Secureworks

Qualys Support Resources

Last Updated: December 2019

★★★★★ Have Feedback?

Secureworks

Copyright

Secureworks

Table of Contents

★★★★★ Have Feedback?

Secureworks

Qualys Support Resources

Qualys maintains a number of resources for its various modules and products. This document helps you find the materials most pertinent to your solution. The materials referenced may be updated over time, so please refer to this document when looking to review any guides or recorded sessions to ensure the most up to date information is accessed.

This guide provides your organization a good introduction to the Vulnerability Management service after implementation. It also serves as an ongoing resource for new and current team members by providing a good starting foundation of knowledge, and the ability to enhance that knowledge in more expert areas at an individual's own pace.

For answers to the most frequently asked Qualys questions, please refer to the Qualys FAQ.

General Documentation

General Qualys documentation and best practice documents are maintained at the following URL:

https://www.qualys.com/documentation/

The **Get Started** section will be of particular interest to new VMS clients in order to understand the portal and initialize some of the setup configurations for your subscription.

General Training

General Qualys training, including a video library, self-paced training, and instructor-led training, can be found at the following URL:

https://www.qualys.com/training/

The training contained at this link will provide an overview of the content available to you. This includes a link to a video library of recorded sessions, the ability to sign up for instructor-led sessions, as well as a library of recommended viewing for some of the most popular courses.

Secureworks

Core Module

Vulnerability Scanning (VM)

The Vulnerability Scanning module is the core of the Secureworks VMS service and is required in order to purchase any of the VM Add-On services. VM and the Add-On services to VM have to be co-termed, as there can only be one subscription end date for all of these services.

Secureworks Vulnerability Scanning provides vulnerability management without the hardware, software, and maintenance requirements of most scanning products. Qualys technology is supported by Secureworks' dedicated Vulnerability Management Services team, reducing administration and maintenance burdens so you can focus on protecting your assets and reducing business risk.

- Vulnerability Management Resource Site – This resource site for Vulnerability Management (as well as Threat Protection and Security Configuration Assessment) provides links to videos, technical resources, new features, latest news, and community discussion.
- VM Video Series – This album contains self-paced training classes for Vulnerability Management that you can take on demand. Some recommended classes are listed below.
- API Resources – This resource site provides API documentation, release notes, sample code, as well as community discussion.

The following are recommended self-paced training classes maintained by Qualys that will help you with the most common tasks performed within the VM module:

- Introduction to Assets - This is an introduction to assets as part the Qualys Vulnerability Management Self-Paced Training Series.
- Asset Groups - This video identifies the different components of an Asset Group. It describes the steps for creating and modifying Asset Groups to organize the host assets in your subscription. Asset Groups are demonstrated as scanning and reporting targets and are used to assign access privileges to a Qualys user account.
- Scanning - This video is about Scanning and covers several topics including configuring scans, viewing scan results, scheduling scans, configuring unauthenticated and/or authenticated scans, option profiles, and more.
- Mapping – This video is about Mapping and covers several topics including configuring maps, mapping option profile settings, host discovery during mapping, map results, and more
- Reporting – This video is about Reporting and covers several topics including scan report templates, how to create reports, importing report templates, report trending, schedule reporting, best practices, and more.
- Remediation – This video describes the basic components of a Remediation Policy. A policy is created to assign detected vulnerabilities to a specific user account. A second policy is created to ignore a selected list of vulnerabilities. The order of policy evaluation and precedence is explained.

Add-on Capabilities to VM

Cloud Agent for VM

Extends clients' security throughout the enterprise by collecting vulnerability data on each host, even when the host is not connected to the network. Cloud Agent provides faster and more accurate scan results, and allows real-time vulnerability management and policy compliance scanning.

- Cloud Agent Getting Started Guide – This guide presents the information you need to install the agents on your IT assets, get started with managing your assets, and use Qualys Platform Apps.
- Linux Installation Guide – This document guides you through the process of installing Cloud Agent on your Linux devices.
- Mac Installation Guide – This document guides you through the process of installing Cloud Agent on your Mac devices.
- Windows Installation Guide – This document guides you through the process of installing Cloud Agent on your Windows devices.
- Cloud Agent Video – This five-minute video provides you with an introduction to the Qualys Cloud Agent.

Threat Protection

A cloud-based solution that helps IT professionals automatically prioritize vulnerabilities posing the greatest risk by correlating active threats against vulnerabilities. Also includes a Live Threat Intelligence Feed and how many client assets are impacted by each threat.

- Threat Protection Datasheet – This overview document highlights the benefits and key features of ThreatPROTECT.
- Introduction to Qualys ThreatPROTECT – This seven-minute video provides a high-level introduction to using the ThreatPROTECT module.

Continuous Monitoring

Constantly monitors the perimeter, detects changes in the network, and provides alerts on security loopholes before they turn into breaches.

- Walk-through Demo – This quick minute and thirty-second overview video provides a high-level demo of how the Continuous Monitoring module can help you.
- Continuous Monitoring API User Guide – This guide provides you with the information you need to utilize the API functions to download information from your Continues Monitoring application.
- Continuous Monitoring Resource Site – This resource site for Continuous Monitoring provides links to top resources, technical resources, and community discussion.

Security Configuration Assessment (SCA)

Qualys SCA is an add-on for Qualys Vulnerability Management that lets you assess, report, monitor, and remediate security-related configuration issues based on the Center for Internet Security (CIS) Benchmarks.

- SCA Datasheet – This data sheet provides a high-level overview of the SCA add-on module, highlighting benefits, key features, and detailed features.
- SCA Getting Started Guide – This guide provides the information you need to know to get started with the SCA add-on module, from adding assets, to importing and building the CIS policy, to generating a report.

AssetView

AssetView provides a powerful cloud-based solution for a complete, continuously updated inventory of all IT assets, wherever they reside. This community also covers CMDB Sync (SYN) for synchronizing asset information from Qualys into ServiceNow CMDB

- AssetView Resource Site – This resource site for AssetView provides links to top articles, self-paced training, and community discussion.
- AssetView Video Series – This album contains all self-paced classes for AssetView and Threat Protections, including an introduction, asset tagging, widgets and dashboards, and more.
- Dashboards – This post reviews dashboard options to highlight the ways data can be presented for differing audiences that you can replicate or alter for your own uses.

★★★★★ Have Feedback?

Add-On Modules

PCI Compliance

Provides scanning of in-scope PCI IP addresses, review of submitted false positive exceptions, reporting, and attestation signing as specified by the PCI SSC. Secureworks is a PCI Approved Scanning Vendor (ASV).

- PCI Compliance Resource Site – This resource site for PCI Compliance provides links to self-paced training, technical resources, latest news, and community discussion.
- PCI Getting Started – This Getting Started Guide is a downloadable PDF that provides all the information you need to get started with your PCI Scanning service.

PCI is often bundled along with other complimentary services (such as external scanning). If you are a client that has a PCI subscription as part of your service but are not required to submit a quarterly attested (PCI) report, or you have another vendor that facilitates this on your behalf, there are still technical benefits to your VMS setup that cannot be achieved without the PCI option being enabled.

When you launch a scan using the Payment Card Industry option profile a light web application scan will be invoked that will test for common web application vulnerabilities, which would not normally be tested under a standard vulnerability scan. This cannot be achieved without that module being enabled.

Be aware that these benefits are available to you simply by allowing the PCI subscription to be created and configured by Secureworks, even if you do not log into PCI or run any PCI scans.

The following self-paced training classes maintained by Qualys will help you with the most common PCI Compliance topics:

- PCI Compliance Overview - This video provides an overview of the PCI DSS Lifecycle, and identifies the various PCI stakeholders. The different roles and services provided by the PCI Security Standards Council are identified. Differences between requirements and recommendations is discussed, and the requirements covered by Qualys PCI Compliance are identified. An overview of Qualys' complete coverage of the PCI DSS (including all Qualys applications) is provided, along with the Advanced Workflow features only available within Qualys PCI Compliance. An overview of the Qualys PCI Compliance user interface is demonstrated.
- Compliance Reporting - This video provides discussion and analysis of the PCI DSS 11.2.2 reporting requirement. A seven step "Report Flow" is discussed. Steps to create PCI Compliance reports using the Report Generation Wizard, are demonstrated. Report status definitions, and a discussion of report status changes are provided. Examples of an Executive and Technical Report are demonstrated. Report submission steps and requirements are discussed. The Open Services Report (PCI DSS 1.1.6) is defined and demonstrated.
- Compliance Scanning - This video focuses on the requirements and processes for performing "external" network vulnerability scans, using Qualys' PCI Compliance application. Scans are performed using Qualys' pool of Internet Scanner Appliances. A workflow diagram of the "external" scan process is provided, including steps to: 1) submit "false positive" requests to Qualys, 2) submit your compliance reports to Qualys, and 3) submit "certified" PCI compliance reports to your acquiring bank.

Web Application Scanning

Consists of automated, self-service vulnerability scanning of internal- and external-facing web-based applications.

- Web Application Scanning Resource Site - This resource site for Web Application Scanning provides links to key features, videos and webcasts, top resources, technical resources, and community discussion.
- WAS Video Series – This album contains all self-paced classes for Web Application Scanning, from an introduction to more focused and detailed topics.
- Selenium Scripting Resources – Browse all posts in the Qualys community tagged with “selenium.”

Secureworks

Policy Compliance (PC)

Automates the process of assessing server and application configuration compliance, useful for clients subject to compliance mandates such as PCI and HIPAA.

- Policy Compliance Resource Site - This resource site for Policy Compliance and FIM provides links to features, videos, top resources, technical resources, and community discussion.
- Policy Compliance Video Series – This album contains all self-paced classes for Policy Compliance, from an introduction to controls and policy to reporting.
- PC Self-Paced Training & Certification – This site lists all available self-paced training and certification classes, including for Policy Compliance.
- Scanning Docker – This post reviews how to use the Policy Compliance module to scan Docker technology.

Add-on Capability to PC

Cloud Agent for PC

Extends clients' security throughout the enterprise by collecting vulnerability data on each host, even when the host is not connected to the network. Cloud Agent provides faster and more accurate scan results, and allows real-time vulnerability management and policy compliance scanning

- Cloud Agent Getting Started Guide – This guide presents the information you need to install the agents on your IT assets, get started with managing your assets, and using Qualys Platform Apps.
- Linux Installation Guide – This document guides you through the process of installing Cloud Agent on your Linux devices.
- Mac Installation Guide – This document guides you through the process of installing Cloud Agent on your Mac devices.
- Windows Installation Guide – This document guides you through the process of installing Cloud Agent on your Windows devices.
- Cloud Agent Video – This five-minute video provides you with an introduction to the Qualys Cloud Agent.

Secureworks

Scanner Appliances

Easily install the physical Scanner Appliance on your network or deploy a virtual or cloud scanner to your account in just a few minutes. The Scanner Appliance is a robust, scalable solution for scanning networks of all sizes including large distributed networks and web applications on your internal network.

Scanners enable the Vulnerability scanning of internal hosts on your network. Without a scanner, these internal hosts cannot be scanned as a part of your Vulnerability Management program. The Scanners should sit on the same subnet as the hosts you wish to scan, and can be configured in multiple ways:

- **Physical Scanner** – Hardware shipped to you to rack and cable on the network
- **Virtual** –Set up using a VM
- **Cloud** – Added to your cloud environment to enable the scanning of hosts within your cloud domain

We will look at each in more detail below.

Physical Scanner

No pre-configuration details are required to ship your physical scanner. The *Qualys Scanner Quick Start Guide* included in the Welcome Kit guides you through the process of activating the scanner once received. The following documents contain details you may find helpful:

- Physical Scanner User Guide – This comprehensive guide contains network requirements, quick start steps, a tour of the scanner appliance, and troubleshooting steps.
- Physical Scanner Quick Start Guide – This quick two-page guide provides you with high-level overview of getting started with your scanner appliance.

Virtual Scanner

No pre-configuration details are required to enable your virtual scanner. If a virtual scanner is required then this will be available to your once your subscription is created. You can find guidance to activate the device in the following guides:

- Virtual Scanner User Guide – This comprehensive guide contains information about adding a virtual scanner, configuration settings, and troubleshooting.
- Virtual Scanner Quick Start Guide – This short article highlights available distributions and technical details of the virtual scanner. The article includes resource and network configuration requirements for your virtual appliance. Our recommendation is to get as close to the maximum resource configuration (with no less than two processors if possible). These settings will align the performance capabilities of your virtual scanner most closely to that of a physical scanner appliance.

Cloud Scanners (AWS / Azure)

No pre-configuration details are required to enable your cloud scanner. If a cloud scanner is required then this will be available to you once your subscription is created. There is no separate Qualys cloud scanner offering from Secureworks; you would just use a virtual scanner license for the Qualys Cloud Scanners from AWS or Azure. You can find guidance to activate the device in the following guides:

- AWS scanner configuration guidance here
- Azure guidance here

Secureworks

Self-Service Modules

These are additional modules that are available within the Qualys subscription, but not managed by the Secureworks VMS team. While the Secureworks VMS team does not directly manage these self-service modules, you can still contact the team by creating a Service Request in the Client Portal and they will work with Qualys support to address your request.

File Integrity Monitoring (FIM)

Qualys File Integrity Monitoring (FIM) is a highly scalable and centralized cloud app that logs, detects and identifies critical changes, incidents, and risks resulting from normal and malicious events

- FIM Getting Started Guide – This guide helps you to install the needed lightweight agents on your assets, configure FIM monitoring profiles, and view your events.
- FIM Datasheet - This data sheet provides a high-level overview of the FIM add-on module, highlighting benefits and key features.
- Introduction to FIM Video – This 13-minute introductory video shows you how to get started with FIM.

Indicators of Compromise (IoC)

A new extension to the Qualys Cloud platform that delivers a continuous view of suspicious activity on IT assets, including presence of known malware and other threat actors.

- About Indication of Compromise (IoC) – This page provides an overview of this new extension including highlights and key capabilities.
- IOC Press Release – This press release reviews how this extension provides visibility of compromised assets and threat hunting capabilities.

Security Assessment Questionnaire (SAQ)

Qualys Security Assessment Questionnaire simplifies assessment of internal IT assets and vendor risk. It assesses business risk with automated campaigns and efficiently collects and analyzes information from third-party vendors for rapid audit processes.

- SAQ Datasheet and Whitepaper – The datasheet provides a quick glance at the benefits and key features of SAQ, while the whitepaper helps you to understand six scenarios where you need cloud-based, automated risk assessments of third parties and internal staff, and to learn how SAQ automates and streamlines this entire lifecycle.
- Getting Started with SAQ Video – This five-minute introductory video will show you how to get started with SAQ to create automated campaigns that help you analyze your business risk and compliance information.

CMDB Sync

Certified app for automatically synchronizing data from Qualys Asset Inventory with the ServiceNow Configuration Management Database.

- Qualys CMDB Sync – This page highlights the benefits and key features of CMDB Sync.
- Qualys App for CMDB Sync Documentation – This document guides you through initial setup, schedules setup, application-specific properties, sync, and reports with a section on troubleshooting and an FAQ.

★★★★★ Have Feedback?

Web Application Firewall (WAF)

Web Application Firewall protects websites against attacks on server vulnerabilities and web app defects; makes it possible to strongly secure web apps against cross-site scripting (XSS), SQL injection, corrupted requests and other attacks; and complements Qualys WAS with one-click virtual patches.

- WAF Getting Started Guide – This guide will help you get started, create application profiles, define your web application, and more.
- WAF Deployment Overview – This page provides an overview of the WAF deployment process.
- WAF New Web Application Firewall Innovations – This 25-minute video unveils new Web Application Firewall innovations that increase customer control, enhance customization, and add to confidence in application security.

CertView

Inventory and assess certificates and underlying SSL/TLS configurations and vulnerabilities across external-facing assets to prevent downtime and outages, and to mitigate risks associated with expired or vulnerable SSL/TLS certificates and configurations.

- CertView Scan Set up Guide – This quick guide helps you to set up and launch a CertView scan.
- CertView Getting Started Video – This seven-minute video shows you the steps to get up and running with CertView.
- SSL/TLS Deployment Best Practices – This GitHub resource provides clear and concise instructions to help you spend the minimum time possible to deploy a secure site or web application, focusing on advice that is practical and easy to follow.

CloudView

Visibility and Continuous Security of your Public Cloud Infrastructure. Allows organizations to continuously monitor and secure public cloud infrastructure against misconfigurations, malicious behavior and non-standard deployment

- CloudView User Guide – This guide provides an overview of the CloudView service, information on creating AWS and Azure connectors, how to view your resources and misconfigurations, and API information.
- Introduction to CloudView Video - This video shows how to setup the CloudView connectors for AWS and Microsoft Azure, how to view and query the resources collected, how to evaluate resources against policies, remediate failures and configure dashboards.

Cloud Inventory

Cloud Inventory continuously discovers and tracks assets and resources such as instances and virtual machines, storage buckets, databases, security groups, ACLs, ELBs, and users, across all regions, multiple accounts and multiple cloud platforms. You can view all this information in one central place.

- For an overview of the cloud Platform, watch the short video here.

Cloud Security Assessment

Cloud Security Assessment continuously monitors and assesses your cloud assets and resources for misconfigurations and non-standard deployments. The service boosts the security of your public clouds by identifying threats caused by misconfigurations, unwarranted access, and non-standard deployments. It automates security monitoring against industry standards, regulatory mandates and best practices to prevent issues like leaky storage buckets, unrestricted security groups, and crypto-mining attacks.

Qualys Cloud Security Assessment gives you an “at-a-glance” comprehensive picture of your cloud inventory, the location of assets across global regions, and full visibility into the public cloud security posture of all assets and resources.

- For an introduction of the Security Assessment service, watch the short video here.

Container Security

Container Security addresses vulnerability management for images and containers across cloud and on-premise environments. This version supports Discovery, Inventory and near-real time tracking of container environments, Vulnerability analysis for images and containers, Vulnerability analysis for registries, and Integration with CI/CD pipeline using APIs (DevOps flow)

Container Security utilises a new ‘Container Sensor’ – providing native container support, distributed as a docker image designed for the native support of docker environments.

- Container Security User Guide – This guide will help you get acquainted with the Qualys solutions for securing your Container environments like Images, Containers and Docker Hosts using the Qualys Cloud Security Platform.
- Introduction to Container Security Video – This video provides a high-level overview of Qualys Container Sensor and the Qualys Container Security application. Descriptions are provided for sensor deployment, as well as working with images, containers, and events.