

VMS Services Manual – Gold Clients

Last Updated: April 2018

Copyright

Copyright 2007-2018. SecureWorks®, Inc. All Rights Reserved.

This publication contains information that is confidential and proprietary to Secureworks and is subject to your confidentiality obligations set forth in your contract with Secureworks or affiliates thereof. This publication and related hardware and software are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright law. Copying and/or reverse engineering of any Secureworks hardware, software, documentation, or training materials is strictly prohibited.

This publication and related Secureworks software remain the exclusive property of Secureworks. No part of this publication or related software may be reproduced, stored in a retrieval system, or transmitted in any form or any means, electronic or mechanical, photocopying, recording, or otherwise without the prior written permission from Secureworks.

Due to continued service development, the information in this publication and related software may change without notice. Please report any errors to Secureworks in writing. Secureworks does not warrant that this publication or related hardware or software is error-free. Please refer to your contract with Secureworks for any provided warranty information.

Secureworks and iSensor are registered trademarks of Secureworks. All other trademarks are the property of the respective owners.

Document Revision and Approval History

Revision Number	Revision Date	Summary of Changes	Changes Marked
1.0	August 2014	New Document	NA
2.0	April 2016	Edited Company name, logo, font	
3.0	March 2017	Added information for CM, TP, and Agents	
4.0	January 2018	Updated branding, Client Portal information	
5.0	April 2018	Feedback link added	

Table of Contents

Document Revision and Approval History	3
Introduction	8
Purpose	8
Scope.....	8
Contact Information	9
Contacting the SOC.....	9
Contacting Secureworks VMS Support	9
Secureworks Client Portal.....	10
Accessing the Client Portal.....	10
Before you Begin.....	10
Step One – Create Your Portal Password as the First Authentication Factor	10
Step Two – Set up and Register Duo Mobile.....	10
Step Three – Generate your Certificate to Receive Encrypted Emails.....	10
Adding Users as Authorized Contacts with Security Questions.....	10
Using the Client Portal Ticketing System	11
Maintenance Notifications	11
Qualys	12
User Role Comparison	12
Requesting Access to Qualys Subscriptions.....	13
Importing Qualys Data.....	13
VMS Service Level Agreements (SLAs).....	14
Vulnerability Scanning Service.....	14
Asset Group Request.....	14
VM Scan Request	14
Excluded Host List	14
PCI Scanning Service.....	14
PCI Scan Request.....	14
False Positive Request	14
Attestation Report Request.....	15
Web Application Scanning Service.....	15
Web Application Setup Request	15
Web Application Scan Request	15
SLAs for all VMS Scanning Services	15
P1 – Critical Priority Issue	15
P2 – High Priority Issue.....	15
Getting Started with VMS Services	16
Accessing Your Qualys Subscription	16
Selecting a Qualys Module.....	16

Filling Service Activation Profiles (SAP)	17
Information Gathering SAP Form.....	17
External Asset Group SAP Form	17
Internal Asset Group SAP Form	18
Scan Request SAP Form.....	18
VMS Scanner SAP US Form	18
PCI Subscription Setup Form	18
Web Application Scanning Subscription Form.....	18
Submitting Completed SAP Forms.....	18
Secureworks Vulnerability Management Services	20
VMS Service Implementation Workflow	20
VM SAP Forms.....	21
Scanner Appliance Information	21
Physical Specifications for the Physical Scanner	22
Scoping for Additional Scanner Appliances.....	22
Virtual Scanner Qualification Matrix.....	22
Asset Groups.....	23
Creating Asset Groups	23
Self-Serve Option.....	23
Maps	25
Launching or Scheduling Maps	25
Self-Serve Options	25
Self-Serve Option.....	26
Scans.....	29
Vulnerability Scanning.....	29
Launching or Scheduling Scans.....	29
Self-Serve Option.....	30
Self-Serve Option.....	31
Retrieving Scan Results	32
Excluding IPs.....	33
Submitting Exclusions	33
Self-Serve Option.....	33
Option Profiles	35
Creating Option Profiles	35
Self-Serve Option.....	35
Search Lists.....	38
Creating Search Lists	38
Self-Serve Option.....	38
Notification Options for Qualys Scans	40
Receiving Scan Completion Notifications.....	40

Enabling Scan Notification Emails	40
Receiving Scan Summary Emails upon Scan Completion	41
Stopping Running Scans	43
Self-Serve Option	43
Scanner Appliance Troubleshooting	44
Approach to an Offline Scanner	44
Scanner Appliance Interface Map	44
Scanner Appliance Error Codes	44
Verify Basic Connectivity	45
Confirming Client Prerequisites are In Place	45
Perform the Laptop Test	46
Reports	47
Report Templates	47
Scorecard Reports	47
Running Scorecard Reports	47
Creating Report Templates	48
Quarterly Scan Review	52
Scheduling a Quarterly Scan Reviews	52
Qualys Vulnerability Severity Level Information	53
Severity Levels	53
Confirmed Vulnerabilities	53
Potential Vulnerabilities	53
Information Gathered	54
Half Red / Half Yellow	54
Secureworks PCI Service (PCI)	55
PCI Service Implementation Workflow	55
PCI SAP Forms	55
Accessing the Qualys PCI Portal	56
Option 1 - Access PCI Portal Directly	56
Option 2 - Access PCI Portal from within your Qualys Subscription	56
Linking PCI Subscription and Qualys Subscription	58
Getting Started Guide for PCI	59
SLAs for PCI Services	60
False Positive Submission	60
Attestation Submission	61
Secureworks Policy Compliance (PC) Service	63
Secureworks Continuous Monitoring (CM) Service	64
Secureworks ThreatPROTECT Service	65
Secureworks Cloud Agent Service	66
Secureworks Web Application Scanning Service	67

Classification: //SecureWorks/Confidential - Limited External Distribution:

WAS Service Implementation Workflow	67
WAS SAP Forms	68
Web Applications	68
Web Application Scanning.....	68
Web Crawling and Link Discovery	69
Vulnerability Testing.....	69
Creating Web Applications	71
Self-Serve Option.....	71
Web Application Option Profiles	72
Creating Web Application Option Profiles.....	72
Web Application Search Lists.....	73
Creating Web Application Search Lists.....	73
Scanning Web Applications	74
Self-Serve Option.....	74
Self-Serve Option.....	75
Retrieving Web Application Scan Results	76
Web Application Reports	77
Creating Reports	77
Getting Started Guide for WAS	78
Appendix A – Authenticated Scanning Guides.....	79
Policy Compliance Authenticated Scanning Guides	79
Vulnerability Scanning Authenticated Scanning Guides	79
Appendix B - API Guides.....	80
Appendix C – Qualys “How to” videos	81
Qualys Vulnerability Management Video Series	81
Qualys Web Application Scanning Video Series.....	81
Qualys Policy Compliance Video Series	81
Appendix D – Secureworks VMS Service Descriptions.....	82

Introduction

Thank you for choosing Secureworks Vulnerability Management Services! Your Vulnerability Management Services will be powered by the Qualys Suite.

This document will serve as your guide to getting started with the Qualys Tool for Internal/External vulnerability scanning, PCI scanning, Policy Compliance Scanning and Web Application Scanning.

Purpose

The Secureworks VMS Services Manual is intended to be a living document, with periodic updates and revisions to reflect the evolving nature of the services over time. This manual and the Secureworks MSS Deployment Guide should provide a comprehensive overview of the specific Secureworks MSS service delivery model in effect.

This document is not designed to supplant, supersede or otherwise displace any information or obligations contained in the binding contractual material agreed to and executed by both Secureworks and the Client, but rather to provide a clear, consolidated reference point for a wide-ranging scope of baseline interaction of activities that will occur between the parties in the natural course of deployment and operation of the suite of MSS services.

Scope

This document will provide high-level information and highlight interface processes for the design, deployment, ongoing operation, collaboration and governance of all of the aspects of the MSS Service delivery.

Contact Information

Contacting the SOC

You can reach the Secureworks Security Operations Center (SOC) by creating a Service Request in the [Client Portal](#), or by calling:

- › Inside the US: 1-877-838-7960
- › United Kingdom: 0808 234 2477
- › Australia: 1800 760 854
- › All Other Locations: +1 404-235-1044

Contacting Secureworks VMS Support

In the event you need to contact Secureworks for assistance with the Vulnerability Scanning Service, you can reach the VMS Team by:

- › Email: vms-support@secureworks.com
- › Phone: call the SOC at a number listed above and select **option 6**

Please note that the VMS team is available to assist you M-F 8am-5pm EST.

Secureworks Client Portal

Accessing the Client Portal

Before you Begin

After your Portal account is created, you will receive an email from the Secureworks Security Operations Center (SOC) (service@secureworks.com). The email is titled "Secureworks Portal Registration and Certificate Setup". Locate the email in your inbox to get started.

Step One – Create Your Portal Password as the First Authentication Factor

1. Click on the link in the email and follow the prompts to create your Portal password: <https://portal.secureworks.com/idm/resetpassword>.
2. The Reset Password page displays. Type your email address associated with your Portal account and click **RESET PASSWORD**. An email is sent to your account.
3. Open the Password Reset Request email and click the link in the email to create your password.
4. Enter and retype your new Portal password then click **RESET PASSWORD**.

Step Two – Set up and Register Duo Mobile

Now it is time to set up your second authentication factor using Duo Mobile and your mobile phone, landline phone, or tablet.

1. Log in to the Portal with your new Portal password: <https://portal.secureworks.com/portal>.
2. The **Duo Start Setup** screen displays. Scroll down, click **START SETUP**, and follow the directions on the screen. If you have questions about setting up your devices to support Duo Mobile authentication, see the [Two Factor Authentication for New and Existing Portal Users](#) manual for more detailed information.

Step Three – Generate your Certificate to Receive Encrypted Emails.

After completing the preceding steps and logging in to the Portal for the first time, you will be prompted to generate your Security Certificate to receive encrypted emails.

1. Enter a new certificate password of your choosing and then verify your new password. Click **GENERATE CERTIFICATE**.

IMPORTANT: This is your new **CERTIFICATE** password—not your Portal password—used only when importing your certificate into your email client.

Please see the [Two Factor Authentication for New and Existing Portal Users](#) manual for instructions on how to import your certificate into your email application. The certificate is only used for receiving encrypted emails.

Adding Users as Authorized Contacts with Security Questions

Portal users assigned the role of User Admin can add new users via the Portal at any time by selecting **USER MANAGEMENT** from the **Administration** tab. For further guidance, click the [Help](#) link from the top toolbar of the Portal, or navigate to the [Learning Center](#) and locate the *User Management Manual*.

To have the Secureworks SOC create the user accounts for you, create a Service Request from the Portal, or [call the SOC](#).

Using the Client Portal Ticketing System

The Client Portal Ticketing System facilitates secure authenticated communication with the Secureworks SOC. Downloading and importing your certificate authorizes you to receive encrypted email notifications from the SOC and Secureworks. For more information on the ticketing process, please see the *Ticket Management Manual* available on the [Learning Center](#).

Maintenance Notifications

Secureworks may schedule maintenance and/or upgrade outages with a 24-hour notice to designated client contacts; however, every effort is made to give clients a 3-5 business day notice. Secureworks may also schedule emergency/non-scheduled maintenance outages with a 24-hour notice to designated client contacts. Secureworks will make commercially reasonable efforts to conduct all client-impacting maintenance after 6:00PM Pacific Standard Time and will notify clients of Portal upgrades within 24-36 hours of the completion of the maintenance.

For more information on maintenance notification, please refer to your Service Level agreements.

Qualys

User Role Comparison

The following table provides a comparison of privileges granted to user roles for vulnerability management.

● = privilege is granted to the user role

o = privilege may be assigned by a Manager user

X = privilege may be assigned by Manager user (when subscription is configured to allow it)

Manager privileges apply to all user configurations (such as asset groups, option profiles, schedules, and saved results), regardless of who created them. Unit Manager privileges apply to user configurations created within their respective business units. Scanner and Reader privileges apply to personal configurations only. Remediation User has pre-defined and limited privileges. User administrator has privileges to create and edit users except Manager and User administrator. To know more about user roles, refer to [user roles](#).

Privileges	Manager	Unit Manager	Scanner	Reader	Remediation User	Administrator User
Account Setup						
Configure your dashboard	●	●	●	●		
Change your Home page	●	●	●	●		
Change your password	●	●	●	●	●	●
Reporting						
Run reports	●	●	●	●		
Manage report templates	●	●	●	●		
Manage distribution groups	●	●	●	●		
Ignore vulnerabilities	●	●	o	o		
Purge host information	●	o	o	o		
Remediation						
Manually create tickets	●	●	●	●		
Edit tickets	●	●	●	●	●	
Close/ignore tickets	●	●	o	o	●	
Delete tickets	●	●	o	o		
Manage remediation policy	●	o				
Scanner Appliances						
Install scanner appliances	●	●				
Manage virtual scanner appliances	●	o	X			
Network Mapping & Vulnerability Scanning						
View map and scan history	●	●	●			
Launch maps and scans	●	●	●			
Schedule maps and scans	●	●	●			
Cancel maps and scans	●	●	●			
Pause/resume scans	●	●	●			
Setup storage options to auto delete results	●	●	●			
General Management						
Manage search lists	●	●	●	●		
Manage asset tags (Learn more)	●	●	●	●		
Manage asset groups	●	●	●			

Manage option profiles	●	o	o			
Distribute global option profiles and templates	●	o				
Manage user accounts	●	●				●
Manage authentication records and vaults	●	o	X			
Add and edit host assets	●	o				
Add and edit domain assets	●	o				
Manage business units	●					●
Manage distribution groups	●	●	●	●		●
Manage networks	●					
Subscription Setup						
Edit global excluded hosts list	●	●				
Set global user permissions	●					
Setup business units - enable the new IP limit feature	●					
Setup business risk	●					
Setup security risk	●					
Define host attribute names	●					
Setup CVSS	●					
Set account and password security options	●					
Set remediation transition options	●					
Set the primary contact for the subscription	●					
KnowledgeBase						
View vulnerabilities	●	●	●	●	●	
Edit vulnerabilities - severity and content	●					
Add OVAL vulnerabilities	●					
Disable vulnerabilities	●					

Requesting Access to Qualys Subscriptions

To have the Secureworks SOC create the Qualys user accounts for you, follow the below process:

Please create a Service Request in the Client Portal or call the SOC at 1-877-838-7960. Include the requested Qualys user role for the account (Manager, Scanner, Reader, Remediation User, Administrator User).

Importing Qualys Data

If your organization subscribes to the Vulnerability Management (VM) service using the Qualys scanning platform, your recent Qualys VM scan results are regularly imported into the Client Portal.

These results are available for use by the SOC to enhance the analysis of events, and they are also available for you to view in the Portal. The import process also creates any previously unknown assets found in Qualys scan results, making them available for analysis in the Portal.

The Concern Index and Business Risk Trend dashboard charts use your Qualys scan results in calculations.

VMS Service Level Agreements (SLAs)

This section details the various SLAs that pertain to each specific VMS Service.

Vulnerability Scanning Service

The SLAs described below pertain to the Internal/External Vulnerability Scanning Service.

Asset Group Request

The Secureworks VMS team will perform the addition, modification or removal of Asset Groups within three (3) business days from the time the request is submitted.

The Secureworks VMS team will reach out to the requestor if clarifications are needed. If clarifications are needed and the VMS team is unable to get a response back from the requestor, the request will not be processed until the clarifications are received.

VM Scan Request

The Secureworks VMS team will perform the scheduling, modification or removal of a scan request within three (3) business days from the time the request is submitted.

The Secureworks VMS team will reach out to the requestor if clarifications are needed. If clarifications are needed and the VMS team is unable to get a response back from the requestor, the request will not be processed until the clarifications are received.

Excluded Host List

The Secureworks VMS team will modify the Excluded Host List within three (3) business days from the time the request is submitted.

The Secureworks VMS team will reach out to the requestor if clarifications are needed. If clarifications are needed and the VMS team is unable to get a response back from the requestor, the request will not be processed until the clarifications are received.

PCI Scanning Service

The SLAs listed pertain to the PCI Scanning Service.

PCI Scan Request

The Secureworks VMS team will perform the scheduling, modification or removal of a PCI scan within three (3) business days from the time the request is submitted.

The Secureworks VMS team will reach out to the requestor if clarifications are needed. If clarifications are needed and the VMS team is unable to get a response back from the requestor, the request will not be processed until the clarifications are received.

False Positive Request

The Secureworks VMS team will begin working to analyze false positive submissions and provide an initial written response accepting, rejecting, or requesting more information from Client within five (5) business days from receipt of Client's false positive exception request.

Time for complete resolution of the false positive request is contingent upon the Client providing sufficient evidence of a compensating control or false positive and therefore is not subject to SLA.

Attestation Report Request

The Secureworks VMS team will review and then digitally sign (if correct) or reject (if problems or discrepancies are found), all Client attestations, within two (2) business days of receipt, subject to the availability of the Qualys PCI Portal.

Web Application Scanning Service

The SLAs described below pertain to the Web Application Scanning Service.

Web Application Setup Request

The Secureworks VMS team will configure the web application within three (3) business days from the time the request is submitted.

Web Application Scan Request

The Secureworks VMS team will perform the scheduling, modification or removal of a PCI scan within three (3) business days from the time the request is submitted.

SLAs for all VMS Scanning Services

The listed SLAs pertain to all of the VMS Scanning Services.

P1 – Critical Priority Issue

In the event of a P1 Issue (defined as an issue that prevents the Client from accessing the Service), the Secureworks VMS team will provide an initial response within 8 hours. Status updates will be provided within 1 business day following updates from the Vendor.

P2 – High Priority Issue

In the event of a P2 Issue (defined as an issue in which the Client can access the Service, however, one or more significant functions are unavailable, such as the ability to launch a scan or map), the Secureworks VMS team will provide an initial response within 24 hours. Status updates will be provided within 2 business days following updates from the Vendor.

Getting Started with VMS Services

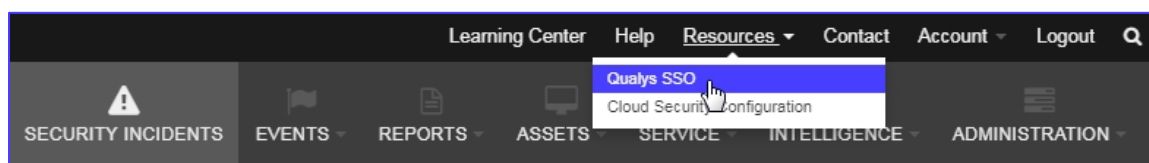
This section contains general information pertaining to working with the Secureworks team and the primary actions you will need to know in order to utilize your VMS services.

Accessing Your Qualys Subscription

The Secureworks Vulnerability Scanning Service leverages the Qualys Single Sign On (SSO) Functionality.

To access your Qualys Subscription, follow these steps:

1. Navigate to the Secureworks [Client Portal](#).
2. From the **Resources** menu option, select **QUALYS SSO**.



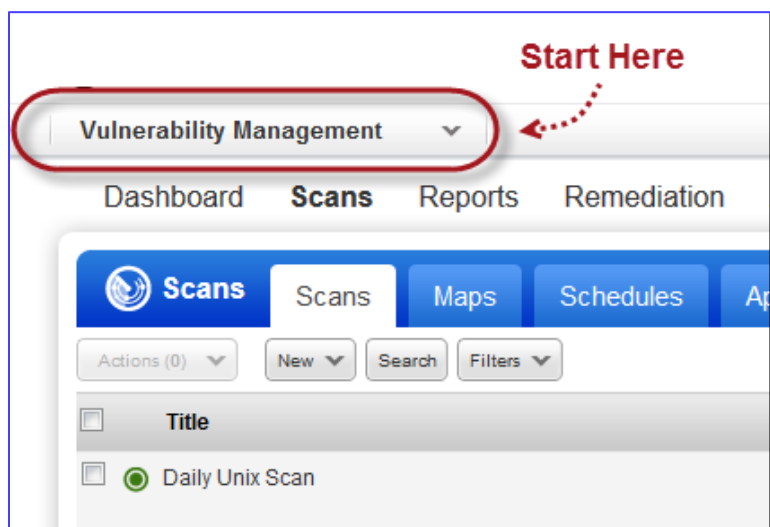
3. The **Qualys SSO Subscription** dialog displays. Select the desired subscription from the dropdown menu and click **SUBMIT**.
4. A new browser tab opens and displays your subscription.

Selecting a Qualys Module

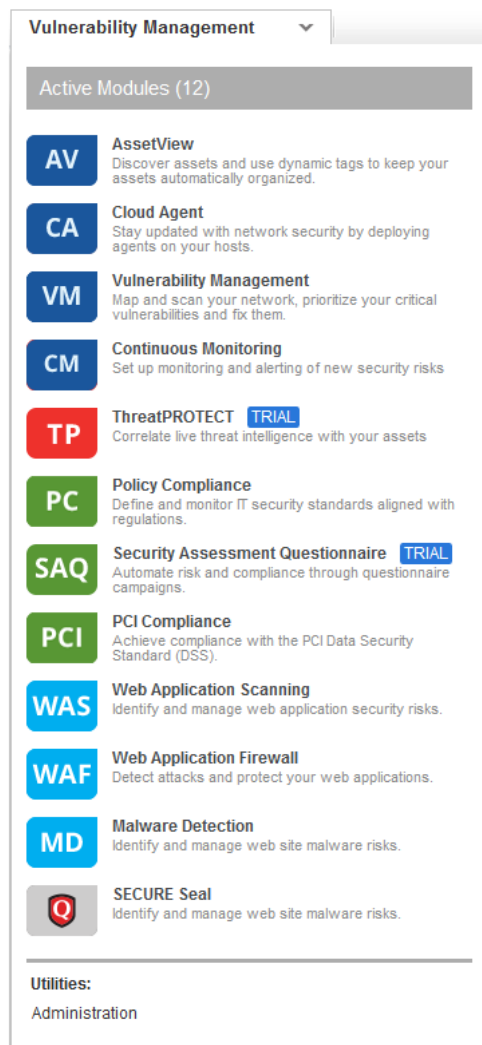
Once you are logged in to your Qualys subscription, you will automatically be placed into the Vulnerability Management module.

To access a different module, follow these steps:

1. Click on the Vulnerability Management drop down arrow.



2. Select the desired module from the list and you will be switched to that module.



Filling Service Activation Profiles (SAP)

There are several SAP forms that you will receive as part of the deployment process.

The SAP forms are described as follows.

Information Gathering SAP Form

- › Purpose: This form gathers the basic information that needs to be configured in the Qualys portal by the Secureworks engineer.
- › Notes: IPs to be added and users needing access to Qualys are detailed on this form.

External Asset Group SAP Form

- › Purpose: This form gathers the necessary information for the VMS team to build out the client's External Asset Groups within the Qualys portal for External Vulnerability Scanning.
- › Automation: The VMS team has automation scripts that utilize the data in this form to have the asset groups built in the Qualys portal leveraging the Qualys API.

- › Notes: This SAP form can be used one or multiple times by the client throughout the term of their contract. VMS receives this form from our client base via email or attached to a ticket. This form is distributed by Secureworks Engineer to the client during service implementation but is not required to turn services up.
- › SLA: There is a three (3) business day SLA for the VMS team to process this type of request.

Internal Asset Group SAP Form

- › Purpose: This form gathers the necessary information for the VMS team to build out the client's Internal Asset Groups within the Qualys portal for Internal Vulnerability Scanning.
- › Automation: The VMS team has automation scripts that utilize the data in this form to have the asset groups built in the Qualys portal leveraging the Qualys API.
- › Notes: This SAP form can be used one or multiple times by the client throughout the term of their contract. VMS receives this form from our client base via email or attached to a ticket. This form is distributed by Secureworks Engineer to the client during service implementation but is not required to turn services up.
- › SLA: There is a three (3) business day SLA for the VMS team to process this type of request.

Scan Request SAP Form

- › Purpose: This form gathers the information that the VMS team needs to schedule scans in the Qualys portal.
- › Automation: The VMS team has automation scripts that utilize the data in this form to have the scan schedules built in the Qualys portal leveraging the Qualys API.
- › Notes: This SAP form can be used one or multiple times by the client throughout the term of their contract. VMS receives this form from our client base via email or attached to a ticket. This form is distributed by Secureworks Engineer to the client during service implementation but is not required to turn services up.
- › SLA: There is a three (3) business day SLA for the VMS team to process this type of request.

VMS Scanner SAP US Form

- › Purpose: This form gathers the necessary information for Secureworks Engineer to have the physical Qualys scanner appliances built and shipped to the client.
- › Notes: Device configuration information such as IP address, netmask, gateway, etc are collected on this form. The device is then pre-configured based on the client's settings and can be cabled and racked when it arrives onsite.

PCI Subscription Setup Form

- › Purpose: This form gathers the basic information for the Secureworks Engineer to build out a Qualys PCI Subscription.
- › Notes: This form gathers the in scope IPs, the users who need access and other PCI relevant information required to setup the PCI Subscription.

Web Application Scanning Subscription Form

- › Purpose: This form gathers information from the client to have their web applications built in the Qualys portal.
- › Notes: This form gathers the necessary information on how the client wants the web application configured within the Qualys portal.
- › SLA: There is a three (3) business day SLA for the VMS team to process this type of request.

Submitting Completed SAP Forms

During service deployment, these forms will be submitted to the Secureworks Engineer who will initiate your services.

Once services are deployed, you can continue to use the SAP forms and submit them to the VMS team directly for processing. Completed SAP forms can be submitted via email to vms-support@secureworks.com or by creating a Service Request on the Secureworks Client Portal and attaching the forms.

Secureworks Vulnerability Management Services

The Secureworks Vulnerability Management Services (referred herein as "VMS") delivers vulnerability assessments of the Client's environment. VMS consists of automated and recurring vulnerability and scanning.

VMS Service Implementation Workflow

For service deployment of the Vulnerability Management Service, the Secureworks Engineer assigned to the project will reach out to the client to request a kick off call. During this call, the relevant forms to collect the needed information from the client will be discussed, along with the process for the implementation.

The client will need to supply the filled out forms for the deployment to continue. Once the forms have been returned, or if the client has any questions, a technical review call can be requested to discuss the forms or any other technical questions regarding the service that is being deployed.

Once the forms have been completed and returned, the Secureworks Engineer will proceed with getting the service deployed and handed over to the VMS Engineering team for ongoing service delivery and support.







This is an outline of the deployment process and related documentation:

Staging	Kickoff	Implementation
Order Received		
Project assigned		
	SIF created	
	SAPs selected (attached below)	
		VMS Scanner SAP
		Information Gathering SAP
		Scan Request SAP
		External Asset Group SAP (if required)
		Internal Asset Group SAP (if required)
Begin Initial Process		
	Contact client	
	Request Kickoff Call	
During Kickoff Call		
	Review Contracts	
	Discuss Process	
	Provide SIF and SAPs	
	Provide Implementation Requirements	
	Discuss Action Items and Next Steps	
	Schedule Technical Review Call	
	Outline project plan	
Client action items		
	Complete SIF and SAPs	
	Return to PM assigned	
Technical Review Call		
	Review the SIF and SAPs	
		Confirm IP(s) information
		Confirm shipping address(es)

Classification: //SecureWorks/Confidential - Limited External Distribution:

		Confirm IP's for scanning
		Review Users and associated role level
	Confirm project plan status	
Preconfigure and ship scanners		
	Scanners shipped per information provided via the SIF and SAPs	
Populate Qualys Portal		
	Users permitted access per SAP	
	IP information imported per SAP	
Scanners arrive onsite		
	Client racks, stacks and powers on scanner	
	Client confirms access requirements are in place	
	PM and/or client verify connectivity to the appliance via the Qualys portal	
		Troubleshoot if issue with connectivity
Qualys Welcome Guide distributed		
Service Activation and Project Closure		

VM SAP Forms

 VMS Scanner SAP - US.xlsx	 Information Gathering SAP.xlsx	 External Asset Group SAP Form.xlsx
 Internal Asset Group SAP Form.xlsx	 Scan_Request_SAP.xlsx	 SIF VMS.xlsx

Scanner Appliance Information

Qualys provides two options for scanner appliances – a physical scanner and a virtual scanner.

Physical Specifications for the Physical Scanner

Configuration	
CPU	Intel Xeon® Quad-Core 3.5GHz, 8M Cache
Memory	16GB DDR3-1600
Hard Drive	1TB, 2.5", SATA 6Gb/s, 5400RPM
Ethernet	Two GbE ports
USB	Two USB 2.0 ports
Power Input	100-240 VAC, 50-60Hz, 4A Single phase
Power Consumption	Max: 91W (310 BTU/hr); Typical: 80W (273 BTU/hr)
Dimension	1.75 (H) x 17 (W) x 14 (D) inches
Weight	12.65 lbs.
Environment	
Acoustic Noise	~45 dBA acoustic noise level at 23°C
Operating Conditions	0°C to 35°C, from 0 to 5,000 feet; 20% to 90% RH
Storage Conditions	-10°C to 70°C; 10% to 85% R.H. (non-condensing)
Operating Vibration	.3 Grms, 10 to 500 Hz, 5 minutes per axis
In-Package Shock	In accordance with ISTA 2A
Regulatory	ETL (conforms to UL STD 60950-1, CSA STD C22.2 No. 60950-1), CE
EMC	FCC Part 15 Class A (conforms to EN 55022/24, EN 61000, CISPR 22)
Environmental	RoHS
Other certifications	Per specific requirements

Network Requirements: Configuration Options and Best Practices for Internal Scanning for Physical Scanner can be found in the following PDF guide: [Qualys Scanner Appliance User Guide](#)

Scoping for Additional Scanner Appliances

The general rule of thumb is one scanner appliance (physical or virtual) for approximately 5000 IPs.

Additional scoping discussion will likely be needed as factors such as physical location, network bandwidth size, firewall placement, etc., can come into play in determining the amount of scanner appliances that will be needed.

Virtual Scanner Qualification Matrix

Detailed information on selecting which platform to deploy a virtual scanner on can be found here: [Virtual Scanner Qualification Matrix](#)

Technical Details and reference material on the virtual scanner appliances can be found here: [Virtual Scanner Reference Material](#)

Asset Groups

Asset Groups are logical groups of host assets that can be based on importance, priority, location, function, etc.

Using asset groups makes scanning, mapping and reporting more efficient. You can scan and map a group repeatedly and know that the same IPs are included every time.

By organizing assets into subsections of your network, you can limit the scope of the scan target, making the results and remediation tasks more manageable.

Creating Asset Groups

To have the Secureworks VMS Team create an asset group, do the following:

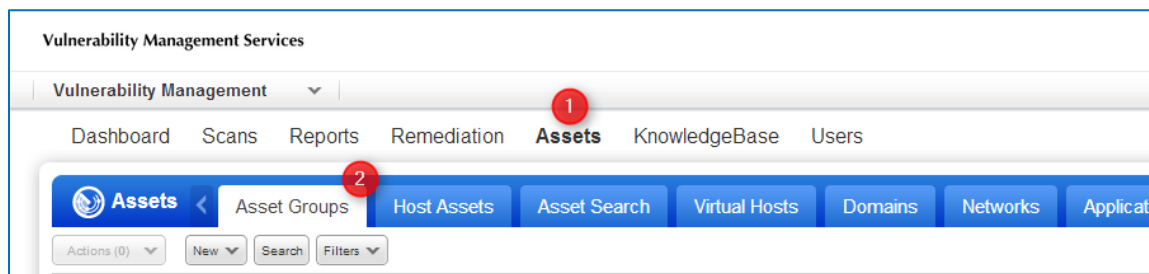
1. Fill out the Internal Asset Group SAP Form for internal asset groups.
2. Fill out the External Asset Group SAP Form for external asset groups.
3. Submit the completed SAP forms to the Secureworks VMS Team either by emailing it to vms-support@secureworks.com or by creating a Service Request on the [Secureworks Client Portal](#) and attaching the forms.

The VMS team will process the request within three (3) business days or reach out to the requestor if clarifications are needed. If clarifications are needed and the VMS team is unable to get a response back from the requestor, the request will not be processed until the clarifications are received.

Self-Serve Option

To Create an Asset Group, do the following:

1. Click the **ASSETS** tab and then click **ASSET GROUPS**.



2. Click the **NEW** menu and select **ASSET GROUP**.
3. In the window that displays, use the tabs on the left hand side to fill in the relevant information.

The screenshot shows the 'New Asset Group' window with the 'Asset Group Title' tab active. The 'Title' field is empty. The 'Network' dropdown is set to 'Another Network'. The 'Owner' dropdown is set to 'CIS Team Manager: veng, Inc'. The 'Cancel' and 'Save' buttons are at the bottom.

- a. Title: Enter a unique name for this asset group. It should be easy to remember and descriptive of the IPs and domains included. Include a maximum of 255 characters. If you change the asset group title, the new title is automatically updated in all associated scheduled tasks and report templates.
- b. Network: This option is only visible if you have the overlapping IP support feature enabled on your subscription.
- c. Owner: Select the owner for the asset group that you are creating.
- d. Select IPs, DNS, NetBIOS, or Domains tab to enter in hosts to your asset group.

The screenshot shows the 'New Asset Group' window with the 'IPs' tab active. The 'Enter or Select IPs/Ranges' text area contains the example '192.168.0.87-192.168.0.92, 192.168.0.200'. The 'Display each IP/Range on new line' checkbox is unchecked. The 'Cancel' and 'Save' buttons are at the bottom.

- e. Click the Scanner Appliances Tab to add Scanner Appliances to the asset group.

If you want to...	Then...
Enter in Business relevant information or define CVSS information for the asset group	Click the Business/CVSS information tab
Add Comments in your asset group	Click the Comments tab

- 4. Click **SAVE** once you have entered in all of the information for your asset group.

Maps

Mapping discovers all network devices that can be seen from the Internet (or internal network if using a scanner appliance) and reports comprehensive information about them.

Mapping Your Network Perimeter: The mapping service produces a map of visible devices on your network perimeter. These are devices that can be "seen" from the Internet. It provides you with an outside-in perspective of your network elements. The scope of the network discovery includes the devices found for a domain through the domain's DNS (Domain Name Server), plus the devices between those devices and the Internet. For this reason, the map report may include more devices than those identified by a domain.

Mapping Your Internal Network: Using a scanner appliance, the mapping service can produce a map of visible devices on your internal network. The appliance is installed inside your network environment to discover and map all devices that can be "seen" from the Intranet. The scope of the network discovery includes the devices found for a domain through the internal DNS in your network, plus the devices between those devices and the scanner appliance. For this reason, the map report may include more devices than those identified by a domain.

There are two primary events that take place during the mapping process:

Host Discovery: When a target domain is provided, the service gathers data from public records to identify hosts in the domain using various methods including Whois lookups, DNS zone transfer, and DNS brute force. The service then checks availability of each discovered host. For each host, the service checks whether the host is connected to the network, whether it has been shut down and whether it forbids all Internet connections.

The service pings each host using ICMP, TCP, and UDP probes. The TCP and UDP probes are sent to default ports for common services, such as DNS, TELNET, SMTP, HTTP and SNMP. If these probes trigger at least one response from the host, the host is considered "alive."

Basic Information Gathering: The mapping service attempts to identify the operating system installed on each host and scans 13 standard TCP ports to determine which ports are open. Note that by performing basic information gathering, additional scan tests are launched, which may result in the detection of additional devices, such as routers.

Launching or Scheduling Maps

Within the Qualys tool, you have the ability to run an "on demand" map or create a map schedule.

To have the Secureworks VMS Team schedule a map task to run at a specific date and time, do the following:

1. Fill out the Scan Request SAP form.
2. Submit the completed SAP forms to the Secureworks VMS Team either by emailing it to vms-support@secureworks.com or by creating a Service Request on the Secureworks Client Portal and attaching the forms.

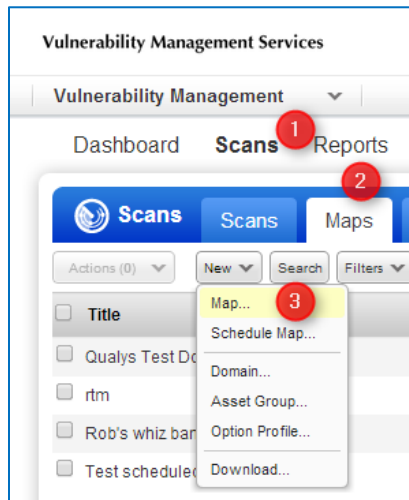
The VMS team will process the request within three (3) business days or reach out to the requestor if clarifications are needed. If clarifications are needed and the VMS team is unable to get a response back from the requestor, the request will not be processed until the clarifications are received.

Self-Serve Options

To Launch an On Demand Map, do the following:

(Please note the map will be launched at the time you complete the task).

1. Go to **SCANS** → **MAPS** and select **NEW MAP** from the **NEW** drop down menu.



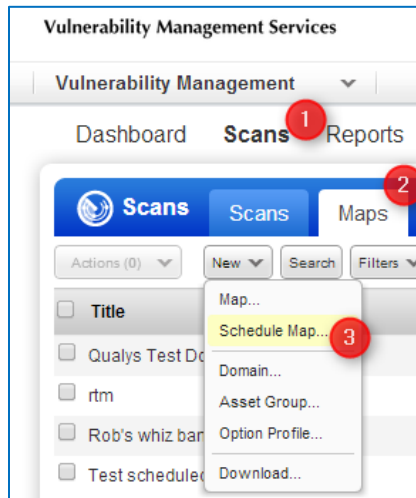
2. Fill in the following information:
 - Title: Provide a title for the scan. The title may contain a maximum of 64 characters and cannot be in use by another scan task.
 - Option Profile: Select an Option Profile to apply to the vulnerability scan.
 - Scanner Appliance: (appears only when there are internal scanner appliances in your account) Select a scanner option to apply to this scan task.
 - Asset Groups: You can scan against an IP or range of IPs in your subscription or you can choose an Asset Group.
 - Check off Domains or IPs you want to map based on the settings in your Asset Group
3. Click **LAUNCH**.

Self-Serve Option

To Schedule a Map to launch at a future date, do the following:

Classification: //SecureWorks/Confidential - Limited External Distribution:

1. Go to **SCANS** → **MAPS** and select **SCHEDULE MAP** from the **NEW** drop down menu.



2. Fill in the following information on the Task Title tab:
 - Title: Provide a title for the scan. The title may contain a maximum of 64 characters and cannot be in use by another scan task.
 - Task Owner: Select an owner for this map task.
 - Option Profile: Select an Option Profile to apply to the vulnerability scan.
 - Scanner Appliance: (appears only when there are internal scanner appliances in your account) Select a scanner option to apply to this scan task.
3. Fill in the following information on the Target Domains tab:
 - Asset Groups: You can scan against an IP or range of IPs in your subscription or you can choose an Asset Group.
 - Check off Domains or IPs you want to map based on the settings in your Asset Group.
4. Fill in the following information on the Scheduling tab:
 - Start: Fill in the start date, start time, timezone and DST.
 - Duration: Select if you want the scan to Cancel after a set number of hours.
 - Occurs: Fill in the frequency of the scan task (Daily, Weekly, Monthly).
 - Ends After: If you only want to scan to run one (1) time, enter 1 and put a select the box.

New Scheduled Map Launch Help

Task Title >

Target Domains >

Scheduling >

Notifications >

Schedule Status >

Scheduling

Start: Jul 16, 2014 00:00 DST

Duration: ☐ Cancel after 01 hours

Occurs: Daily 1 days

☐ Ends after occurrences

5. Click the **NOTIFICATIONS** tab to have emails sent out prior to the scan task launching.
6. Click the **SCHEDULE STATUS** tab if you want to deactivate this scan schedule task.
7. Click **SAVE**.

Scans

Vulnerability scans analyze your network for vulnerabilities, using the Vulnerability KnowledgeBase hosted by the service, the industry's largest and most comprehensive database of vulnerability signatures.

Vulnerability Scanning

Vulnerability scanning analyzes the security of your network using the largest and most up to date Knowledgebase of vulnerability checks. When you launch vulnerability scans, the service detects vulnerabilities using an adaptive process that runs only tests applicable to each host scanned. The service first gathers information about each host, such as its operating system and version, ports and services, and then selects the appropriate test modules.

Host Discovery: The service checks availability of target hosts. For each host, the service checks whether the host is connected to the Internet, whether it has been shut down and whether it forbids all Internet connections. The service pings each target host using ICMP, TCP, and UDP probes. The TCP and UDP probes are sent to default ports for common services on each host, such as DNS, TELNET, SMTP, HTTP and SNMP. If these probes trigger at least one response from the host, the host is considered "alive."

The types of probes sent and the list of ports scanned during host discovery are configurable through your additional options.

If the host is not "alive" then the scan process will not proceed. You may choose to scan dead hosts through your scan options, but that option may increase scan time and is not suggested for Class C or larger networks.

Port Scanning: The service finds all open TCP and UDP ports on target hosts. The list of TCP and UDP ports scanned is configurable through your scan options.

OS Detection: The service attempts to identify the operating system installed on target hosts. This is accomplished through TCP/IP stack fingerprinting, OS fingerprinting on redirected ports, and is enhanced by additional information gathered during the scan process, such as NetBIOS information gathering.

Service Discovery: When a TCP or UDP port is reported as open, the scanning service uses several discovery methods to identify which service is running on the port, and confirms the type of service running to obtain the most accurate data.

Authentication: Authentication to hosts is optional for a vulnerability scan. For a vulnerability scan with authentication enabled, the service authenticates to target hosts based on the selected authentication types in the option profile and the authentication records in the user account. The service uses the credentials for target hosts as defined in authentication records. If authentication to a host is not successful, the service performs vulnerability assessment without authentication.

Vulnerability Assessment: Using the information gathered about each target host in the scanning steps, the service begins vulnerability assessment. The service scans for all vulnerabilities in the KnowledgeBase or a selected list of vulnerabilities, based on the user's scan settings. The service runs vulnerability tests that are applicable to each target host based on the information gathered for the host.

Launching or Scheduling Scans

Within the Qualys tool, you have the ability to run an "on demand" scan or create a scan schedule.

To have the Secureworks VMS Team schedule a scan task to run at a specific date and time, do the following:

1. Fill out the Scan Request SAP form.
2. Submit the completed SAP forms to the Secureworks VMS Team either by emailing it to vms-support@secureworks.com or by creating a Service Request on the [Secureworks Client Portal](#) and attaching the forms.

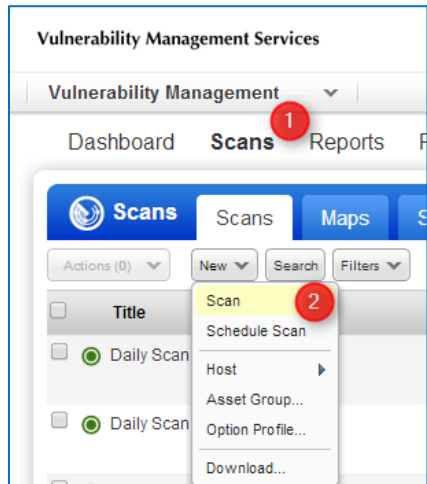
The VMS team will process the request within three (3) business days or reach out to the requestor if clarifications are needed. If clarifications are needed and the VMS team is unable to get a response back from the requestor, the request will not be processed until the clarifications are received.

Self-Serve Option

To Launch an On Demand Scan, do the following:

(Please note the scan will be launched at the time you complete the task).

1. Click on **SCANS** and select **SCAN** from the **NEW** drop down menu.

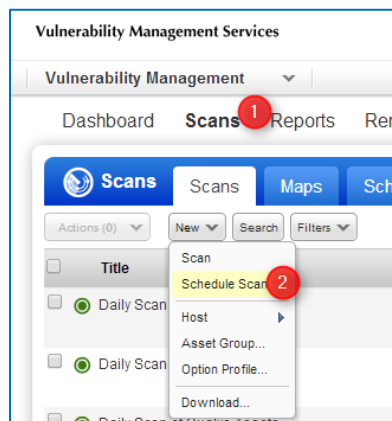


2. Fill in the following information:
 - Title: Provide a title for the scan. The title may contain a maximum of 64 characters and cannot be in use by another scan task.
 - Option Profile: Select an Option Profile to apply to the vulnerability scan.
 - Scanner Appliance: (appears only when there are internal scanner appliances in your account) Select a scanner option to apply to this scan task.
 - Target Hosts: You can scan against an IP or range of IPs in your subscription or you can choose an Asset Group.
3. Click **LAUNCH**.

Self-Serve Option

To Schedule a Scan to launch at a future time, do the following:

1. Click on **SCANS** and select **SCHEDULE SCAN** from the **NEW** drop down menu.



2. Fill in the following information on the Task Title tab:

Title: Provide a title for the scan. The title may contain a maximum of 64 characters and cannot be in use by another scan task.

Task Owner: Select an owner for this scheduled scan task.

Option Profile: Select an Option Profile to apply to the vulnerability scan.

Scanner Appliance: (appears only when there are internal scanner appliances in your account) Select a scanner option to apply to this scan task.

3. Fill in the following information on the Target Hosts tab:

- o Select whether you want to choose targets based on Assets or Tags

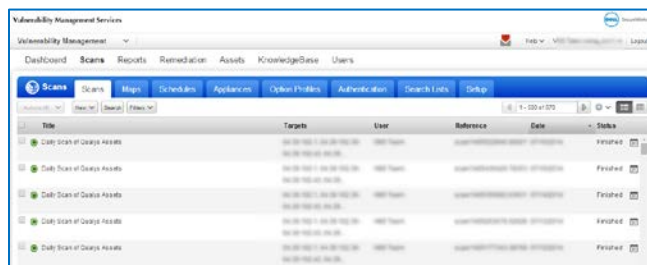
Classification: //SecureWorks/Confidential - Limited External Distribution:

- Asset Groups: Select which asset groups to scan.
 - IPs/Ranges: Select which IPs or ranges you want to scan.
 - Excluded IPs/Ranges: Enter in any IPs or ranges that you do not want to be scanned. Please note that this applies ONLY to this scan task only.
4. Fill in the following information on the Scheduling Tab:
- Start: Fill in the start date, start time, timezone and DST.
 - Duration: Select if you want the scan to Pause or Cancel after a set number of hours.
 - Resume Days: If you want the scan to Pause after so many hours and then automatically resume daily, etc.
 - Occurs: Fill in the frequency of the scan task (Daily, Weekly, Monthly).
 - Ends After: If you only want to scan to run one (1) time, enter 1, then select the box.
5. Click the **NOTIFICATIONS** tab if you want to have emails sent out prior to the scan task launching.
6. Click the **SCHEDULE STATUS** tab if you want to deactivate this scan schedule task.
7. Click **SAVE**.

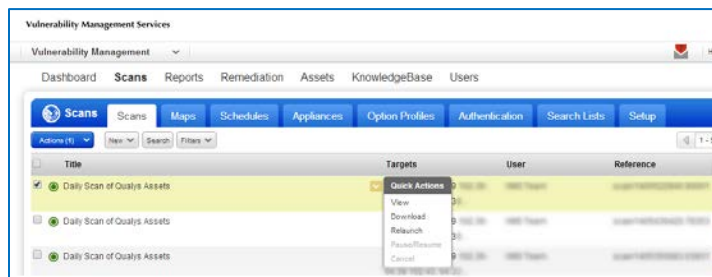
Retrieving Scan Results

Within the Qualys tool, you can view the results for your scans and maps by doing the following:

1. Click the **SCAN** tab and either select **SCANS** to view Scan results or **MAP** to view Map results. A list of scans (or maps) you have run and their Status displays.



2. Use the blue down arrow to view the results, download the results, or re-launch the scan/map task.



Excluding IPs

Within Qualys, you can configure an Excluded Hosts list. There is one global excluded host list for the subscription. The list may be edited as often as necessary to meet the changing demands of your organization.

This list of IPs will never be mapped or scanned by the service, even if specified as part of a map or scan target. No scanning traffic, including ICMP, TCP and UDP probes, will be sent to excluded hosts.

IPs not currently in the subscription may also be added to the excluded hosts list, ensuring that they will not be scanned even if later added to the subscription.

Please note that excluded hosts may still appear in map results if discovered via a DNS method. If the IP belonging to a DNS server is included in the excluded hosts list and this server is used to resolve DNS names for hosts in the map target, then the service will still send normal requests to the DNS server. The server, however, will not be scanned for vulnerabilities.

Submitting Exclusions

To have the Secureworks VMS Team update the Excluded Host List, do the following:

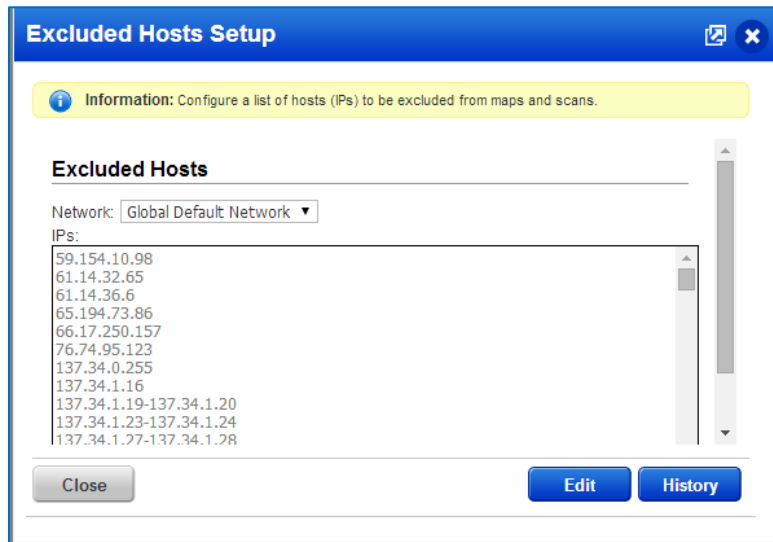
1. Send an excel document containing the IPs that should be added to the global Excluded Host List to vms-support@secureworks.com.
 - o The list must be in Excel format with one IP address, IP range or CIDR block per cell in one column.
 - o No spaces or special characters other than a dash (-) or a forward slash (/) are allowed.
 - o All duplicate and/or overlapping IPs must be removed prior to submitting to the VMS team to process.
 - o The processing of the do not scan list has a three (3) business day SLA from the VMS team.
2. Once the VMS team receives the updated do not scan list, the existing list of IPs currently in the Excluded Host List will be removed.
3. The team will add in all of the IPs in the most current revision of the do not scan list
4. The VMS team will validate that all of the IPs that should be included in the Excluded Host List have been correctly added.
5. The team will reply to the requestor indicating that the request has been processed.

IMPORTANT: Any scans running or launching during the time that the Excluded Host List is being updated will NOT leverage the new list and will leverage the previous list of IPs.

Self-Serve Option

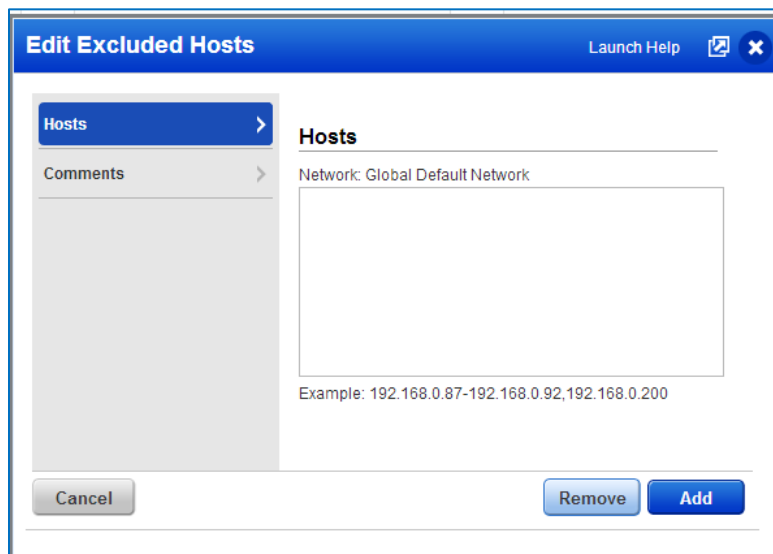
To add hosts to the Excluded Hosts List, do the following:

1. Go to **SCANS → SETUP → EXCLUDED HOSTS**



In the window that opens, you will see all of the hosts currently included in the Excluded Hosts List.

2. Click **EDIT** to add or remove hosts.



3. Enter the hosts you want to add (or remove).
4. Enter a comment on why you are adding (or removing) the host.

Option Profiles

Option Profiles are sets of preferences to be applied to map and scan tasks. Several option profiles are provided by the service for your convenience, but you can also create your own option profiles.

Option Profiles provided by the service: Initial Options: The Initial Options profile is initially set as the default profile for vulnerability scans and scheduled vulnerability scans. The default profile is intended for global use to ensure compliance with corporate security policies.

Payment Card Industry (PCI) Options: (This profile is only available if the Payment Card Industry (PCI) compliance feature is enabled for your subscription.) Use the PCI option profile to find and eliminate network security vulnerabilities associated with electronic commerce. This option profile contains scan configuration settings that have been optimized to test compliance with the Payment Card Industry Data Security Standard.

Qualys Top 20 Options: Use the Qualys Top 20 option profile to scan for the 20 most prevalent vulnerabilities determined by Qualys. The Qualys Top 20 list includes the 10 most prevalent internal vulnerabilities (detected on private IPs) and the 10 most prevalent external vulnerabilities (detected on public IPs). The Qualys Top 20 list is updated automatically and continuously from a statistically representative sample of thousands of networks. The list of included vulnerabilities is not editable.

SANS20 Options: You'll notice the title is "2008 SANS20 Options" if your subscription was created using version 6.18 or later. (Important: The SANS Top 20 list was last updated in 2008. For more accurate information on the most prevalent and critical real-world vulnerabilities use the Qualys Top 20 list.) Use the 2008 SANS 20 option profile to scan for the SANS Top 20 vulnerabilities. The SANS Institute publishes a list of the 20 most critical Internet security vulnerabilities, including top vulnerabilities in Windows systems, Unix systems, cross-platform applications and networking products. For each of the top 20 vulnerabilities, the service scans for multiple QIDs. The list of included vulnerabilities is not editable.

Creating Option Profiles

To have the Secureworks VMS Team create an option profile, do the following:

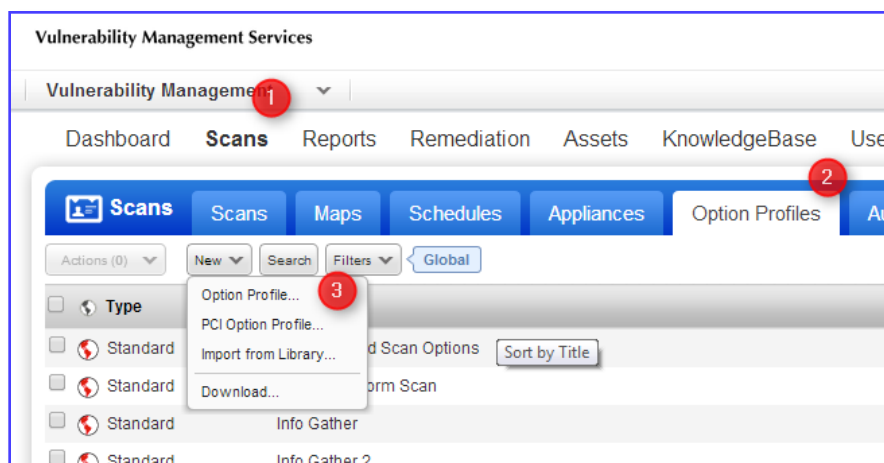
Send an email to vms-support@secureworks.com or create a Service Request on the [Secureworks Client Portal](#) with the specific requirements for profile.

The VMS team will process the request within three (3) business days or reach out to the requestor if clarifications are needed. If clarifications are needed and the VMS team is unable to get a response back from the requestor, the request will not be processed until the clarifications are received.

Self-Serve Option

To create an Option Profile, do the following:

1. Go to **SCANS → OPTION PROFILES** and select **OPTION PROFILE** from the **NEW** drop down menu.



Classification: //SecureWorks/Confidential - Limited External Distribution:

2. Enter in a title for the Option Profile, select an owner, and determine if any of the checkboxes need to be selected.

3. Select the Options you want to apply on the Scan Tab.

4. Select the Options you want for the Map settings on the Map tab.

New Option Profile Launch Help

Option Profile Title: **Map**

Scan: **Map**

Additional: **Additional**

Perform Basic Information Gathering on

☒ All Hosts
☐ Registered Hosts only
☐ Netblock Hosts only
☐ None

TCP Ports (maximum 20)
☒ Standard Scan (13 ports) [View list](#)
☐ Additional

(ex: 1-7, 8080)

UDP Ports (maximum 10)
☐ Standard Scan (6 ports) [View list](#)
☐ Additional

(ex: 1-8, 8080)

Options
☒ Perform Live Host Sweep Note: Edit host discovery options on the Additional tab.

Performance
 Configure performance options for mapping your network.
 Overall Performance: Normal [Configure...](#)

Authentication
 Authentication enables the scanner to log into hosts at scan time to extend detection capabilities. See the online help for more information.

5. Select the Additional Options you want on the Additional Tab.

New Option Profile Launch Help

Option Profile Title: **Additional**

Scan: **Additional**

Map: **Map**

Additional: **Additional**

Host Discovery

TCP Ports
☒ TCP (maximum 20)
☒ Standard Scan (13 ports) [View list](#)
☐ Additional

(ex: 1-6, 1024)

UDP Ports
☒ UDP (maximum 6)
☒ Standard Scan (6 ports) [View list](#)
☐ Custom [Configure...](#)

☒ ICMP

Blocked Resources
 Specify ports protected by your firewall/IDS. This option overrides TCP and UDP port settings on the Scan tab and is only applicable to scans.
☒ WatchGuard default blocked ports [View list](#)
☐ Custom port list

(ex: 111,431,2004)

Specify IP addresses and ranges protected by your firewall/IDS.
☒ All registered IPs
☐ Custom IP list

(ex: 204.121.23.1-204.121.23.9,119.36.0.1)

6. Click **SAVE**.

Search Lists

A search list is a subset of vulnerability checks based on certain criteria that you can define. Search Lists can either be Static Lists or Dynamic Lists.

Static Search Lists include a specific list of QID's.

Dynamic Search Lists include a set of vulnerability search criteria to create a dynamic list of QID's. This list will automatically be updated when new vulnerabilities are added to the Knowledgebase that meet the defined criteria.

Creating Search Lists

To have the Secureworks VMS Team create a search list, do the following:

Send an email to vms-support@secureworks.com or create a Service Request on the [Secureworks Client Portal](#) with the specific requirements for the search list.

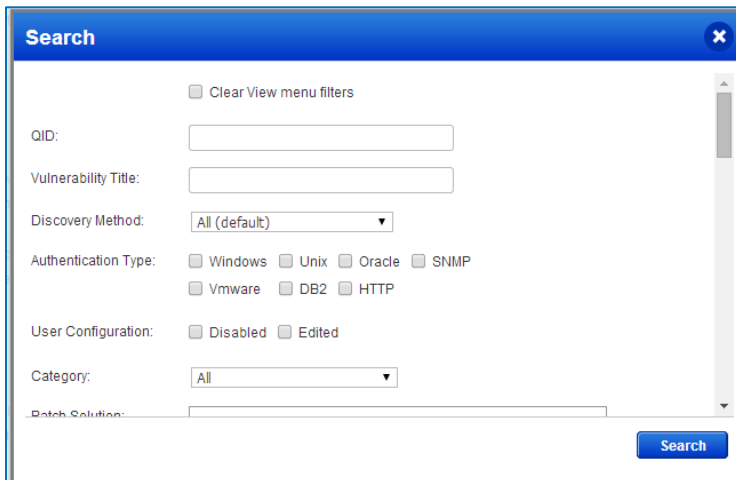
The VMS team will process the request within three (3) business days or reach out to the requestor if clarifications are needed. If clarifications are needed and the VMS team is unable to get a response back from the requestor, the request will not be processed until the clarifications are received.

Self-Serve Option

To create a search list, do the following:

1. Click the **REPORTS** tab and select the **SEARCH LISTS** tab.
2. Click the **NEW** menu and select either a **STATIC LIST** or **DYNAMIC LIST**.
3. For a Static List:
 - a. Enter a title for the search list.
 - b. Select an Owner for the list.

- c. On the QIDs tab, click the **SELECT** button to open the Knowledgebase or click the **MANUAL** button to manually enter the QIDs you want to include.
- d. If you clicked the **SELECT** button, you can search the Knowledgebase for the QIDs you want to include by clicking the Search button.



Search [X]

☐ Clear View menu filters

QID:

Vulnerability Title:

Discovery Method:

Authentication Type: ☐ Windows ☐ Unix ☐ Oracle ☐ SNMP
☐ Vmware ☐ DB2 ☐ HTTP

User Configuration: ☐ Disabled ☐ Edited

Category:

Patch Solution:

Search

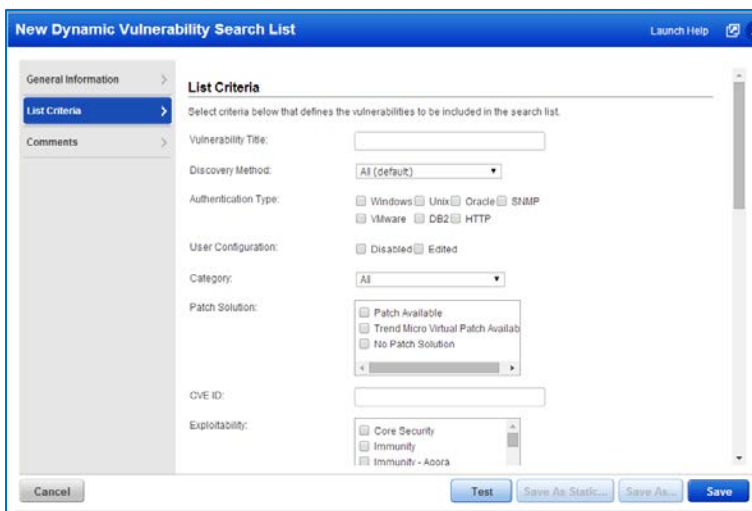
e. Enter in your search criteria. Once the results display, select the QIDs you want to include then click the OK button.

f. Click **SAVE**.

4. For a Dynamic List:

a. Enter a title for the search list.

b. Click the **LIST CRITERIA** tab and select the criteria to build the dynamic list.



New Dynamic Vulnerability Search List Launch Help

General Information > **List Criteria** > Comments >

Select criteria below that defines the vulnerabilities to be included in the search list.

Vulnerability Title:

Discovery Method:

Authentication Type: ☐ Windows ☐ Unix ☐ Oracle ☐ SNMP
☐ Vmware ☐ DB2 ☐ HTTP

User Configuration: ☐ Disabled ☐ Edited

Category:

Patch Solution: ☐ Patch Available
☐ Trend Micro Virtual Patch Available
☐ No Patch Solution

CVE ID:

Exploitability: ☐ Core Security
☐ Immunity
☐ Immunity - Adora

Cancel **Test** **Save As Static...** **Save As...** **Save**

c. Click **SAVE**.

Notification Options for Qualys Scans

Depending on configuration options, a Qualys user can receive notification emails when a scan is about to start and once a scan completes. Non-Qualys users can receive notifications when a scan is about to start, but not once a scan completes.

Receiving Scan Completion Notifications

Follow the below steps to set up your Qualys User Account to receive Scan Completion Notifications:

1. Access your Qualys subscription.
2. Click on the **USERS** tab.
3. Locate your user account and click **EDIT** on the Quick Actions menu.
4. Once in the Edit User window, click on the **OPTIONS** tab.
5. You can opt in to receive the Scan Complete Notification by editing your account under Notification Options. You can select “On” or “Off” for “Scan Complete Notification” and “On” or “Off” for “Scan Summary Notification (vulnerability scans only)”.

The screenshot shows the 'Edit User' window with the 'Options' tab selected. The 'Notification Options' section is highlighted with a red box. It contains the following settings:

- Latest Controls:** ☐ Monthly ☐ Weekly ☒ None
- Latest Vulnerabilities:** ☐ Weekly ☐ Daily ☒ None
- Scan Complete Notification:** ☒ On ☐ Off
- Scan Summary Notification (vulnerability scans only):** ☒ On ☐ Off
- Map Notification:** ☐ On ☒ Off
- Report Notification:** ☐ All reports ☐ My reports ☒ No notification
- Exception Notification:** ☐ My exceptions ☒ No notification
- Other Notifications:** ☐ Daily trouble tickets updates ☐ Scanner Appliance heartbeat check

Enabling Scan Notification Emails

Qualys allows you to distribute Scan Notification Emails prior to a scan starting. Follow the below steps to configure this for your scans:

1. Click on the **SCANS** tab and then click on **SCHEDULES**.
2. Either create a new scheduled scan task and enable the notification options, or select an existing scheduled scan task.
3. Once in the Scheduled Vulnerability Scan window, locate the Notifications tab.

4. Select the check box to Notify Task Owner so the owner of the scan also receives the email notification.
5. Select the number of days/hours/minutes in advance of the scan that you want the notice to be sent out.
6. Enter in any additional email addresses that you wish the scan notification be sent to in the text box. Be sure to follow the guidelines for how the emails should be formatted within the text box.
7. Enter a custom message for the scan notification email in the text box if desired. Click **SAVE**.

Receiving Scan Summary Emails upon Scan Completion

Only Qualys users who have access to the assets that were scanned and who also have the notification options enabled for “Scan Complete” and “Scan Summary” from above will receive Scan Complete/Scan Summary notifications.

Once a scan is complete, any user with access to the hosts that were scanned and with the notifications options enabled will receive an email that looks similar to:

The Scan Complete email notification is sent when the scan status is “Finished” and the option “Scan Complete Notification” is turned on in your account under Notification Options. Each email includes a scan summary and a secure link to the saved scan results report.

A sample Scan Complete email for a vulnerability scan is below showing vulnerability counts and trends. (For the first scan of a host in your subscription, there will be no trend information.)

From: Qualys Support
 To: jkim@qualys.com
 Date: Mon, Jun 04, 2014 at 10:44 AM
 Subject: Qualys: Scan Completed

 Email scan summary by Qualys
 Scan Title (Status): My First Scan
 Start Date: 06/04/2014 at 09:59:22 (GMT-0700)
 Duration: 00:04:38
 Target Groups: No Group
 Hosts Scanned: 1
 Active Hosts: 1
 Option Profile: Initial Options
 Launched By: Jason Kim (quays_ak12)
 Company: Qualys, Inc.
 Launch Type: On demand

Scan Status: Finished
Next Action: None

Summary of discovered Vulnerabilities (Trend)

Severity 5 "Urgent": 1 (-8)
Severity 4 "Critical": 2 (-15)
Severity 3 "Serious": 7 (-13)
Severity 2 "Medium": 5 (-11)
Severity 1 "Minimal": 1 (-3)
Total: 16

Summary of Potential Vulnerabilities

Severity 5 "Urgent": 3 (+3)
Severity 4 "Critical": 1 (+1)
Severity 3 "Serious": 0 (=)
Severity 2 "Medium": 2 (-2)
Severity 1 "Minimal": 0 (-1)
Total: 6

Summary of Information Gathered

Severity 3 "Serious": 4
Severity 2 "Medium": 6
Severity 1 "Minimal": 16
Total: 26

(+)(-)(=): Difference with previous detection for each host/vulnerability pair. For a complete explanation of trend information, refer to the online help.

Click here to view your full scan report:

https://Qualys.qualys.com/fo/report/report_view.php?ref=scan/1309378087.24272&authfirst=true&em=1

For more information, please email your primary contact: <mailto:nwood@qualys.com>

(c) Copyright 1999-2014 Qualys, Inc. All rights reserved.
<http://www.qualys.com>

Stopping Running Scans

Any user with Qualys Scanner or Manager access and access to the targets in the scan, can stop/pause the scan from within the Qualys portal.

To have the Secureworks Team stop a scan for you, do the following:

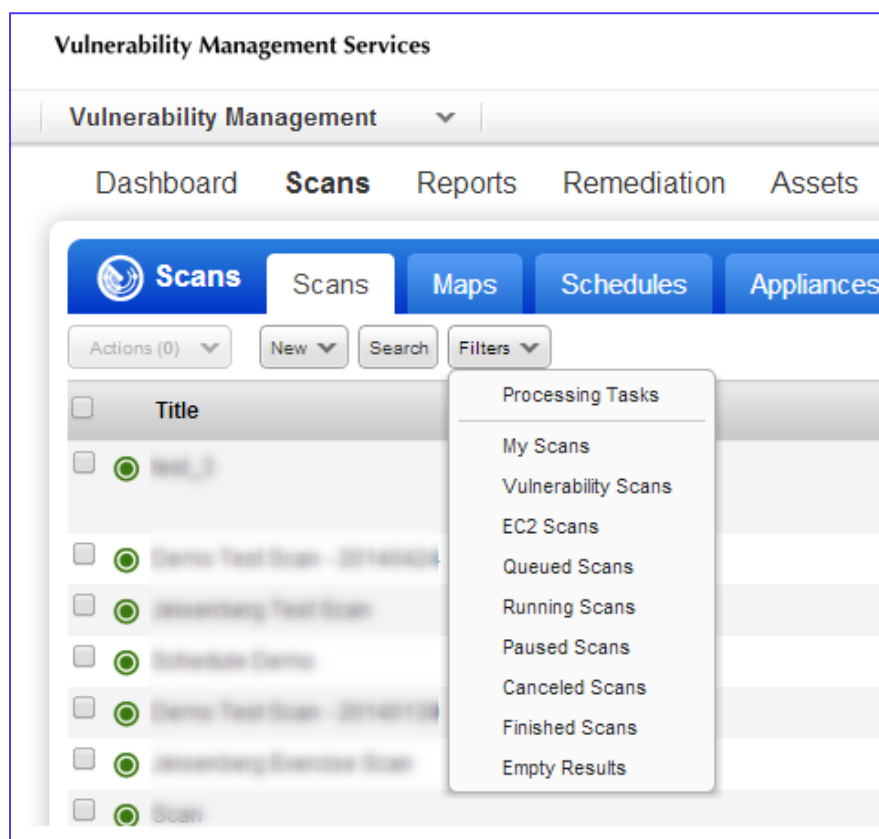
Any authorized POC can call in to the Secureworks SOC and request that a scan be stopped or paused.

The caller will need to be an authorized contact and will need to know the scan title(s) that they want stopped. The Secureworks SOC personnel will attempt to stop the scan and will reach out to the on-call VMS Engineer in the event they are unable to do so and require further assistance.

Self-Serve Option

To stop a scan from within the Qualys portal, follow the below directions:

1. Access your Qualys subscription.
2. Click on the **SCANS** tab.
3. Use the **FILTERS** drop down menu to select Running Scans.



4. Hover over the scan you want to stop and click the blue drop down arrow (Quick Actions menu).
 - o Select Pause to pause a scan in progress. When a scan is paused, scan results for hosts already scanned are saved. The scan remains paused until a user resumes or cancels the task (note the service cancels a paused scan automatically after 10 days). Once resumed, the remaining hosts will be scanned and all scan results will be combined into one scan results report.
 - o Select Cancel to cancel a scan in progress.

Classification: //SecureWorks/Confidential - Limited External Distribution:

Scanner Appliance Troubleshooting

This section describes troubleshooting techniques you use to respond to errors and performance conditions when using the Qualys Scanner Appliances.

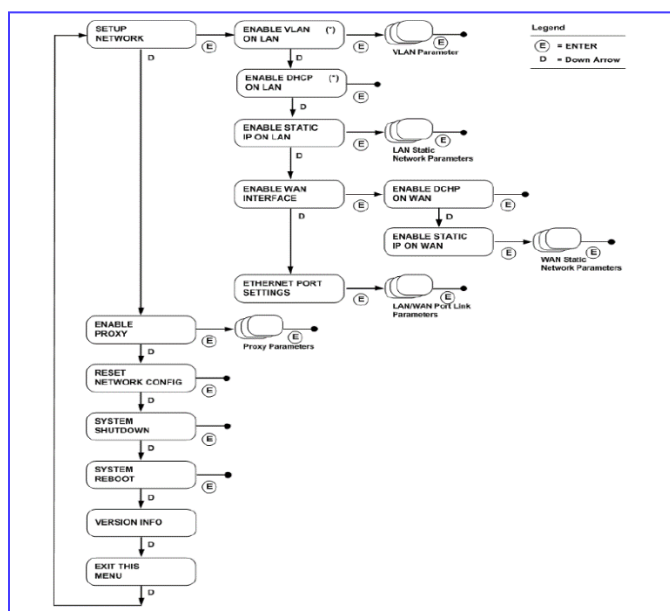
Approach to an Offline Scanner

Below is a list of high level techniques you can take to troubleshoot an offline scanner appliance. These topics are covered in more detail in each section below:

- > Reboot the Scanner Appliance;
- > Check the front display of the device for any error codes;
- > Verify that the scanner is plugged in and cabled to the LAN port and that there are connectivity lights on the port;
- > Verify that the scanner can be pinged;
- > Verify that the appropriate Firewall rules have been put in place;
- > Confirm that the same rules have been put in place on any Web Content Filtering Devices;
- > Perform the “Laptop Test”;
- > Walk through the interface to validate that the IP information as well as Ethernet Port Settings have been set correctly.

Scanner Appliance Interface Map

The picture is a graphical representation of the Scanner Appliance Interface.



Scanner Appliance Error Codes

A functional Scanner Appliance will have the short name of the device and the IP on the front display. An offline Scanner Appliance may display any of the Error Codes below. It is important to take note of the error code if one is being displayed.

Classification: //SecureWorks/Confidential - Limited External Distribution:

Network Error Code Description

- › E00 or E01 - Internal error (NTLM Proxy error)
- › E02 - Internal error (Proxy error)
- › E03 - Proxy configuration error
- › E04 - No connectivity after the Proxy was disabled
- › E05 - DNS lookup of the Qualys server failed (maybe network connectivity problem)
- › E06 - Cannot reach the Qualys server via HTTPS
- › E07 - Invalid LAN IP address or LAN gateway address
- › E08 - Invalid WAN IP address or WAN gateway address
- › E09 LAN IP address or LAN gateway address cannot be 127.0.0.1
- › E10 Could not configure the LAN interface
- › E11 WAN IP address or WAN gateway address cannot be 127.0.0.1
- › E12 Could not configure the WAN interface
- › E13 DNS lookup of the Qualys server failed due to a network connectivity problem
- › E14 DNS lookup of the Qualys server failed during the “SA Login” or “Activation Code” step due to a network connectivity problem

Verify Basic Connectivity

Try these basic connectivity troubleshooting steps when your Qualys Scanner Appliance is offline.

- › Verify that the scanner is plugged in and cabled to the LAN Port.
- › Verify that there are connectivity lights on the LAN Port.
- › Verify that the Scanner Appliance can be pinged.

Confirming Client Prerequisites are In Place

The Qualys Scanner Appliance needs the following Client-side prerequisites to be in place.

- › Outbound Firewall Rules Need to be in Place:
 - Add an outbound firewall rule allowing the Scanner Appliance’s management interface IP (WAN interface IP in split network configuration, LAN interface IP otherwise) to form its connection to management platform.
 - SRC: IP of the scanner
 - DST: qualysguard.qualys.com for US platform or qualysguard.qualys.eu for EU platform
 - DST: orchestrator.qualys.com for US platform or orchestrator.qualys.eu for EU platform
 - DST: dist01.sjdc01.qualys.com for US platform or dist.qualys.eu for EU platform
 - DST: nochost.sjdc01.qualys.com for US platform or monitoring.qualys.eu for EU platform

- DST: scanservice1.qualys.com for US platform or scanservice1..qualys.eu for EU platform
 - DST: all in 64.39.96.0/20
 - SVC: TCP 443
- › The Same Rules Set for the Firewall Need to be Set on Web Content Filtering Devices.
- › DNS Resolution Requirements:
- The scanner needs to be able to resolve these addresses on each active interface
 - qualysguard.qualys.com for US platform or qualysguard.qualys.eu for EU platform
 - orchestrator.qualys.com for US platform or orchestrator.qualys.eu for EU platform
 - dist01.sjdc01.qualys.com for US platform or dist.qualys.eu for EU platform
 - nochost.sjdc01.qualys.com for US platform or monitoring.qualys.eu for EU platform
 - scanservice1.qualys.com for US platform or scanservice1.qualys.eu for EU platform
- › For consistent and accurate results the scanner should have a Static IP address and record in DNS.

Perform the Laptop Test

After you have followed the above troubleshooting techniques and validated that the Scanner Appliance is configured correctly, you can try the Laptop Test.

- › Configure a laptop with the same IP information as the appliance.
- › Plug into the same network port with the same cable.
- › Connect to each site below and take a screen shot to the results.
- For US platform:
 - <https://qualysguard.qualys.com>
 - <https://orchestrator.qualys.com>
 - <https://dist01.sjdc01.qualys.com>
 - <https://nochost.sjdc01.qualys.com>
 - <https://scanservice1.qualys.com>
 - For EU platform:
 - <https://qualysguard.qualys.eu>
 - <https://orchestrator.qualys.eu>
 - <https://dist.qualys.eu>
 - <https://monitoring.qualys.eu>
 - <https://scanservice1.qualys.eu>

Reports

In Addition to viewing the scan results, you also have the option to produce customized reports based on the scan results.

Depending on your subscription level (Express or Enterprise), you will either have a section titled Report or Report Templates.

Within these sections, you will see a subset of reports that are included with the service.

Report Templates

Technical Report: Use this template to generate a report with the most recent scan data. This report does not show trends, meaning that it does not compare the most recent scan to previous scans. It includes the IP addresses (or ranges) from your most recent scan, and includes individual host details, which are sorted by host.

Executive Report: Use this template to generate a trend report providing a global view of your network security. This template creates a report that compares your scan results over the last 8 weeks, displays a bar graph outlining the total vulnerabilities by severity and a flow graph comparing the total vulnerabilities by severity over time. This report does not include individual host results or specific vulnerability information; therefore, it can be easily distributed because it does not contain sensitive data.

High Severity Report: Use this template to generate a report identifying all severity 4 and severity 5 vulnerabilities on your network. The following are filtered from this report: severity 1-3 vulnerabilities, potential vulnerabilities, information gathered, disabled checks and ignored checks.

Qualys Patch Report: Use this template to generate a patch report based on the current vulnerability detection data in your account. The resulting patch report shows the patches that need to be applied to fix the detected vulnerabilities on all hosts in your account. The detailed results in the report include a table of QIDs that will be fixed by applying each missing patch, and links for available patches are displayed if available.

Qualys Top 20 Report: Use this template to generate a report identifying the Qualys Top 20 vulnerabilities on your network. The Qualys Top 20 list includes the 10 most prevalent internal vulnerabilities (detected on private IPs) and the 10 most prevalent external vulnerabilities (detected on public IPs). The Qualys Top 20 list is updated automatically and continuously from a statistically representative sample of thousands of networks.

SANS Top 20 Report: Use this template to generate a report identifying the SANS Top 20 vulnerabilities on your network. The SANS Institute publishes a list of the 20 most critical Internet security vulnerabilities, including top vulnerabilities in Windows systems, Unix systems, cross-platform applications and networking products. For each of the top 20 vulnerabilities, the service scans for multiple QIDs and reports results for those detected.

Scorecard Reports

Within Qualys, there are several “Scorecard” reports that can be run. Scorecard reports provide vulnerability data and statistics based on the most up to date information and current vulnerability status for each host.

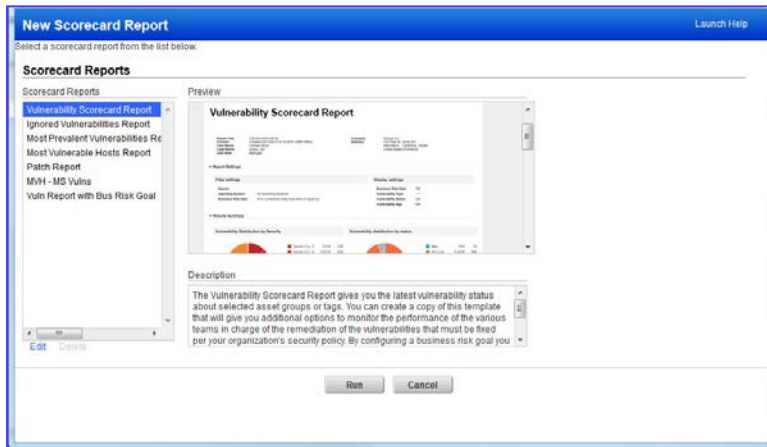
These reports include:

- › Asset Group Vulnerability Report: Identifies vulnerabilities with severity levels 3-5.
- › Ignored Vulnerabilities Report: Identifies vulnerabilities that are currently ignored.
- › Most Prevalent Vulnerabilities Report: Identifies vulnerabilities with the highest number of detected instances.
- › Most Vulnerable Hosts Report: Identifies hosts with the highest number of critical vulnerabilities.
- › Patch Scorecard Report: Identifies hosts with missing patches and software.

Running Scorecard Reports

To run a Scorecard report, do the following:

1. Click the **REPORTS** tab.
2. Click the **NEW** menu and select **SCORECARD REPORT**. The following window displays:



3. Highlight the report you want to run, then click **RUN**.
4. Select the Report Format for the report.
5. Select which subset of Asset Groups you want to run the report on.
6. Click **RUN**.

Creating Report Templates

Within the Qualys tool, there are ways to create your own report templates to narrow down information to only your specific criteria.

To create a report template, do the following:

1. Within the Report tab, select **TEMPLATES**. In the window that opens, you will notice you have several options available.
2. In the Report Title section, give the report a unique title and select the owner of the report.
3. In the Scan Results Selection are the following options:
 - Run Time (manual): The run time (manual) option provides a view of your risk at a particular moment in time (at the time of the scan). Vulnerability data and hosts included in your report are specific to the scans that you choose at run time. Note that you can view saved scans from the scan history list (select Scan on the left menu).
 - Status: Use Current vulnerability information (Auto): The status (auto) options provide the most up-to-date information and current vulnerability status for hosts specified in your report template. Vulnerability data is automatically collected based on the most recent scan data.
 - Status with Trend: Trend information is precisely calculated when analyzing results generated with the same scan options, and results generated for a full scan compared to a partial scan.
 - Hosts:
 - *Asset Groups*: Enter the name of each asset group to include. Click Select to choose from a list of groups in your account.
 - *IPs/Ranges*: Enter IP addresses/ranges to include. Click Select to choose from a list of IPs in your account.
4. In the Report Summary section, select the types of graphics to display.
5. In the Detailed Results section, select how to sort the information and which detailed information to include in the report.

6. Click the **FILTER** tab to display additional Filter Options.
7. Select one of these options to identify vulnerabilities to include:
 - Complete: Select to include all detected vulnerabilities in reports generated by this template.
 - Custom: Select to include only specific vulnerabilities in reports generated by this template. Add one or more vulnerability search lists to include. When you use this template generate a report, only the vulnerabilities defined in the selected search lists are included. It is not recommended that you use this feature with results from a partial vulnerability scan since you may end up with a blank report.
 - Select Exclude QIDs: (optional) to identify specific vulnerabilities to exclude from reports generated by this template. Add one or more vulnerability search lists to exclude. When you use this template to generate a report, the QIDs defined in the selected search lists are excluded.
 - If you add search lists to both the Custom list and to the Exclude QIDs list, then the service will first add the QIDs from the Custom list and then remove the QIDs from the Exclude QIDs list. If one or more QIDs match both lists, then those QIDs will not appear in the report. If all QIDs match both lists, then the report will be empty. Refer to the Report Filters section in the Scan Report Appendix to see the list of QIDs that matched the included search lists, the list of QIDs that matched the excluded search lists, and the resulting QIDs which is the difference between the two lists.
8. For Vulnerability Filters, specify which types of vulnerabilities you want to include in the report:
 - New: New vulnerabilities are issues that have not been previously detected.
 - Active: Active vulnerabilities are issues that are on-going. These vulnerabilities were detected on previous scans and are still being detected.
 - Re-Opened: Re-Opened vulnerabilities are issues that were likely resolved and then re-introduced for some reason. These vulnerabilities were detected in earlier scans, and subsequently were not detected because they were resolved or fixed. In the most recent scan, these vulnerabilities were detected again.
 - Fixed: Fixed vulnerabilities are those vulnerabilities that have been resolved. These vulnerabilities were detected in previous scans, but were not detected in the most recent scan.
 - Active: Active checks include all checks that are not disabled or ignored.
 - Disabled: Disabled checks include all checks that were previously disabled through the KnowledgeBase. Only Managers can disable vulnerability checks allowing them to be globally filtered from all hosts in all reports. If you include disabled checks, they appear grayed out in your host results.

- Ignored: (Only available when Scan Results Selection is set to Auto.) Ignored checks include all checks that were previously ignored. Any user can ignore vulnerability checks on a per host/IP basis, allowing the vulnerability check to be filtered for that particular host. If you include ignored checks, they appear grayed out in your host results.

9. You can also select specify Operating Systems to Include as well as specific categories to include.

10. Click the **SERVICE** and **PORTS** tab to flag specific services and ports as either required or unauthorized.

11. Services:

- Required Services: When a "required" service is not detected, it will be identified as a vulnerability in the report.
- Available Services: This is a list of services from which you can identify required and unauthorized services. Add and Remove services between this list and the Required Services and Unauthorized Services lists.
- Unauthorized Services: When an "unauthorized" service is detected, it will be identified as a vulnerability in the report.
- Service Info: Displays more information about available services to help you determine which services are required and which are unauthorized. Select the service you're interested in and click View.

12. Ports:

- Required Ports: Enter ports that are required, separating each with a comma. When a "required" port is not detected, it will be identified as a vulnerability in the report.
- Unauthorized Ports: Enter ports that are unauthorized, separating each with a comma. When an "unauthorized" port is detected, it will be identified as a vulnerability in the report.

Scan Results Selection

☐ Run Time: Select individual scan results at run time (Manual)
☒ Status: Use current vulnerability information (Auto)
☐ Status with Trend: Analyze vulnerability history (Auto)

☒ Include weekly vulnerability information for the past 1 week
☐ Only include scan results from the specified time frame
☐ Include vulnerability information for the past 2 detections

Asset Groups Select
 IPs/Ranges Select
Example: 192.168.0.87-192.168.0.92, 192.168.0.200

Display | Filter **Services and Ports** | User Access

Services

Required Services

<< Add

Add All

Remove >>

Remove All

Available Services

ActiveSync

elprovertpc

ekak trojan

amandeidx

oml

Apple Airport Management

Applix

Applix exnet

Applix TM1 Admin Server

Applix TM1 Server

View...

Unauthorized Services

Add >>

Add All

<< Remove

Remove All

Service Info

Ports

Required Ports:

Unauthorized Ports:

Quarterly Scan Review

As part of the Gold Service Tier, you are entitled to Quarterly Scan Review calls. These calls are limited to four (4) per calendar year and are limited to one (1) hour each.

Quarterly scan review calls can be used to review scan findings, answer questions related to scan results, discuss remediation strategies, and to discuss your program goals to see where utilizing Qualys can assist in achieving those goals.

Scheduling a Quarterly Scan Reviews

The Client can contact the Secureworks VMS Team by emailing vms-support@secureworks.com ten (10) days prior to the requested date to schedule a conference call for the quarterly scan review. If the Client has any specific items they want to cover, including those in the email request will allow the Secureworks VMS Team time to research and prepare for the call in advance.

Qualys Vulnerability Severity Level Information






Qualys vulnerabilities are automatically classified by severity level in vulnerability scan reports.

Severity Levels

The service assigns every vulnerability in the KnowledgeBase a severity level, which is determined by the security risk associated with its exploitation. The possible consequences related to each vulnerability, potential vulnerability and information gathered severity level are described below. The guidance below is followed for all vulnerabilities. In addition to this broad guidance the service also takes into consideration factors like complexity of the exploit and likelihood of the exploit to work under normal conditions. Network location and privileges needed by an attacker to execute a successful attack are considered. Prevalence of the affected software and existence of known attacks, worm or malware also plays a role.

Confirmed Vulnerabilities






A Confirmed Vulnerability is a design flaw or misconfiguration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a Confirmed Vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

Severity icon	Severity level	Description
	5 - Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security.
	4 - Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information.
	3 - Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders.
	2 - Medium	Intruders may be able to collect sensitive information from the host. With this type of information, intruders can easily exploit known vulnerabilities specific to software versions.
	1 - Minimal	Intruders can collection information about the host and may be able to use this information to find and exploit other vulnerabilities.

Potential Vulnerabilities




A Potential Vulnerability is a vulnerability that we cannot confirm exists. In these cases, at least one necessary condition for the vulnerability is detected. The only way to verify the existence of this type of vulnerability would be to perform an intrusive scan on your network, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate potential vulnerabilities further. The service can verify the existence of some potential vulnerabilities when trusted scanning is enabled.

IMPORTANT: When viewing scan results and some other reports in XML and CSV formats, the vulnerability type "potential" is identified as "practice". In this case the term "practice" (as a CSV column title or an XML element name) is identical in meaning to the vulnerability type "potential".


Severity icon	Severity level	Description
	5 - Urgent	If the vulnerability exists, intruders can easily gain control of the host, which can lead to the compromise of your entire network security.
	4 - Critical	If the vulnerability exists, intruders can possibly gain control of the host or there may be potential leakage of highly sensitive information.
	3 - Serious	If the vulnerability exists, intruders may be able to gain access to information stored on the host, including security settings. This could result in potential misuse of the host by intruders.
	2 - Medium	If the vulnerability exists, intruders may be able to collect sensitive information from the host. With this type of information, intruders can easily exploit known vulnerabilities.
	1 - Minimal	If the vulnerability exists, intruders can collect information about the host and may be able to use this information to find and exploit other vulnerabilities.

Information Gathered

Information Gathered is a vulnerability that includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered issues include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity icon	Severity level	Description
	3 - Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.
	2 - Medium	Intruders may be able to determine the operating system running on the host and view banner versions.
	1 - Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and firewalls.

Half Red / Half Yellow

Vulnerabilities assigned a Half Red / Half Yellow severity level (such as ) in the KnowledgeBase represent vulnerabilities that may be confirmed in some cases and not confirmed in other cases because of various factors affecting scan results. If the vulnerability is confirmed during a scan, it appears as a red vulnerability in the results. If it cannot be confirmed, it appears as a yellow potential vulnerability in the results. For example, without Windows Authentication enabled, there may not be enough information gathered to accurately identify the operating system on the target host, or detect installed fixes and patches. Thus, related vulnerabilities will go unconfirmed and appear as potential vulnerabilities in the results. When Windows Authentication is enabled, subsequent scans may result in more accurate detection and the same issues may be confirmed.

Additionally, scans may not result in enough information for confirming certain vulnerabilities due to the scan options applied to the scan, and the services running at the time of the scan.

Secureworks PCI Service (PCI)

The Secureworks® Payment Card Industry (PCI) Scanning Services (referred to herein as “PCI Scanning Services” consist of vulnerability scanning of PCI in-scope IP addresses, professional security review of Client submitted false positive exceptions, reports available via the PCI Portal, and attestation signing as specified by the PCI Security Standards Council.

Secureworks is a PCI Security Standards Council Approved Scanning Vendor (ASV), and delivers the Services in accordance with the PCI ASV Guidelines.

PCI Service Implementation Workflow

For service deployment of the PCI Service, the Secureworks Engineer assigned to the project will reach out to the client to request a kick off call. During this call, the relevant forms to collect needed information from the client will be discussed, along with the process for the implementation.

The client will need to supply the filled out forms for the deployment to continue. Once the forms have been returned, or if the client has any questions, a technical review call can be requested to discuss the forms or any other technical questions regarding the service that is being deployed.

Once the forms have been completed and returned, the Secureworks Engineer will proceed with getting the service deployed and handed over to the VMS Engineering team for ongoing service delivery and support.

PCI SAP Forms



Information
Gathering SAP (002).



PCI Subscription
Setup Request.docx



SIF PCI.xlsx

This is an outline of the deployment process and related documentation:

Staging	Kickoff	Implementation
Order Received		
Project assigned	SIF created SAPs selected	
		PCI Subscription Setup Request Information Gathering SAP
Begin Initial Process	Contact client Request Kickoff Call	
During Kickoff Call	Review Contracts Discuss Process Provide SIF and SAPs	

Staging	Kickoff	Implementation
	Provide Implementation Requirements Discuss Action Items and Next Steps Schedule Technical Review Call Outline project plan	
Client action items	Complete SIF and SAPs Return to PM assigned	
Technical Review Call	Review the SIF and SAPs	
		Confirm IP('s) information Confirm IP's for scanning Review Users and associated role level
	Confirm project plan status	
Populate Qualys Portal	Users permitted access per SAP IP information imported per SAP	
Qualys Welcome Guide distributed		
Service Activation and Project Closure		

Accessing the Qualys PCI Portal

To access your PCI portal, there are two options:

Option 1 - Access PCI Portal Directly

1. Navigate to [Secureworks PCI Portal](#).
2. Enter your username and password. (If you do not remember your username or password, [contact](#) the VMS team for a password reset.)

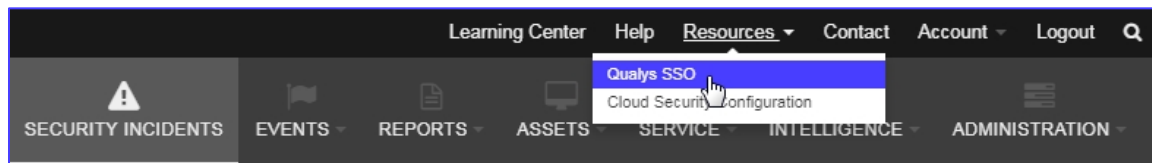
Upon successfully entering your username and password, you will be logged in to the PCI portal.

Option 2 - Access PCI Portal from within your Qualys Subscription

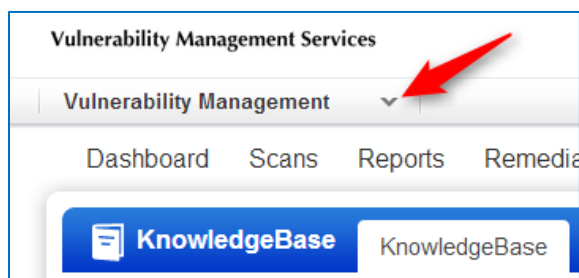
If you have not done so already, navigate to the section titled [Linking your PCI Subscription to your Qualys Subscription](#).

If you have configured your Qualys subscription to link to your PCI subscription, do the following:

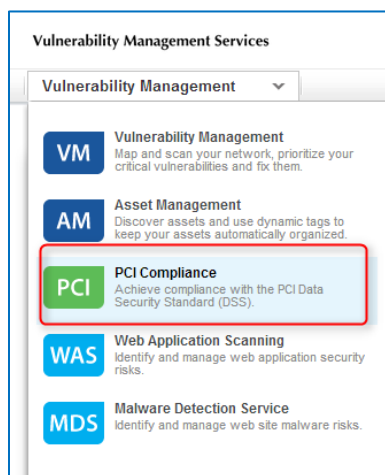
1. Navigate to the Secureworks [Client Portal](#).
2. From the **Resources** menu option, select **QUALYS SSO**.



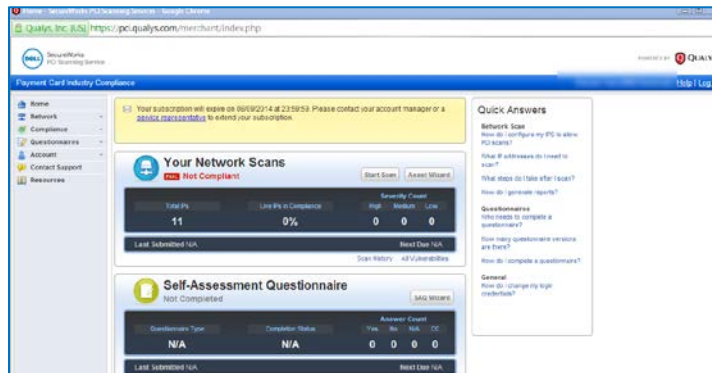
3. The **Qualys SSO Subscription** dialog displays. Select the desired subscription from the dropdown menu and click **SUBMIT**.
4. A new browser tab opens and displays your subscription.
5. Click the Vulnerability Management drop down arrow.



6. Select PCI Compliance from the drop down.



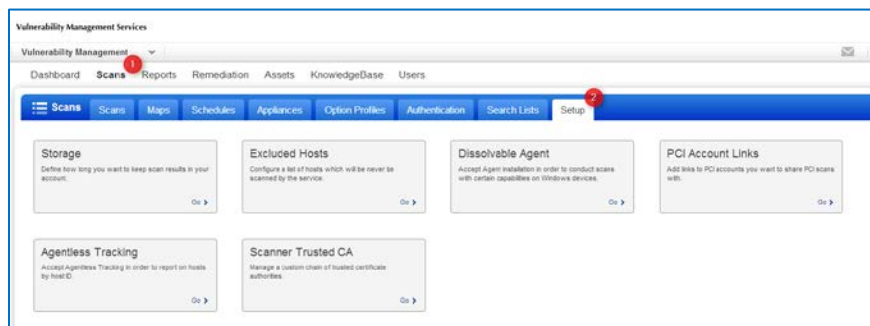
7. You are automatically logged in to the PCI portal.



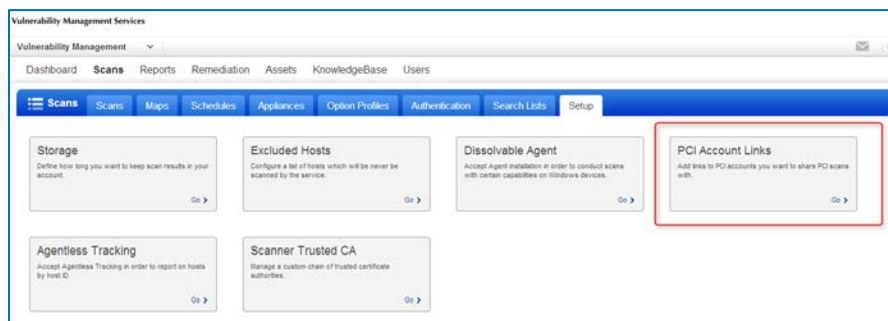
Linking PCI Subscription and Qualys Subscription

Qualys provides you the ability to link your PCI Subscription and your Qualys subscription to easily log in to your PCI portal and to share PCI specific scans conducted in Qualys with the PCI portal to meet PCI goals.

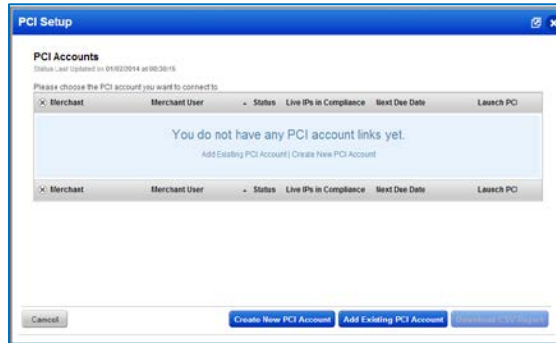
1. From within your Qualys subscription, click on **SCANS → SETUP**.



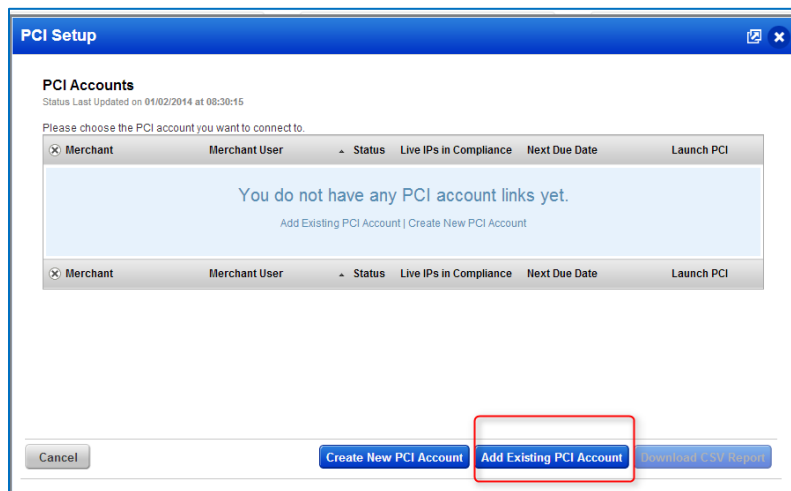
2. Click on the **PCI ACCOUNT LINKS** option.



The **PCI Setup** screen displays.



- Click the **ADD EXISTING PCI ACCOUNT** button.



- Enter your user login and password that you use to access the PCI portal.

- Click **SAVE**.

Getting Started Guide for PCI

Please visit the below link for helpful information on the Secureworks/Qualys PCI portal.

The Getting Started Guide will take you through the PCI portal and walk you through adding assets, launching scans, viewing scan results, creating reports, submitting false positives ,and additional options. Click here: [PCI Getting Started Guide](#)

SLAs for PCI Services

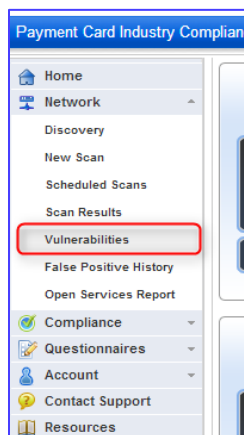
The Secureworks VMS team has a few SLAs in place for the PCI Service.

- › Scheduling Scans and re-scans: There is a three (3) business day SLA to process scan requests and re-scan requests.
- › False Positive Requests: There is a five (5) business day SLA for the VMS team to accept/reject or request additional evidence/information on false positive requests.
- › Attestation Requests: There is a two (2) business day SLA for the VMS team to accept/reject attestation signing requests.

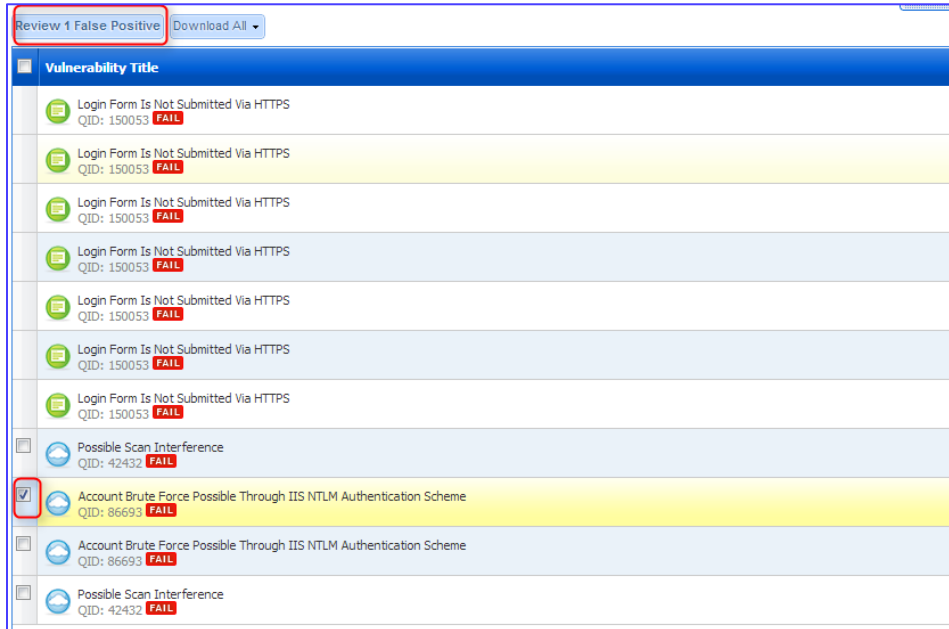
False Positive Submission

The Secureworks VMS Team is an Approved Scanning Vendor (ASV) and as such, can process false positive requests. All False Positive Submissions must be submitted from within the Qualys PCI Portal using the built in workflow for submitting false positive requests. False Positive requests and evidence must be submitted by the Client by following the below process:

1. Access the Qualys PCI Portal.
2. Select **NETWORK** → **VULNERABILITIES** from the left side of the screen



3. Select the checkbox next to the vulnerability/vulnerabilities for which you wish to submit false positives.
4. Click the **REVIEW FALSE POSITIVES** button at the top.



5. Enter in any supporting evidence that you can within the text boxes in the next screen.
 - o Additional supporting evidence, such as screenshots, can be supplied to the Secureworks VMS team by creating a Service Request in the Secureworks Client Portal or emailing vms-support@secureworks.com with the following information:
 - IP Address of the host you are submitting evidence for
 - QID of the vulnerability you are submitting evidence for
 - Supporting evidence
6. Click the **SUBMIT FALSE POSITIVE REQUEST** button.
7. The Secureworks VMS team will process the request and reach out to the requestor if additional information is needed.

Attestation Submission

The Secureworks VMS Team is an Approved Scanning Vendor (ASV) and as such, can process the signing of Attestation Requests. All Attestation Signing Requests must be submitted from within the Qualys PCI Portal using the built in workflow for submitting false positive requests. Attestation requests must be submitted by the Client by following the below process:

1. Access the Qualys PCI Portal.
2. Select **COMPLIANCE** → **COMPLIANCE** Status from the left side of the screen.
3. Select the **GENERATE** button to bring up the Report Generation Wizard.



Classification: //SecureWorks/Confidential - Limited External Distribution:

4. Click **NEXT** on the Report Generation Wizard to move through submitting the report.
5. You may see some vulnerabilities appear and the wizard asking if they are securely implemented. You will need to supply an answer for each IP and vulnerability identified here. Once you are done, click **NEXT**

Report Generation Wizard

Special Notes

Special Notes identify the presence of certain software that may pose a risk to your environment due to insecure implementation rather than an exploitable vulnerability. This software may include remote access software and point-of-sale (POS) software.

All of the issues that require Special Notes are listed below. Please provide appropriate information for each.

Enter a single comment for all issues

IP/Hostname	Issue	Securely Implemented?
150004	150004 - Path-Based Vulnerability	<input type="radio"/> Yes <input type="radio"/> No
150004	150004 - Path-Based Vulnerability	<input type="radio"/> Yes <input type="radio"/> No
150004	150004 - Path-Based Vulnerability	<input type="radio"/> Yes <input type="radio"/> No
150004	150004 - Path-Based Vulnerability	<input type="radio"/> Yes <input type="radio"/> No
150004	150004 - Path-Based Vulnerability	<input type="radio"/> Yes <input type="radio"/> No
150004	150004 - Path-Based Vulnerability	<input type="radio"/> Yes <input type="radio"/> No

Cancel

Previous

Next

6. On the next screen, enter your name and job title and click **NEXT**
7. Enter a title for the reports and click **NEXT**
8. Click the **GENERATE REPORT** button. The Report Generation Wizard will create a PCI Executive Report and a PCI Technical Report.
9. You will now need to 'Request Review' of the reports which will send the reports to the Secureworks VMS Team to review. At this point, the reports will have a watermark indicating that they are "Not Official PCI Reports."
10. Once the Secureworks VMS Team attests to the reports, the watermark will be removed and you can proceed with supplying the reports to your acquiring banks.







Secureworks Policy Compliance (PC) Service

For details on working with the Qualys Policy Compliance Module, visit the below link to access the “Policy Compliance Getting Started Guide.” This guide will walk you through adding IPs for PC, Configuring Scan Options, Configuring Authentication, Scanning, Building a Policy, Checking Compliance Status and Running Reports, etc.

[Policy Compliance Getting Started Guide](#)

Authentication is required for the Policy Compliance Service. We are providing the documentation for you here so that you will have all of the requirements needed.

REFERENCE DOCUMENTS

 qualys-authenticated -scanning-windows-u;	 qualys-authenticated -scanning-windows.p	 qualys-authenticated -scanning-unix.pdf
 qualys-authenticated -scanning-ms-sql-serv	 qualys-authenticated -scanning-db2.pdf	 qualys-authenticated -scanning-oracle-pc.z

Secureworks Continuous Monitoring (CM) Service

For details on working with the Qualys Continuous Monitoring Module, visit the below link to access the “Continuous Monitoring Community Site.” This site will provide you with resources and information for using Continuous Monitoring.

[Continuous Monitoring Community Site](#)

Secureworks ThreatPROTECT Service

For details on working with the Qualys ThreatPROTECT Module, visit the below links to access the Qualys documentation on ThreatPROTECT. These links will provide you with information on the module and how it can be leveraged in your subscription.

- › [ThreatPROTECT Datasheet](#)
- › [Introduction to Qualys ThreatPROTECT](#)

Secureworks Cloud Agent Service

For details on working with the Qualys Cloud Agent, visit the below link to access the “Cloud Agent Community Site.” This site will provide you with resources and information for using Cloud Agent. Additionally, the introduction video and Getting Started guide will walk you through your first steps of using the module.

- > [Cloud Agent Community Site](#)
- > [Cloud Agent Introduction](#)
- > [Cloud Agent Getting Started Guide](#)
- > [Cloud Agent Installation Guide \(Windows\)](#)
- > [Cloud Agent Installation Guide \(Linux\)](#)
- > [Cloud Agent Installation Guide \(Mac\)](#)



qualys-cloud-agent
-unix-install-guide.pdf

Secureworks Web Application Scanning Service

Web application scanning analyzes the security of your network using the largest and most up to date Knowledgebase of vulnerability checks. When you launch web application scans, the service detects vulnerabilities using an adaptive process that runs only tests applicable to each host scanned.

WAS Service Implementation Workflow

For service deployment of the Web Application Scanning Service, the Secureworks Engineer assigned to the project will reach out to the client to request a kick off call. During this call, the relevant forms to collect needed information from the client will be discussed, along with the process for the implementation.

The client will need to supply the filled out forms for the deployment to continue. Once the forms have been returned, or if the client has any questions, a technical review call can be requested to discuss the forms or any other technical questions regarding the service that is being deployed.

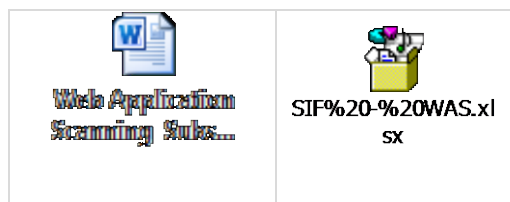
Once the forms have been completed and returned, the Secureworks Engineer will proceed with getting the service deployed and handed over to the VMS Engineering team for ongoing service delivery and support.

This is an outline of the deployment process and related documentation:

Staging	Kickoff	Implementation
Order Received		
Project assigned	SIF created SAPs selected	
		Web Application Scanning Subscription (per WAS app) Information Gathering SAP
Begin Initial Process	Contact client Request Kickoff Call	
During Kickoff Call	Review Contracts Discuss Process Provide SIF and SAPs Provide Implementation Requirements Discuss Action Items and Next Steps Schedule Technical Review Call Outline project plan	
Client action items	Complete SIF and SAPs	

Staging	Kickoff	Implementation
	Return to PM assigned	
Technical Review Call	Review the SIF and SAPs	
		Confirm IP('s) information Confirm IP's for scanning Review Users and associated role level
	Confirm project plan status	
Populate Qualys Portal	Users permitted access per SAP IP information imported per SAP	
Qualys Welcome Guide distributed		
Service Activation and Project Closure		

WAS SAP Forms



Web Applications

A web application is a user-defined configuration that identifies a scan target—the web application that you want to test for security vulnerabilities. A starting URL is required. Optionally, you can specify; credentials to be used for authenticated scanning, black and white lists to define areas not to be scanned, settings to observe Robots.txt and Sitemap.xml, and to use header injection.

Web Application Scanning

Web Crawling and Link Discovery: The service requests links and forms, parses HTML for parameter analysis and form values, and interacts with the web application (see below). It also extracts JavaScript based links and has the capability to find custom links.

Data Analysis: The service performs static, off-line analysis of HTTP headers, HTML content and other responses from the web application.

Vulnerability Testing: The service performs dynamic, on-line analysis of the web application. Vulnerability testing is not performed for a discovery scan.

Web Crawling and Link Discovery

During a web application scan, the scanning engine monitors the target web application server's response time. This occurs during the entire web application scan, including web crawling and link discovery, and vulnerability testing. If the scanning engine detects a trend showing the average response time from the target web application is becoming slower (scan time is increasing), the scanning engine automatically inserts a delay until the trend is normal.

The web crawler crawls all domains and sub-domains it finds starting from the URI defined in the web application configuration, parsing HTML and extracting links it finds. By default the web crawler will crawl all domains and sub-domains from the starting URI. In the web application configuration, the scope of the scanning may be changed to one of these options: limit crawling to the starting URI and its sub-directories, crawl only sub-domains, or crawl specified domains.

Following links: The web crawler automatically balances the web site crawling to follow links down the web site branch (number of clicks) and across the branch (links at the same level), and tracks unique links that have already been crawled. This enables the crawler to obtain a high degree of site coverage while avoiding the re-scanning of redundant and recursive links. The list of links crawled is identified by QID 150009 Links Crawled.

Maximum number of links to crawl: The web crawler crawls up to 5,000 links per web application. The number of links includes form submission, links requested as an anonymous user and links requested as an authenticated user. The user may configure this setting.

External links: Any external links and external form actions that are found to be present for a web application are not crawled. We use the term "external" to refer to links discovered on a host (FQDN or IP address) which is not the virtual host (starting host) or domain added for multi-site support. External links not crawled are identified as information gathered by QID 150010 External Links Discovered and QID 150014 External Form Actions Discovered.

Black List/White List: Important! Automated web application scanning has the potential of causing data loss. The black list feature allows you to prevent the web crawler from making certain requests for certain links in your web application.

Vulnerability Testing

The WAS scanning engine uses a well-known methodology called "*True and False*" inference to determine if there is a blind SQL injection vulnerability. Basically, it uses two payloads: one with a "*True condition*" and another with a "*False condition*". If there is a blind SQL injection vulnerability, the query with the "True condition" payload will cause the web application to return a different response than the "False condition".

A good example of a "True condition" payload would be ' AND 1=1. Since 1 always equals 1, the condition is true. An example of a "False condition" payload would be ' AND 1=2. Since 1 does not equal 2, the condition is false.

For example, let's say there is a web application with a textbox that searches for client names and displays the results inside a table. And let's assume that if someone searches for John there is one result only. When scanning for the blind SQL injection vulnerability, the WAS scanning engine uses two payloads.

- **True condition payload:** This injects the string John' AND 1=1 to issue the query "*return John only if 1=1*". Since 1 always equals 1 the condition is true. The result is John, which is the same result as using the string John.

- **False condition payload:** This injects the string John' AND 1=2 to issue the query "*return John only if 1=2*". Since 1 is never equal to 2, the condition is false. The result is nothing or "No results found".

With the results from the two payloads, the WAS scanning engine draws the conclusion that there is a blind SQL injection vulnerability. Even though there is no one called "*John' AND 1=1*" in the database the web application displays the information for "John" if a search is done with that query string.

Example:

These few lines demonstrate an insecure query that is created by appending the user-supplied data (name):

```
On Error Resume Next ' Page traps error and do not display it
Set oRSu = oCONv.Execute("SELECT fname, name FROM customers WHERE name = '" &
Request("txtSearch") & "'")
If oRSu.BOF Or Err.Number <> 0 Then
Response.Write "No results found!"
End If
```

Classification: //SecureWorks/Confidential - Limited External Distribution:

If no checks are performed against the name parameter, then the query may be arbitrarily modified and sent to the database as shown in these two examples of a completed query:

```
SELECT fname, name FROM customers WHERE name='<B>John' AND 1=1</B>
SELECT fname, name FROM customers WHERE name= 'John'; SHUTDOWN WITH NOWAIT
```

In the first case the database will return "John" since the condition AND 1=1 is always true.

Impact: The scope of a SQL injection exploit varies greatly. If any SQL statement can be injected into the query, then the attacker has the equivalent access of a database administrator. This access could lead to theft of data, malicious corruption of data, or deletion of data.

Solution: SQL injection vulnerabilities can be addressed in three areas: input validation, query creation, and database security.

All input received from the web client should be validated for correct content. If a value's type or content range is known beforehand, then stricter filters should be applied. For example, an email address should be in a specific format and only contain characters that make it a valid address; or numeric fields like a USA zip code should be limited to five digit values.

Prepared statements (sometimes referred to as parameterized statements) provide strong protection from SQL injection. Prepared statements are precompiled SQL queries whose parameters can be modified when the query is executed. Prepared statements enforce the logic of the query and will fail if the query cannot be compiled correctly. Programming languages that support prepared statements provide specific functions for creating queries. These functions are more secure than string concatenation for assigning user-supplied data to a query.

Stored procedures are precompiled queries that reside in the database. Like prepared statements, they also enforce separation of query data and logic. SQL statements that call stored procedures should not be created via string concatenation; otherwise their security benefits are negated.

SQL injection exploits can be mitigated by the use of Access Control Lists or role-based access within the database. For example, a read-only account would prevent an attacker from modifying data, but would not prevent the user from viewing unauthorized data. Table and row-based access controls potentially minimize the scope of a compromise, but they do not prevent exploits.

Example of a secure query created with a prepared statement:

```
PreparedStatement ps = "SELECT name,email FROM users WHERE userid=?"; ps.setInt(1, userid);
```

Testing: The first step in this test is to understand when our application connects to a DB Server in order to access some data. Typical examples of cases when an application needs to talk to a DB include:

- › Authentication forms: when authentication is performed using a web form, chances are that the user credentials are checked against a database that contains all usernames and passwords (or, better, password hashes).
- › Search engines: the string submitted by the user could be used in a SQL query that extracts all relevant records from a database.
- › E-Commerce sites: the products and their characteristics (price, description, availability, ...) are very likely to be stored in a relational database.

The tester has to make a list of all input fields whose values could be used in crafting a SQL query, including the hidden fields of POST requests and then test them separately, trying to interfere with the query and to generate an error. The very first test usually consists of adding a single quote (') or a semicolon (;) to the field under test. The first is used in SQL as a string terminator and, if not filtered by the application, would lead to an incorrect query. The second is used to end a SQL statement and, if it is not filtered, it is also likely to generate an error. The output of a vulnerable field might resemble the following (on a Microsoft SQL Server, in this case):

```
Microsoft OLE DB Provider for ODBC Drivers error '80040e14'
[Microsoft][ODBC SQL Server Driver][SQL Server]Unclosed quotation mark before the
character string ''.
/target/target.asp, line 113
```

Also comments (--) and other SQL keywords like 'AND' and 'OR' can be used to try to modify the query. A very simple but sometimes still effective technique is simply to insert a string where a number is expected, as an error like the following might be generated:

```
Microsoft OLE DB Provider for ODBC Drivers error '80040e07'  
[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the  
varchar value 'test' to a column of data type int.  
/target/target.asp, line 113
```

A full error message, like those in the examples, provides a wealth of information to the tester in order to mount a successful injection. However, applications often do not provide so much detail: a simple '500 Server Error' or a custom error page might be issued, meaning that we need to use blind injection techniques. In any case, it is very important to test *each field separately*: only one variable must vary while all the others remain constant, in order to precisely understand which parameters are vulnerable and which are not.

Creating Web Applications

To have the Secureworks VMS Team create a Web Application, do the following:

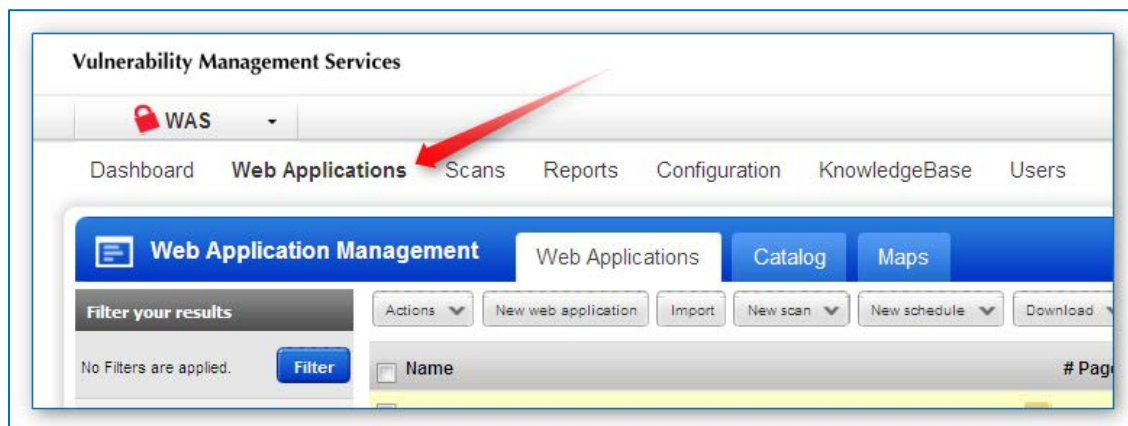
1. Fill out the Web Application Scanning Subscription Form.
2. Submit the completed SAP form to the Secureworks VMS Team either by emailing it to vms-support@secureworks.com or by creating a Service Request on the [Secureworks Client Portal](#) and attaching the forms.

The VMS team will process the request within three (3) business days or reach out to the requestor if clarifications are needed. If clarifications are needed and the VMS team is unable to get a response back from the requestor, the request will not be processed until the clarifications are received.

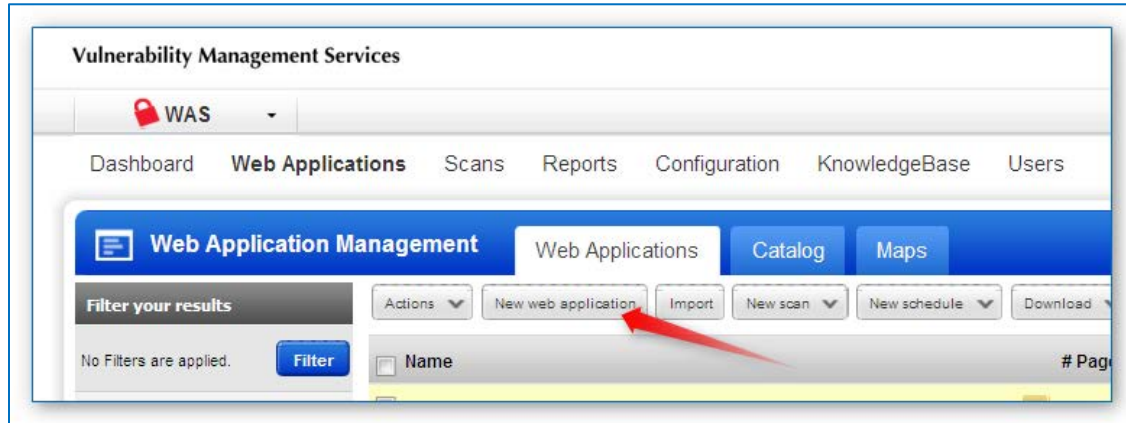
Self-Serve Option

To create a web application, do the following:

1. Click the **WEB APPLICATIONS** dashboard.



2. Click **NEW WEB APPLICATION**.



3. The Web Application Creation wizard displays. Fill in the following information:
 - Basic Information: Enter a unique name for this web application. It should be easy to remember and descriptive of the web application. You can also enter business information that can help you categorize your web applications as well as a comments field. Once complete press Continue.
 - Configuration: Enter the web application URL, target scope and default configuration.
 - Authentication: Create an authentication record which will allow the scanner to authenticate to the target web application. If you click on Add Record this will open the "Web Application Authentication Record Creation" wizard.
 - Black & White Lists: You may enter either URLs or regular expression pattern matches to either prevent URLs from being scanned or to have links scanned even if a black list would normally block a URL.
 - Advanced Settings: On this screen you can enter some details about how your web application should be scanned, such as using robots.txt, enforcing those directives and custom header injection.
 - Tags: Tags assigned to a web application will allow users with the same tag(s) to see them.
 - Review and Confirm: This screen will show you an overview of the web application as you just created it. If everything looks good, click **FINISH**.

Web Application Option Profiles

When launching or scheduling a web application scan, you'll be required to apply an option profile to the task. Option profile settings configure crawling, sensitive content detection, vulnerability detection and password brute forcing.

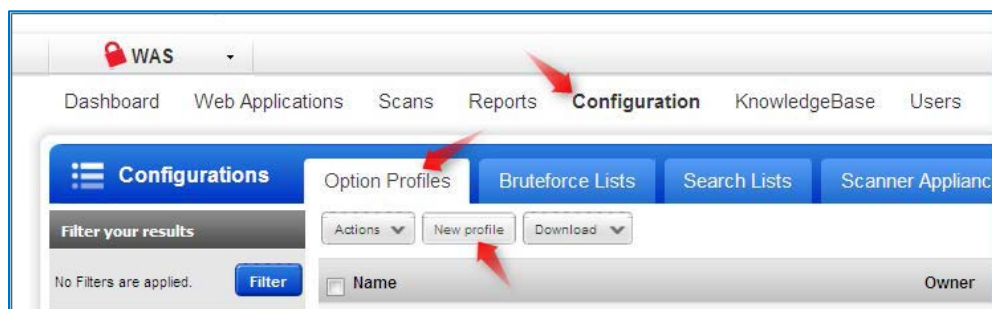
Web Application Option Profiles provided by the service:

Initial WAS Options: The Initial Options profile is initially set as the default profile for web application scans. The default profile is intended for global use to ensure compliance with corporate security policies.

Creating Web Application Option Profiles

To create an Option Profile, do the following:

1. Click on **CONFIGURATION** dashboard.
2. Click the **OPTION PROFILES** tab.
3. Click **NEW PROFILE**.



4. Enter a title for the profile and click **CONTINUE**.
5. Select what type of forms you want to submit, maximum number links to crawl and adjust the performance slider to meet your needs and click **CONTINUE**.
6. Select either complete vulnerability detection or a custom set and click **CONTINUE**.
7. Select which sensitive content you also want to look for, if any and click **CONTINUE**.
8. Enable or disable password brute forcing and configure how aggressive it should behave and click **CONTINUE**.
9. Assign tag(s) as necessary and click **CONTINUE**.
10. Review your settings and press Finish.

Web Application Search Lists

Search lists are custom lists of vulnerabilities that you can apply to a web application profile. You can create both static lists and dynamic lists.

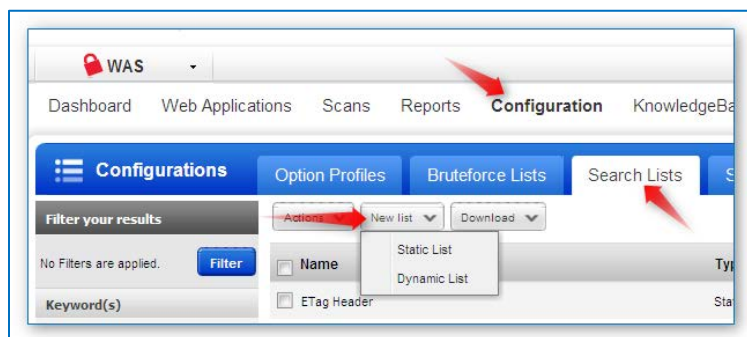
Static Search Lists: A static search list includes a list of vulnerabilities (QIDs) that you select.

Dynamic Search Lists: When a dynamic search list is used, the service queries the Knowledgebase to find all QIDs that currently match the search criteria and then includes those QIDs in the action. Dynamic search lists are updated automatically by the service as new QIDs are added to the Knowledgebase and new patch information becomes available.

Creating Web Application Search Lists

To create a search list, do the following:

1. Select **CONFIGURATION** to go to the Configurations section.
2. Click the **SEARCH LISTS** tab.



3. Click **NEW LIST** and choose which type of list you want to create.

For a Static List do the following:	For a Dynamic List, do the following:
<ol style="list-style-type: none"> 1. Enter in a title for the search list and/or comments and press Continue. 2. If you already know the QID(s) press Add and enter them otherwise press Select. 3. Use the search box to find the vulnerability or use the Advanced Search button for more detailed search. 4. Click the OK button to add the QID(s) to the list. 5. Press Continue. 6. Add any tags to this list and press Continue. 7. Review the list and make sure it's correct and press Finish. 	<ol style="list-style-type: none"> 1. Enter in a title and/or comments for the search list. 2. Filter the selection for the list based on the criteria listed and press Continue. 3. Add any tags to the list and press Continue. 4. Review and confirm everything is correct and press Finish.

Scanning Web Applications

You can launch scans on web applications using the launch scan and schedule scan wizards.

To have the Secureworks VMS Team schedule a web application scan to run at a specific date and time, do the following:

Send a request to the Secureworks VMS Team either by emailing it to vms-support@secureworks.com or by creating a Service Request on the [Secureworks Client Portal](#) with the following information:

- › Scan Title (must be unique)
- › Web Application Name (as it is displayed in the Qualys portal)
- › Requested Scan Start Date/Time/Time Zone
- › Authentication Record
- › Option Profile
- › Scanner Appliance
- › Duration for the scan

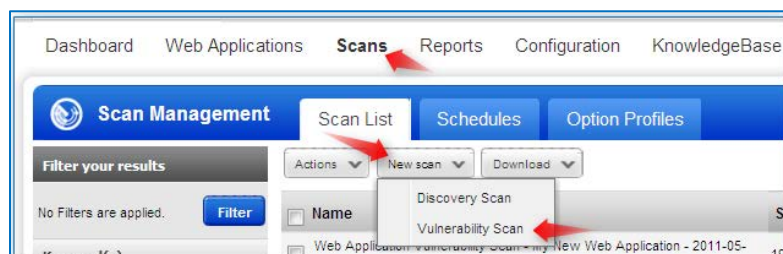
The VMS team will process the request within three (3) business days or reach out to the requestor if clarifications are needed. If clarifications are needed and the VMS team is unable to get a response back from the requestor, the request will not be processed until the clarifications are received.

Self-Serve Option

To launch a scan, do the following:

(Please note the scan will be launched at the time you complete the task).

1. Click the **SCANS** dashboard, **SCAN LIST** tab, and then **NEW SCAN**. Choose **VULNERABILITY** Scan.

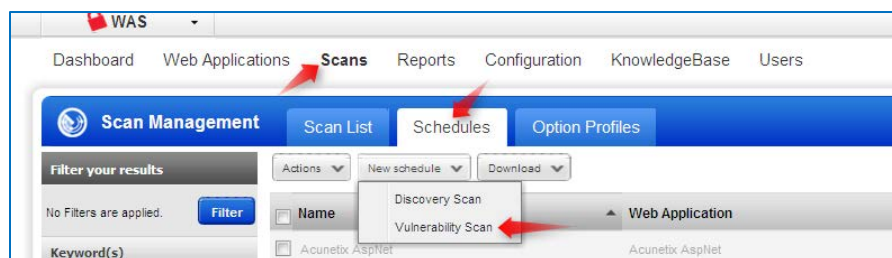


2. Fill in the following information:
 - Scan name: Provide a title for the scan. The title cannot be in use by another scan task.
 - Web Application: Select an web application you've already created.
 - Authentication Record: Select the record you want to use for this web application
 - Option Profile: Select which options profile you want you use. If you have not created one, use the "Initial WAS Options."
 - Scanner Appliance: Select a scanner option to apply to this scan task.
3. Click **CONTINUE**.
4. Review and confirm the settings are correct and click **FINISH**.

Self-Serve Option

To Schedule a Scan to launch at a future time, do the following:

1. Click the **SCANS** dashboard, **SCHEDULES** tab, and **NEW SCHEDULE**.



2. Fill in the following information on the Basic Information section:
 - Scan name: Provide a title for the scan. The title cannot be in use by another scan task.
 - Web Application: Select an web application you've already created.
 - Authentication Record: Select the record you want to use for this web application.
 - Option Profile: Select which options profile you want you use. If you have not created one, use the "Initial WAS Options."
 - Scanner Appliance: Select a scanner option to apply to this scan task.
3. Fill in the following information on the **SCHEDULING** tab:
 - Start Date: Fill in the start date when you want the scan to execute.
 - Time: Fill in the time when you want the scan to execute.
 - Time zone: Select from the pull down which time zone you want to use.

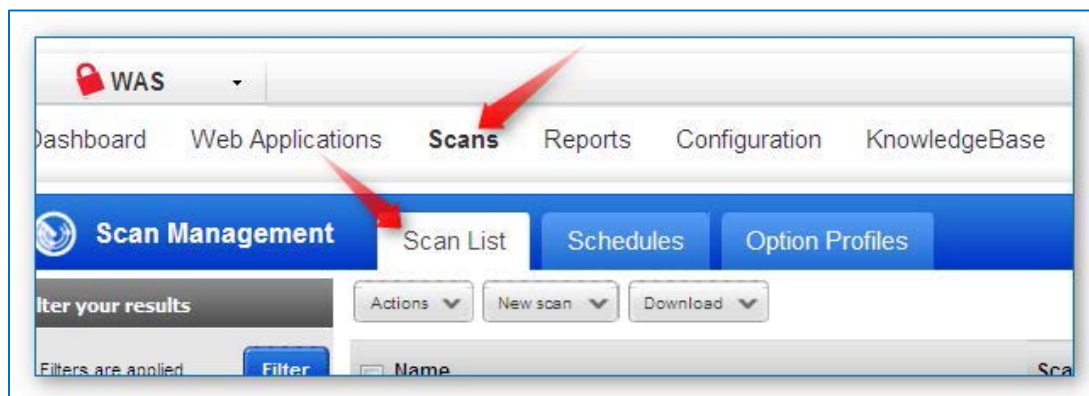
Classification: //SecureWorks/Confidential - Limited External Distribution:

- Duration: Select if you want the scan to cancel after a set number of hours.
 - Mode: If you would like the scan to recur on a regular basis, select either Daily, weekly or monthly. Once you have selected, the options will change.
4. Fill in the following information on the **NOTIFICATION** tab if you want to be notified when the scan is starting:
- Activate Notification: This enables notifications.
 - Notification Timing: Select if you'd like to know Day(s), Hour(s), or Minute(s) before the scan executes and specify an integer value.
 - Email addresses: These will be additional email address you want to notify. If you leave this blank, it will only notify the schedule owner's email listed in their account.
 - Custom Message: Enter whatever message you'd like to send here.
5. Review and Confirm the settings are correct and then click **FINISH**

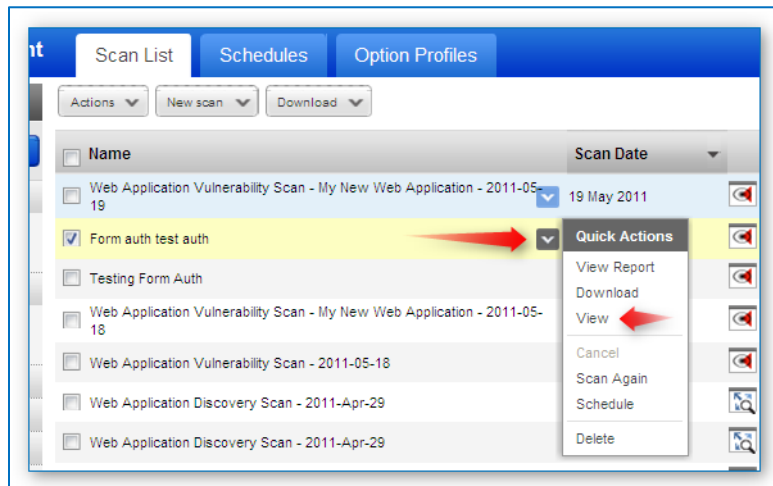
Retrieving Web Application Scan Results

Within the Qualys WAS tool, you can view the results for your scans by doing the following:

1. Click the **SCAN** dashboard.
2. Click the **SCAN LIST** tab. You will see the list of scans you have run and their Status.
3. Click on the scan you want to view the results and click on the down arrow icon to open the quick actions menu.



4. Select **VIEW**.



In Addition to viewing the scan results, you also have the option to produce customized reports based on the scan results.

Web Application Reports

Web Application Report: The Web Application Report identifies vulnerabilities and sensitive content detected by the most recent scan of a selected web application.

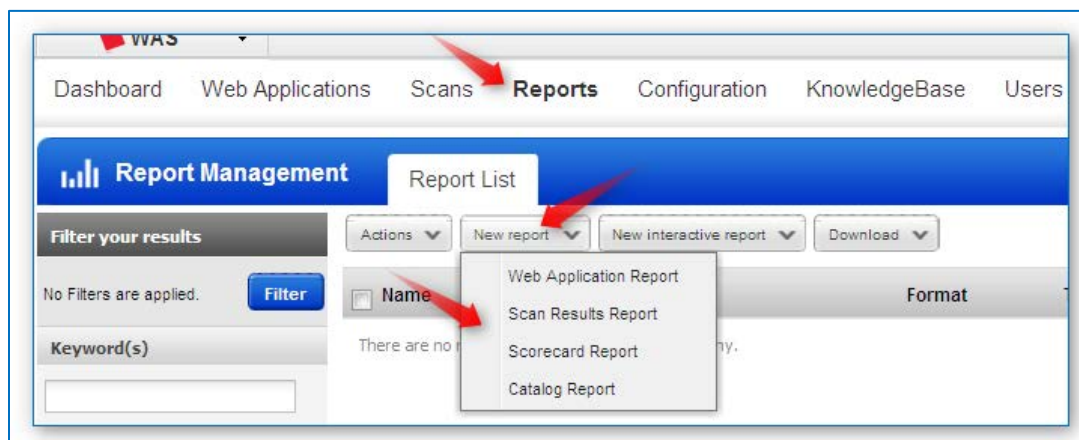
Scan Results Report: The Scan Results Report identifies vulnerabilities and sensitive content detected by a web application scan. You select a particular scan task to report on.

Scorecard Report: The Scorecard Report is provided by the service for reporting on web application scan data for different business groups and functions. A scorecard report identifies the vulnerabilities and sensitive contents detected for one or more target web applications. The scorecard report includes the most recent scan data for the target web applications.

Catalog Report: The Catalog Report provides a listing of catalog entries added within a time period that you specify. You can run the report for all catalog entries or for entries with a specific status. You have the option to sort the report by IP Address, Port, NetBIOS name, Status and FQDN.

Creating Reports

1. Click the **REPORTS** dashboard.
2. Click **NEW REPORT** and select which report you want to create.
3. The wizard launches to guide you through the creation of the selected report.



Classification: //SecureWorks/Confidential - Limited External Distribution:







Getting Started Guide for WAS

Please visit the below link for helpful information on the Secureworks/Qualys WAS portal. The Getting Started Guide will take you through the WAS portal and walk you through configuring web applications, scheduling scans, and generating reports.






[WAS Getting Started Guide](#)

Appendix A – Authenticated Scanning Guides

Policy Compliance Authenticated Scanning Guides

 qualys-authenticated -scanning-windows-u.	 qualys-authenticated -scanning-windows.p	 qualys-authenticated -scanning-unix.pdf
 qualys-authenticated -scanning-ms-sql-ser	 qualys-authenticated -scanning-db2.pdf	 qualys-authenticated -scanning-oracle-pc.z

Vulnerability Scanning Authenticated Scanning Guides

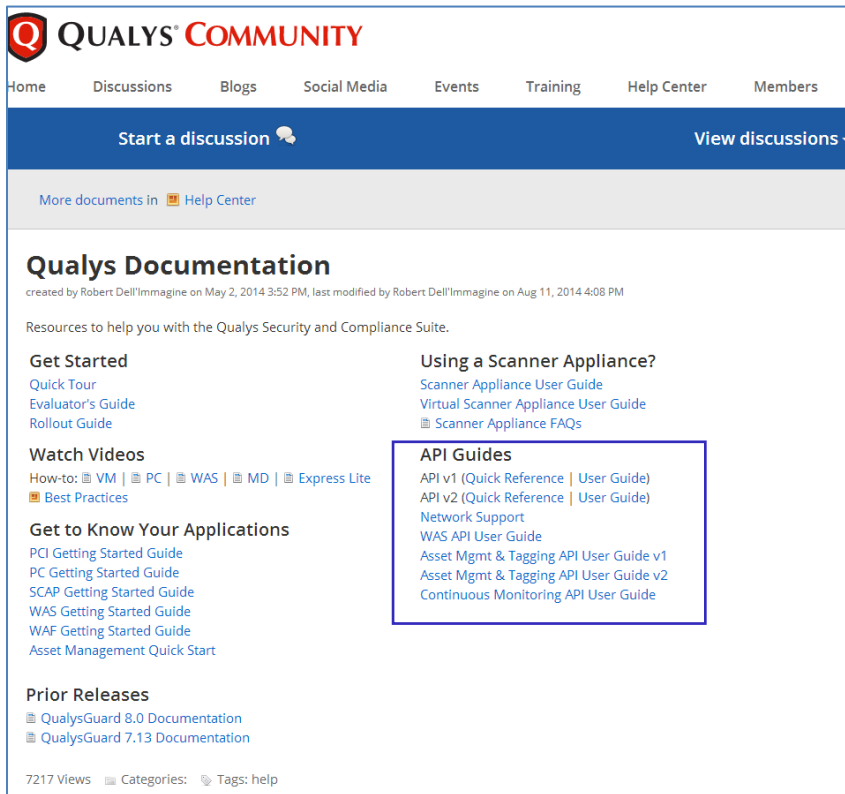
 qualys-authenticated -scanning-windows-u.	 qualys-authenticated -scanning-windows (2	 qualys-authenticated -scanning-unix (2).pd
 qualys-authenticated -scanning-oracle-vm.:	 qualys-authenticated -scanning-db2 (2).pdf	

Appendix B - API Guides

Qualys provides several API Guides that can be referenced in the event you wish to utilize the API functionality.

The following link will bring you to the Qualys Documentation page and the various API Guides can be accessed from here.

<https://community.qualys.com/docs/DOC-4802>



QUALYS® COMMUNITY

Home Discussions Blogs Social Media Events Training Help Center Members

Start a discussion View discussions -

More documents in Help Center

Qualys Documentation

created by Robert Dell'Imagine on May 2, 2014 3:52 PM, last modified by Robert Dell'Imagine on Aug 11, 2014 4:08 PM

Resources to help you with the Qualys Security and Compliance Suite.

- Get Started**
 - Quick Tour
 - Evaluator's Guide
 - Rollout Guide
- Watch Videos**
 - How-to: VM | PC | WAS | MD | Express Lite
 - Best Practices
- Get to Know Your Applications**
 - PCI Getting Started Guide
 - PC Getting Started Guide
 - SCAP Getting Started Guide
 - WAS Getting Started Guide
 - WAF Getting Started Guide
 - Asset Management Quick Start
- Prior Releases**
 - QualysGuard 8.0 Documentation
 - QualysGuard 7.13 Documentation

- Using a Scanner Appliance?**
 - Scanner Appliance User Guide
 - Virtual Scanner Appliance User Guide
 - Scanner Appliance FAQs
- API Guides**
 - API v1 (Quick Reference | User Guide)
 - API v2 (Quick Reference | User Guide)
 - Network Support
 - WAS API User Guide
 - Asset Mgmt & Tagging API User Guide v1
 - Asset Mgmt & Tagging API User Guide v2
 - Continuous Monitoring API User Guide

7217 Views Categories: Tags: help

Appendix C – Qualys “How to” videos

Qualys provides several short videos to get you started using the Qualys Suite of products.

Qualys Vulnerability Management Video Series

The below link will take you to the Qualys VM Video Series page. Here you will find videos on topics that include Scans, Reports, Remediation, and Assets.

[Qualys Vulnerability Management Video Series](#)

Qualys Web Application Scanning Video Series

The below link will take you to the Qualys WAS Video Series page. Here you will find videos on topics that include Creating Web Applications, Discovery and Cataloging, Scanning, Reporting, New Features, Selenium Introduction, and Selenium Setup and Use.

[Qualys Web Application Scanning Video Series](#)

Qualys Policy Compliance Video Series

The below link will take you to the Qualys PC Video Series page. Here you will find videos on topics that include Trusted Scanning, Creating Policies, Reporting, Dashboard, and Policy Import and Export.

[Qualys Policy Compliance Video Series](#)

Appendix D – Secureworks VMS Service Descriptions

Here are the various Secureworks Vulnerability Management Service Descriptions. These Service Descriptions outline the service that the Secureworks VMS team provides for each service.

Service Descriptions

 Vulnerability Management Service	 Vulnerability Management and Pr
--	---