities on target hosts, not just vulnerabilities on scanned ports. You can choose this option only for light port scans or those where None + Additional Ports are configured. Learn about authoritative scans How it works - This will force close any vulnerabilities that were not found, as long as the QIDs were included in search list
Authoritative Option for light scans This option changes the processing of scan data so that vulnerability status (New, Active, Reopened, Fixed) is updated for all vulnerabilities on target hosts, not just vulnerabilities on scanned ports. You can choose this option only for light port scans or those where None + Additional Ports are configured. Learn about authoritative scans

Jan 3, 2024 10 of 34

real Creating an Scan Option Profile for Vulnerability Assessment

In the Performance section, click on the Configure button.



Jan 3, 2024 11 of 34

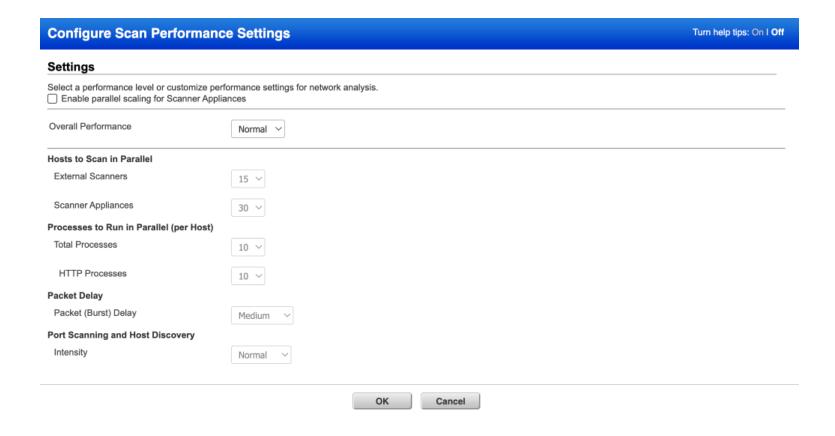
creating an Scan Option Profile for Vulnerability Assessment

Parallel scaling can be useful when you have scanners with different performance characteristics. More information on parallel scaling can be found here. Click the checkbox next to "Enable parallel scaling for Scanner Appliances".

Jan 3, 2024 12 of 34



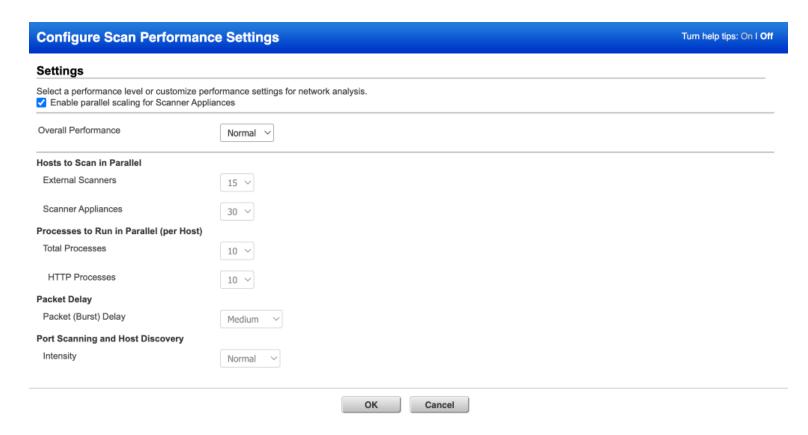
Creating an Scan Option Profile for Vulnerability Assessment



Jan 3, 2024 13 of 34

riorad Creating an Scan Option Profile for Vulnerability Assessment

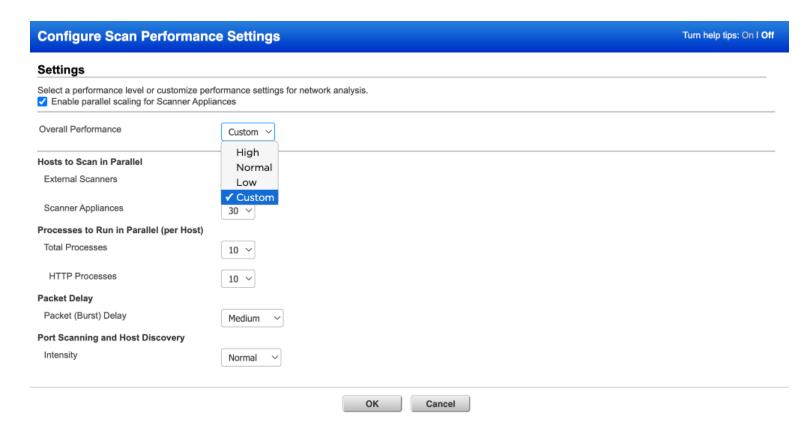
i Click the first drop-down.



Jan 3, 2024 14 of 34



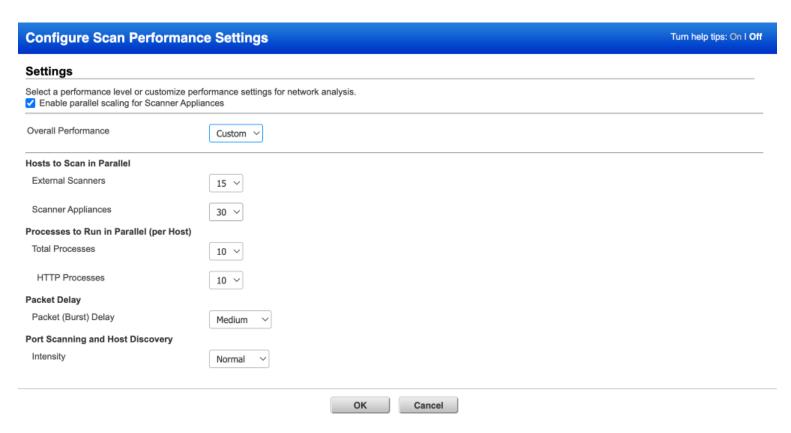
Select Custom



Jan 3, 2024 15 of 34

rad Creating an Scan Option Profile for Vulnerability Assessment

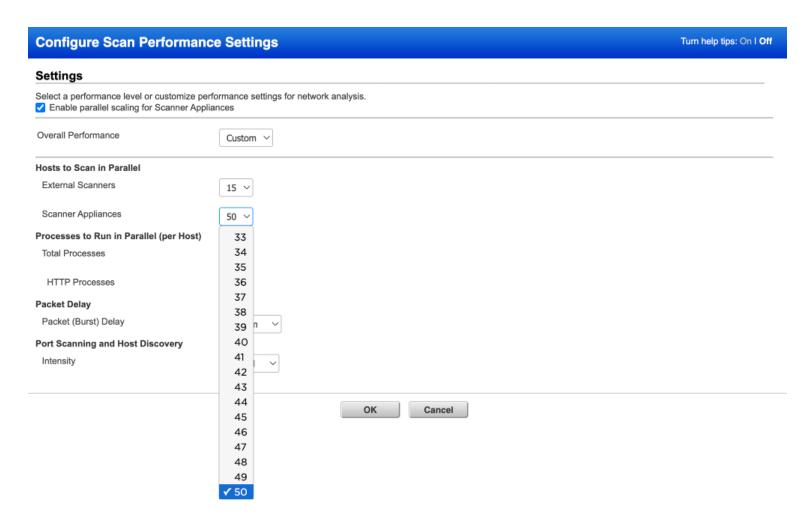
Selecting "Custom" means that the settings are now writable. Click the drop-down next to "Scanner Appliances".



Jan 3, 2024 16 of 34

rad Creating an Scan Option Profile for Vulnerability Assessment

This setting determines how many hosts each appliance will target concurrently. Select 50

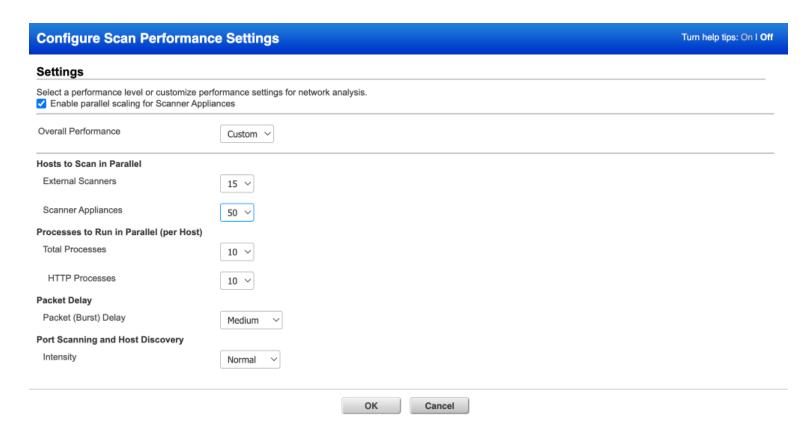


Jan 3, 2024 17 of 34



Creating an Scan Option Profile for Vulnerability Assessment

Click OK



Jan 3, 2024 18 of 34

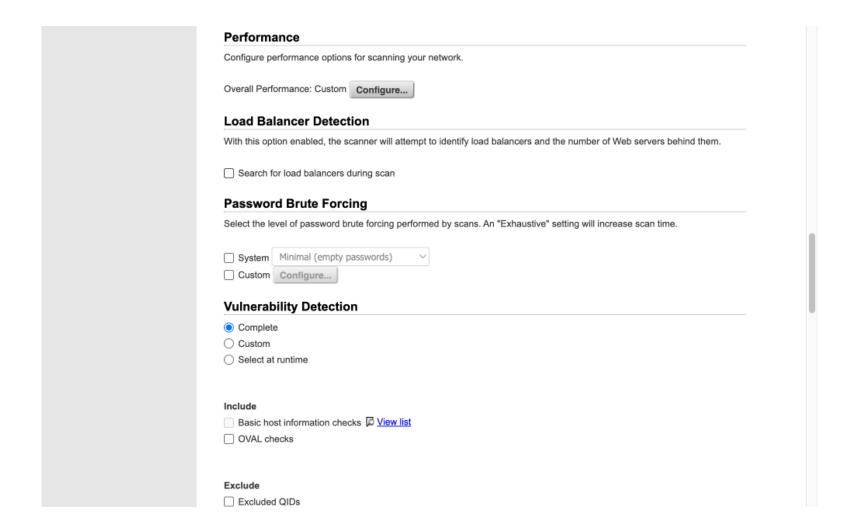
riorad Creating an Scan Option Profile for Vulnerability Assessment

In the Load Balancer Detection section, click the checkbox next to "Search for load balancers during scan". The scanner will check each host to see if it is a load balancer, and how many web servers are behind it.

Jan 3, 2024 19 of 34



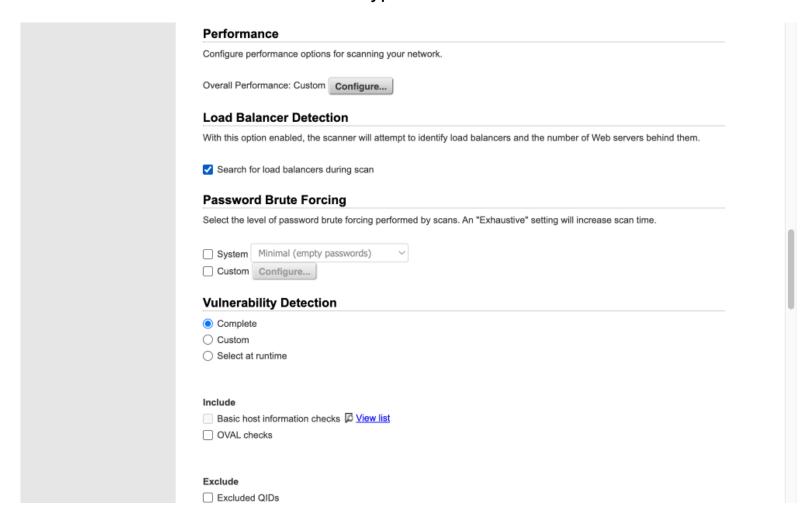
Creating an Scan Option Profile for Vulnerability Assessment



Jan 3, 2024 20 of 34

reating I Creating an Scan Option Profile for Vulnerability Assessment

For a regular vulnerability assessment, Complete Vulnerability Detection is recommended. The Custom radio button is used for other scan types. Click on the scrollbar to scroll down.



Jan 3, 2024 21 of 34

riorad Creating an Scan Option Profile for Vulnerability Assessment

Using authentication enables the scanner to remotely login to the target host with credentials that you provide in an Authentication Record. Authenticated scanning provides more accurate results and fewer false positives. Click the Windows checkbox.

Jan 3, 2024 22 of 34



Tiorad Creating an Scan Option Profile for Vulnerability Assessment

uthentication enables the scan	ner to log into hosts at scan time to extend detection capabilities. See the online help to learn
ow to configure this option.	
Windows	
Unix/Cisco/Network SSH	
Attempt least privilege for	Unix (skip root delegation in Unix record)
Oracle	
Oracle Listener	
SNMP	
VMware	
DB2	
HTTP	
MySQL	
Tomcat Server	
MongoDB	
Palo Alto Networks Firewall	
Oracle WebLogic Server	
Jboss Server	
Sybase	
est Authentication	
When enabled, the scanner will	test authentication to target hosts. No other scan tests will occur. You must choose at least on
uthentication type.	
Enable authentication testing	
Additional Certificate I	Detection
ve'il find certificates on ports/se	rvices with full port scans by default. Enable this option to find certificates in more locations us

Jan 3, 2024 23 of 34

i Click the checkbox next to Unix / Cisco / Network SSH

Authentication enables the scanner to lo	og into hosts at scan time to extend detection capabilities. See the online help to learn
how to configure this option.	
✓ Windows	
☐ Unix/Cisco/Network SSH	
Attempt least privilege for Unix (sk	kip root delegation in Unix record)
Oracle	
Oracle Listener	
SNMP	
☐ VMware	
☐ DB2	
☐ HTTP	
☐ MySQL	
☐ Tomcat Server	
MongoDB	
 Palo Alto Networks Firewall 	
Oracle WebLogic Server	
☐ Jboss Server	
Sybase	
Test Authentication	
When enabled, the scanner will test aut	thentication to target hosts. No other scan tests will occur. You must choose at least on
authentication type.	
☐ Enable authentication testing	
_	
Additional Certificate Detect	tion

Jan 3, 2024 24 of 34

i Click the scrollbar to scroll down.

Authentication enables the scanner to log	into hosts at scan time to extend detection capabilities. See the online help to learn
how to configure this option.	
✓ Windows	
Unix/Cisco/Network SSH	
Attempt least privilege for Unix (skip	root delegation in Unix record)
Oracle	
Oracle Listener	
SNMP	
☐ VMware	
☐ DB2	
☐ HTTP	
☐ MySQL	
☐ Tomcat Server	
☐ MongoDB	
Palo Alto Networks Firewall	
Oracle WebLogic Server	
☐ Jboss Server	
☐ Sybase	
Test Authentication	
When enabled, the scanner will test author	entication to target hosts. No other scan tests will occur. You must choose at least or
authentication type.	
☐ Enable authentication testing	
_	
Additional Certificate Detecti	on

Jan 3, 2024 25 of 34

creating an Scan Option Profile for Vulnerability Assessment

Click on the checkbox next to "Enable additional certificate detection". This option enables you to look for the certificates beyond the traditional ports only.

authentication, for example in Apache, Tomcat, Jboss, Java KeyStore and Windows IIS. Authentication is required. Enable additional certificate detection Dissolvable Agent	We'll find certificates on p	ports/services with full port scans by default. Enable this option to find certificates in more locations using
Dissolvable Agent The Dissolvable Agent has been accepted for your subscription. You can now select it for this profile, and select the Windows Share Enumeration feature (requires the Agent). Enable the Dissolvable Agent Enable Windows Share Enumeration Lite OS Scan When this option is selected and QID 45017 is included in the scan, the scan job reduces OS detection testing of targets during host discovery phase before vulnerability testing. Several expensive OS detection methods are excluded (i.e. telnet, msrpc, ntp, and more). Enable lite OS detection Add a Custom HTTP Header value	authentication, for examp	ple in Apache, Tomcat, Jboss, Java KeyStore and Windows IIS. Authentication is required.
The Dissolvable Agent has been accepted for your subscription. You can now select it for this profile, and select the Windows Share Enumeration feature (requires the Agent). Enable the Dissolvable Agent Enable Windows Share Enumeration Lite OS Scan	Enable additional cer	tificate detection
Share Enumeration feature (requires the Agent). Enable the Dissolvable Agent Enable Windows Share Enumeration Lite OS Scan When this option is selected and QID 45017 is included in the scan, the scan job reduces OS detection testing of targets during host discovery phase before vulnerability testing. Several expensive OS detection methods are excluded (i.e. telnet, msrpc, ntp, and more). Enable lite OS detection Add a Custom HTTP Header value	Dissolvable Agen	nt
□ Enable the Dissolvable Agent □ Enable Windows Share Enumeration Lite OS Scan When this option is selected and QID 45017 is included in the scan, the scan job reduces OS detection testing of targets during host discovery phase before vulnerability testing. Several expensive OS detection methods are excluded (i.e. telnet, msrpc, ntp, and more). □ Enable lite OS detection Add a Custom HTTP Header value	The <u>Dissolvable Agent</u> ha	as been accepted for your subscription. You can now select it for this profile, and select the Windows
Lite OS Scan When this option is selected and QID 45017 is included in the scan, the scan job reduces OS detection testing of targets during host discovery phase before vulnerability testing. Several expensive OS detection methods are excluded (i.e. telnet, msrpc, ntp, and more). □ Enable lite OS detection Add a Custom HTTP Header value	Share Enumeration featu	ure (requires the Agent).
Lite OS Scan When this option is selected and QID 45017 is included in the scan, the scan job reduces OS detection testing of targets during host discovery phase before vulnerability testing. Several expensive OS detection methods are excluded (i.e. telnet, msrpc, ntp, and more). □ Enable lite OS detection Add a Custom HTTP Header value	☐ Enable the Dissolva	able Agent
When this option is selected and QID 45017 is included in the scan, the scan job reduces OS detection testing of targets during host discovery phase before vulnerability testing. Several expensive OS detection methods are excluded (i.e. telnet, msrpc, ntp, and more). Enable lite OS detection Add a Custom HTTP Header value	Enable Windows Sha	are Enumeration
host discovery phase before vulnerability testing. Several expensive OS detection methods are excluded (i.e. telnet, msrpc, ntp, and more). □ Enable lite OS detection Add a Custom HTTP Header value	Lite OS Scan	
and more). □ Enable lite OS detection Add a Custom HTTP Header value	When this option is selec	cted and QID 45017 is included in the scan, the scan job reduces OS detection testing of targets during
Add a Custom HTTP Header value		fore vulnerability testing. Several expensive OS detection methods are excluded (i.e. telnet, msrpc, ntp,
	Enable lite OS detect	tion
Set a custom value in order to drop defenses (such as logging, IPs, etc) when authorized scans are being run.	Add a Custom HT	TTP Header value
	Set a custom value in ord	der to drop defenses (such as logging, IPs, etc) when authorized scans are being run.
Host-Alive Testing		

Jan 3, 2024 26 of 34

creating an Scan Option Profile for Vulnerability Assessment

Click the checkbox next to "Enable the Dissolvable Agent". At scan time the Agent is installed on Windows devices to collect data, and once the scan is complete it removes itself completely from target systems. Click here for more information.

Jan 3, 2024 27 of 34



Tiorad Creating an Scan Option Profile for Vulnerability Assessment

Additional Cert	tificate Detection
	on ports/services with full port scans by default. Enable this option to find certificates in more locations using ample in Apache, Tomcat, Jboss, Java KeyStore and Windows IIS. Authentication is required .
Enable additional	certificate detection
Dissolvable Ag	ent
	has been accepted for your subscription. You can now select it for this profile, and select the Windows eature (requires the Agent).
☐ Enable the Disso	olvable Agent
Enable Windows	Share Enumeration
Lite OS Scan	
	elected and QID 45017 is included in the scan, the scan job reduces OS detection testing of targets during before vulnerability testing. Several expensive OS detection methods are excluded (i.e. telnet, msrpc, ntp,
☐ Enable lite OS det	tection
Add a Custom	HTTP Header value
Set a custom value in	order to drop defenses (such as logging, IPs, etc) when authorized scans are being run.
Host-Alive Test	ting
When enabled, scan	testing will report hosts found alive during the discovery or port scanning process. Other testing will not

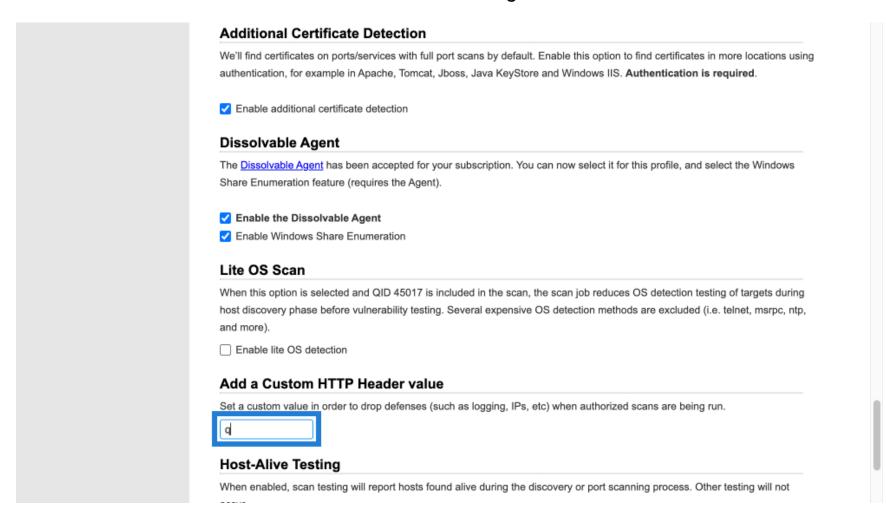
Jan 3, 2024 28 of 34

Click the checkbox next to "Enable Windows Share Enumeration".

	ts/services with full port scans by default. Enable this option to find certificates in more locations using in Apache, Tomcat, Jboss, Java KeyStore and Windows IIS. Authentication is required .
Enable additional certific	cate detection
Dissolvable Agent	
The <u>Dissolvable Agent</u> has Share Enumeration feature	been accepted for your subscription. You can now select it for this profile, and select the Windows (requires the Agent).
Enable the Dissolvable	Agent
 Enable Windows Share 	Enumeration
Lite OS Scan	
	d and QID 45017 is included in the scan, the scan job reduces OS detection testing of targets during a vulnerability testing. Several expensive OS detection methods are excluded (i.e. telnet, msrpc, ntp,
☐ Enable lite OS detection	
Add a Custom HTT	P Header value
Set a custom value in order	to drop defenses (such as logging, IPs, etc) when authorized scans are being run.
Host-Alive Testing	

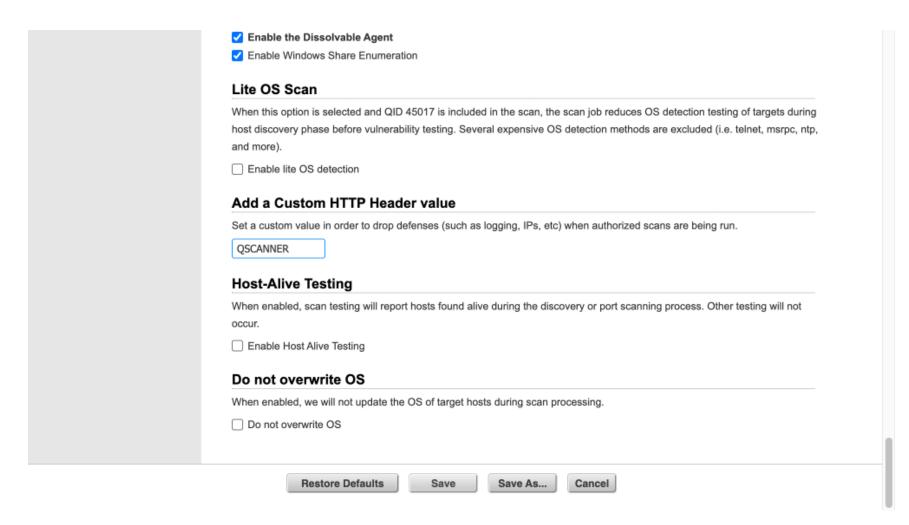
Jan 3, 2024 29 of 34

Under "Add a Custom HTTP Header value", type QSCANNER in the text box. This adds a specific HTTP header value to scans when authorized scans are being run.



Jan 3, 2024 30 of 34

Click the Save button.



Jan 3, 2024 31 of 34

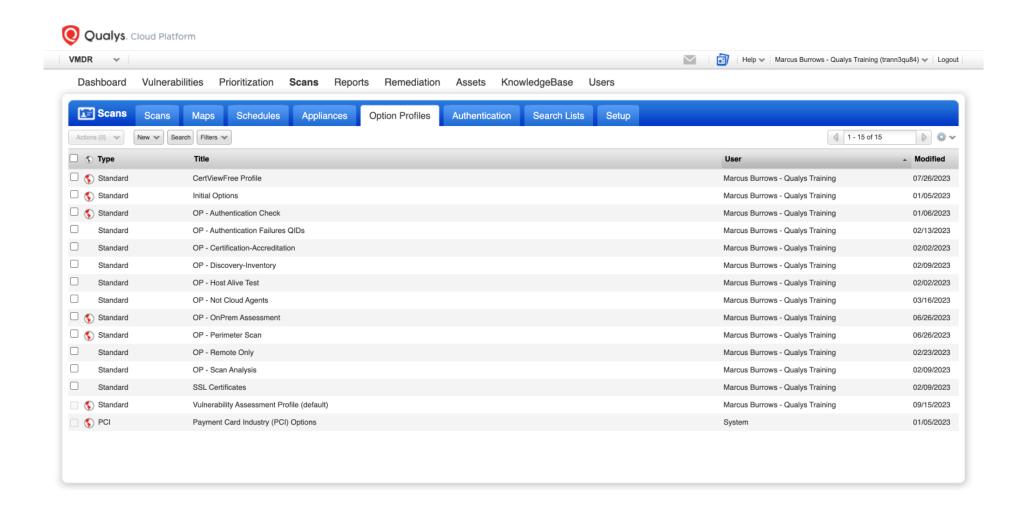
creating an Scan Option Profile for Vulnerability Assessment

There are other Option Profiles which you can create for different scenarios. In this lab you have created a default vulnerability assessment profile, suitable for on-premises scanning. That's it, you're done! You may now close this browser tab.

Jan 3, 2024 32 of 34



Creating an Scan Option Profile for Vulnerability Assessment



Jan 3, 2024 33 of 34



Scan to go to the interactive player

Jan 3, 2024 34 of 34