

# Vulnerability Management Services (VMS) Welcome Guide

Last Updated: April 2020

## Copyright

Copyright 2007-2020. 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.

Table of Contents

**Document Information.....4**  
Document History .....4  
Documentation Update Requests.....4  
Contact Us .....4  
**Welcome to Secureworks VMS.....5**  
Accessing your VMS Subscription.....5  
VMS Welcome Kit.....6  
Included Documents .....7  
Submitting Completed SAP Forms .....7  
**VMS Service Level Tiers.....8**  
Secureworks Co-Managed VMS .....8  
Platinum Tier (Program Managed VMS) .....9  
**Getting Started .....10**  
Healthy Start.....10  
Map Scans.....10  
Vulnerability Scans .....10  
Scanner Appliance Heartbeat Check Notification .....10

## Document Information

### Document History

Document Revision #	Date Created:	Comments:
1.0	07/31/2018	Created
2.0	10/16/2019	Updated to reflect GOLD client status and new provisioning process
2.1	04/01/2020	Learning Center info updated

### Documentation Update Requests

To request modifications or notify the author of errors in this document, please notify your Secureworks representative. During initial implementation, notify your Provisioning Engineer. After initial implementation, please notify the Secureworks SOC by creating a Service Request in the Client Portal

### Contact Us

You can reach the Secureworks Security Operations Center 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

# Welcome to Secureworks VMS

Thank you for choosing Secureworks Vulnerability Management Service!

Secureworks Vulnerability Management Service (VMS) partners with Qualys Vulnerability Management technology to perform highly accurate internal and external scan audits across network devices, servers, web applications, databases, and other assets in on premise and cloud environments. Different service levels are available depending on the needs of your organization.

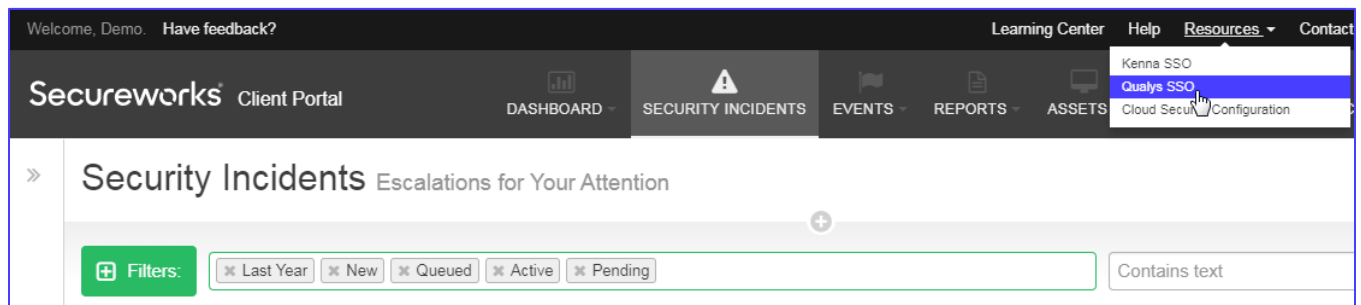
Provided as an on-demand service, Secureworks Vulnerability Scanning service provides world-class vulnerability management without the hardware, software and maintenance requirements of most scanning products. The Qualys Vulnerability Management technology is fully managed and maintained by Secureworks' dedicated vulnerability management team, eliminating administration and maintenance burdens.

## Accessing your VMS Subscription

Secureworks VMS is powered by Qualys, which can be accessed easily via Single sign-on from the Secureworks Client Portal, enabling a seamless transition between your Secureworks security information and the Qualys dashboard. If you are setting up your Client Portal account for the first time, please see the [Two-Factor Authentication Quick Start Guide](#), and if you need additional assistance, [contact the SOC](#) 24 hours a day, 7 days a week.

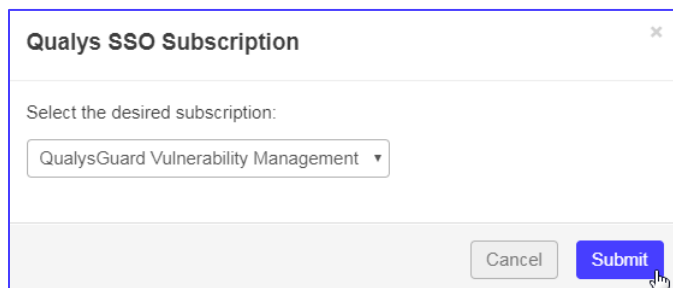
To access your service, follow these steps:

1. Log in to the Secureworks Client Portal at <https://portal.secureworks.com/portal>.
2. From the **RESOURCES** menu in the top toolbar, select **QUALYS SSO**.



**NOTE:** The options available from the **RESOURCES** menu are dependent on your contracted services.

3. The Qualys SSO Subscription dialog displays. Select the desired subscription from the dropdown menu and click **SUBMIT**.

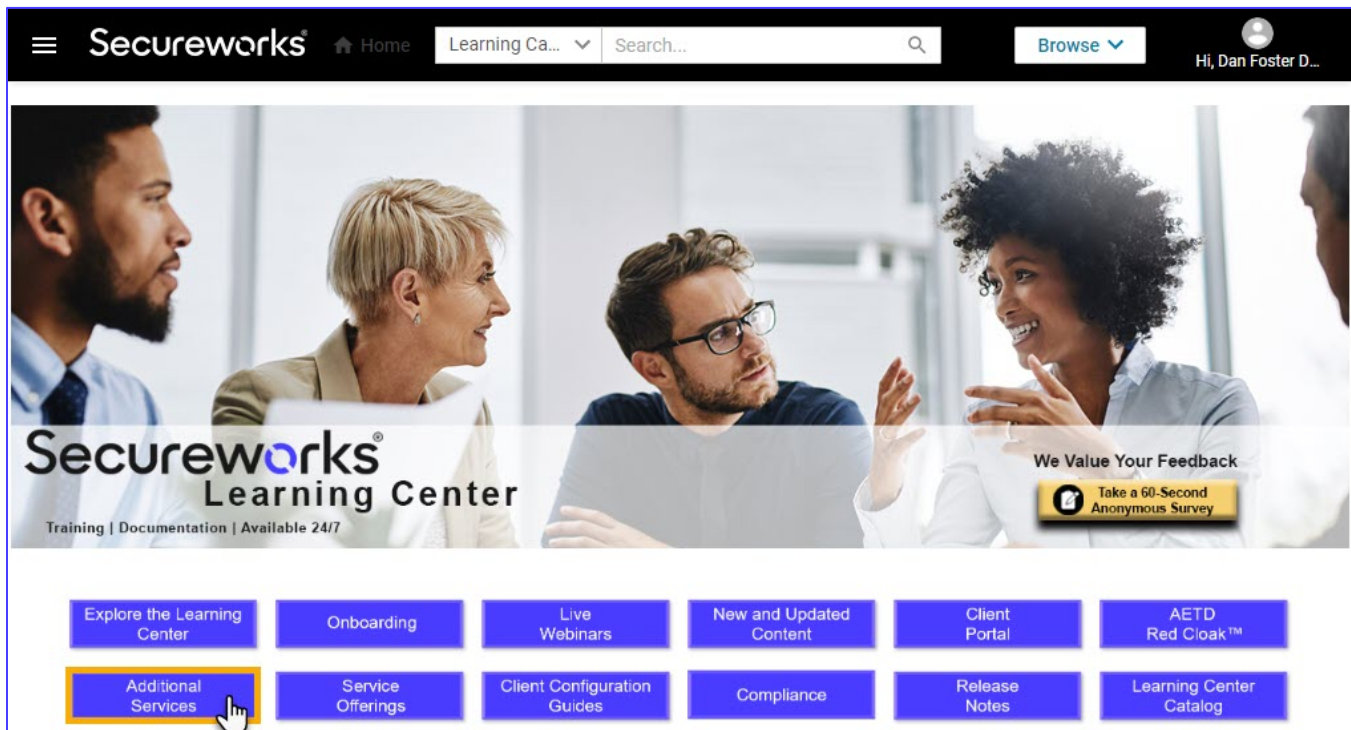


A new browser tab opens and displays your subscription

## VMS Welcome Kit

You will find the VMS Welcome Kit in the Learning Center of the Client Portal. This can be accessed using your Secureworks Client Portal credentials, which are also used to enable single sign-on access to your VMS subscription.

Your Onboarding team will work with you to enable access to the Client Portal and introduce the Welcome Kit. To locate the Welcome Kit, navigate to the [Learning Center](#) and select Additional Services:



On the **Additional Services** page, select Scanning Services to access the available VMS documentation. The Welcome Kit, which will be required to activate your services, contains other support documentation to help you get started with your services and resources to consult for assistance.

## Additional Services

The Additional Services Workspace contains all of the documentation and training for clients with Carbon Black, Log Management & Retention, Qualys, and other services.

<b>Endpoint Services</b>	You can find documentation related to CrowdStrike and AETD Carbon Black services on this page.
<b>Log Management &amp; Retention</b>	Training and documentation for Log Management Services such as LogLogic/LogVault are housed here.
<b>Scanning Services</b>	Find the documentation you need for your Vulnerability Management Services.
<b>Security &amp; Risk Consulting</b>	Our Security & Risk Consulting group provides several documents regarding their offerings that you can find here.
<b>Threat Intelligence</b>	You can find documentation related to Secureworks Threat Intelligence Services here. Please also visit <a href="#">this page</a> for training on using the Intelligence module of the Client Portal.

## Included Documents

Please review the documentation included in the Welcome Kit, which will help us to configure your subscription. If you have any queries around the documents please let your implementation Project Manager know and we will work to address any questions raised.

The following list includes descriptions of the documents that are needed to allow us to set up your service and for you to use the service to its full potential:

- › **2 - Qualys Support Resources** – This document links to the latest documentation and training materials from Qualys for utilizing your services, including how to set up and use your scanners, reporting, and utilizing both the VM and add-on services that may form a part of your subscription.
- › **3 - Information Gathering SAP (Service Activation Profile)** – This form is required to gather all of the internal and external IP ranges for this subscription. User access should also be detailed on the second tab of this spreadsheet with the relevant access rights. This document is critical in allowing us to configure the subscription as required.
- › **4 - Qualys Scanner Quick Start Guide** – This document is ONLY required for configuring a physical scanner (not for cloud or virtual scanners). This guide should be followed to configure the Qualys scanner once delivery is received. A scanner is required to run internal scans on your network. The **Info Gathering SAP** will allow us to collect your scanning host details, and to build out the subscription for this in advance of the device being delivered. Please take care to follow the **EU** Network configuration for any scanners based outside of the US, and the **US** configuration detailed in the quick start guide, for scanners based within the US.
- › **5/6 - Internal/External Asset Group SAP** – For GOLD service level clients only, these forms allow you to detail logical groupings of the external and internal scan IPs to make handling these in the portal more meaningful. These groups can also be created in the portal once the subscription is setup, so these forms are not required for the setup of service.
- › **7 - Scan Request SAP** – For GOLD service level clients only, this form allows the scheduling of a scan. This can be done in the portal once the subscription is setup, so this form is not required for the setup of the service.
- › **8 - PCI Subscription Setup Request** – This form is required to detail your PCI subscription, if you contract this service with Secureworks.
- › **9 - Web Application Scanning Subscription Setup Request** – This form is required to configure the WAS scanning service. This service will be activated at the same time as your Qualys Vulnerability scanning subscription with or without the submission of this completed document.
- › **10 - WAS Web App SAP** – For clients who have purchased the WAS services as part of their Vulnerability Scanning solution, this form allows the compilation of multiple Web Apps to be created in the Qualys portal.

## Submitting Completed SAP Forms

During service deployment, these forms will be submitted to the Secureworks representative who will initiate your services. The following forms may be required to initiate your service:

- › The *Qualys Support Resources* document should be reviewed by all clients in order to access support and training for all services.
- › Vulnerability Management clients should complete the *Information Gathering SAP*, as well as following instructions in the scanner quick start guide to configure any physical scanners needed as a part of the subscription.
- › Clients purchasing Web Application Scanning and PCI as part of their Vulnerability Management Services should complete the *Web Application Scanning* and *PCI Subscription Setup Request* forms.

The completion and return of these forms is essential to ensure the most accurate and speedy configuration and initialization of your services.

Additionally, for clients wishing to utilize the Secureworks VMS team to further manage the Qualys subscription:

- › The *Internal /External Asset Group SAP* can be used to communicate desired groupings of hosts, and can be resubmitted if groupings change.
- › The *Scan Request SAP* can be used to request a scan to be scheduled, and can be resubmitted as needed through the life of the subscription.
- › The *WAS Web App SAP* for WAS clients allows you to submit your full list of Web Apps for initial configuration.

Once services are deployed, you can continue to use the SAP forms and submit them to the VMS team directly for processing. Securely submit completed SAP forms by creating a Service Request in the Secureworks Client Portal and attaching the forms, or, if the security posture in your organization allows these details to be distributed by email, via email to [vms-support@secureworks.com](mailto:vms-support@secureworks.com).

## VMS Service Level Tiers

The following section provides an overview of the differences between the service level tiers. For more information, please consult the Service Description document, which you can find in the Secureworks [Learning Center](#) on the **Service Offerings > Service Descriptions** page.

### Secureworks Co-Managed VMS

Secureworks VMS (Co-Managed) Service provides all of the standard technical scanning functionality for a self-managed service, including (for example) full access to the Secureworks Client Portal and SSO access to the Qualys Scanning Portal to perform self-service asset discovery with visual network mapping, in-depth vulnerability scanning, remediation tracking with workflow, trending, and reporting.

Additionally, the SOC team can deliver your scan management services. These scan management functions include scheduling scans, setting up profiles, quarterly scan reviews upon client request, and the importing of assets groups, values, and system owners, outlined in the following table.

Service Level Tiers Matrix		
Service Feature	Gold	Description
Vulnerability Reporting	✓	Self-Service vulnerability reporting within the capabilities offered in the Qualys tool.
Secureworks Client Reporting	✓	Vulnerability data available through the Enterprise Security Portal.
Initial Implementation Support	✓	Implementation team available remotely for implementation support.
24x7 SOC Support	✓	SOC documents requests for engineering support. SOC is available to assist with user-access issues, stop scans, or Service unavailable issues.
Specialized VMS Support	✓	Secureworks VMS Team can assist with questions regarding the Service, reporting, troubleshooting, and other VMS questions that require a deeper dive. Available Monday – Friday, 9a.m.-5p.m. EST.
Scan Scheduling	✓	Secureworks schedules and manages recurring scans.
Quarterly Scan Review	✓	Secureworks reviews scan results with client each quarter upon client request.
Profile Set Up	✓	Secureworks works with client to establish a specific number of initial scan profiles based on client criteria.
Group/Asset Value/Asset Owner Entry	✓	Secureworks imports client-created group, asset, and owner data.
Upfront Asset Classification	Optional Add-on through SRC	Optional pre-scan classification of assets by Secureworks SRC.



## Platinum Tier (Program Managed VMS)

Secureworks VMS Platinum (Program Managed) Service provides an end-to-end vulnerability management service. It includes implementation of the vulnerability scanning, creation and analysis of reports, prioritization of vulnerabilities based on business context, tracking of the client's IT Ops team's progress against remediation actions for discovered vulnerabilities, as well as overall program management and continuous improvement of the client's vulnerability management program.

Using the resources based in the Security Centre of Excellence (SCoE) in Bucharest, Romania, our VMS Platinum team works directly with clients to define areas of key risk, analyzes scanning results with intelligence-driven context, customizes reporting for clear visibility, and orchestrates remediation.

The VMS Platinum solution may be sold with VMS Qualys licenses (optional) or the client may opt to bring their own license (BYOL) from either Qualys, Rapid 7, or Tenable.

Secureworks VMS Platinum includes the following:

- › Run by resources from SCoE for advanced support
- › Assistance with setting up scanning subscription, configuration, and credentialing (with license)
- › 24x7 access through Client Portal via SSO (with license); or access through existing scanning infrastructure
- › Building/importing policies into the scanning tool
- › Reporting features including defining report criteria, setting up standard reports, and creation of customized reports
- › Classification and prioritization of external and internal vulnerabilities
- › Client-specific remediation advice, prioritized on risk and uniqueness of client environment
- › Review scan results and reports for accuracy
- › Develop remediation action plan
- › Consultation with client on a regular basis (scope will depend on the client contract) regarding targeted recommendations for improvement, overall development of client's VMS program

VMS Platinum is only relevant if you have an established mature VMS Program, as the Secureworks VMS Platinum (Program Managed) Service does not include the following items, which are considered to be out-of-scope:

- › Initial assessment of the client's vulnerability posture and vulnerability management program
- › Design and Build service for a VMS program structure (if you are starting with no or an inadequate VMS program)
- › Determination of scanner positioning
- › Assignment of asset value or business criticality
- › Any activities related to setting up a VMS program as opposed to running an existing, mature VMS program

## Getting Started

---

This section reviews some of the services offered and guidance to clients to get the most of their Vulnerability Management Service following implementation.

### Healthy Start

All new Vulnerability Service clients will be eligible to attend a Healthy Start Program to help get you accustomed to using and getting the most out of your subscription.

The Healthy Start program is tailored to focus on the areas that will be of most benefit to each client, and includes, but is not limited to, the following:

- › Interface orientation of all tabs and sections
- › Scanner appliance health check
- › Dashboard configuration and manipulation
- › Review of the knowledgebase and basic understanding of how to read vulnerabilities (Qualys IDs)
- › How to add an asset and create an asset group
- › How to set up an on-demand scan and schedule a scan
- › Review of Option Profiles
- › Review of scan data
- › Overview of scan templates and reports

Once the subscription is created a Transition Call will be co-ordinated by your Implementation Project Manager, to introduce the VMS team and review the status of the subscription in preparation for the Healthy Start program Kick-Off.

### Map Scans

Covered in Healthy Start, but advisable to run in advance, a Map scan is suggested to get more detail of your scan environment so that the detailed hosts can be most accurately assessed.

Navigate to the [Mapping – The Basics](#) page for the most up-to-date information on mapping, including what to map and how to map.

These scans should be run on a regular basis to keep track of your continually evolving network and ensure the accuracy of the hosts that form a part of your subscription

### Vulnerability Scans

Vulnerability scans should be scheduled and run regularly. We recommend scanning weekly if possible, but at least every 30 days, and including internal and external assets, depending on your subscription.

### Scanner Appliance Heartbeat Check Notification

To ensure you are kept apprised of your scanner appliance health, you can opt in to the Scanner Appliance Heartbeat Check notification to receive an email when Qualys discovers your appliance is offline after some number of heartbeat checks (1-5). This heartbeat check lets you know whether the appliance is ready to perform scans and is able to get the most recent software updates. To opt in to the notifications, follow these steps:

1. Go to **SCANS > APPLIANCES**. Edit your appliance (hover over an appliance and select **EDIT** from the menu). Under **General Information**, select the **NOTIFICATION** option and the number of missed heartbeat checks before Qualys sends you an email.
2. Select **USER PROFILE** below your user name (in the top right corner). Go to Options and select the **SCANNER APPLIANCE HEARTBEAT CHECK** notification option.