



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.

Qualys Cloud Platform

VMDR

Dashboard Vulnerabilities Prioritization **Scans** Reports Remediation Assets KnowledgeBase Users

Scans Maps Schedules Appliances Option Profiles Authentication Search Lists Setup

Actions (0) New Search Filters 1 - 14 of 14

Type	Title	User	Modified
<input type="checkbox"/> Standard	CertViewFree Profile	Marcus Burrows - Qualys Training	07/26/2023
<input type="checkbox"/> Standard	Initial Options	Marcus Burrows - Qualys Training	01/05/2023
<input type="checkbox"/> Standard	OP - Authentication Check	Marcus Burrows - Qualys Training	01/06/2023
<input type="checkbox"/> Standard	OP - Authentication Failures QIDs	Marcus Burrows - Qualys Training	02/13/2023
<input type="checkbox"/> Standard	OP - Certification-Accreditation	Marcus Burrows - Qualys Training	02/02/2023
<input type="checkbox"/> Standard	OP - Discovery-Inventory	Marcus Burrows - Qualys Training	02/09/2023
<input type="checkbox"/> Standard	OP - Host Alive Test	Marcus Burrows - Qualys Training	02/02/2023
<input type="checkbox"/> Standard	OP - Not Cloud Agents	Marcus Burrows - Qualys Training	03/16/2023
<input type="checkbox"/> Standard	OP - OnPrem Assessment (default)	Marcus Burrows - Qualys Training	06/26/2023
<input type="checkbox"/> Standard	OP - Perimeter Scan	Marcus Burrows - Qualys Training	06/26/2023
<input type="checkbox"/> Standard	OP - Remote Only	Marcus Burrows - Qualys Training	02/23/2023
<input type="checkbox"/> Standard	OP - Scan Analysis	Marcus Burrows - Qualys Training	02/09/2023
<input type="checkbox"/> Standard	SSL Certificates	Marcus Burrows - Qualys Training	02/09/2023
<input type="checkbox"/> PCI	Payment Card Industry (PCI) Options	System	01/05/2023



On the Option Profiles tab, click the New button.

Qualys Cloud Platform

VMDR

Dashboard Vulnerabilities Prioritization **Scans** Reports Remediation Assets KnowledgeBase Users

Scans Scans Maps Schedules Appliances **Option Profiles** Authentication Search Lists Setup

Actions (0) New Search Filters 1 - 14 of 14

<input type="checkbox"/>	Type	Title	User	Modified
<input type="checkbox"/>	Standard	CertViewFree Profile	Marcus Burrows - Qualys Training	07/26/2023
<input type="checkbox"/>	Standard	Initial Options	Marcus Burrows - Qualys Training	01/05/2023
<input type="checkbox"/>	Standard	OP - Authentication Check	Marcus Burrows - Qualys Training	01/06/2023
<input type="checkbox"/>	Standard	OP - Authentication Failures QIDs	Marcus Burrows - Qualys Training	02/13/2023
<input type="checkbox"/>	Standard	OP - Certification-Accreditation	Marcus Burrows - Qualys Training	02/02/2023
<input type="checkbox"/>	Standard	OP - Discovery-Inventory	Marcus Burrows - Qualys Training	02/09/2023
<input type="checkbox"/>	Standard	OP - Host Alive Test	Marcus Burrows - Qualys Training	02/02/2023
<input type="checkbox"/>	Standard	OP - Not Cloud Agents	Marcus Burrows - Qualys Training	03/16/2023
<input type="checkbox"/>	Standard	OP - OnPrem Assessment (default)	Marcus Burrows - Qualys Training	06/26/2023
<input type="checkbox"/>	Standard	OP - Perimeter Scan	Marcus Burrows - Qualys Training	06/26/2023
<input type="checkbox"/>	Standard	OP - Remote Only	Marcus Burrows - Qualys Training	02/23/2023
<input type="checkbox"/>	Standard	OP - Scan Analysis	Marcus Burrows - Qualys Training	02/09/2023
<input type="checkbox"/>	Standard	SSL Certificates	Marcus Burrows - Qualys Training	02/09/2023
<input type="checkbox"/>	PCI	Payment Card Industry (PCI) Options	System	01/05/2023



Click [Option Profile...](#)

Qualys Cloud Platform


VMDR

Dashboard Vulnerabilities Prioritization **Scans** Reports Remediation Assets KnowledgeBase Users

Scans Scans Maps Schedules Appliances **Option Profiles** Authentication Search Lists Setup

Actions (0) New Search Filters 1 - 14 of 14

Type		User	Modified
<input type="checkbox"/> Standard	OP - Authentication Check	Marcus Burrows - Qualys Training	07/26/2023
<input type="checkbox"/> Standard	OP - Authentication Failures QIDs	Marcus Burrows - Qualys Training	01/05/2023
<input type="checkbox"/> Standard	OP - Certification-Accreditation	Marcus Burrows - Qualys Training	01/06/2023
<input type="checkbox"/> Standard	OP - Discovery-Inventory	Marcus Burrows - Qualys Training	02/13/2023
<input type="checkbox"/> Standard	OP - Host Alive Test	Marcus Burrows - Qualys Training	02/02/2023
<input type="checkbox"/> Standard	OP - Not Cloud Agents	Marcus Burrows - Qualys Training	02/09/2023
<input type="checkbox"/> Standard	OP - OnPrem Assessment (default)	Marcus Burrows - Qualys Training	02/02/2023
<input type="checkbox"/> Standard	OP - Perimeter Scan	Marcus Burrows - Qualys Training	03/16/2023
<input type="checkbox"/> Standard	OP - Remote Only	Marcus Burrows - Qualys Training	06/26/2023
<input type="checkbox"/> Standard	OP - Scan Analysis	Marcus Burrows - Qualys Training	06/26/2023
<input type="checkbox"/> Standard	SSL Certificates	Marcus Burrows - Qualys Training	02/23/2023
<input type="checkbox"/> Standard	Payment Card Industry (PCI) Options	Marcus Burrows - Qualys Training	02/09/2023
<input type="checkbox"/> PCI		System	02/09/2023

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

New Option Profile

Turn help tips: [On](#) | [Off](#)
[Launch Help](#)

Option Profile Title

Scan

Map

System Authentication

Additional

Option Profile Title

Title: *

Owner

Marcus Burrows - Qualys Training (Manager: trann3qu84)

☐ Set this as the default option profile when launching maps and scans

☐ Make this a globally available option profile

☐ Make this option profile available to all offline scanners

Restore Defaults

Save

Save As...

Cancel



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

New Option Profile

Turn help tips: On | Off Launch Help

Option Profile Title

Scan

Map

System Authentication

Additional

Option Profile Title

Title: *
Vulnerability Assessment Profile

Owner
Marcus Burrows - Qualys Training (Manager: trann3qu84)

☐ Set this as the default option profile when launching maps and scans
 ☐ Make this a globally available option profile
 ☐ Make this option profile available to all offline scanners

Restore Defaults

Save

Save As...

Cancel



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.

New Option Profile

Turn help tips: On | **Off** | [Launch Help](#)

Option Profile Title >

Scan >

Map >

System Authentication >

Additional >

Option Profile Title

Title: *

Owner

☒ Set this as the default option profile when launching maps and scans

☒ Make this a globally available option profile

☐ Make this option profile available to all offline scanners

Restore Defaults

Save

Save As...

Cancel



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.

Edit Option Profile

Turn help tips: On | Off Launch Help

Option Profile Title >

Scan >

Map >

System Authentication >

Additional >

Scan

Ports

TCP Ports

Select the TCP ports you want scanned. A "Full" setting may increase scan time and is not recommended for Class C or larger networks.

☐ None

☐ Full

☒ Standard Scan (about 1,900 ports) [View list](#)

☐ Light Scan (about 160 ports) [View list](#)

☐ Additional (up to 12,500 ports)

(ex: 1-1024, 8080)

☐ Perform 3-way Handshake

UDP Ports

Select the UDP ports you want scanned.



Standard Scan is also recommended for UDP ports. Again, click on the [scrollbar](#) to scroll down.

UDP Ports

Select the UDP ports you want scanned.

☐ None
☐ Full
☒ Standard Scan (about 180 ports) [View list](#)
☐ Light Scan (about 30 ports) [View list](#)
☐ Additional (up to 20,500 ports)

(ex: 1-1024, 8080)

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 lists for the scan (in the option profile under Vulnerability Detection > Custom). Vulnerability status changes are made only to QIDs in the included search lists.

☐ Enable Authoritative Option for light scans

Scan Dead Hosts

By default dead hosts are ignored. Including them may increase scan time, and is not suggested for Class C or larger networks.



In the Performance section, click on the [Configure](#) button.

Performance

Configure performance options for scanning your network.

Overall Performance: Normal [Configure...](#)

Load Balancer Detection

With this option enabled, the scanner will attempt to identify load balancers and the number of Web servers behind them.

☐ Search for load balancers during scan

Password Brute Forcing

Select the level of password brute forcing performed by scans. An "Exhaustive" setting will increase scan time.

☐ System Minimal (empty passwords) ▼

☐ Custom [Configure...](#)

Vulnerability Detection

☒ Complete

☐ Custom

☐ Select at runtime

Include

☒ Basic host information checks [View list](#)

☐ OVAL checks



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".

Configure Scan Performance Settings

Turn help tips: On | Off

Settings

Select a performance level or customize performance settings for network analysis.

☐ Enable parallel scaling for Scanner Appliances

Overall Performance

Normal

Hosts to Scan in Parallel

External Scanners

15

Scanner Appliances

30

Processes to Run in Parallel (per Host)

Total Processes

10

HTTP Processes

10

Packet Delay

Packet (Burst) Delay

Medium

Port Scanning and Host Discovery

Intensity

Normal

OK

Cancel



Click the [first drop-down](#).

Configure Scan Performance Settings

Turn help tips: On | Off

Settings

Select a performance level or customize performance settings for network analysis.

☒ Enable parallel scaling for Scanner Appliances

Overall Performance

Normal

Hosts to Scan in Parallel

External Scanners

15

Scanner Appliances

30

Processes to Run in Parallel (per Host)

Total Processes

10

HTTP Processes

10

Packet Delay

Packet (Burst) Delay

Medium

Port Scanning and Host Discovery

Intensity

Normal

OK

Cancel



Select Custom

Configure Scan Performance Settings

Turn help tips: On | Off

Settings

Select a performance level or customize performance settings for network analysis.

☒ Enable parallel scaling for Scanner Appliances

Overall Performance

Custom

Hosts to Scan in Parallel

High

Normal

Low

☒ Custom

External Scanners

Scanner Appliances

30

Processes to Run in Parallel (per Host)

Total Processes

10

HTTP Processes

10

Packet Delay

Packet (Burst) Delay

Medium

Port Scanning and Host Discovery

Intensity

Normal

OK

Cancel



Selecting "Custom" means that the settings are now writable. Click the [drop-down](#) next to "Scanner Appliances".

Configure Scan Performance Settings
Turn help tips: On | Off

Settings

Select a performance level or customize performance settings for network analysis.

☒ Enable parallel scaling for Scanner Appliances

Overall Performance

Custom ▾

Hosts to Scan in Parallel

External Scanners

15 ▾

Scanner Appliances

30 ▾

Processes to Run in Parallel (per Host)

Total Processes

10 ▾

HTTP Processes

10 ▾

Packet Delay

Packet (Burst) Delay

Medium ▾

Port Scanning and Host Discovery

Intensity

Normal ▾

OK

Cancel



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

Configure Scan Performance Settings

Turn help tips: On | Off

Settings

Select a performance level or customize performance settings for network analysis.

☒ Enable parallel scaling for Scanner Appliances

Overall Performance Custom

Hosts to Scan in Parallel

External Scanners 15

Scanner Appliances 50

Processes to Run in Parallel (per Host)

Total Processes 33

HTTP Processes 34

Packet Delay 35

Packet (Burst) Delay 36

Port Scanning and Host Discovery 37

Intensity 38

39

40

41

42

43

44

45

46

47

48

49

✓ 50

OK

Cancel



Click **OK**

Configure Scan Performance Settings

Turn help tips: On | Off

Settings

Select a performance level or customize performance settings for network analysis.

☒ Enable parallel scaling for Scanner Appliances

Overall Performance

Custom

Hosts to Scan in Parallel

External Scanners

15

Scanner Appliances

50

Processes to Run in Parallel (per Host)

Total Processes

10

HTTP Processes

10

Packet Delay

Packet (Burst) Delay

Medium

Port Scanning and Host Discovery

Intensity

Normal

OK

Cancel



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.

Performance

Configure performance options for scanning your network.

Overall Performance: Custom Configure...

Load Balancer Detection

With this option enabled, the scanner will attempt to identify load balancers and the number of Web servers behind them.

☐ Search for load balancers during scan

Password Brute Forcing

Select the level of password brute forcing performed by scans. An "Exhaustive" setting will increase scan time.

☐ System Minimal (empty passwords) ▼
☐ Custom Configure...

Vulnerability Detection

☒ Complete
☐ Custom
☐ Select at runtime

Include

☐ Basic host information checks [View list](#)
☐ OVAL checks

Exclude

☐ Excluded QIDs



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.

Performance
Configure performance options for scanning your network.

Overall Performance: Custom [Configure...](#)

Load Balancer Detection
With this option enabled, the scanner will attempt to identify load balancers and the number of Web servers behind them.

☒ Search for load balancers during scan

Password Brute Forcing
Select the level of password brute forcing performed by scans. An "Exhaustive" setting will increase scan time.

☐ System Minimal (empty passwords) [View list](#)

☐ Custom [Configure...](#)

Vulnerability Detection

☒ Complete

☐ Custom

☐ Select at runtime

Include

☒ Basic host information checks [View list](#)

☐ OVAL checks

Exclude

☐ Excluded QIDs



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](#).

Authentication

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 authentication to target hosts. No other scan tests will occur. You must choose at least one authentication type.

- ☐ Enable authentication testing

Additional Certificate Detection

We'll find certificates on ports/services with full port scans by default. Enable this option to find certificates in more locations using



Click the [checkbox](#) next to Unix / Cisco / Network SSH

Authentication

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 authentication to target hosts. No other scan tests will occur. You must choose at least one authentication type.

- ☐ Enable authentication testing

Additional Certificate Detection

We'll find certificates on ports/services with full port scans by default. Enable this option to find certificates in more locations using



Click the [scrollbar](#) to scroll down.

Authentication

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 authentication to target hosts. No other scan tests will occur. You must choose at least one authentication type.

- ☐ Enable authentication testing

Additional Certificate Detection

We'll find certificates on ports/services with full port scans by default. Enable this option to find certificates in more locations using



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

Additional Certificate Detection

We'll find certificates on ports/services with full port scans by default. Enable this option to find certificates in more locations using authentication, for example in Apache, Tomcat, Jboss, Java KeyStore and Windows IIS. **Authentication is required.**

☐ Enable additional certificate detection

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

Set a custom value in order to drop defenses (such as logging, IPs, etc) when authorized scans are being run.

Host-Alive Testing

When enabled, scan testing will report hosts found alive during the discovery or port scanning process. Other testing will not



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.

Additional Certificate Detection

We'll find certificates on ports/services with full port scans by default. Enable this option to find certificates in more locations using authentication, for example in Apache, Tomcat, Jboss, Java KeyStore and Windows IIS. **Authentication is required.**

☒ Enable additional certificate detection

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

Set a custom value in order to drop defenses (such as logging, IPs, etc) when authorized scans are being run.

Host-Alive Testing

When enabled, scan testing will report hosts found alive during the discovery or port scanning process. Other testing will not

 Click the [checkbox](#) next to "Enable Windows Share Enumeration".

Additional Certificate Detection

We'll find certificates on ports/services with full port scans by default. Enable this option to find certificates in more locations using authentication, for example in Apache, Tomcat, Jboss, Java KeyStore and Windows IIS. **Authentication is required.**

☒ Enable additional certificate detection

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

Set a custom value in order to drop defenses (such as logging, IPs, etc) when authorized scans are being run.

Host-Alive Testing

When enabled, scan testing will report hosts found alive during the discovery or port scanning process. Other testing will not



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.

Additional Certificate Detection

We'll find certificates on ports/services with full port scans by default. Enable this option to find certificates in more locations using authentication, for example in Apache, Tomcat, Jboss, Java KeyStore and Windows IIS. **Authentication is required.**

☒ Enable additional certificate detection

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

Set a custom value in order to drop defenses (such as logging, IPs, etc) when authorized scans are being run.

Host-Alive Testing

When enabled, scan testing will report hosts found alive during the discovery or port scanning process. Other testing will not



Click the [Save](#) button.

☒ 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

Set a custom value in order to drop defenses (such as logging, IPs, etc) when authorized scans are being run.

Host-Alive Testing

When enabled, scan testing will report hosts found alive during the discovery or port scanning process. Other testing will not occur.

☐ Enable Host Alive Testing

Do not overwrite OS

When enabled, we will not update the OS of target hosts during scan processing.

☐ Do not overwrite OS



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.

Qualys Cloud Platform

VMDR

Dashboard Vulnerabilities Prioritization **Scans** Reports Remediation Assets KnowledgeBase Users

Scans Maps Schedules Appliances Option Profiles Authentication Search Lists Setup

Actions (0) New Search Filters 1 - 15 of 15

<input type="checkbox"/>	Type	Title	User	Modified
<input type="checkbox"/>	Standard	CertViewFree Profile	Marcus Burrows - Qualys Training	07/26/2023
<input type="checkbox"/>	Standard	Initial Options	Marcus Burrows - Qualys Training	01/05/2023
<input type="checkbox"/>	Standard	OP - Authentication Check	Marcus Burrows - Qualys Training	01/06/2023
<input type="checkbox"/>	Standard	OP - Authentication Failures QIDs	Marcus Burrows - Qualys Training	02/13/2023
<input type="checkbox"/>	Standard	OP - Certification-Accreditation	Marcus Burrows - Qualys Training	02/02/2023
<input type="checkbox"/>	Standard	OP - Discovery-Inventory	Marcus Burrows - Qualys Training	02/09/2023
<input type="checkbox"/>	Standard	OP - Host Alive Test	Marcus Burrows - Qualys Training	02/02/2023
<input type="checkbox"/>	Standard	OP - Not Cloud Agents	Marcus Burrows - Qualys Training	03/16/2023
<input type="checkbox"/>	Standard	OP - OnPrem Assessment	Marcus Burrows - Qualys Training	06/26/2023
<input type="checkbox"/>	Standard	OP - Perimeter Scan	Marcus Burrows - Qualys Training	06/26/2023
<input type="checkbox"/>	Standard	OP - Remote Only	Marcus Burrows - Qualys Training	02/23/2023
<input type="checkbox"/>	Standard	OP - Scan Analysis	Marcus Burrows - Qualys Training	02/09/2023
<input type="checkbox"/>	Standard	SSL Certificates	Marcus Burrows - Qualys Training	02/09/2023
<input type="checkbox"/>	Standard	Vulnerability Assessment Profile (default)	Marcus Burrows - Qualys Training	09/15/2023
<input type="checkbox"/>	PCI	Payment Card Industry (PCI) Options	System	01/05/2023



Scan to go to the interactive player