

Sensors, Alert Thresholds, and IoCs

A simple overview of

Curtis Crawford | Lighthouse Labs | 16-May-2024

# Executive Summary

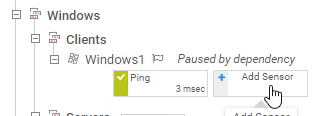
In this short and simple report, we’re going to cover some of the sensors that I have added to PRTG. These sensors will help us monitor one of the machines on our EVE Lab; Windows1.

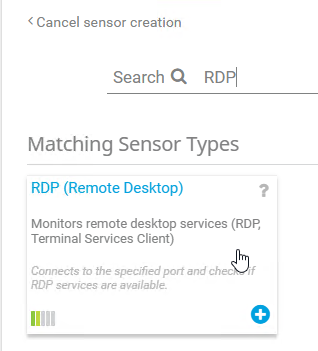
* Knowing that Windows1 is a Remote Desktop (RDP), I’ve opted for a RDP sensor. This will indicate the machine’s general performance and if it’s under an unusual load, we’ll be notified.
* The next sensor I chose is the Win API Eventlog. This can be used to determine if something odd is underway and I personally chose for it to watch out for security events. If multiple security events are happening in a short time, we know something is wrong.

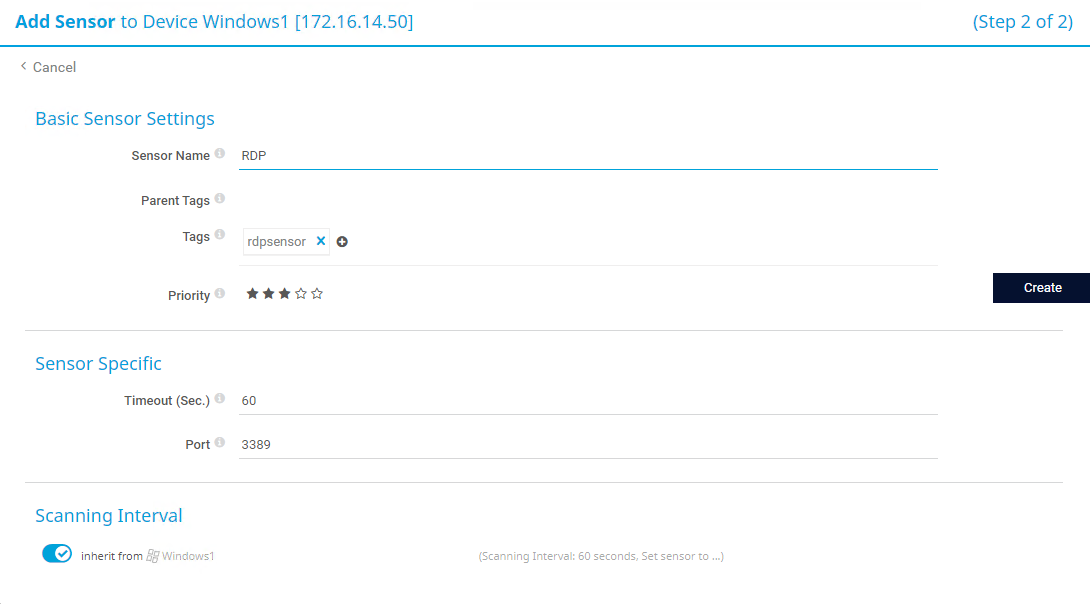
## Process walkthrough

Over the next few pages, we’ll discuss how these sensors were added, configuring them with threshold limits, with detailed instructions and pictures included!

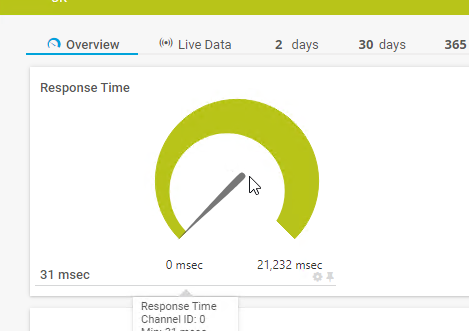
Let’s begin,

Step 1: On your PRTG interface, navigate to the machine you wish to add sensors to, and click the “Add Sensor” button.

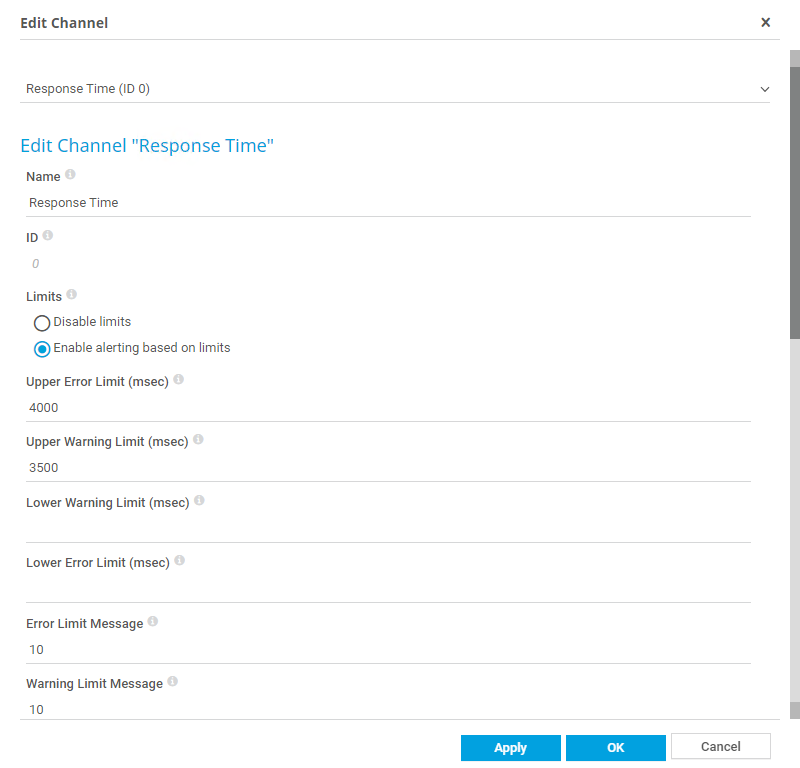
Step 2: In the search bar that you should know see in front of you, type in “RDP” and select the following sensor.

Step 3: Confirm your device’s IP address at the top and then name the sensor whatever you wish. Confirm the amount of time you’d like to pass before you are informed that the sensor has timed out, and make sure you have the right port selected. Is everything good to go? Awesome, click “Create” on the right side of the page!

Step 4: Give your sensor some time to boot-up and get to work, and then you should see something like this:



**Step 4 cont’d – Click on the graph above to edit it’s settings and set thresholds.**

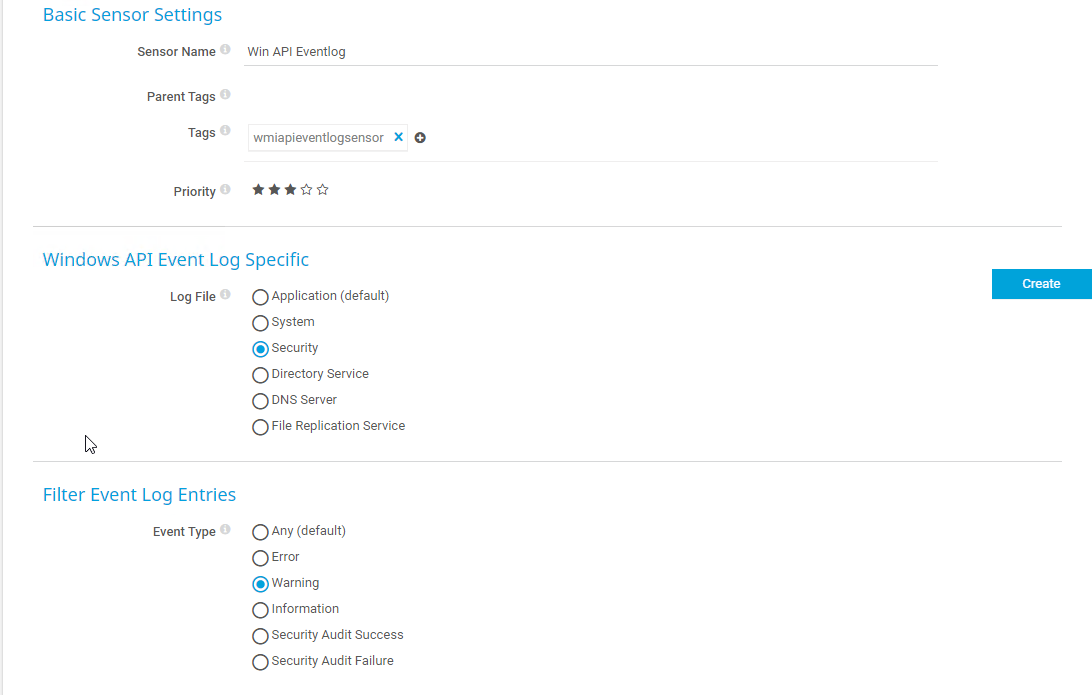
**Step 5: Here we can set limits to where we’ll be notified of an “Error/Warning”, and how many of those messages we’re limited to. Respectively, I’ve set my upper Error Limit to 4000, and Warning Limit to 3500 as this sensor’s response time is usually relatively low. My Message Limit is set to 10 so that I’m not bombarded with notifications.**

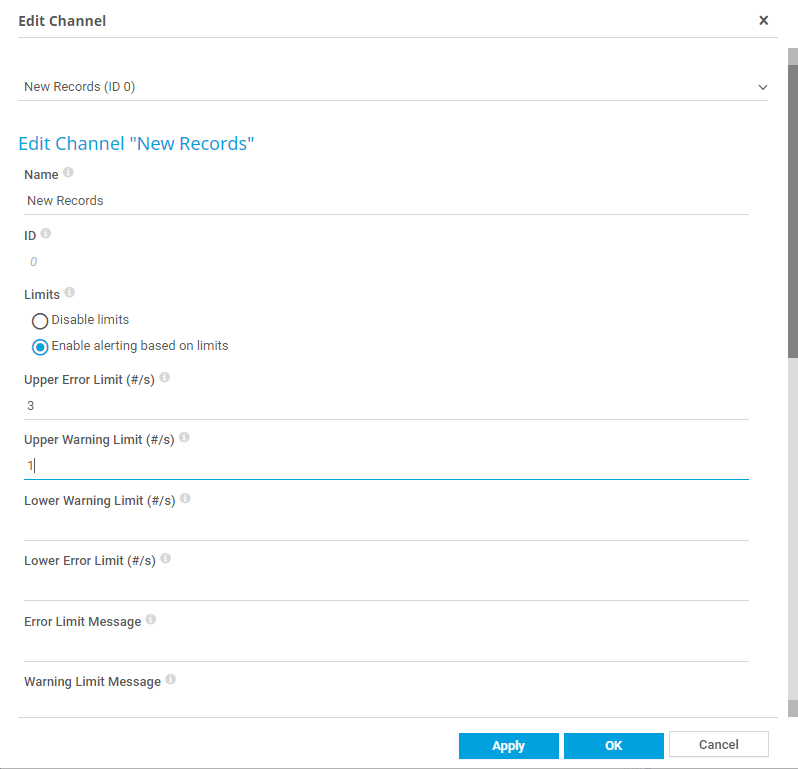
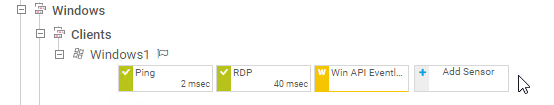
A screenshot of a computer

Description automatically generatedStep 6: Celebrate, you’ve successfully added and configured an RDP Sensor to your machine! We’re not done yet, so let’s continue to Step 7 on the next page.

A screen shot of a computer

Description automatically generatedStep 7: So, you’ve added your first sensor and don’t need my help anymore, eh? Well, I’ll type out the following just in case you decide you need a hand! On this step, we’re going to add another sensor, this one will indicate when Win-Events are happening on our machine and can be customized to only watch for errors and warnings of any kind. Since you already know how to add sensors, when you get to the search bar, this time we’ll type in “Event” and select the following:

Step 8: This particular sensor has a lot of basic settings you can change depending on what your preferences are, but for myself, I chose to have it watch for Security events and Warnings. Once you’ve chosen what you’d like to be notified about, click “Create”!

Step 9: Once the sensor has been created and we’ve given it time to start doing it’s thing, click on the same graph that we did in Step 4. The only difference is that this one will notify us by the # of events happening, instead of the response time. Input the limits that you’d prefer, and click “Apply” and then “Ok”!

Step 10: Congratulations once more, we’ve now added a second sensor to our machine!

Table

Below is a table of the sensors I chose to add, the thresholds I used and why, and the IoC that I believe this sensor will help detect or remediate.

