

BASIC PRTG HACKS

SAINTCON 2018 - /BIN/BUDDHA

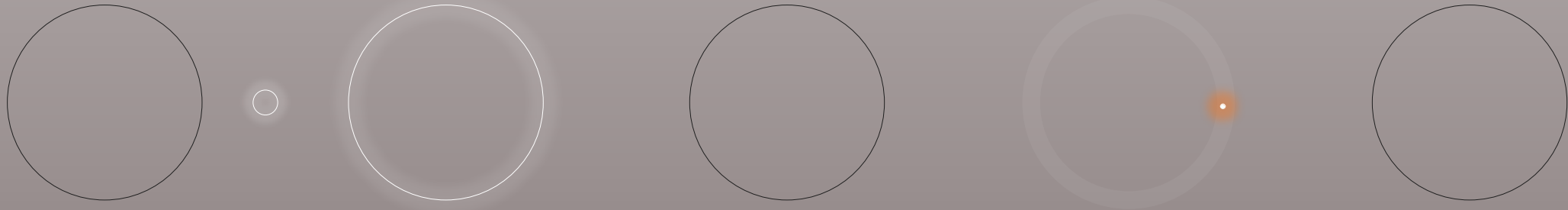
WhoAml

/bin/buddha

- Been did by IT since 1996
 - Cisco/CompTIA/Microsoft certified trainer
 - Dell Hardware & Network OS tech lead
 - College of Southern Idaho Webmaster / SysAdmin
 - Community College Associate Professor
 - Fish Farm'n SysAdmin / DevOps / InfoSec

Why should you listen to me?

Probably shouldn't....

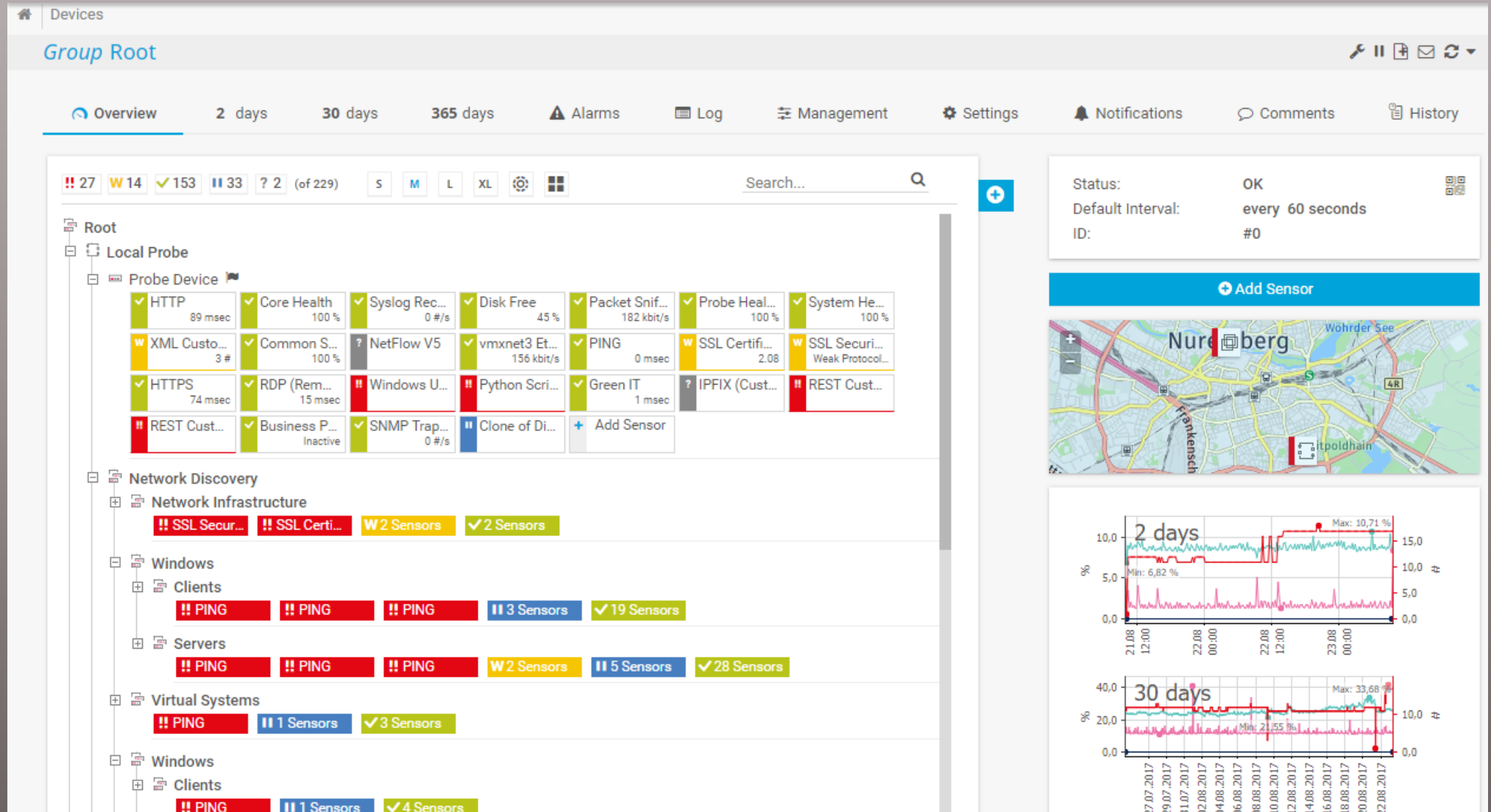


Go find out yourself!

Core SysAdmin role: uptime

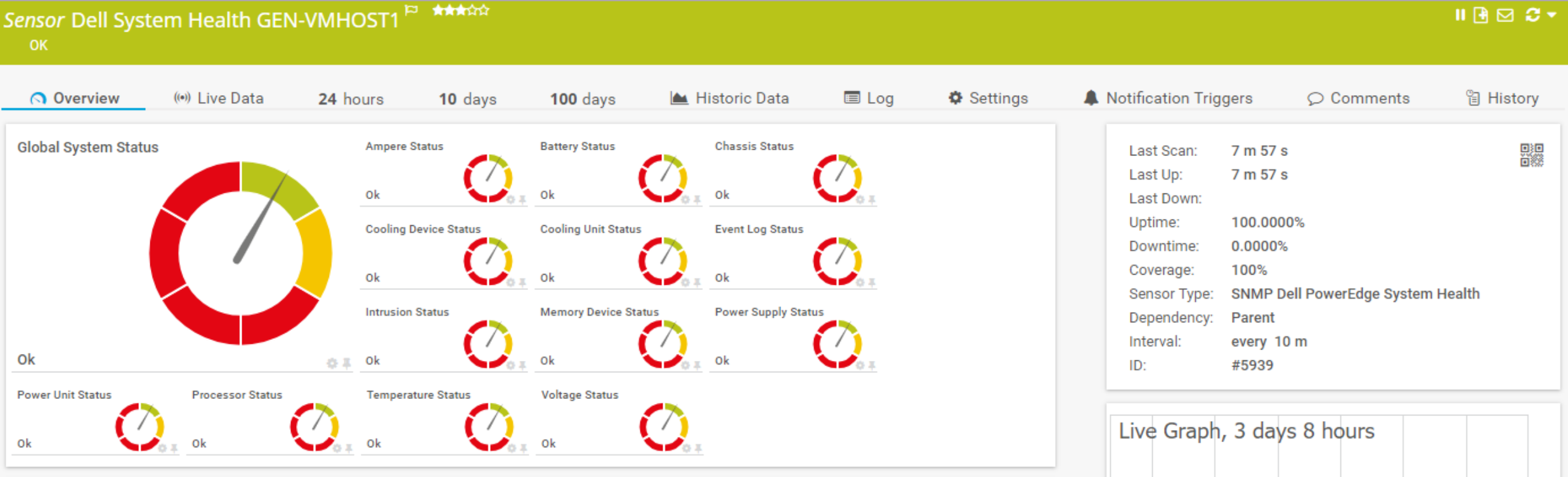


PRTG Interface






https://hlassets.paessler.com/common/files/screenshots/prtg-v17-4/basics/device_tree3.png

Slick monitoring for: Dell/HP server hardware



Slick monitoring for: Hyper-V

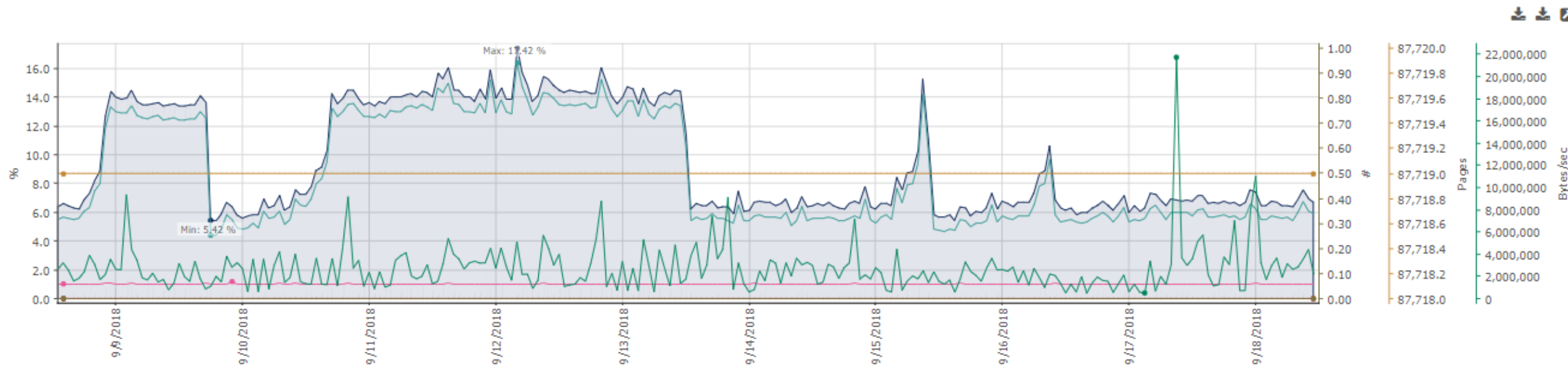
Sensor Hyper-V Host Server 1    

OK



[Overview](#) [Live Data](#) **24 hours** 10 days [100 days](#) [Historic Data](#) [Log](#) [Settings](#) [Notification Triggers](#) [Comments](#) [History](#)

Last Scan: 235 s	Last Up: 235 s	Last Down:	Uptime: 100.0000%	Downtime: 0.0000%	Coverage: 100%	Sensor Type: Hyper-V Host Server	Dependency: Parent	Interval: every 5 m	ID: #5062
---------------------	-------------------	------------	----------------------	----------------------	-------------------	-------------------------------------	-----------------------	------------------------	--------------



PRTG Network Monitor 18.3.43.2323

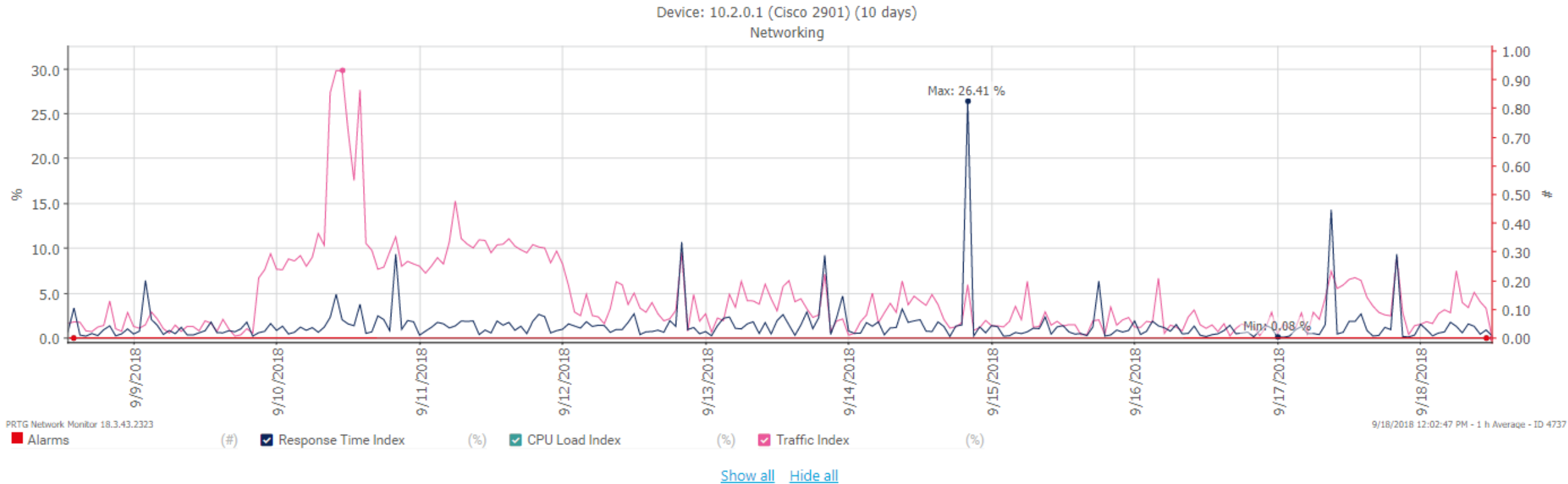
9/18/2018 12:00:38 PM - 1 h Average - ID 5062



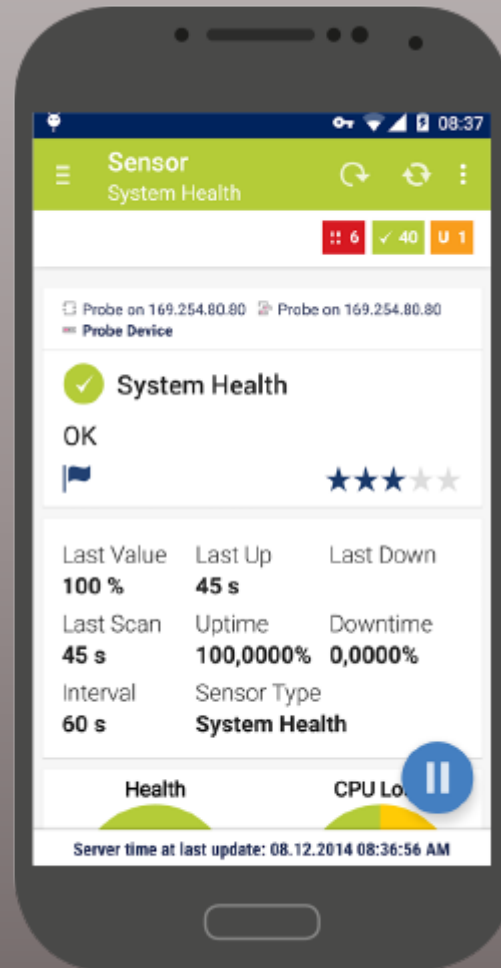
<input checked="" type="checkbox"/> Downtime (%)	<input checked="" type="checkbox"/> CPU Usage Total (%)	<input checked="" type="checkbox"/> CPU Usage Guests (%)	<input checked="" type="checkbox"/> CPU Usage Hypervisor (%)	<input checked="" type="checkbox"/> Host Health Critical (#)
<input checked="" type="checkbox"/> Deposited Pages (Pages)	<input checked="" type="checkbox"/> Network Traffic (Bytes/sec)			

[Show all](#) [Hide all](#)

Slick monitoring for: SNMP



Mobile App with push



<https://hlassets.paessler.com/common/files/screenshots/apps/android/android-01.png>

InfoSec relevance:

- Basic monitor for IT resources:
 - Are your servers mining crypto for someone else?
HODL!
 - Are your database servers shipping a few TB of info overseas?
 - Why is the third interface on the core router higher than last week?
 - Why is the file server writing to every single file on the data drive?

So what about an industrial Hydroelectric plant?



If only...

New Log Entries 6W 1✓ 431II 2Search...

HomeDevicesLibrariesSensorsAlarmsMapsReportsLogsTicketsSetup

Devicesdevice-PC▼Probe DeviceAdd Sensor (Step 1 of 2)

Add Sensor to Device Probe Device [127.0.0.1](Step 1 of 2)

Monitor What?

☐ Availability/Uptime☐ Memory Usage☐ Bandwidth/Traffic☐ Hardware Parameters☐ Speed/Performance☐ Network Infrastructure☐ CPU Usage☐ Custom Sensors☐ Disk Usage

Target System Type?

☐ Windows☐ Email Server☐ Linux/macOS☐ Database☐ Virtualization OS☐ Cloud Services☐ Storage and File Server

Technology Used?

☐ Ping☐ Packet Sniffing☐ SNMP☐ NetFlow, sFlow, jFlow☐ WMI☐ PowerShell☐ Performance Counters☐ Push Message Receiver☐ HTTP☐ PRTG Cloud☐ SSH

< Cancel sensor creation

> Looking for more sensor types? See our PRTG Script World.

Search Hydro

1 Matching Sensor Types


Matching Sensor Types

Hydroelectric Plant?

Monitors generator RPM, KW, vibration

Idaho Power grid connected industrial plant.

+




Looking For More Sensor Types? See our PRTG Script World.

Ninjaneering



NINJANEER

[←](#) [→](#) [↻](#) <http://yourCorp.com/Hydro/Ast/variables.csv>


WebPort

View I/O	Alarm Summary	Diagnostic	Cont
	Alarm History	Files Transfer	Lo

```
"Id";"Name";"Description";"ServerName";"TopicName";"Address";"Coef";"Offset";"LogEnabled";"AlEnabled";"Type";"AlBool";"MemTag";"MbsTcp
Float";"SnmpEnabled";"RTLogEnabled";"AlAutoAck";"ForceRO";"SnmpOID";"AlHint";"AlHigh";"AlLow";"AlTimeDB";"AlLevelDB";"IVGroupA";"IVGro
"IVGroupD";"PageId";"RTLogWindow";"RTLogTimer";"LogDB";"LogTimer";"AlLoLo";"AlHiHi";"MbsTcpRegister";"MbsTcpCoef";"MbsTcpOffset";"EEN"
U";"EAT";"ESH";"SEN";"STO";"SSU";"TEN";"TSU";"FEN";"FFN";"FCO";"AlStat";"ChangeTime";"TagValue";"AlType"
8;"SCADA_Bus_Voltage";"Analog Value - Bus Voltage Approximately 2400
Volts";"ABLOGIX";"A";"SCADA_Bus_Voltage";1.000000;0.000000;0;0;1;0;0;0;0;0;0;0;1;"";0.000000;0.000000;0;0.000000;-1;0;0;0;1;600;10;-
.000000;0.000000;"";"";"";"";"";"";"";"";"";"";"";"";0;"18/09/2018 13:33:51";2386.000000;131090
9;"SCADA_Gen1_Brkr_Clsd";"Unit #1 On
Line";"ABLOGIX";"A";"SCADA_Gen1_Brkr_Clsd";1.000000;0.000000;0;-1;0;-1;0;0;0;0;0;-1;0;1;"";1.000000;0.000000;0;0.000000;-1;0;0;0;1;600
;;1;1.000000;0.000000;"";"";"";"";"";"";"";"";"";"";"";"";2;"17/09/2018 06:53:59";1.000000;3
10;"SCADA_Gen1_Brkr_Opn";"Unit #1 Off
Line";"ABLOGIX";"A";"SCADA_Gen1_Brkr_Opn";1.000000;0.000000;0;-1;0;-1;0;0;0;0;0;-1;0;1;"";0.000000;0.000000;0;0.000000;-1;0;0;0;1;600;
;1;1.000000;0.000000;"";"";"";"";"";"";"";"";"";"";"";"";0;"17/09/2018 06:53:59";0.000000;0
11;"SCADA_Gen1_Power";"Generator #1 Power Analog
Value";"ABLOGIX";"A";"SCADA_Gen1_Power";1.000000;0.000000;-1;0;1;0;0;0;0;0;-1;0;0;1;"";0.000000;0.000000;0;0.000000;-1;0;0;0;1;60000;6
1;1.000000;0.000000;"";"";"";"";"";"";"";"";"";"";"";"";0;"18/09/2018 13:33:39";135.000000;1048576
12;"SCADA_Gen1_Sped";"Generator #1 Speed
(RPM)";"ABLOGIX";"A";"SCADA_Gen1_Sped";1.000000;0.000000;0;0;1;0;0;0;0;0;0;0;1;"";0.000000;0.000000;0;0.000000;-1;0;0;0;1;600;10;-1.
00000;0.000000;"";"";"";"";"";"";"";"";"";"";"";"";0;"18/09/2018 12:00:11";604.000000;-1
13;"SCADA_Gen1_Vib";"Generator #1
Vibration";"ABLOGIX";"A";"SCADA_Gen1_Vib";1.000000;0.000000;-1;0;1;0;0;0;0;0;-1;0;0;1;"";0.000000;0.000000;0;0.000000;-1;0;0;0;1;6000;
;1;1.000000;0.000000;"";"";"";"";"";"";"";"";"";"";"";"";0;"10/09/2018 01:18:32";0.000000;16
14;"SCADA_Gen2_Brkr_Clsd";"Unit #2 On
```

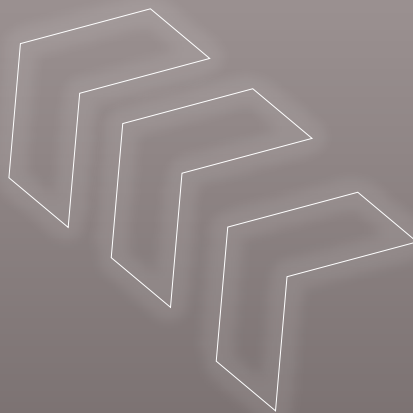
Custom monitor process flow



PowerShell



```
<prtg>
  <result>
    <channel>First channel</channel>
    <value>10</value>
  </result>
  <result>
    <channel>Second channel</channel>
    <value>20</value>
  </result>
</prtg>
```



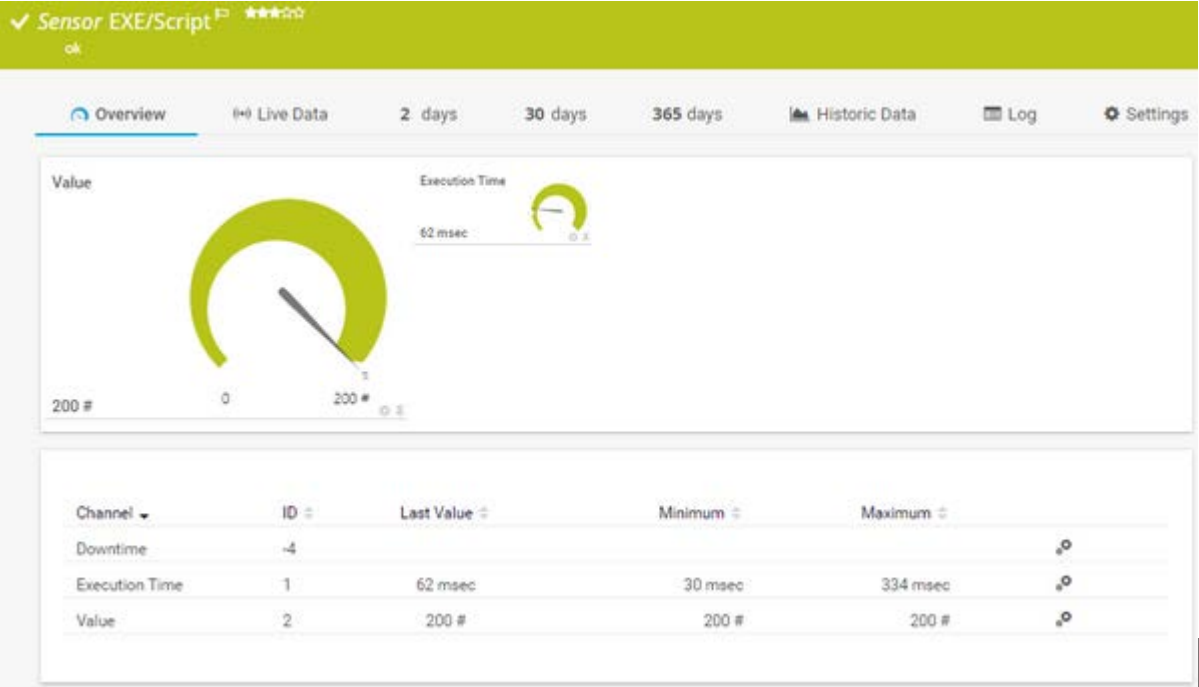
PRTG Manual: EXE/Script Sensor

The EXE/Script sensor runs an executable file (EXE, DLL) or a script (batch file, VBScript, PowerShell) on the computer running the local or remote probe. This option is provided as part of the PRTG Application Programming Interface (API).

This sensor can show the following:

- One value returned by the executable file or script (in one channel only)
- Execution time

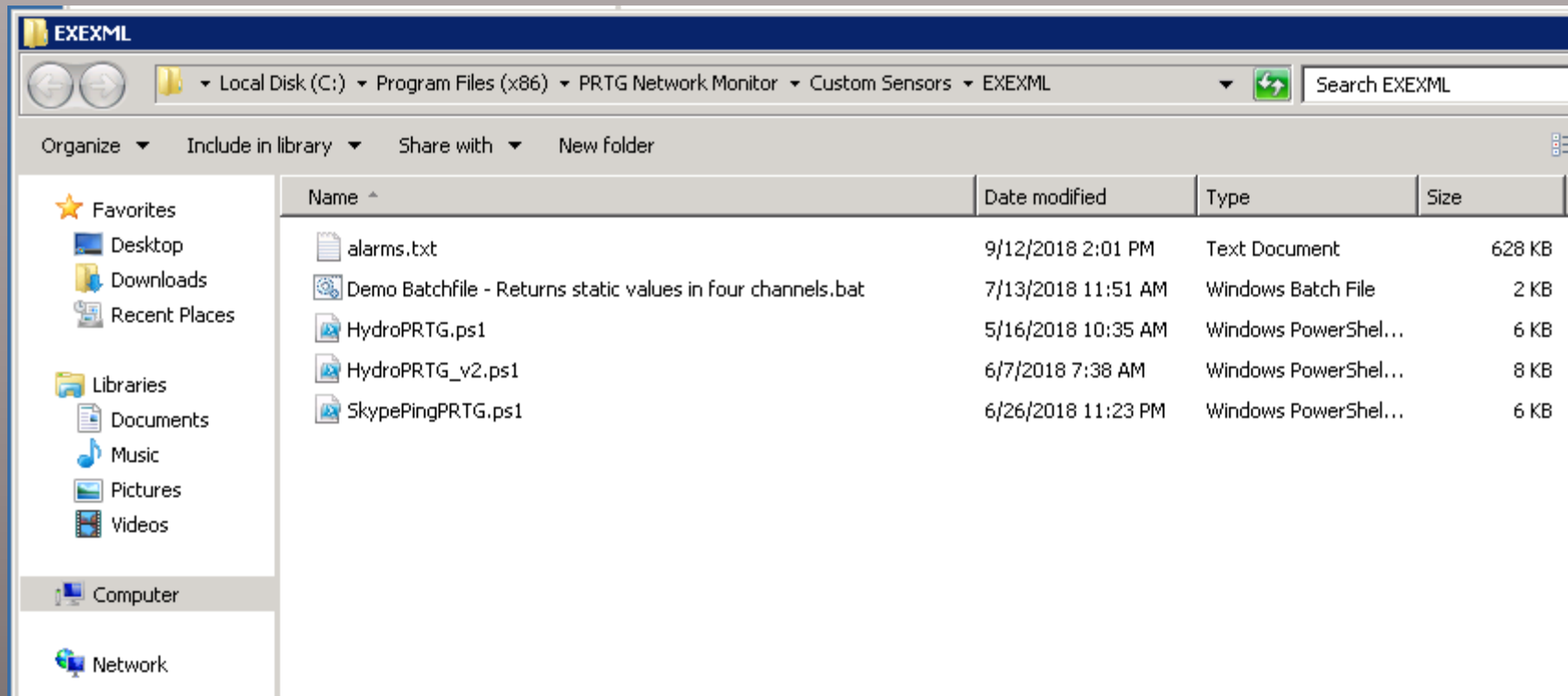
For details about the return value format, see section [Custom Sensors](#).



```
Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Create New Inbox Rule.ps1 HydroPRTG_v2.ps1 X

1 function Set-UseUnsafeHeaderParsing
2 { ... }
34
35 # create a table to store the information
36 $table = New-Object system.Data.DataTable "result"
37 $col1 = New-Object system.Data.DataColumn channel,string
38 $col2 = New-Object system.Data.DataColumn value,decimal
39 $col3 = New-Object system.Data.DataColumn unit,string
40 $col4 = New-Object system.Data.DataColumn warning,string
41 $col5 = New-Object system.Data.DataColumn index,int
42
43 $table.columns.add($($col1))
44 $table.columns.add($($col2))
45 $table.columns.add($($col3))
46 $table.columns.add($($col4))
47 $table.columns.add($($col5))
48
49 # this function produces a well-formatted prtg-xml-output out of a given table
50 function New-Xml
51 {
52     param($RootTag="prtg",$ItemTag="result", $ChildItems="*", $TextTag="OK", $Attributes=$Null)
53
54     Begin {
55         $xml = "<$RootTag>`n"
56     }
57     Process {
58     }
59     End {
60         $xml = "<$RootTag>`n"
61     }
62     Begin {
63     }
64     Process {
65     }
66     End {
67         param($RootTag="prtg",$ItemTag="result", $ChildItems="*", $TextTag="OK", $Attributes=$Null)
68     }
69 }
70 function New-Xml
71 # this function produces a well-formatted prtg-xml-output out of a given table
72
73 $table.columns.add($($col1))
74 $table.columns.add($($col2))
75 $table.columns.add($($col3))
76 $table.columns.add($($col4))
77 $table.columns.add($($col5))
78
79 # this function produces a well-formatted prtg-xml-output out of a given table
80 function New-Xml
81 {
82     param($RootTag="prtg",$ItemTag="result", $ChildItems="*", $TextTag="OK", $Attributes=$Null)
83
84     Begin {
85         $xml = "<$RootTag>`n"
86     }
87     Process {
88     }
89     End {
90         $xml = "<$RootTag>`n"
91     }
92     Begin {
93     }
94     Process {
95     }
96     End {
97         param($RootTag="prtg",$ItemTag="result", $ChildItems="*", $TextTag="OK", $Attributes=$Null)
98     }
99 }
100
```



EXE/Script Advanced



EXE/Script Advanced


[Overview](#) [Live Data](#) **24 hours** **10 days** **100 days** [Historic Data](#) [Log](#) [Settings](#) [Notification Triggers](#) [Comments](#) [History](#)

- This sensor > does not support more than 50 channels officially.
- The executable or script file must be stored on the system of the probe the sensor is created on: If used on a remote probe, the file must be stored on the system running the remote probe. In a cluster setup, please copy the file to every cluster node.
- We recommend Windows 2012 R2 on the probe system for best performance of this sensor.
- If you want to execute a custom Windows Management Instrumentation Query Language (WQL) script, please use the > WMI Custom Sensor.
- Knowledge Base: > What is the Mutex Name in PRTG's EXE/Script Sensor's settings?
- Knowledge Base: > How can I test if parameters are correctly transmitted to my script when using an EXE/Script sensor?
- Knowledge Base: > How can I show special characters with EXE/Script sensors?
- Knowledge Base: > Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?
- Knowledge Base: > How can I use meta-scans for custom EXE/Script sensors?
- Knowledge Base: Why do I have to store SQL sensor queries and custom scripts in files on the probe computer?
- > <https://kb.paessler.com/en/topic/75372>

Save 



Basic Sensor Settings

Sensor Name ⓘ

Hydro Info 

Parent Tags ⓘ

Tags ⓘ

xmlexesensor  

Priority ⓘ

★★★★☆☆

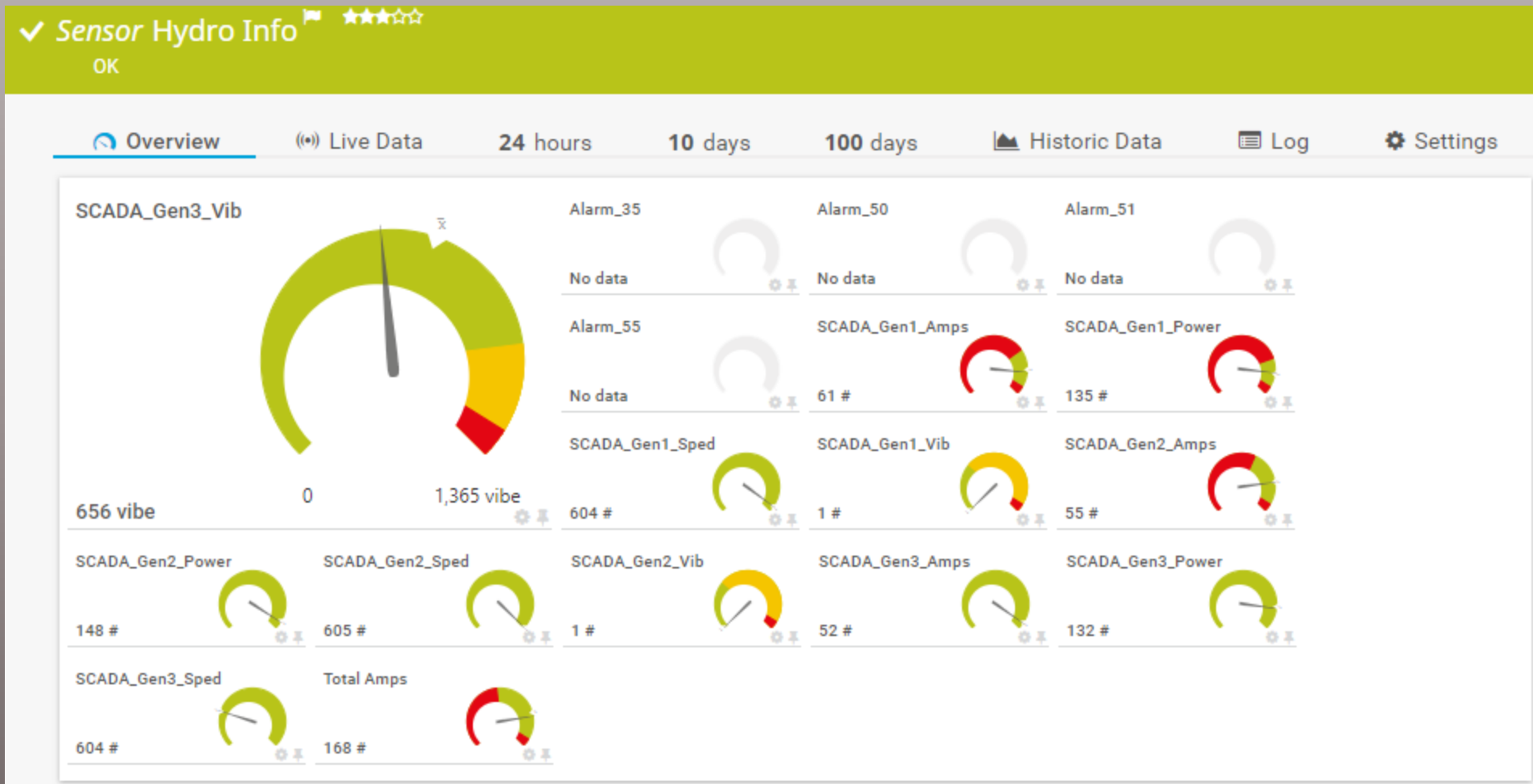
Sensor Settings

EXE/Script ⓘ

HydroPRTG_v2.ps1

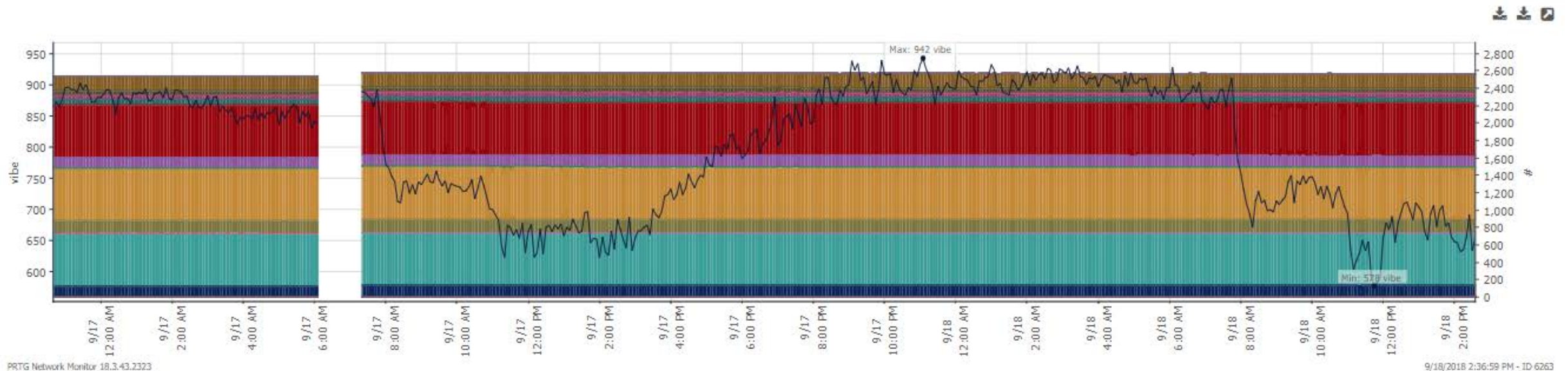
Important: The EXE file has to run on the computer where the parent probe is installed, not on the parent device. The working directory for EXE files is the probe directory. vbs,ps1 or other script files may use different working directories.

EXE/Script Advanced



Overview Live Data 24 hours 10 days 100 days Historic Data Log Settings Notification Triggers Comments History

Last Scan: 111 s Last Up: 111 s Last Down: 5 d 22 h 29 m Uptime: 99.5321% Downtime: 0.4679% Coverage: 97% Sensor Type: EXE/Script Advanced Dependency: Parent Interval: every 5 m ID: #6263



PRTG Network Monitor 18.3.43.2323

9/18/2018 2:36:59 PM - ID 6263



- | | | | | |
|--|--|---|---|---|
| <input checked="" type="checkbox"/> SCADA_Gen1_Power (#) | <input checked="" type="checkbox"/> SCADA_Gen1_Sped (#) | <input checked="" type="checkbox"/> SCADA_Gen1_Vib (#) | <input checked="" type="checkbox"/> SCADA_Gen2_Power (#) | <input checked="" type="checkbox"/> SCADA_Gen2_Sped (#) |
| <input checked="" type="checkbox"/> SCADA_Gen2_Vib (#) | <input checked="" type="checkbox"/> SCADA_Gen3_Power (#) | <input checked="" type="checkbox"/> SCADA_Gen3_Sped (#) | <input checked="" type="checkbox"/> SCADA_Gen3_Vib (vibe) | <input checked="" type="checkbox"/> SCADA_Gen1_Amps (#) |
| <input checked="" type="checkbox"/> SCADA_Gen2_Amps (#) | <input checked="" type="checkbox"/> SCADA_Gen3_Amps (#) | <input checked="" type="checkbox"/> Total Amps (#) | <input checked="" type="checkbox"/> Alarm_35 (#) | <input checked="" type="checkbox"/> Alarm_51 (#) |
| <input checked="" type="checkbox"/> Alarm_55 (#) | <input checked="" type="checkbox"/> Alarm_50 (#) | | | |

[Show all](#) [Hide all](#)

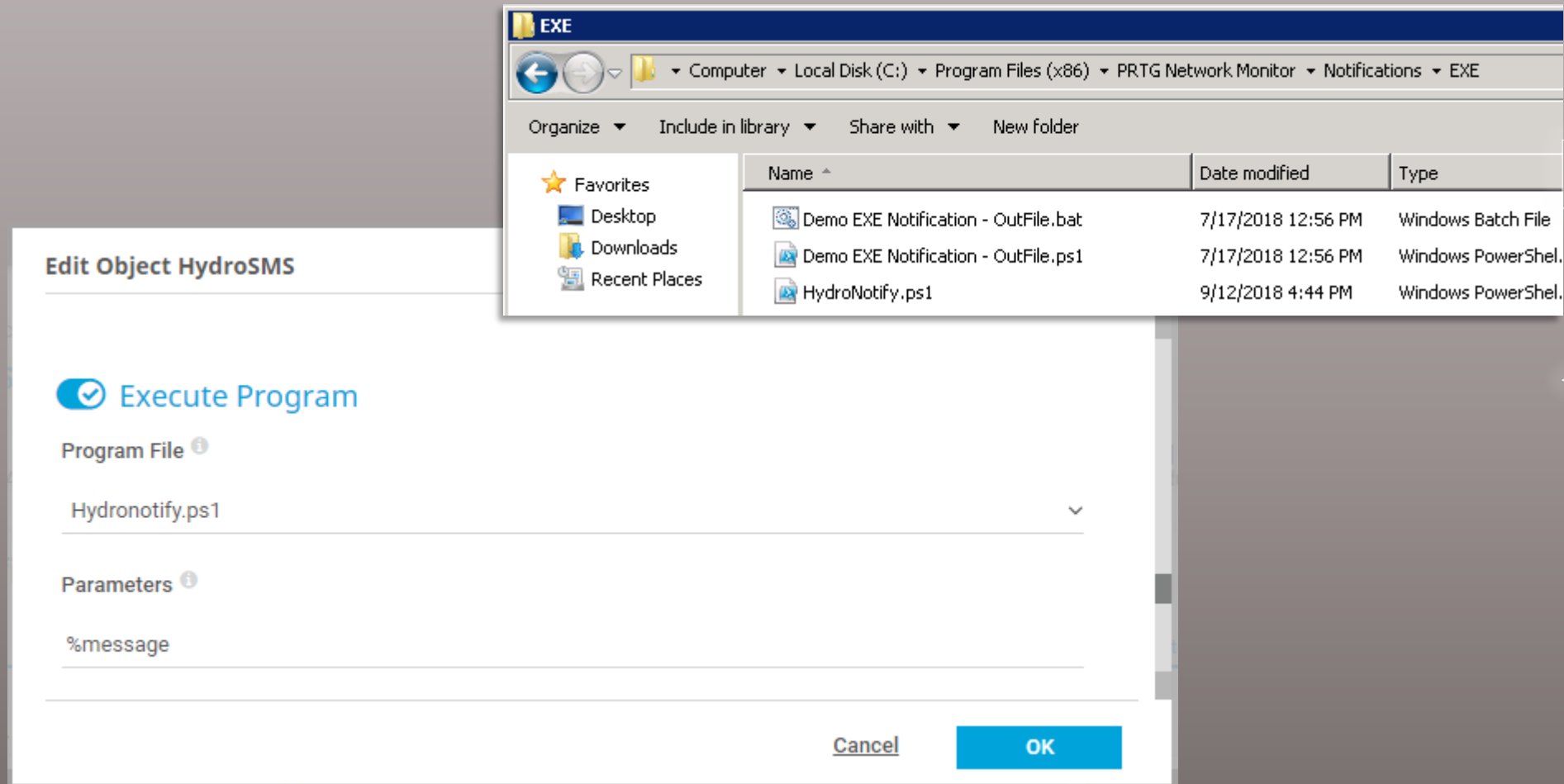
Things PRTG alarm notify by itself:

- Send the sensor name, value, status, Up/Downstate by:
 - SMS (with paid provider)
 - Email
 - Slack / M\$ Teams channel msg
 - SNMP trap
 - Syslog message
 - Mobile App push message
 - HTTP webpage call
 - Create an internal PRTG ticket
- Notification repeat & sensor back up notification

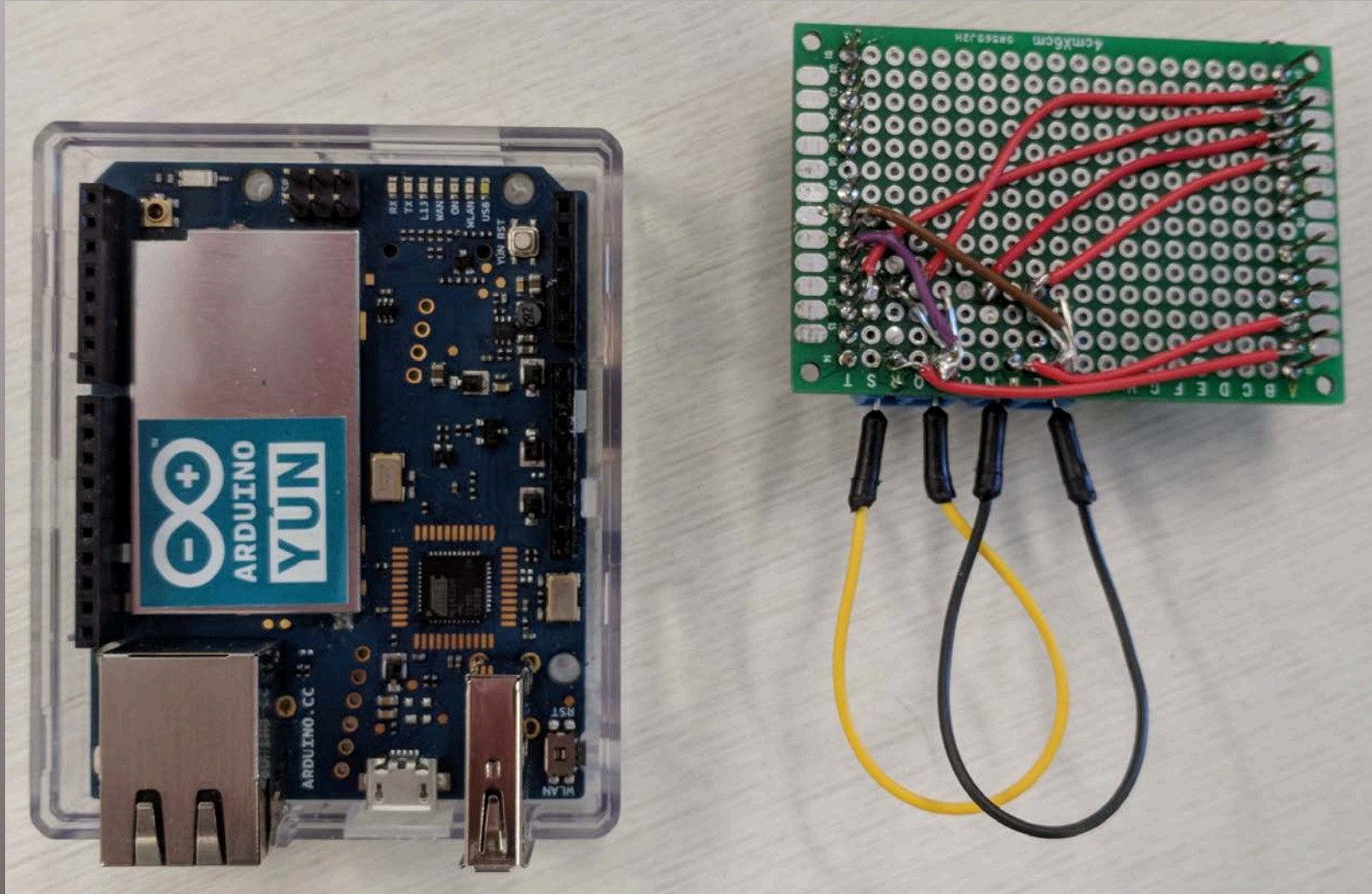
Things you can do with PRTG calling your exe / PowerShell script:



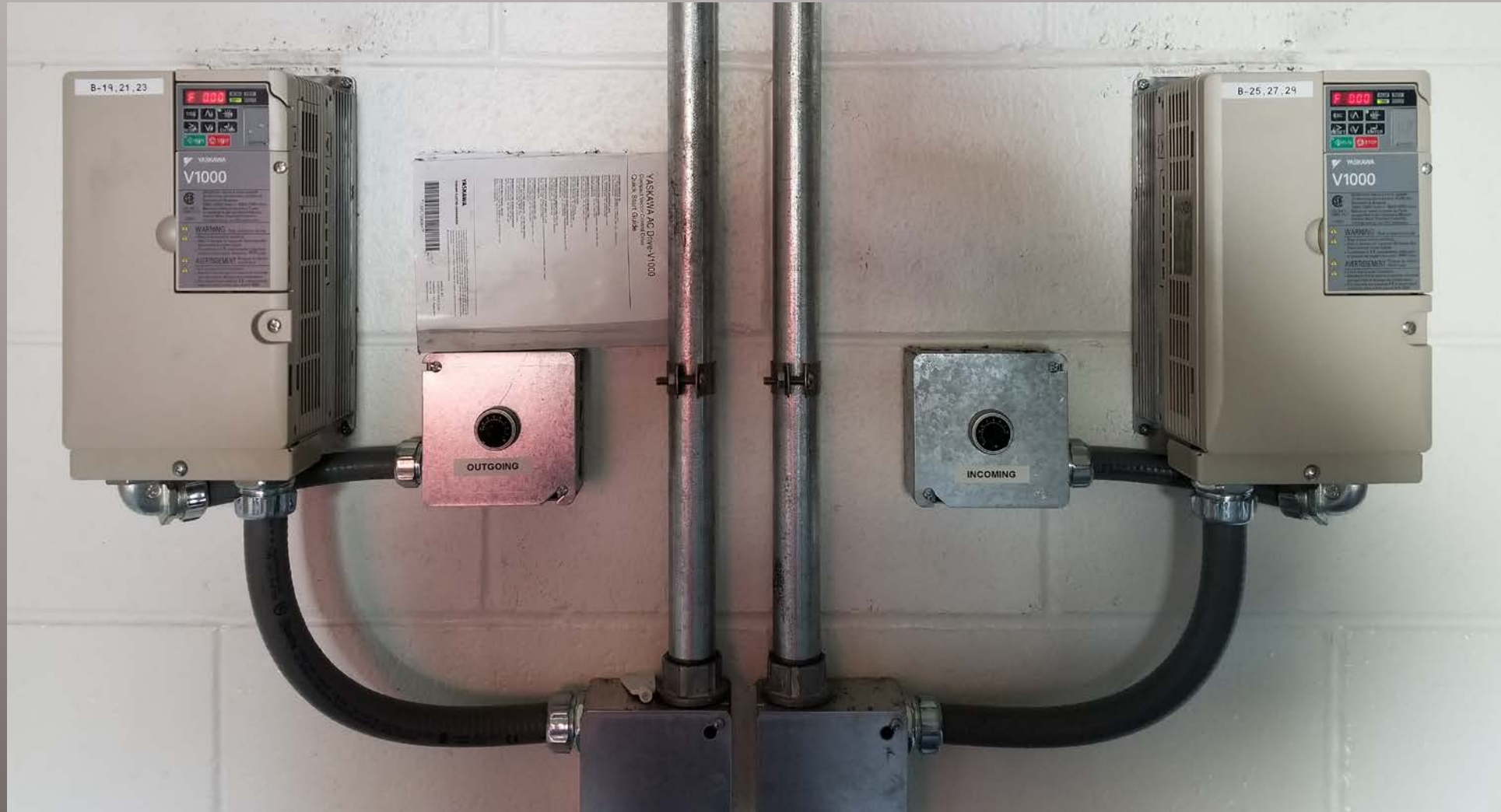
Custom alarm notification script



Custom environmental monitoring using Arduino Yún



Custom environmental monitoring using Arduino Yún



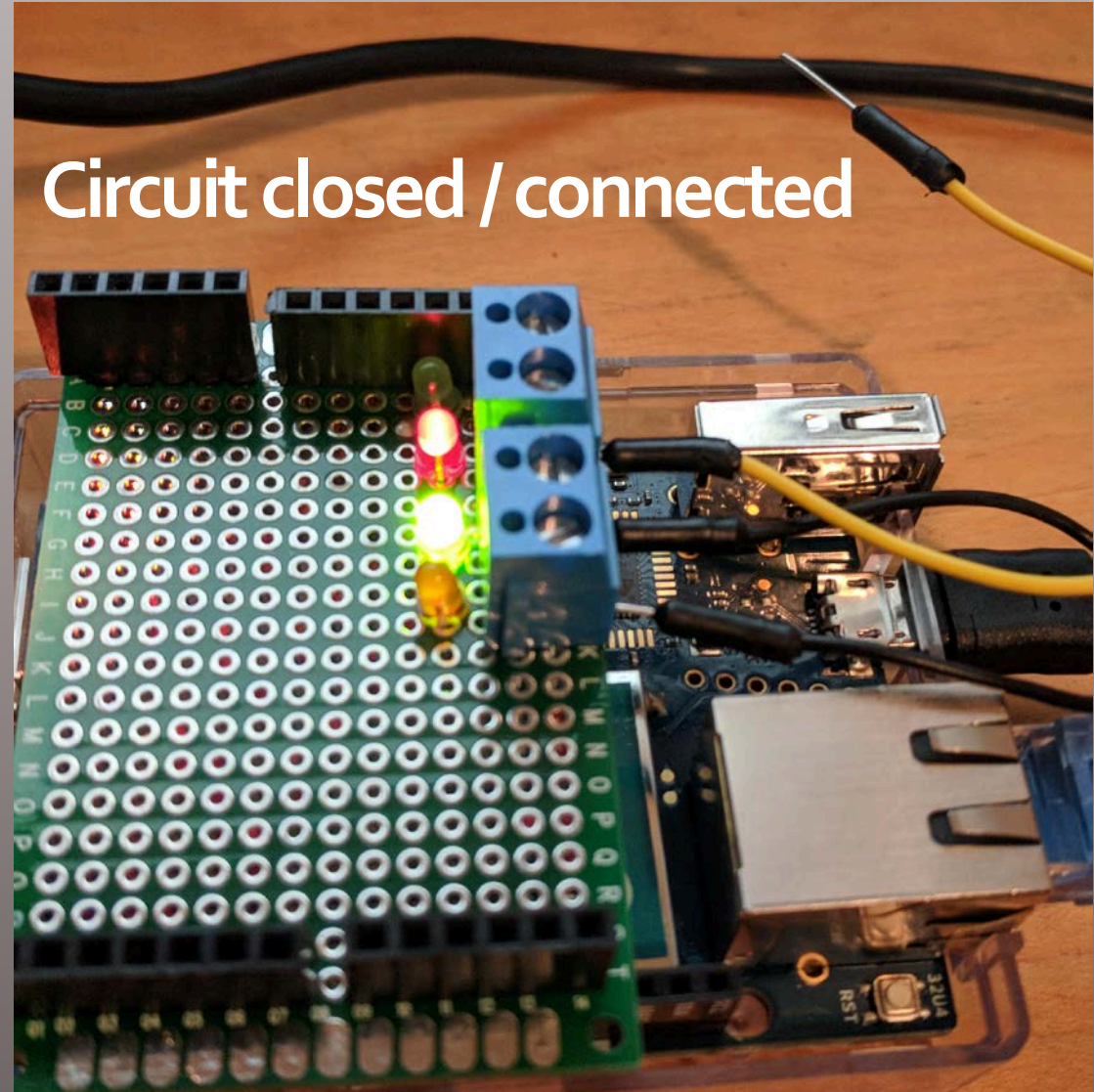
Variable Frequency Drive motor controllers

Custom environmental monitoring using Arduino Yún

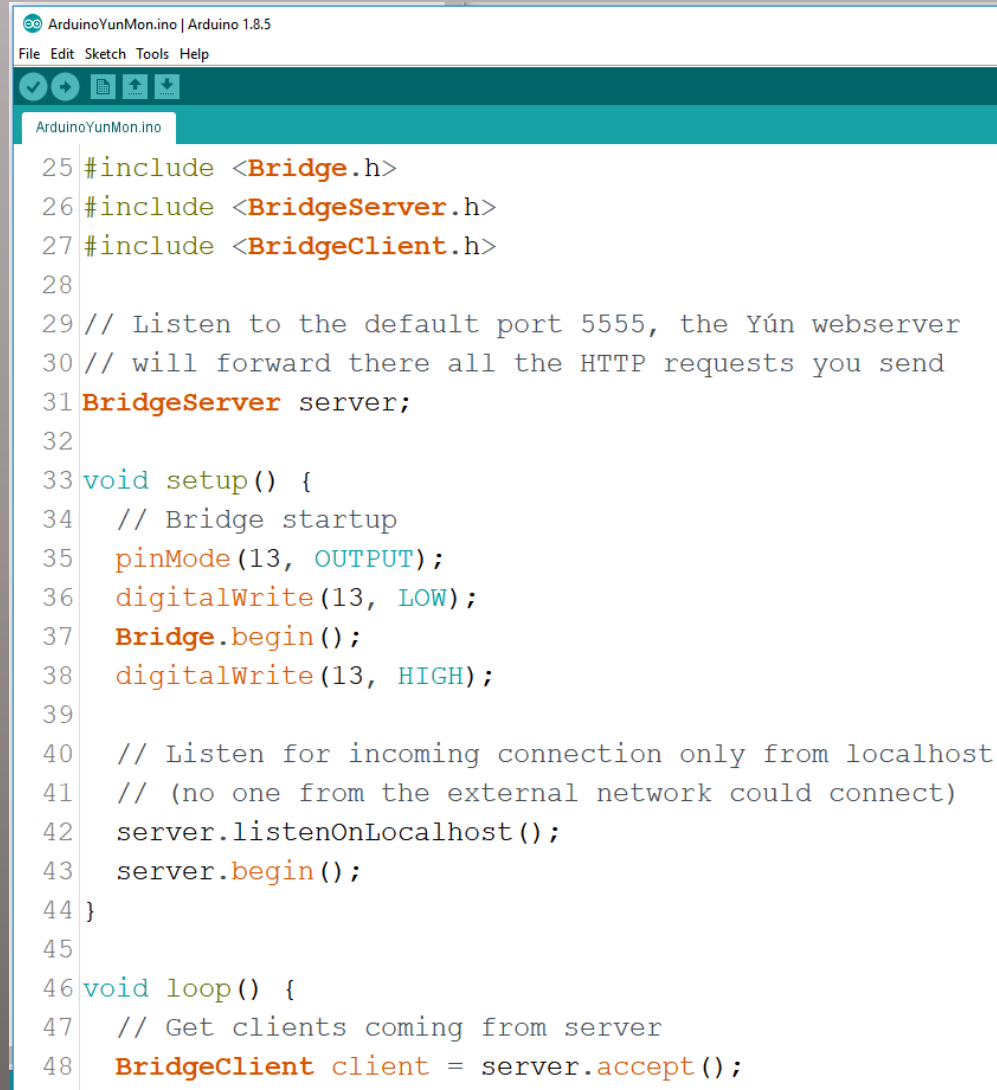


Custom environmental monitoring using Arduino Yún

Circuit closed / connected



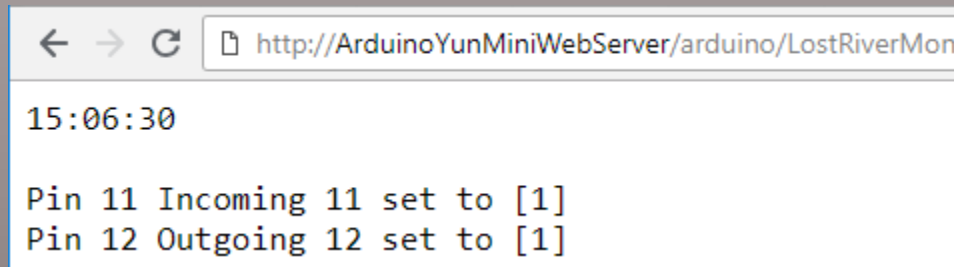
Custom environmental monitoring using Arduino Yún

A screenshot of the Arduino IDE interface. The title bar shows 'ArduinoYunMon.ino | Arduino 1.8.5'. The menu bar includes 'File', 'Edit', 'Sketch', 'Tools', and 'Help'. Below the menu bar is a toolbar with icons for opening, saving, and running. The main text area displays the code for 'ArduinoYunMon.ino'. The code includes headers for Bridge, BridgeServer, and BridgeClient, sets up a BridgeServer on port 5555, and configures a digital pin (13) as an output. It also includes a loop function that accepts clients from the server.

```
25 #include <Bridge.h>
26 #include <BridgeServer.h>
27 #include <BridgeClient.h>
28
29 // Listen to the default port 5555, the Yún webserver
30 // will forward there all the HTTP requests you send
31 BridgeServer server;
32
33 void setup() {
34   // Bridge startup
35   pinMode(13, OUTPUT);
36   digitalWrite(13, LOW);
37   Bridge.begin();
38   digitalWrite(13, HIGH);
39
40   // Listen for incoming connection only from localhost
41   // (no one from the external network could connect)
42   server.listenOnLocalhost();
43   server.begin();
44 }
45
46 void loop() {
47   // Get clients coming from server
48   BridgeClient client = server.accept();
```

<https://github.com/binarybuddha/PRTGhax/blob/master/ArduinoYunMon.ino>

Custom environmental monitoring using Arduino Yún



A screenshot of a web browser window. The address bar shows the URL `http://ArduinoYunMiniWebServer/arduino/LostRiverMon`. The page content displays a timestamp `15:06:30` followed by two lines of status information: `Pin 11 Incoming 11 set to [1]` and `Pin 12 Outgoing 12 set to [1]`. The text is rendered in a monospaced font.

```
← → ↻ http://ArduinoYunMiniWebServer/arduino/LostRiverMon  
15:06:30  
Pin 11 Incoming 11 set to [1]  
Pin 12 Outgoing 12 set to [1]
```




Custom environmental monitoring using Arduino Yún

Add Sensor to Device Lost River [Your Arduino IP]

(Step 2 of 2)

< Cancel

Basic Sensor Settings

Sensor Name ⓘ	Custom HTTP Content 
Parent Tags ⓘ	
Tags ⓘ	httpsensor  
Priority ⓘ	★★★★☆☆

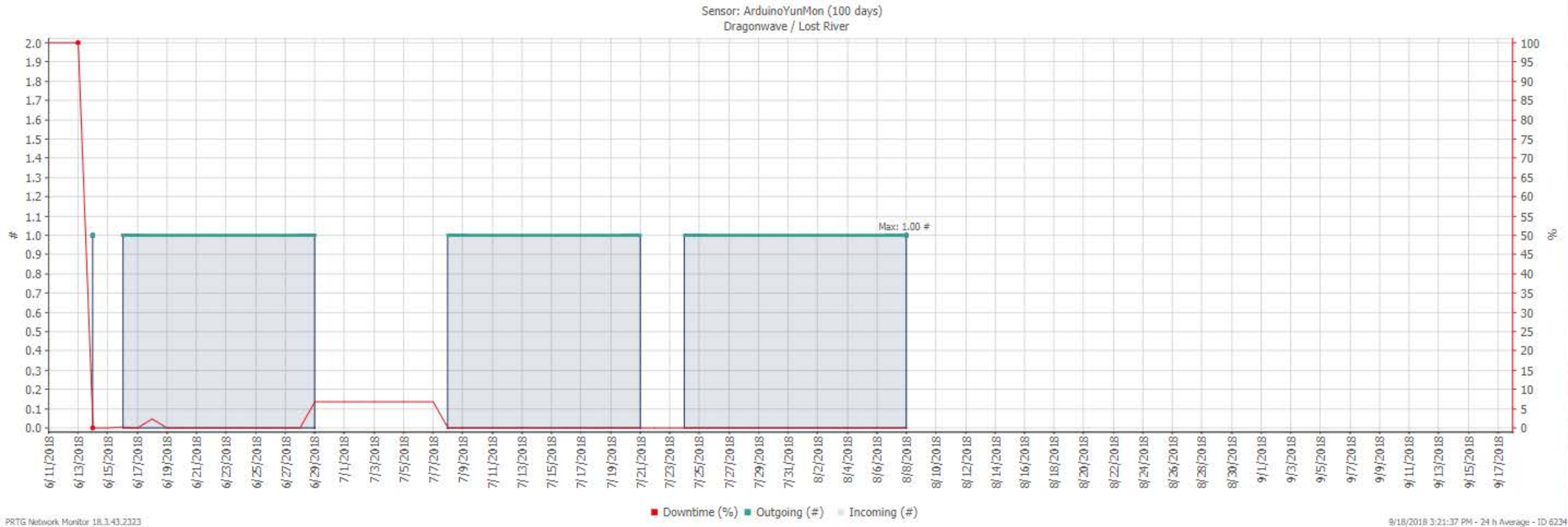
Create



HTTP Specific

Timeout (Sec.) ⓘ	60
Script URL ⓘ	https://YourArduinoIP/arduino/PageName
Value Type ⓘ	<input checked="" type="radio"/> Integer <input type="radio"/> Float
Number of channels ⓘ	2

Custom environmental monitoring using Arduino Yún



Custom environmental monitoring using Arduino Yún

Notification Triggers

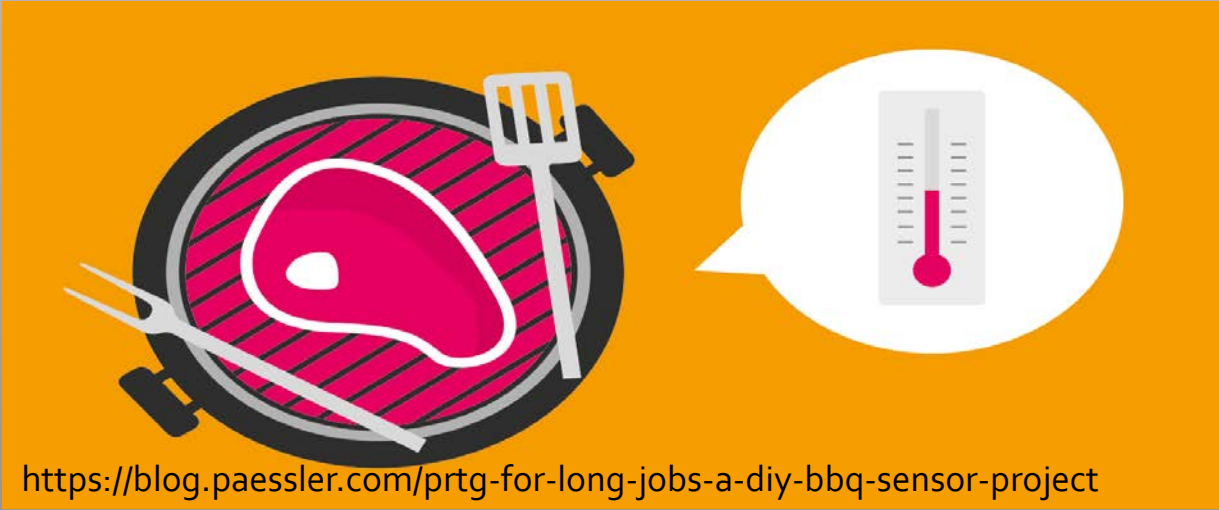
Type ^	Rule	Actions
State Trigger	When sensor state is <u>Down</u> v for at least <u>300</u> seconds perform <u>LostRiverVFDmon</u> v	<div><div>✓</div><div>x</div></div>
	When sensor state is Down for at least <u>830</u> seconds perform <u>15min-LostRiverVFDmon</u> v and repeat every <u>15</u> minutes	
	When condition clears after a notification was triggered perform <u>Push notification to admins 6-</u> v	

Triggers that can be inherited from parent object(s)

- ☐ Inherit all triggers from parent objects and use the triggers defined above
- ☒ Only use the triggers defined above

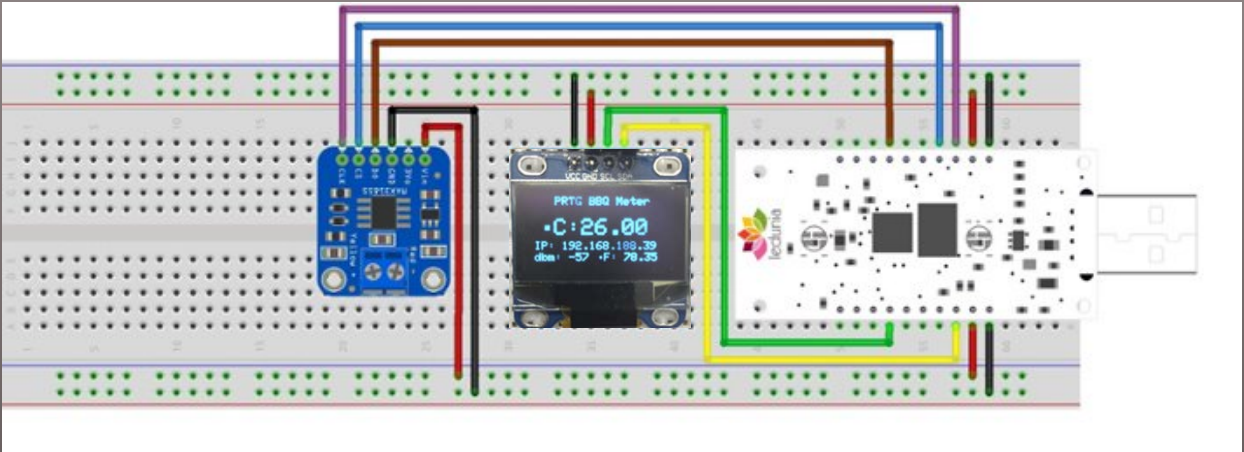
Type ^	Rule	Inherited from
State Trigger	When sensor state is Down for at least 600 seconds perform > Push notification to admins 6-8	<div><div>Your Groovy Corp</div></div>
	When sensor state is Down for at least 900 seconds perform <u>no notification</u> and repeat every 0 minutes	
	When condition clears after a notification was triggered perform > Push notification to admins 6-8	

Superior application for MCU+PRTG:



What Should The Result Look Like Or What Is Actually The Goal Of Monitoring Regarding BBQs?

The following images should provide the necessary incentive to develop [hardware](#) for this and to answer the question as to why a perfect result requires such monitoring.



Superior application for MCU+PRTG:

BASIC SENSOR SETTINGS

Sensor Name

BBQ ledunia

Parent Tags

Tags

restcustomsensor × restsensor ×

Priority

★★★★★

REST SPECIFIC

Timeout (Sec.)

60

Request Method

● GET (default)

○ POST

Request Protocol

● HTTP (default)

○ HTTPS

Authentication Method

● No authentication (default)

○ Basic authentication

○ Token

HTTP Headers

● Do not use custom HTTP headers

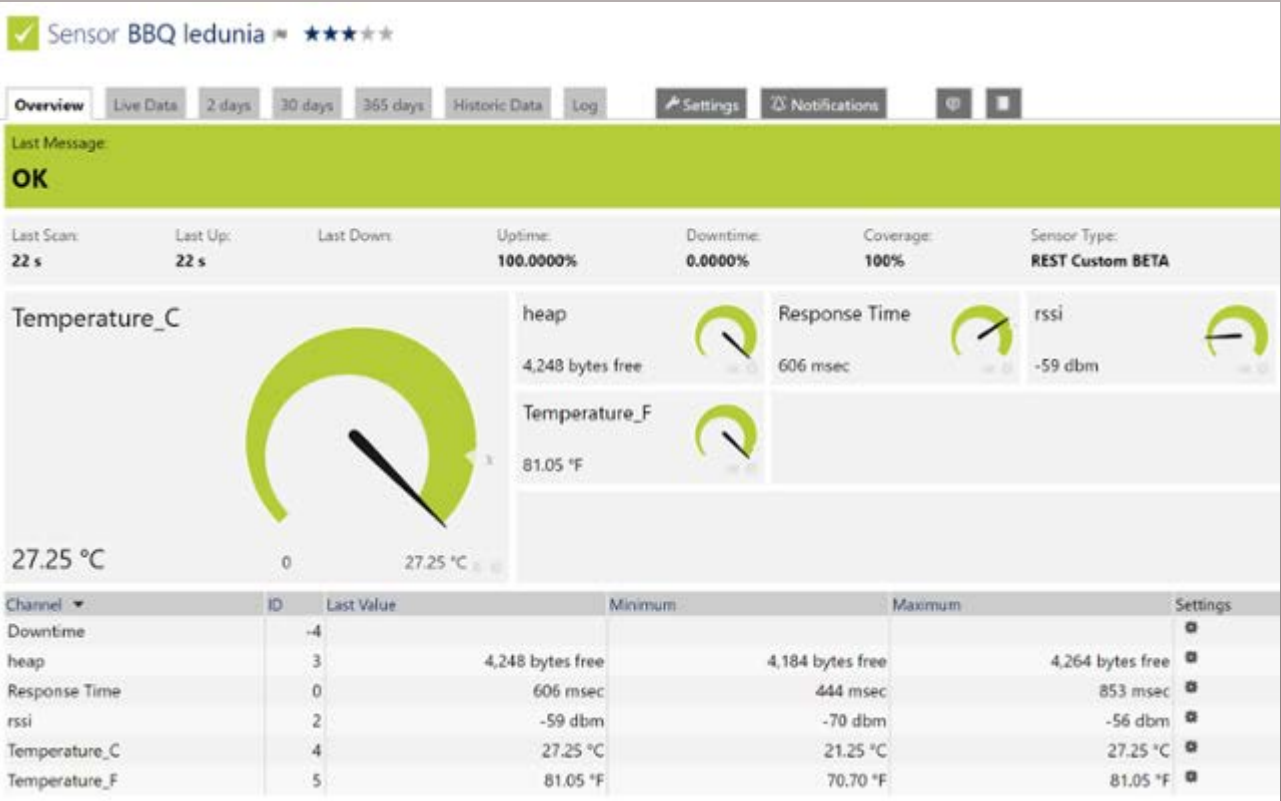
○ Use custom HTTP headers

REST Query

/

REST Configuration

channelDiscovery



InfoSec relevance:

- Your crazy expensive Cisco DNA deployment is useless if your basic services are down.
- PRTG is a decent monitoring platform as when Active Directory is used.
- PowerShell can't easily make charts, push to mobile apps, etc.
- Reasonably easy to interface custom data / notifications



[https://github.com/binarybuddha/
PRTGhax/](https://github.com/binarybuddha/PRTGhax/)



PRTGhax@BinaryBuddha.com



@binarybuddha



SSN: 404-4-1057



P.O. Box 712 Buhl, ID 83316