How to set up Continuous Monitoring for the Perimeter

A couple things to consider

1. Be sure the New Data Security Model is enabled. See Appendix below.

2. Optional – Continuous Scanning. This feature lets you scan constantly – after one scan finishes we’ll start the next automatically. Want to enable the Continuous Scanning feature? If yes see Step 1 of this article from the Qualys Community https://community.qualys.com/docs/DOC-3852

Step 1 – Configure Continuous Monitoring

First you need to change your module from Vulnerability Management to Continuous Monitoring:

Then navigate to Configuration > Monitoring Profiles and click on New Profile:
And in Monitoring Profile Creation window provide Title and put your perimeter address range:

After pressing Continue we need to assign Ruleset, you can use predefined one that will notify you about new host found, a port open, SSL certificate expired and will expire. Or you can create your own Ruleset depending on your monitoring needs:

As a last step you need to define recipients of alerts generated by Qualys when rules define in Ruleset will be meet. Recipients could be Qualys users but also distribution email groups.
Step 2: Add your perimeter network to Qualys subscription

There is several ways how to do this: just one of them would be to navigate to Assets > Host Assets tab, and selecting New and then IP Tracked Hosts:

Then in New Host window in Host IPs you should type your perimeter address range (193.178.132.0/24 in my case, but in yours should be your public IP range) and click Add:

Step 3: Set up a scheduled scan

In next step you need to schedule a scan of your perimeter IPs that will be the information source for Continuous Monitoring.

Just navigate to Scans > Schedules and click on Schedule Scan:
In New Schedule Vulnerability Scan windows fill the fields starting first by filling Task Title and by choosing the right Option Profile and External Scanner Appliances:

Then define your target (the same IP range we added to subscription):
And then go to Scheduling tab, where you will be able to set up the schedule of scanning. This is critical part, as the schedule you are going to choose will affect the frequency of sampling for Continuous Monitoring. And as for many companies daily scans are enough to monitor their perimeter you should consider fully continue scanning to get the most out of Continuous Monitoring. Fully continuous scanning can be achieved by selecting Relaunch on Finish option for the Occurs setting. Remember to set up the right hour and time zone if you are selecting daily scans.

Then click Save and scan will start at scheduled date and time and it will follow schedule as planned.

---

1 **Warning about Continuous Scanning:** When a user configures a scheduled scan to perform continuous scanning our service relaunches a new scan once the previous one finishes. Be aware that each active scan counts towards the concurrent scans limit set for the subscription. Any scan may have impact to your network and the same impact could occur repeatedly, until the schedule is deactivated, canceled or paused.
Appendix: How to accept new data security model

In order to protect our new advanced technologies like asset tagging, report scheduling, one-click data encryption, etc., we are migrating customers to a powerful new data security model. This new model includes advanced encryption and access control technologies that are not only enhanced but can also be used to scan data to perform preprocessing, indexing, and optimization of the data. Please see the documentation for more information.

The following features require the new security model:
- Scheduled reporting
- Zero Day PPTP
- Asset Tagging

**Session Timeout**

Users will automatically be timed out if they do not perform any actions for 24 hours.