

SERVERSCHECK

www.serverscheck.com

ServersCheck Monitoring Software And Monitoring Appliance User Manual

Copyright:

Copyright © 2023 InfraSensing BV
All rights reserved.
Reproduction without permission is prohibited.

Software:

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Trademarks:

ServersCheck is a trademark of InfraSensing .
All other trademarks or registered marks in this manual belong to their respective manufacturers.

Disclaimer:

Information in this document is subject to change without notice and does not represent a commitment on the part of InfraSensing.

InfraSensing provides this document “as is,” without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. InfraSensing reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

InfraSensing has made this document to the best of its abilities. However InfraSensing assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Warranty:

For the warranty on this product please visit [https:// InfraSensing.com/](https://InfraSensing.com/)
OPENING SENSOR GATEWAY OR EXTERNAL SENSOR PROBE VOIDS THE WARRANTY

Table of Content

1. Introduction	6
1.1. ServersCheck Monitoring Software	6
1.2. What's New on version 14+	6
1.3. ServersCheck Monitoring Appliance	7
1.4. Overview of the Appliance	7
1.5. Technical Specifications	7
1.6. Image and Parts of the Appliance	8
1.7. Powering the Appliance	8
1.8. Other Pre-installed software	9
1.9. Installation Requirements of The Monitoring Software	9
2. Getting Started	10
2.1. Installing the Software on Windows	10
2.2. Things to Check before Accessing the Software	14
2.3. Upgrading the Monitoring Software	16
2.4. Accessing the Monitoring Software	19
2.5. Default View for your Monitoring checks	20
2.6. Choosing the Network adapter to use	21
2.7. Setting up Email Alerts	22
2.7.1. Using The Built-In Mail Server	23
2.7.2. Using Your ISP's Mail Server or Open SMTP Server	25
2.7.3. Using SMTP Server	26
2.7.4. Using IMAP Server	27
2.7.5. Using GMAIL	28
2.8. Configuring SMS	32
2.9. Setting Slack Alerts	37
2.10. Setting up Username and Password	40
2.11. Activating the License of your Software	41
3. Setting up Your First Checks	46
3.1. Adding ServersCheck Sensors (Environment, Power, Security, Industrial) & Controls	46
3.2. Editing a Sensor/Check	50

3.3.	Editing a Device and Adding Location	54
3.4.	Adding a Floor Plan	58
3.5.	Adding a Thermal Image	64
3.6.	Controlling Outputs and Relays.....	66
4.	Setting up Other Check Types	67
4.1.	Adding Checks for 3rd Party Sensors (SNMP).....	67
4.2.	Adding Checks for Network Connections	69
4.2.1.	Adding Ping Check	69
4.2.2.	Adding Internet Speed test Check.....	71
4.2.3.	Adding Domain Name Resolution Check.....	73
4.2.4.	Adding Domain Name Expiry Check.....	75
4.2.5.	Adding TCP Port Check.....	77
4.3.	Adding Checks for Network Devices (Routers, Switches, Printers).....	79
4.3.1.	Adding Network Devices via Ping Check.....	79
4.3.2.	Adding Network Devices via TCP Port Check.....	81
4.3.3.	Adding Network Devices via SNMP Check.....	83
4.4.	Adding Checks for Servers (Windows & Linux)	85
4.4.1.	Adding Checks for Windows Servers	87
4.4.2.	Adding Checks for Linux Servers.....	89
4.4.3.	Adding Checks for System Uptime (SNMP)	91
4.4.4.	Adding Checks for SNMP Numeric	93
4.5.	Adding Checks for Websites	95
4.5.1.	Adding SSL Certificate Validity Check.....	95
4.5.2.	Adding HTTP Status Code Check.....	97
4.5.3.	Adding HTTP Header Check	99
4.5.4.	Adding URL Contains Check	101
4.5.5.	Adding URL Contains Check	103
5.	Generating Reports	105
5.1.	Generating By Sensor Names	105
5.2.	Generating By Sensor Types	108
6.	Alerts History	111
7.	Adding Security to your Monitoring Software.....	112
7.1.	NGINX (reverse proxy server).....	116
7.1.1.	Configuring NGINX.....	116

7.2. Running the software on HTTPS mode.....	116
8. Running on Debug Mode.....	117
8.1. Steps to run in Debug Mode.....	117
9. Support Forum	118

1. Introduction

1.1. ServersCheck Monitoring Software

The ServersCheck software is a browser-based tool for monitoring, reporting and alerting on system availability.

It enables you to:

- **Monitor Infrastructure Sensors** - monitor our very own set of sensors <https://ServersCheck.com/sensors/> and any other 3rd party sensors.
- **Network Monitoring** - perform monitoring checks of your own network and also your ISP network.
<https://ServersCheck.com/monitoring-software/network-monitoring.asp>
- **Systems and Server Monitoring** - able to monitor infrastructure and network layers in a server room. And also the systems running in your data center environment: physical, virtual or cloud based
<https://ServersCheck.com/monitoring-software/server-monitoring.asp>
- **Web Applications Monitoring** - ability to monitor the availability and performance of applications running on your environment.
<https://ServersCheck.com/monitoring-software/application-monitoring.asp>

1.2. What's New on version 14+

This is the new version of the ServerCheck Monitoring Software.

- Responsive interface working on any platform: desktop, smart phone or tablet.
- Complete redesign of the software's back-end engine for performance.
- New graphing engine (client based)
- HTML5 powered
- Support for all sensors
- Control capabilities (for IO controls on Sensorhub)
- Desktop notifications via Chrome and Firefox including badge notifications
- Thermal and humidity heat maps redesigned
- Leak maps showing location of water leaks
- Support for 3rd party SNMP sensors

1.3. ServersCheck Monitoring Touch Appliance



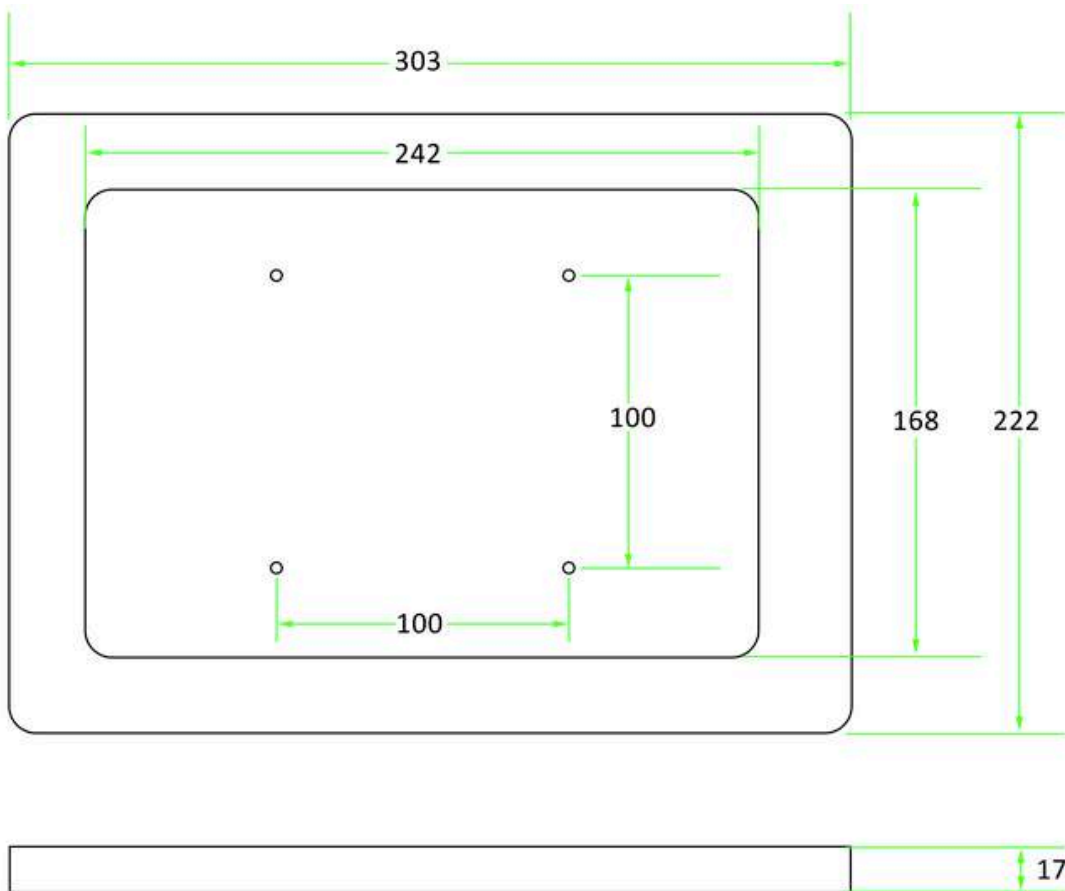
1.4. Overview of the Appliance

The Appliance is a small IOT device with the award winning ServersCheck Monitoring software preloaded and optimized. This award winning software and appliance enables you to centrally monitor, report and alert on your ServersCheck sensors and additional checks. With its innovative design, you can also monitor 3rd party sensors, your network and servers.

1.5. Technical Specifications

- Operating System: Windows 10 Enterprise IoT
- Processor (CPU) : Intel® Pentium® Gold Processor 4425Y / Intel Core M with the optional MON-TOUCH2-LTE
- Memory (RAM) : 4 GB DDR3L / 8GB with the optional MON-TOUCH2-LTE
- GPU : Intel® UHD Graphics 615
- Default Storage : 64 GB / 128 GB with the optional MON-TOUCH2-LTE (can be expanded up to 1TB via SD card)
- Network : Wifi 2.4 and 5 Ghz
- Software : ServersCheck Monitoring Software

1.6. Image and Parts of the Appliance



1.7. Powering the Appliance

1. Connect the following for the initial setup:
 - a. USB keyboard and mouse to any of the USB ports
 - b. HDMI cable for monitor capability
 - c. Using a Micro USB adapter, power the device on (you should see a red light)
2. Press and hold the power button for 10-15 seconds or until the initial image is shown on your screen.
3. Log in using the password "admin" (all in lower-case) under the username ServersCheck.

Note: Any standard USB adapter (such as a cell phone wall charger) with **at least 2A of current** can be used as a power supply. A standard PoE connection can be used as well.

1.8. Other Pre-installed software

In addition to the Monitoring Software, the ff. comes pre-configured on the device:

- Device drivers for Display, Network Adapter, sound, USB, Wifi and Bluetooth
- Optimized Operating System with additional software as needed by ServersCheck

The appliance firewall and network configuration are already optimized to work with the ServersCheck Monitoring Software.

The appliance is made out of the box and start adding checks on your monitoring platform simply by knowing the IP address assigned to your Appliance. (See Section 2.3)

1.9. Installation Requirements of The Monitoring Software

Minimum System Requirements:

- * Processor: Intel Cherry Trail Z8300 Quad Core 1.8GHz
- * Operating System: Pre-installed full edition of Windows 10
- * RAM: 2GB DDR3L
- * Storage Capability: 32GB
- * GPU: Intel HD Graphics, 12 EUs @200-500 Mhz, single-channel memory
- * Windows 7, 8, 10 - Windows Server 2008, 2012 and 2016 (32 bit)
- * Browser: Internet Explorer 10+, Firefox 4+ (Recommended), Safari 6+, Google Chrome 32.0.1700+
- * A TCP/IP protocol stack.

Windows System Requirements:

* **PORT 1272** -- ServersCheck operates by using port 1272. You must ensure that there is no proxy client, such as ISA, running that could prevent ServersCheck from starting its internal webserver.

* **SMS Alerting** -- In order to receive alerts through SMS we recommend for you to Purchase Premium Credits.

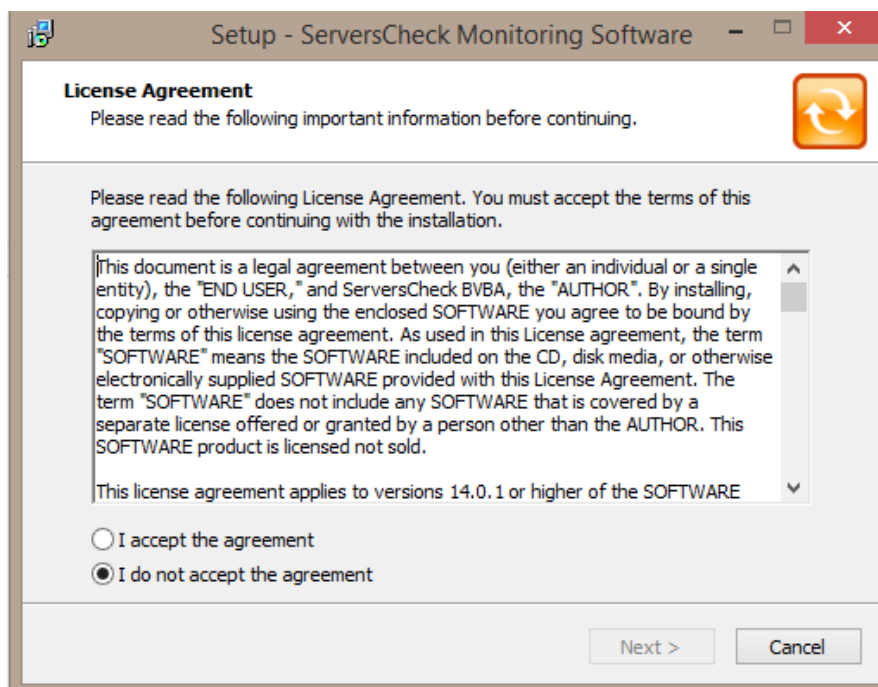
* **Requires Administrative privilege on the computer**

* **with software version 15 and above you can also access the software on port 80 by default**

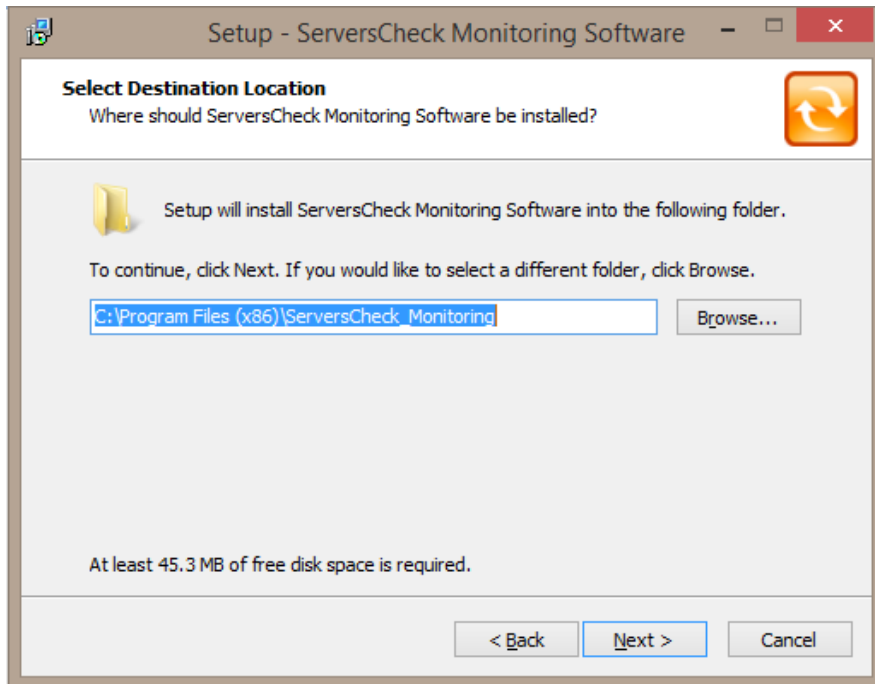
2. Getting Started

2.1. Installing the Software on Windows

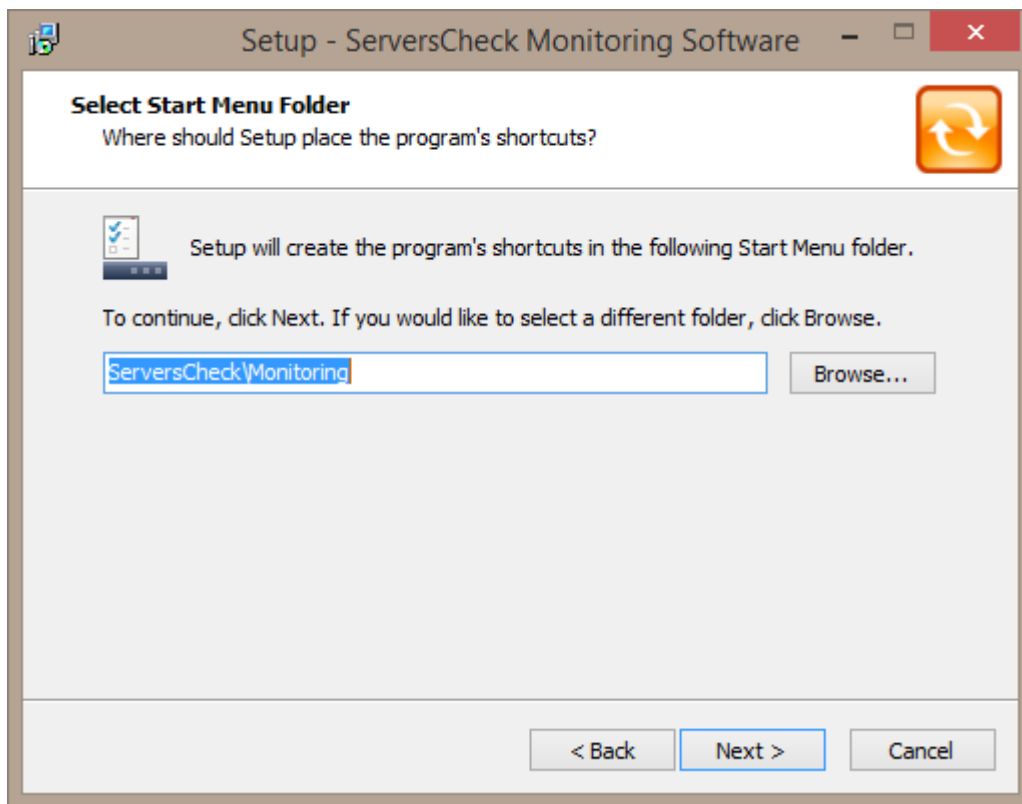
1. Double click the installation file (setup.exe) to start the installation program. Make sure to be logged in as an Administrator on the system on which you will install the software.
2. Follow the on-screen instructions.
3. You will be prompted to accept the terms of the license agreement before you



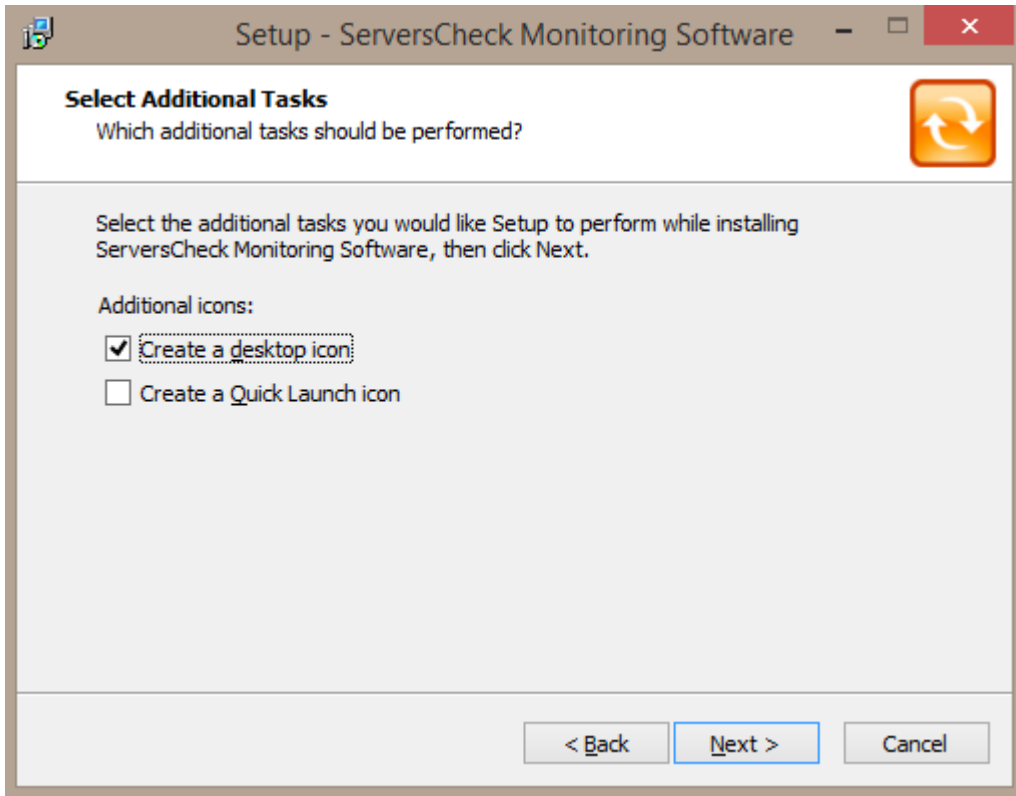
- Next is to specify the target directory to which the application needs to be installed.



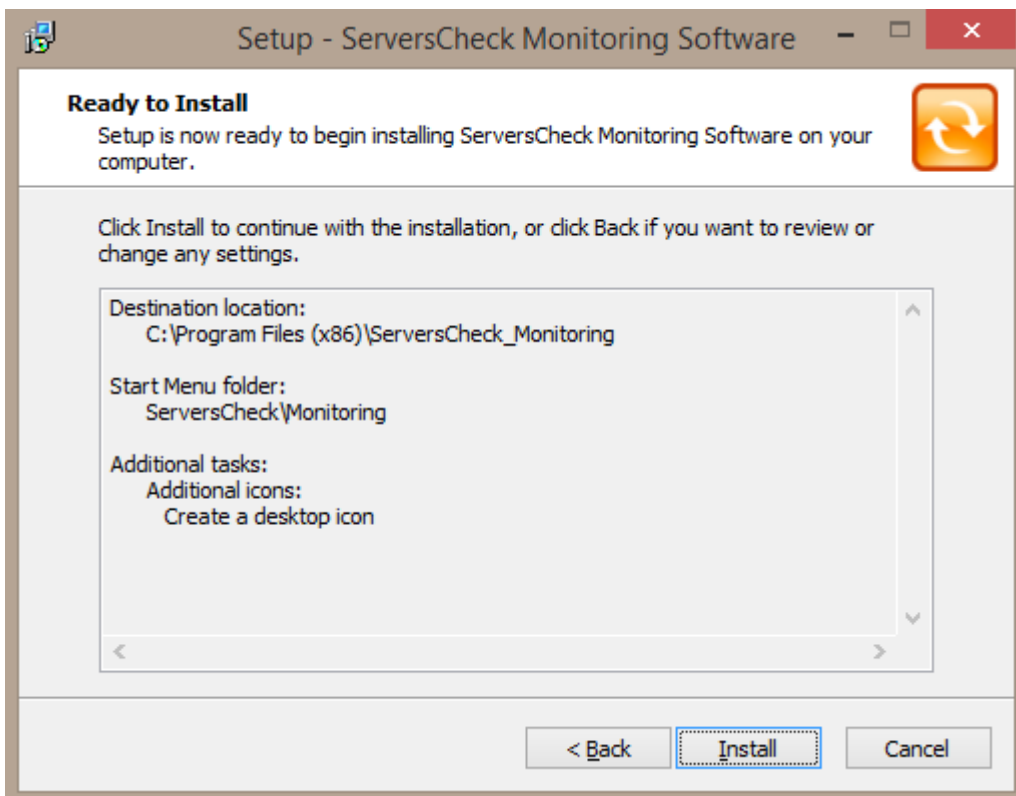
- Start menu items are created on this step. Most users will not need to change this.



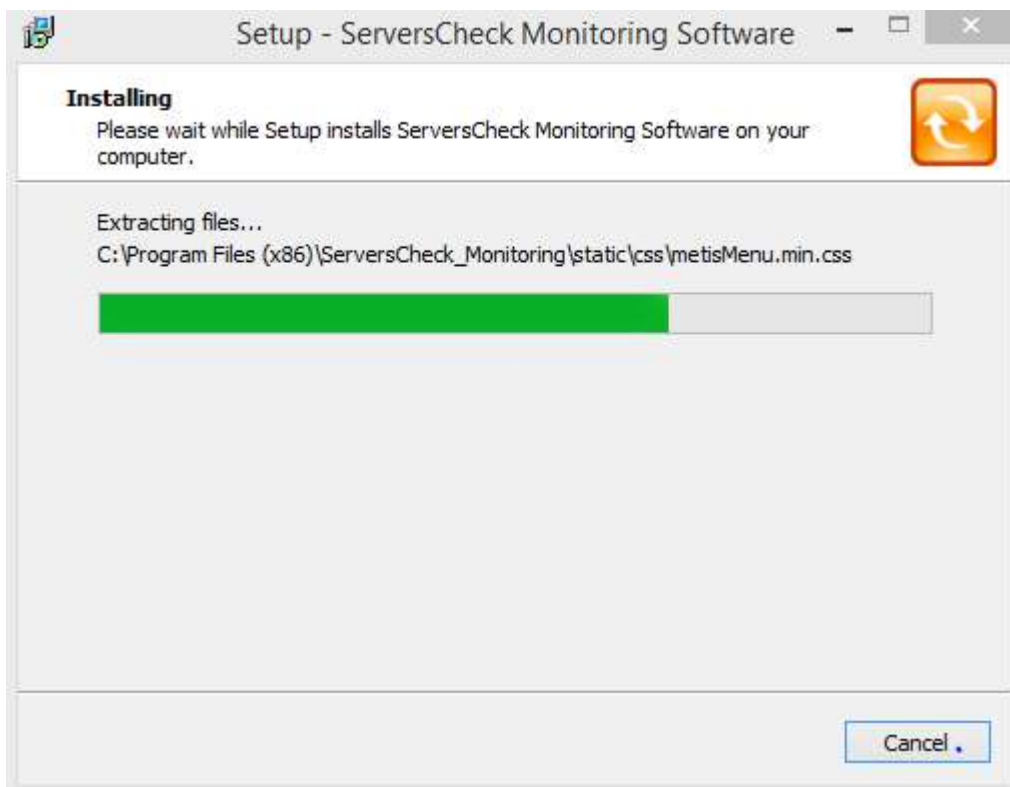
6. Additional options can be configured in this step.



7. An installation summary is then displayed before installation begins.



- The Files are then copied to the specified target directory and the ServersCheck service will automatically be installed as a service.



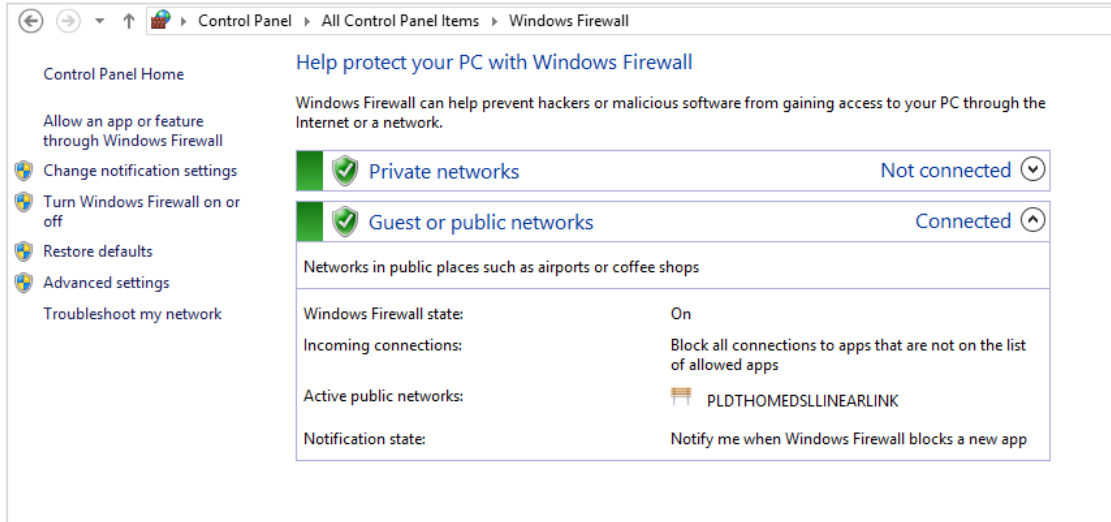
- Installation is completed and the Monitoring Software is ready for use.



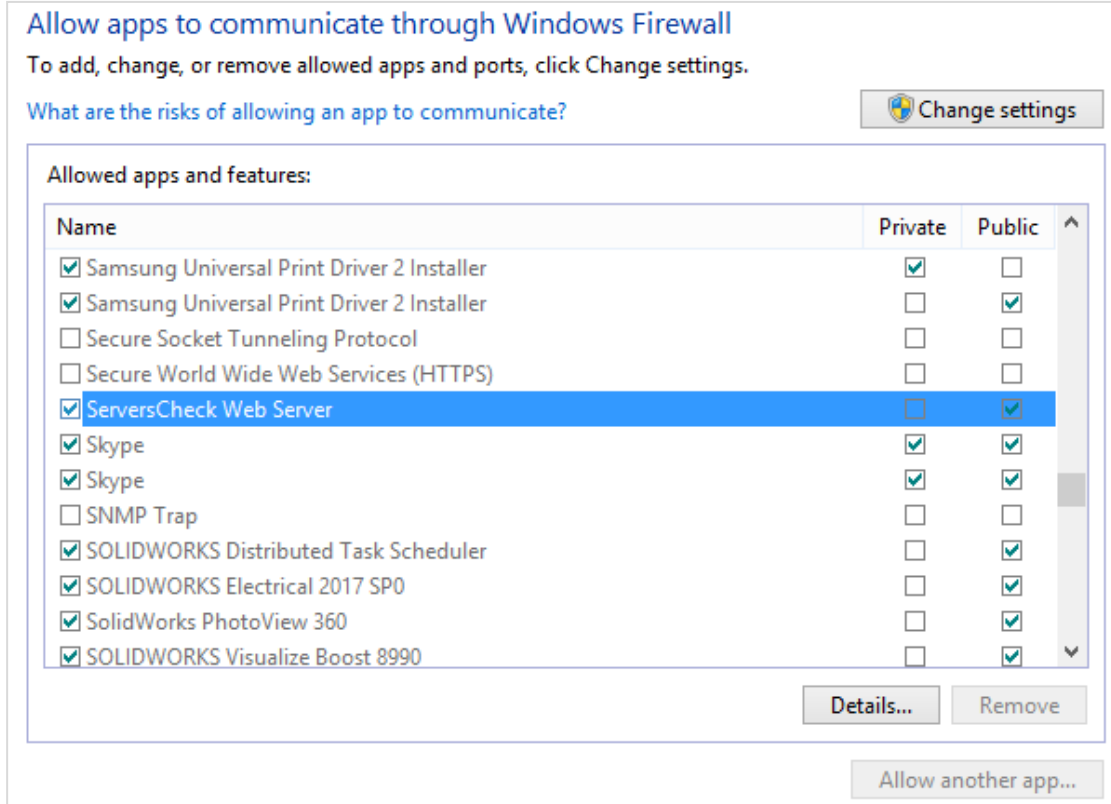
2.2. Things to Check before Accessing the Software

Make sure that the ServersCheck Web Server is allowed on your Windows Firewall.

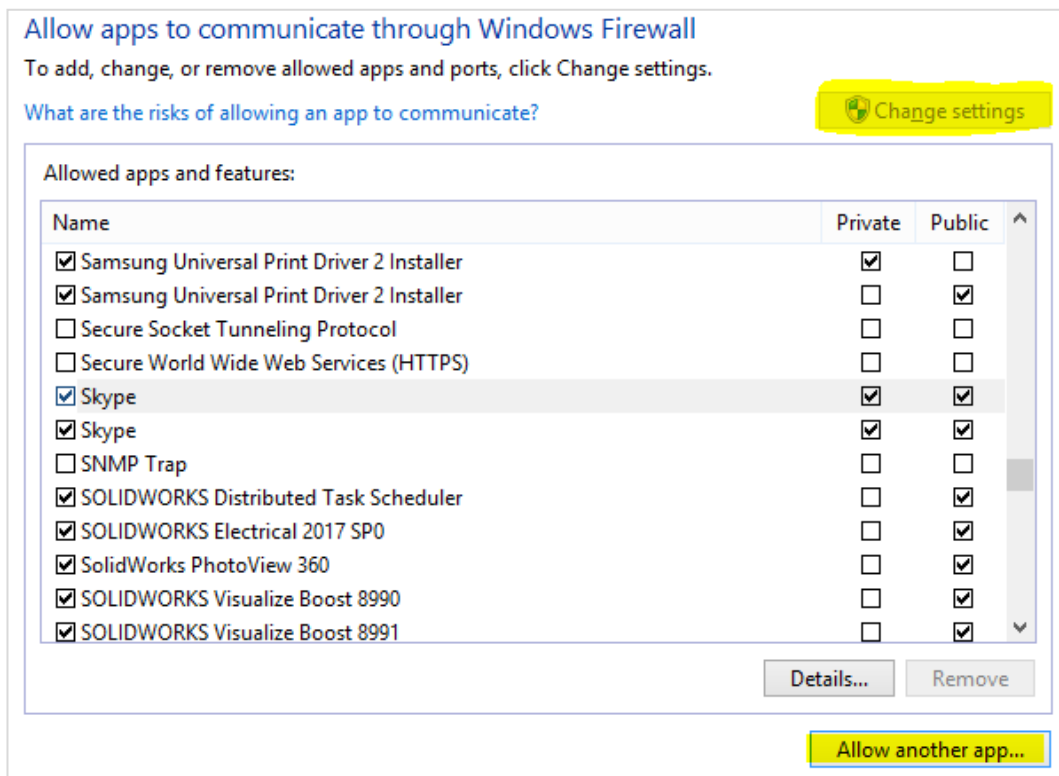
1. Access Control Panel - All Control Panel Items - Windows Firewall



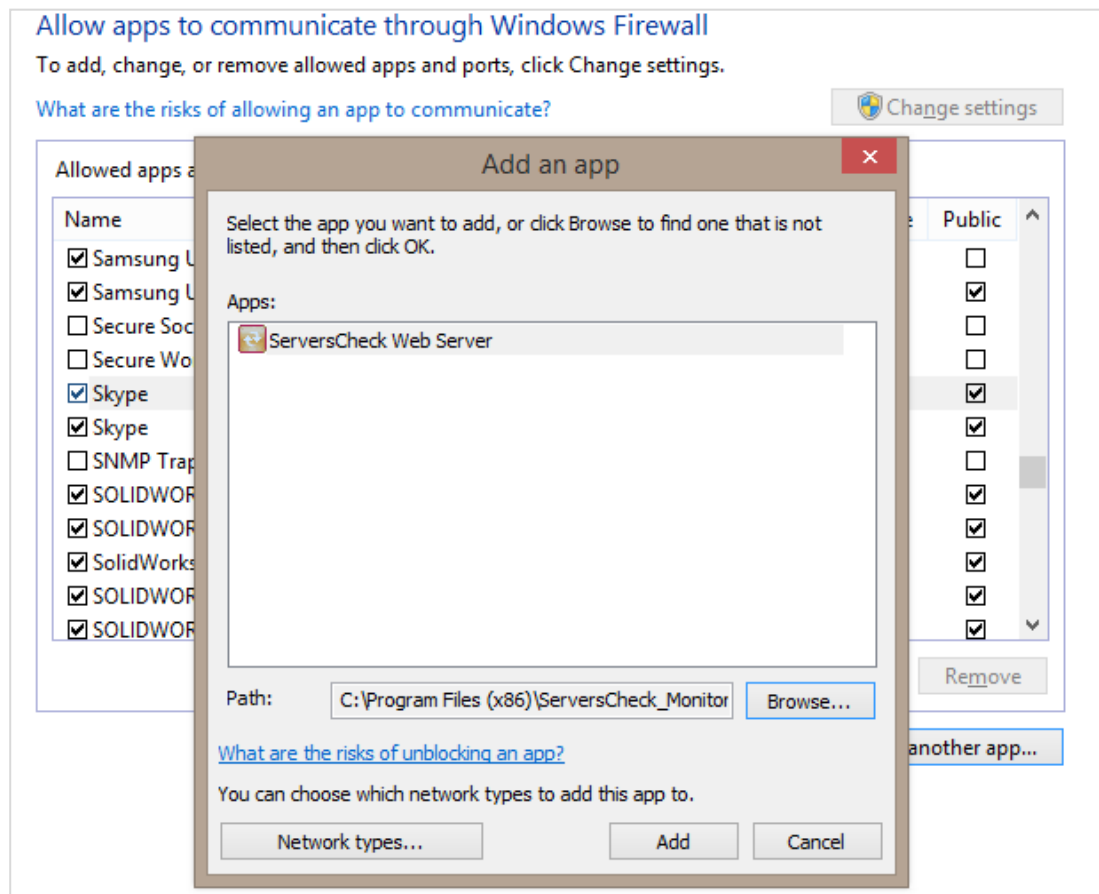
2. Click Allow an app or feature through Windows Firewall on the left hand side and see if ServersCheck Web Server is allowed. If it is not allowed, proceed to Number 3.



3. Click Change Settings, then Allow another app...



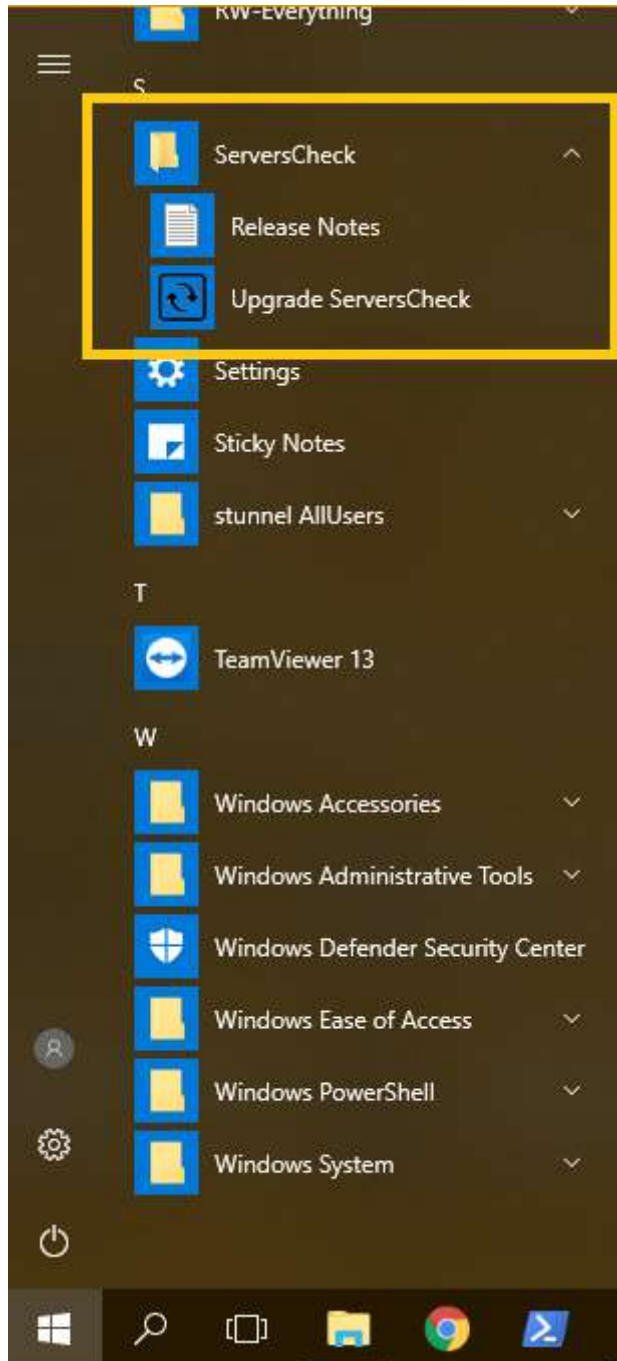
4. Browse through the folders where you saved the software. And select s-server.exe from the list and add it up. And click OK.



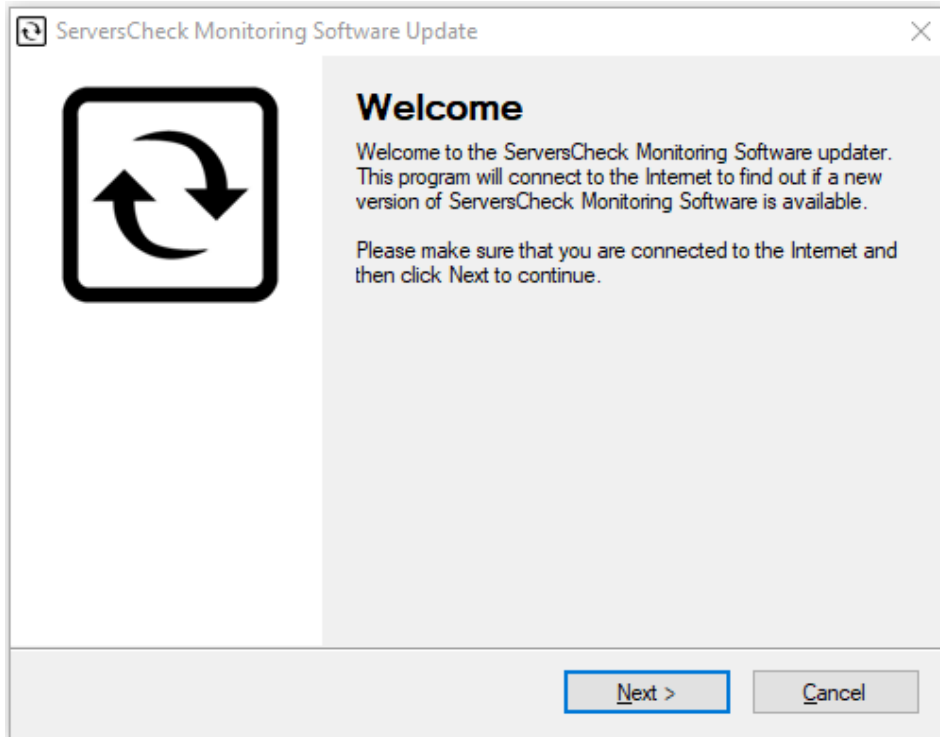
2.3. Upgrading the Monitoring Software

When a new version is available we advise to always upgrade your software and below are the instructions how.

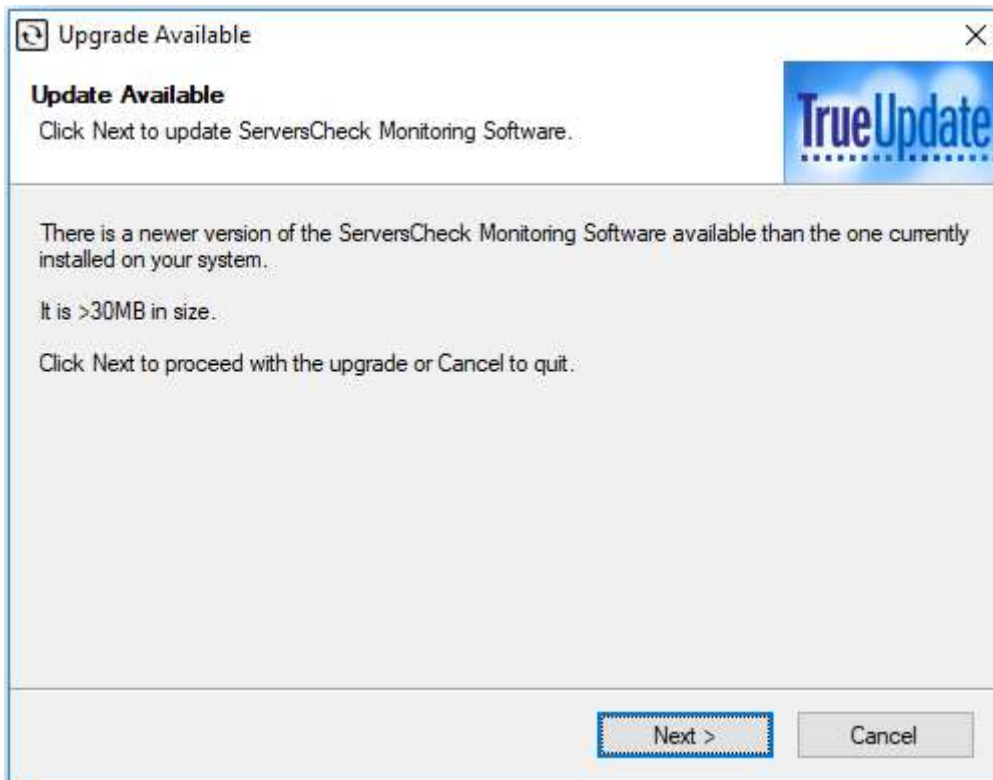
First is to click on the start menu and look for the ServersCheck folder, click on the dropdown menu and choose Upgrade ServersCheck



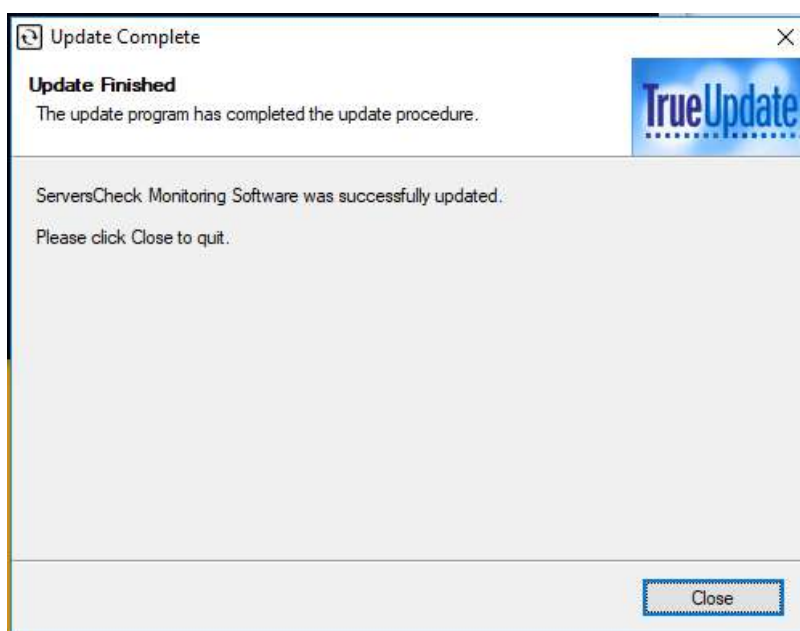
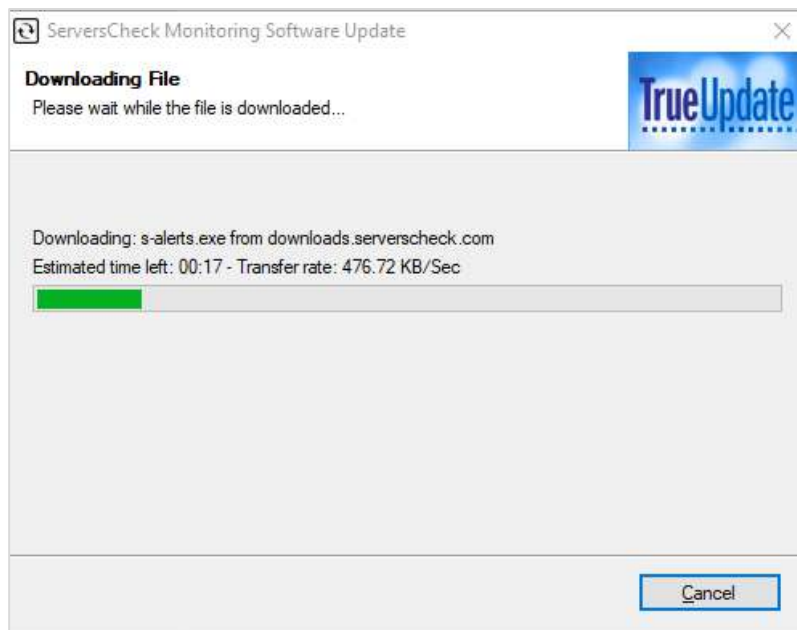
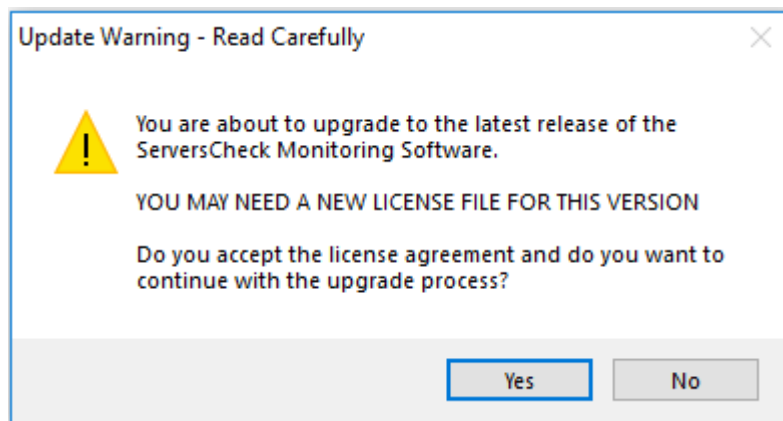
Then a new pop up window will appear



Proceed by clicking next until the installation finishes



If you have the free version or the licensed one, you need to click on YES when a pop up box appears.



2.4. Accessing the Monitoring Software

To connect, open up a web browser on the computer where you installed the software. Type in the URL <http://localhost:1272> as the software runs on port 1272.

* You may logon locally to the server using the pre-installed web browser. By default it will open the url <http://localhost:1272>. When the webserver is accessed locally, then no credentials are required.

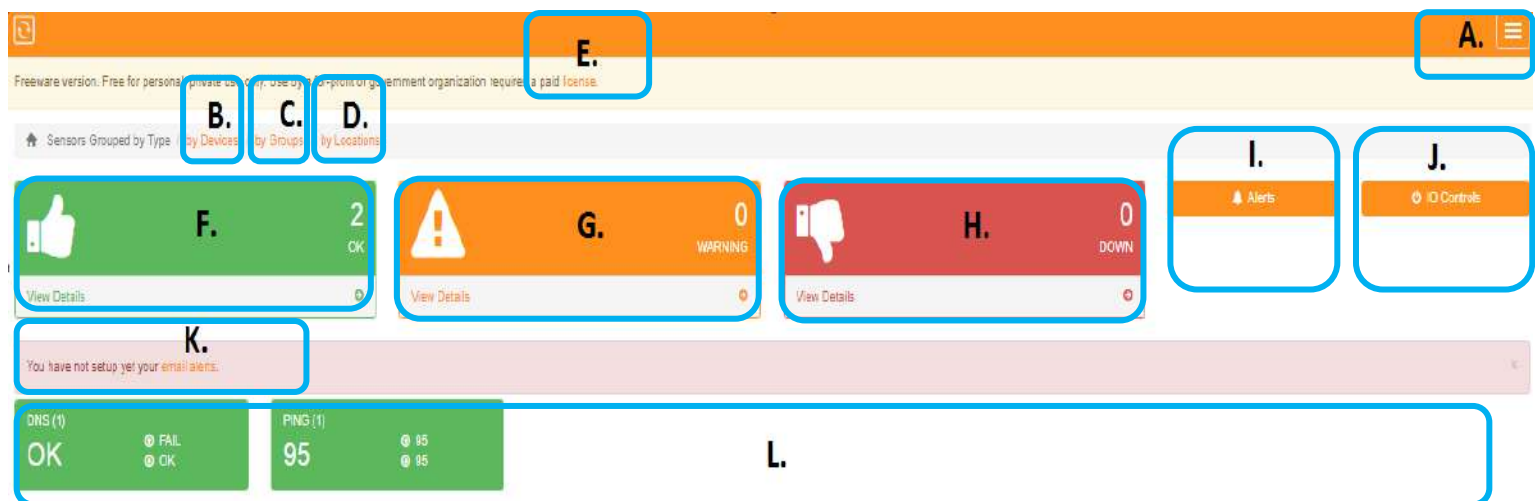
* You can also access the monitoring software through your network by typing in the IP address of the computer/appliance and add :1272.
Example: <http://192.168.1.1:1272>.

With software version 15+ you may access the webserver via <http://localhost> as by default, port 80 is now supported, additional configuration is needed should you want to access the webserver via https, which will be explained on section 6

You will be prompted with a username and password once you made a connection.

Default Username : admin
Default Password : admin

This image below shows the dashboard upon installing the software. This is the default screen of the software.



- A. **Menu options** - shows you the set of options to configure the software.
- B. **Sensors Grouped by Devices** - gives you option to group sensors by devices, e.g. Sensorgateway, Ping, DNS, etc.
- C. **Sensors Grouped by Groups** - gives you option to group sensors by groups.
- D. **Sensors Grouped by Location** - gives you option to group sensors by location on certain address around the world you set for the particular device. If you do have multiple addresses or locations to monitor.
- E. **License** - Freeware versions are free for personal and private use only. For profit and government organization, you need to purchase a license. Clicking would be forwarded to <https://store.ServersCheck.com/> should you need to purchase a license.

F. **Devices with OK status** - lists all sensors that are monitoring fine.

G. **Devices with Warning status** - lists all sensors that has a warning status based on the threshold you set.

H. **Devices with Down status** - lists all sensors that has a down status based on the thresholds you set.

I. **Alerts** - shows the alerts history of all the checks you are monitoring.

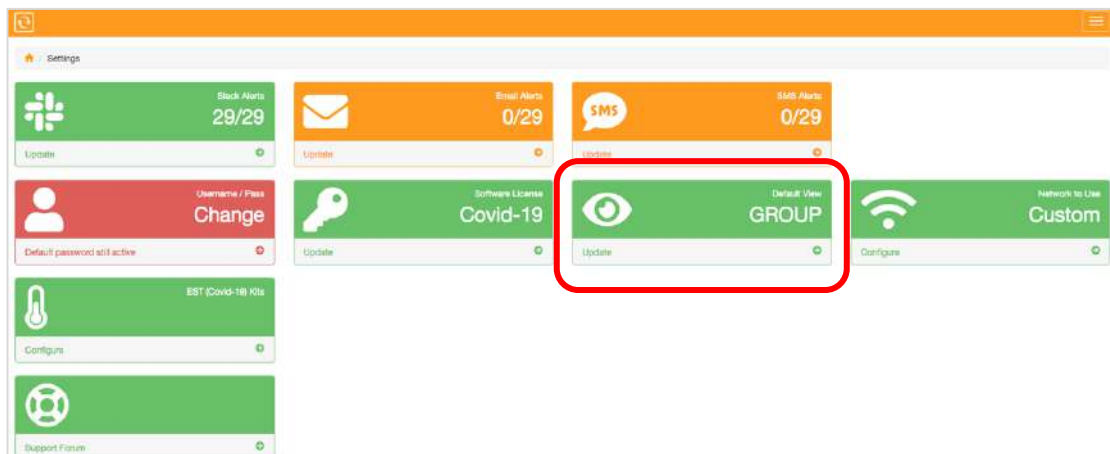
J. **IO Controls** - shows a list of Sensorgateway devices that has the IO controls and to manually override Input/Outputs.

K. **Email Alerts** - For initial installation, you can immediately setup email alerts on the software.

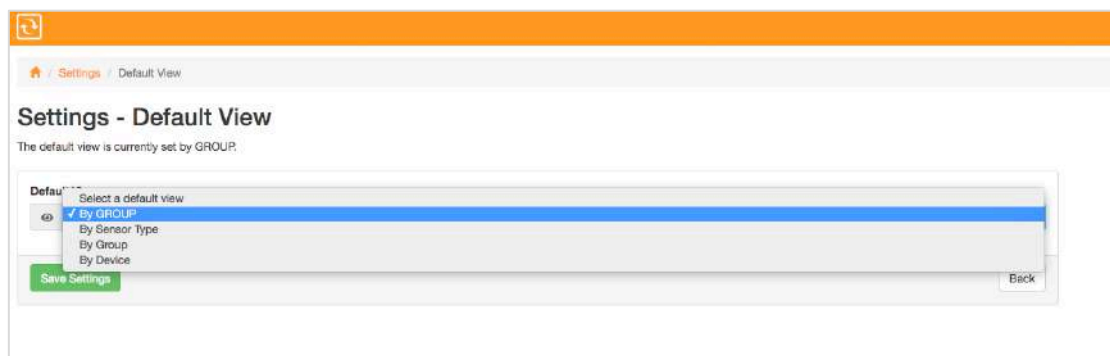
L. **Sensors Field** - shows the lists of sensors/devices including their current values and status.

2.5. Default View for your Monitoring checks

Click Settings and then Default View



You can then have the option to set the default view on the home page of your monitoring software.



2.6. Choosing the Network adapter to use

Under settings click on Network to Use



This option enables you to run the monitoring and alerting processes on specific network adapters. For example you can configure it to run all alerting through your LTE connection and the monitoring through your Ethernet connection. This allows you to receive alerts even when your power or office internet connection is down.

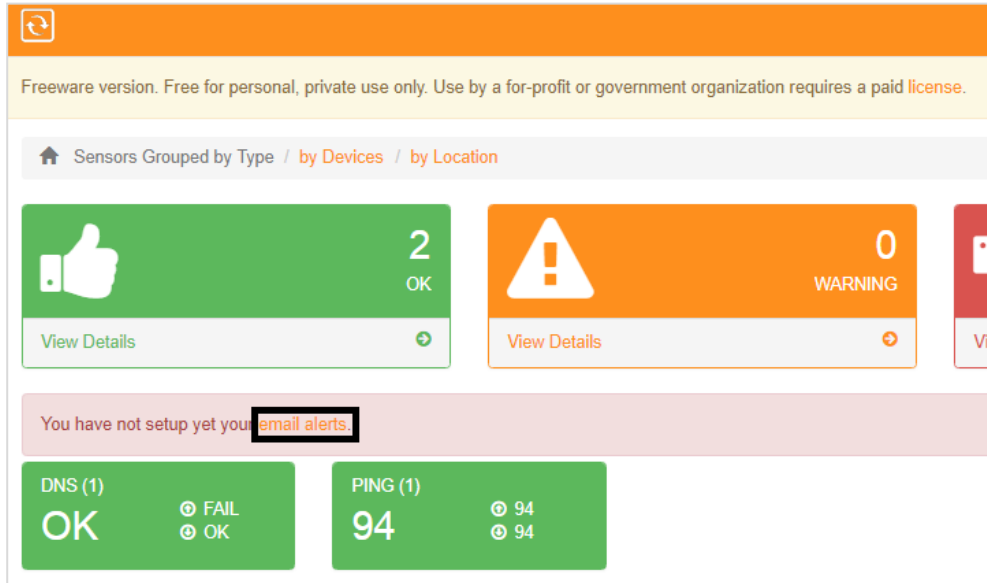
2.7. Setting up Email Alerts

ServersCheck Monitoring Software has the capability to escalate an alert based on user driven configurations.

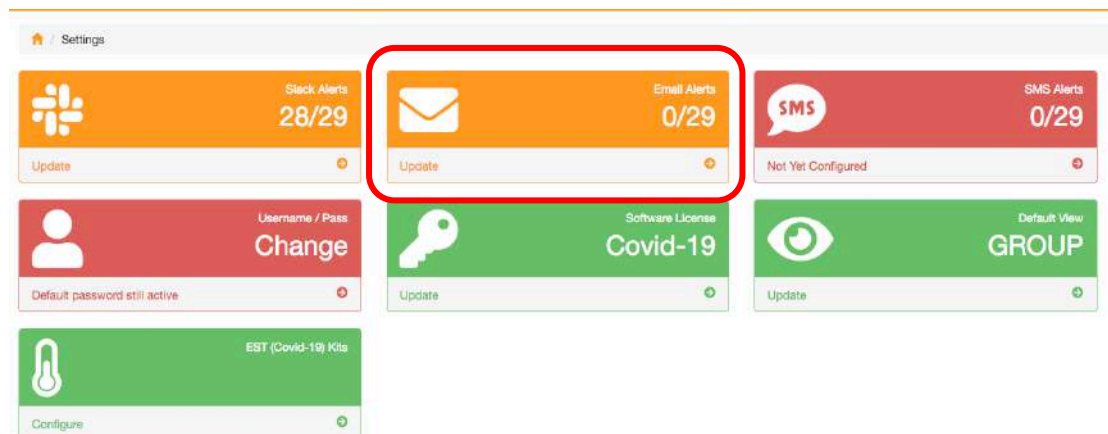
Note: If you are running an anti-virus software in your computer, make sure that you allow the s-alerts.exe to send out emails as AV software may block it. s-alerts.exe is located in the folder where your monitoring software is installed.

There are 2 ways to setup email from the Monitoring Software:

1. From the main Dashboard screen, click **Email Alerts** as shown in the image below.



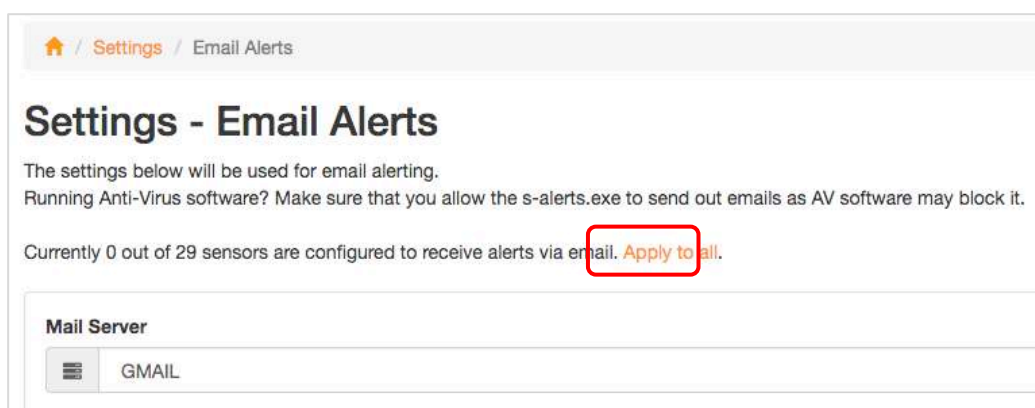
2. Or access Menu - Settings - Email Alerts



ServersCheck Monitoring Software has several ways of sending emails from different server options:

- Built-in Mail Server
- Your ISP's Mail Server or Open SMTP Server
- SMTP Mail Server
- IMAP Mail Server
- Gmail

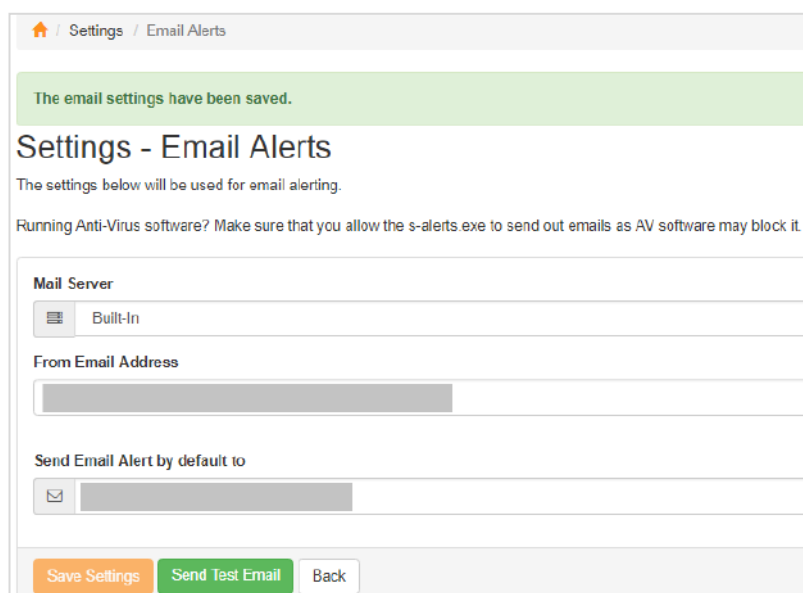
After configuring your email settings you have the option to apply the alert to all your sensors



2.7.1. Using The Built-In Mail Server

This uses ServersCheck's free mail server to send out alerts.

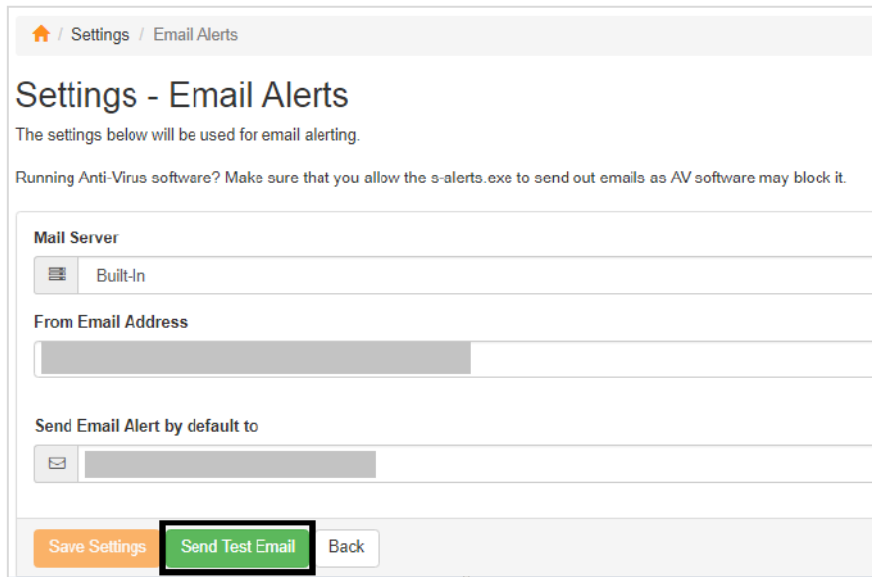
1. Select Built-In Mail Server.



From Email Address - This is the email address used to send the alert emails from.
Send Email Alert by default to - email of the recipient.

Note: To put multiple email addresses, it needs to be separated with a comma (,) and no spaces are allowed.

2. Sending a Test Email.



Home / Settings / Email Alerts

Settings - Email Alerts

The settings below will be used for email alerting.

Running Anti-Virus software? Make sure that you allow the s-alerts.exe to send out emails as AV software may block it.

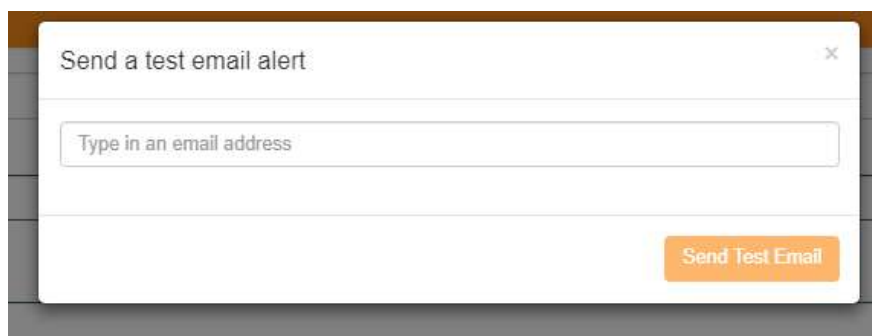
Mail Server

Built-In

From Email Address

Send Email Alert by default to

Type in an email address to which you want to send the test email.



Send a test email alert ✕

2.7.2. Using Your ISP's Mail Server or Open SMTP Server

Here uses an open SMTP server or ISP Mail server that doesn't require authentication.

1. Select ISP Mail Server or Open SMTP Server.

The screenshot shows a web interface for configuring email alerts. At the top, there's a breadcrumb 'Settings / Email Alerts' and a title 'Settings - Email Alerts'. Below the title, there's a note: 'The settings below will be used for email alerting.' and a warning: 'Running Anti-Virus software? Make sure that you allow the s-alerts.exe to send out emails as AV software may block it.' The main form has several sections: 'Mail Server' with a dropdown menu set to 'ISP'; 'From Email Address' with a text input field; 'SMTP Server' with a text input field; 'Server Port' with a text input field containing '25'; and 'Send Email Alert by default to' with a text input field and a small icon. Below the input fields, there's a note: 'Use a comma when entering multiple email addresses. No spaces are allowed.' At the bottom of the form, there are three buttons: 'Save Settings' (orange), 'Send Test Email' (green), and 'Back' (white).

From Email Address - This is the email address used to send the alert emails from.

SMTP Server - Input the IP address or the Domain name of the SMTP Server.

Server Port - Port number of your SMTP Server.

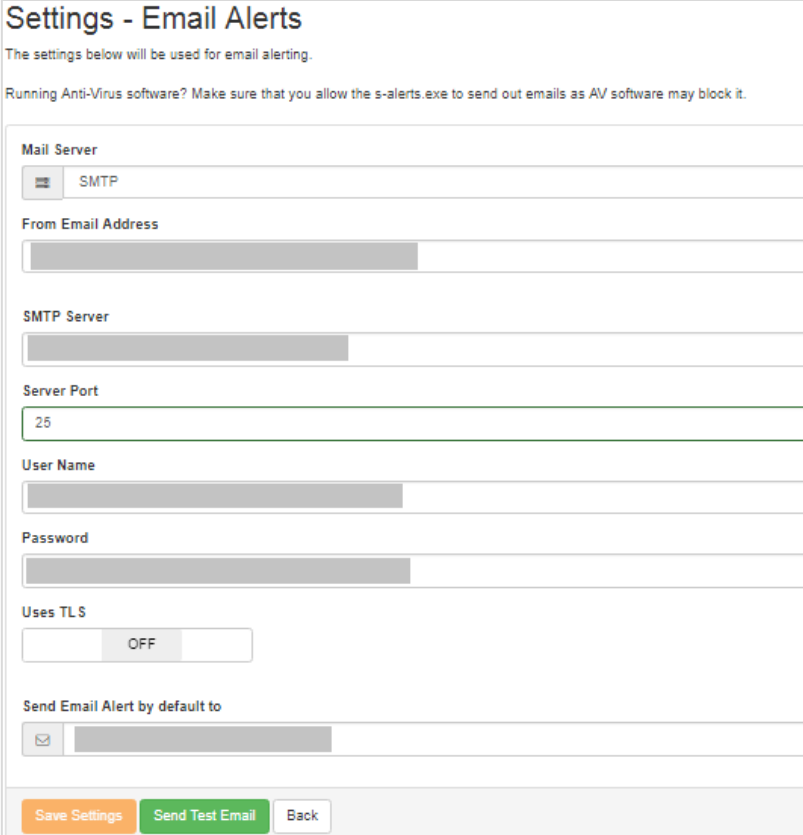
Send Email Alert by default to - Email address to where the email will be sent.

Note: To put multiple email addresses, it needs to be separated with a comma (,) and no spaces are allowed.

2.7.3. Using SMTP Server

This option uses a specific SMTP Server that requires standard username and password for authentication.

1. Select SMTP Mail Server.



From Email Address - This is the email address used to send the alert emails from.

SMTP Server - Input the IP address or the Domain name of the SMTP Server.

Server Port - Port number of your SMTP Server.

Username - The username of the email account you want to send from.

Password - The password of the email account you want to send from.

Uses TLS - can be turned on/off.

Send Email Alert by default to - Email address to where the email will be sent.

Note: To put multiple email addresses, it needs to be separated with a comma (,) and no spaces are allowed.

2.7.4. Using IMAP Server

IMAP stands for Internet Messaging Access Protocol, is an internet standard protocol used by email clients to retrieve email messages from a mail server over TCP/IP.

1. Select IMAP Mail Server

Settings - Email Alerts

The settings below will be used for email alerting.

Running Anti-Virus software? Make sure that you allow the s-alerts.exe to send out emails as AV software may block it.

The screenshot shows a web-based configuration interface for email alerts. It features several input fields and a toggle switch. The 'Mail Server' dropdown is set to 'IMAP'. The 'From Email Address' field is empty. The 'IMAP Server' field is empty. The 'IMAP Port' field contains the number '25'. The 'User Name' and 'Password' fields are empty. The 'Uses TLS' toggle switch is set to 'OFF'. The 'Send Email Alert by default to' field is empty. At the bottom of the form, there are three buttons: 'Save Settings' (orange), 'Send Test Email' (green), and 'Back' (grey).

From Email Address - This is the email address used to send the alert emails from.

IMAP Server - IP address or Domain name of your IMAP Server.

IMAP Port - Port number of the IMAP. Typically uses port 143.

Username - The username of the Email account you want to send from.

Password - The password of the Email account you want to send from.

Uses TLS - Can be turned on/off.

Send Email Alert by default to - Email address to where the email will be sent.

Note: To put multiple email addresses, it needs to be separated with a comma (,) and no spaces are allowed.

2.7.5. Using GMAIL

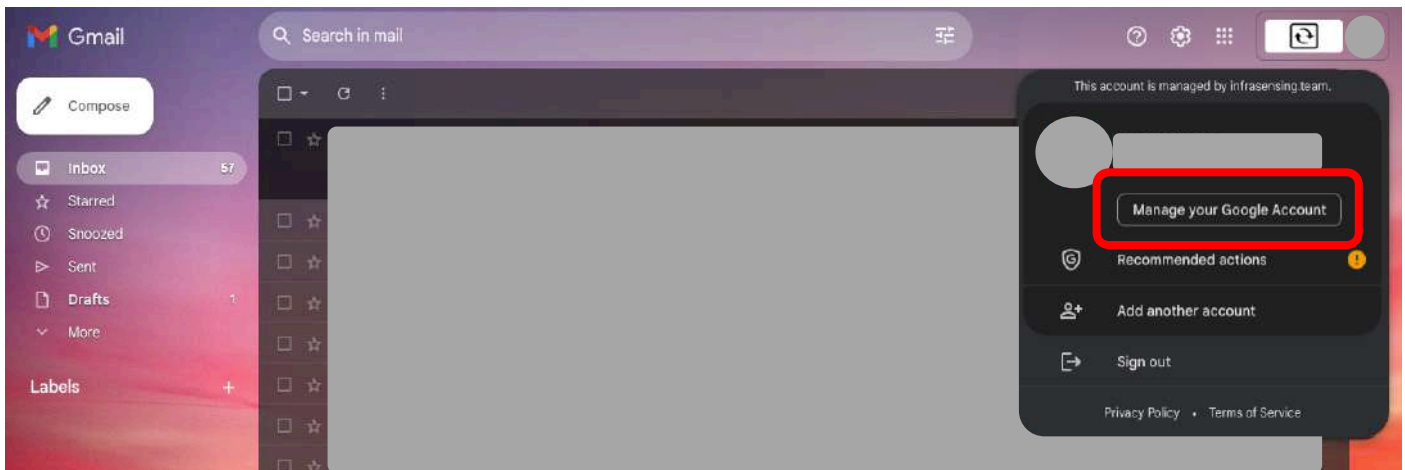
Here is an example of a configuration in Gmail to allow less secured apps to send emails or to connect to their SMTP Server.

To use Gmail as a mail server, you need to have a Gmail account. You may sign up for one at <https://mail.google.com> and port 25 should not be blocked by your ISP.

THINGS TO SET UP FOR GMAIL

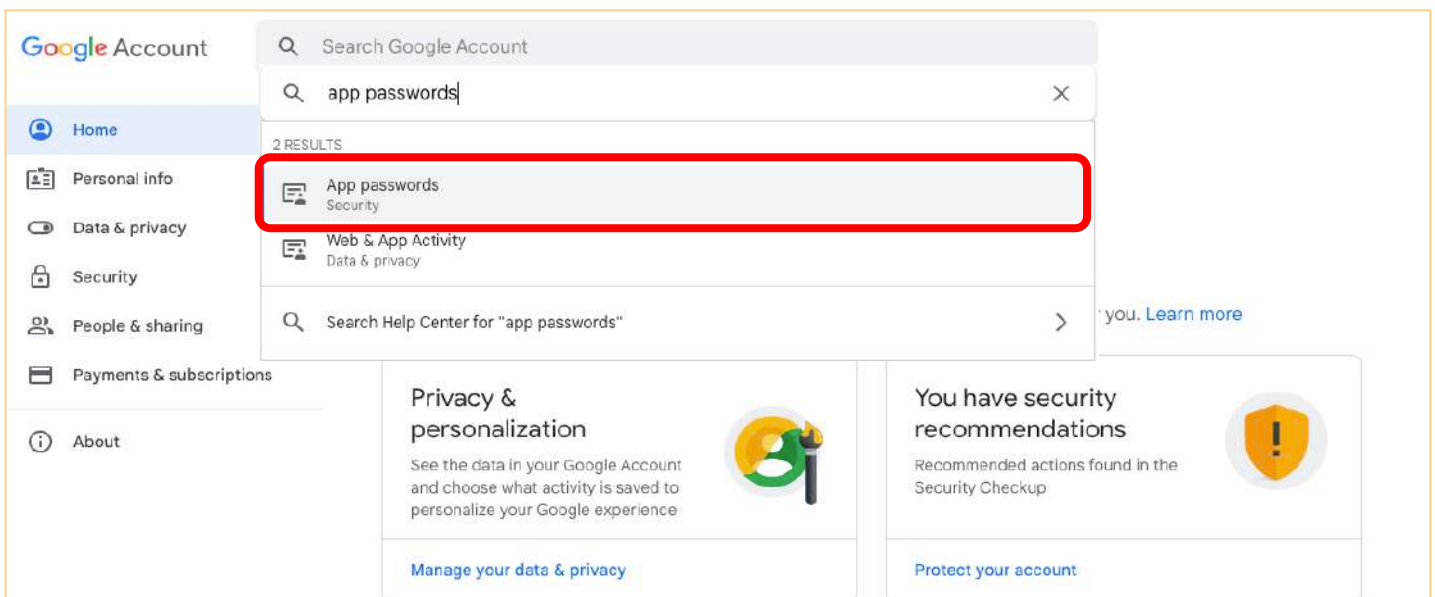
Below are the instructions on how to set it up.

1. Log in to your Gmail Account and access "Manage your Google Account."

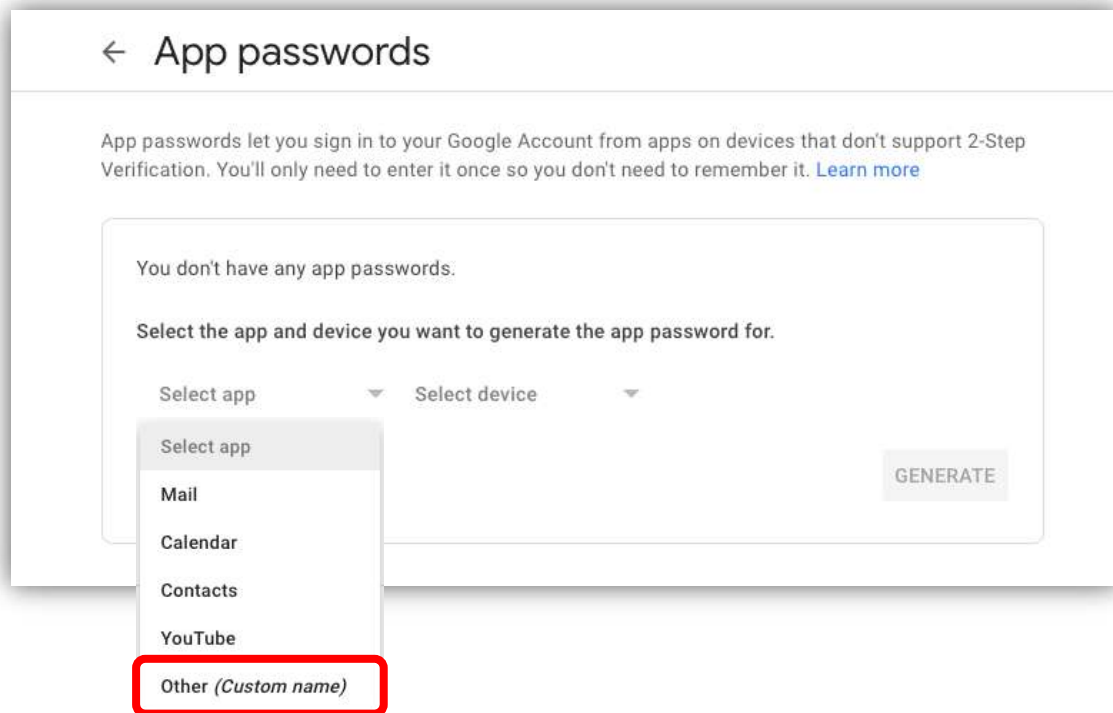


2. On the search bar type in "App Passwords."

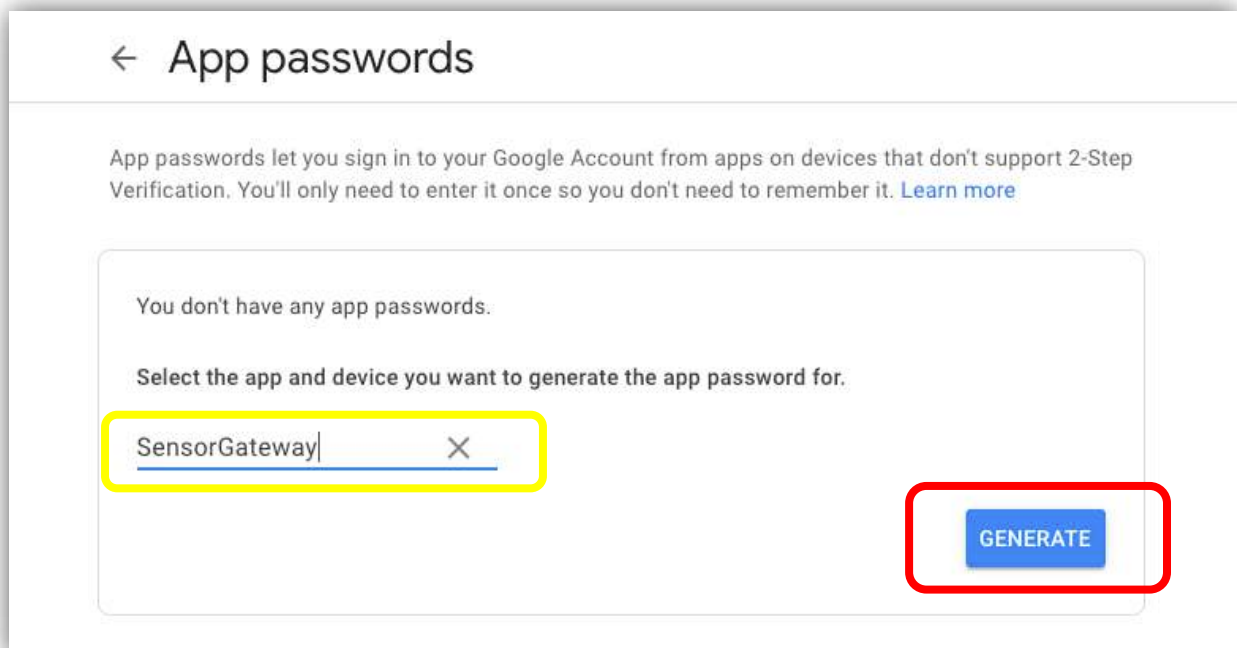
Note: Make sure that your 2-factor authenticator is enabled so that you can access the "App Passwords"



3. Once you click “App Passwords” you will see this pop up message. Just click “Select App” and choose “Other”



4. After you choose “Other” you may type in the name of your device or any name you desire.
5. Once you put in the name of your device, you may now click “Generate” so that it will generate you a password that you need to save for later.



5. After you click “Generate” a pop message will appear. This is now your app password for your device.

Important: Make sure to copy and securely store this password in your notes for future reference. Once you close this pop-up message, the password will not be retrievable. In case you lose it, you will need to follow the same steps again to generate a new password.

Generated app password

Your app password for your device

tezy gpyj eohp aauc

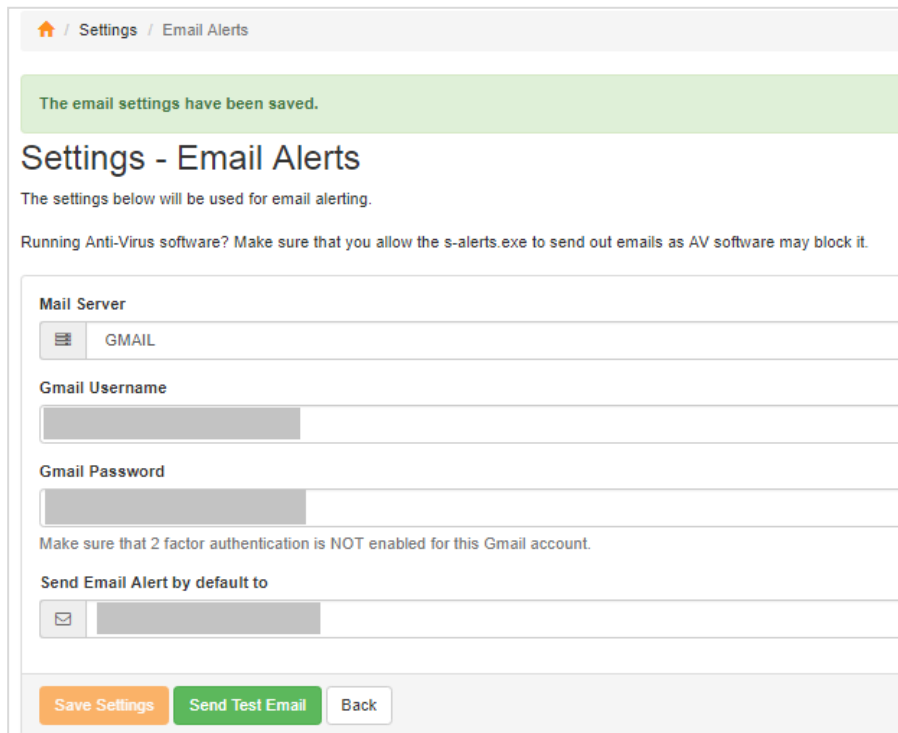
How to use it

Go to the settings for your Google Account in the application or device you are trying to set up. Replace your password with the 16-character password shown above. Just like your normal password, this app password grants complete access to your Google Account. You won't need to remember it, so don't write it down or share it with anyone.

DONE

You are now ready to configure the monitoring software using your Gmail account.

1. Select **GMAIL**.



Gmail Username - Username of your Gmail Account

Gmail Password - In the "Gmail Password" field, kindly retrieve and input the password that was previously saved and paste it into the designated space provided.

Send Email Alert by default to - Email address to where the email will be sent.

Note: To put multiple email addresses, it needs to be separated with a comma (,) and no spaces are allowed.

Note: Make sure that the 2 factor authentication is NOT enabled for your Gmail account.

2.8. Configuring SMS

ServersCheck Monitoring Appliance and Software can send SMS Alerts using this option:

[ServersCheck Premium Alerts](#) - to be purchased with options of 100 credits or 500 credits.

Using ServersCheck Premium Alerts (SMS & Voice Call Alerts)

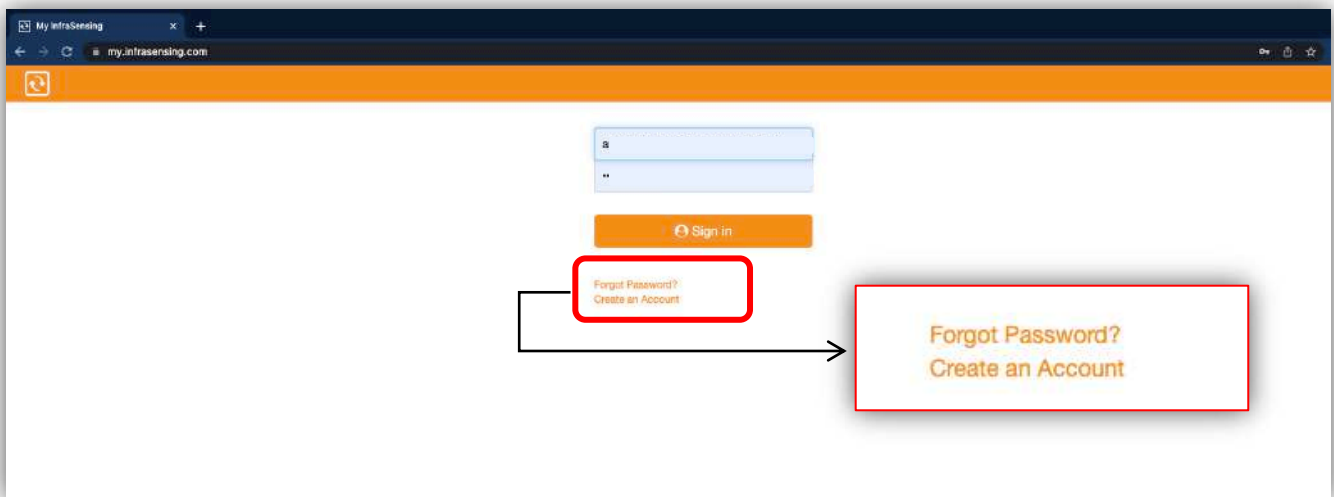
ServersCheck Premium Alerts is an alerting service provided by ServersCheck for SMS and Voice Calls. It can be purchased from our webstore after you have created an account with <https://my.infrasensing.com/> with options of 100 or 500 credits.

Here is also an instructional video on how our Premium Credits work.

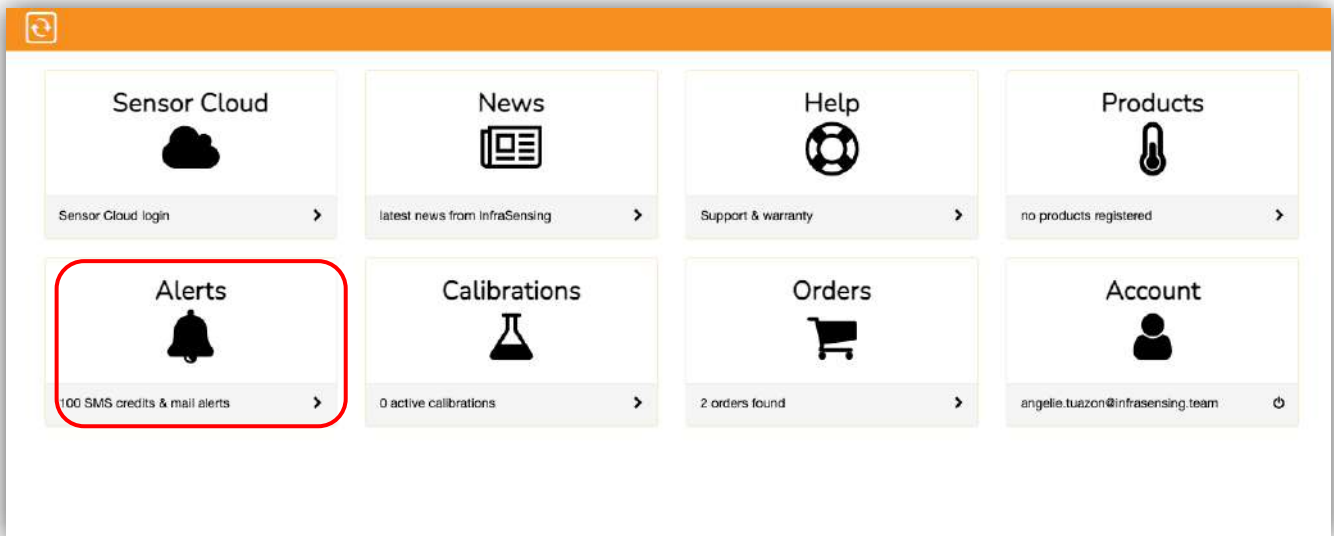
<https://serverscheck.infrasensing.com/sensors/how-it-works.asp?item=SMS>

1. To use this following feature, you are required to have a my.ServersCheck.com account. If you do not have one yet, you may create an account via this URL

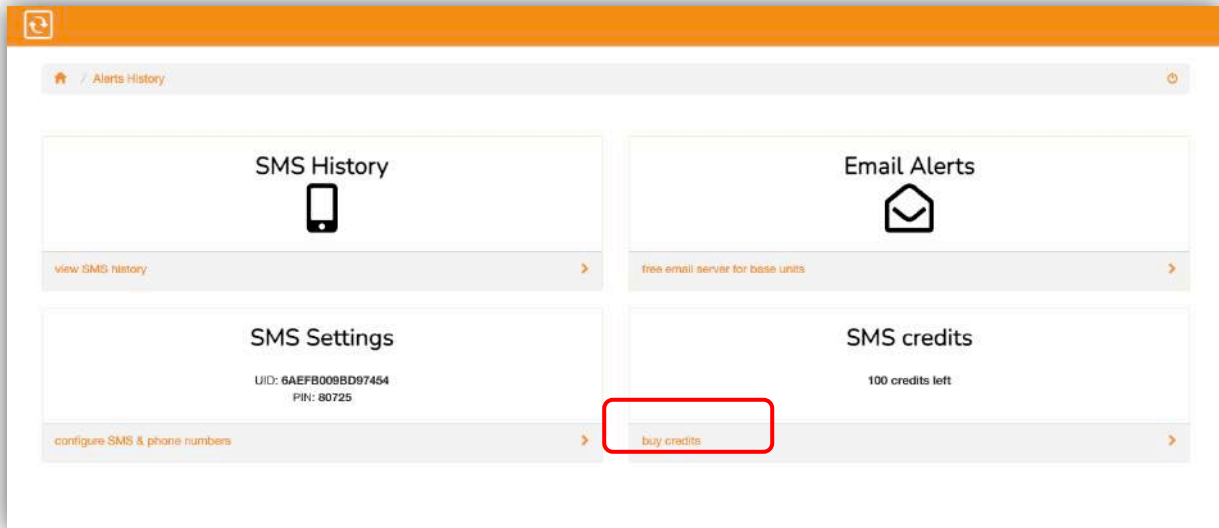
<https://my.infrasensing.com/>



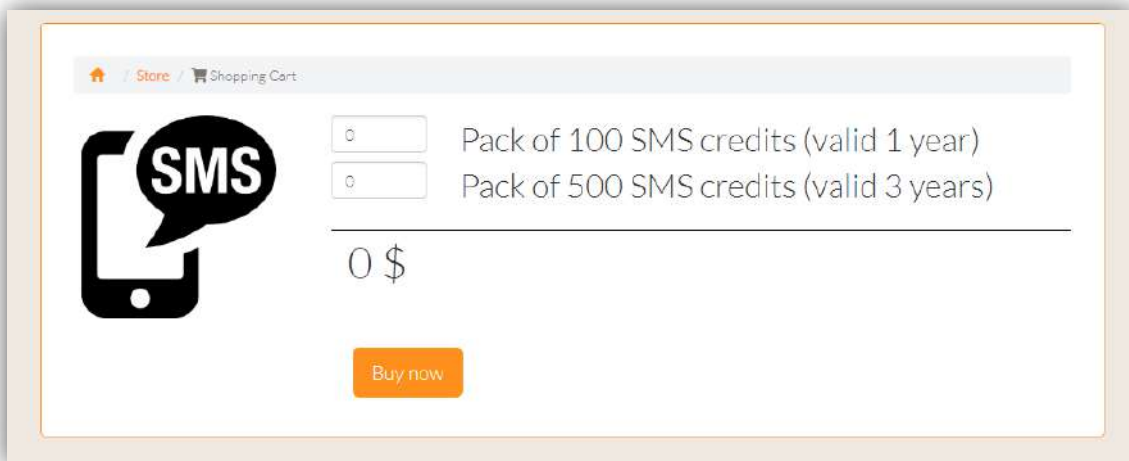
2. After logging in, click **ALERTS**.



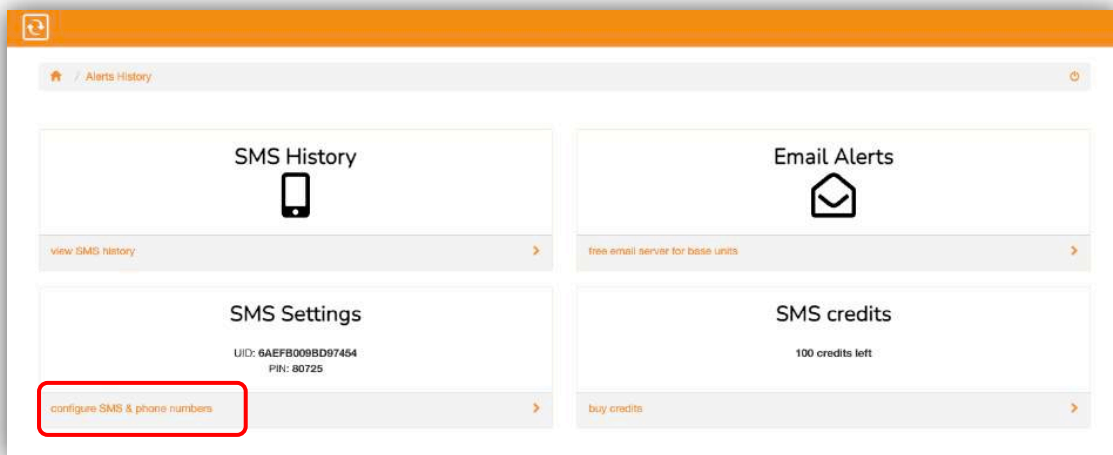
3. From this page, you have an option to **Buy Credits**.



4. You can purchase option of 100 credits (valid for 1 year) or 500 credits (valid for 3 years). 1 credit per SMS, 3 credits per voice call.



5. Once you now have available credits, go back **Alerts** to **configure SMS & phone numbers**



The screenshot shows the 'Alerts / SMS' dashboard. At the top, there's a 'Purchase Credits' button. Below it, three summary boxes are visible: 'Alerts UID: 6AEFB009BD97454 PIN: 80725' with a 'generate new alert uid' button; 'Credits balance 100' with a 'buy credits' button; and 'Registered number(s) +639609102542' with a 'manage numbers' button. The 'Registered number(s)' box is highlighted with a red rectangle. Below these is a table of sent messages with columns for Date, Sent To, Type, and Message Content. The table shows several entries for 'PIN code validation SMS' sent to various numbers. At the bottom, there are pagination controls showing 'Showing 1 to 10 of 12 entries' and 'Previous 1 2 Next'.

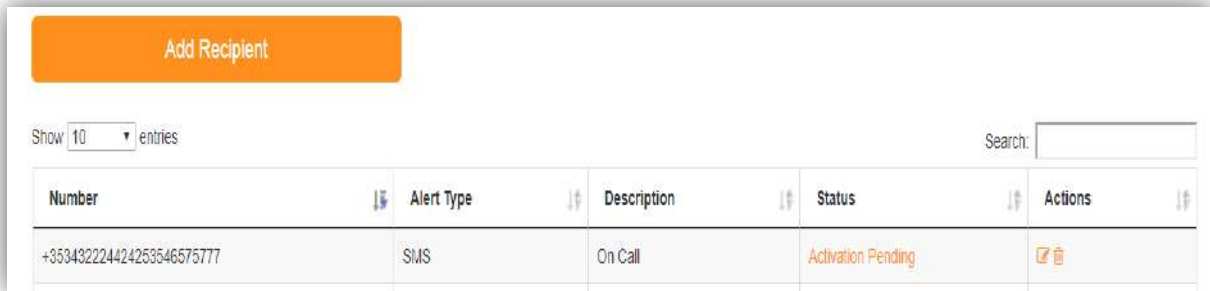
6. Select a **Notification Type** and the **Phone Number**.

You may choose from the list of options:

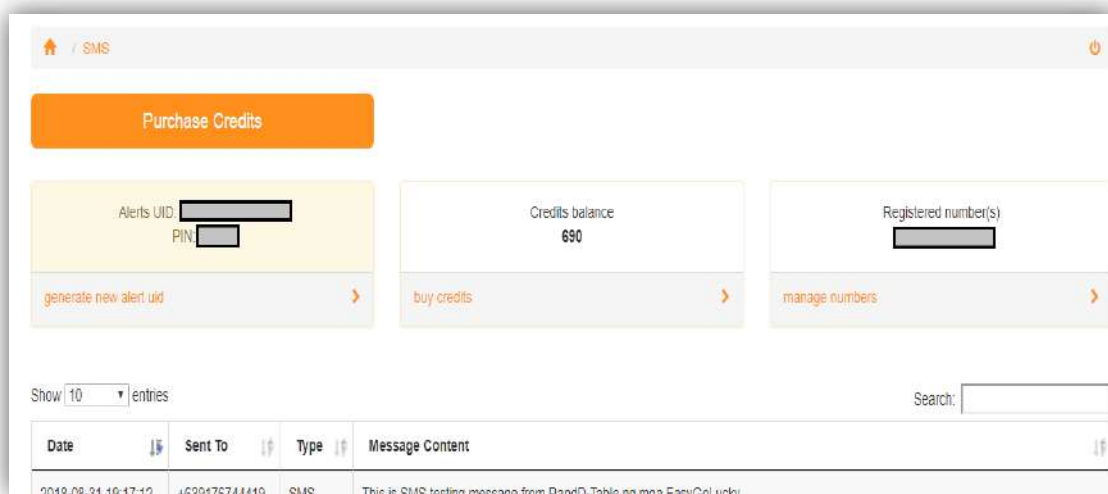
- SMS only
- Voice only
- SMS + Voice

The screenshot shows the 'Add a new phone number' form. The breadcrumb trail at the top reads 'SMS / Registered Numbers / Add Number'. The form has three main sections: 'Notification type' with a dropdown menu; 'Phone Number' with a 'Select a country' dropdown and a text input field for 'Your phone number'; and 'Description' with a text input field containing 'Example: Mike Phone'. At the bottom left of the form is a 'Submit' button. Below the form, there is a small note: 'Alert pricing: 1 credit per SMS sent; 3 credits per voice call.'

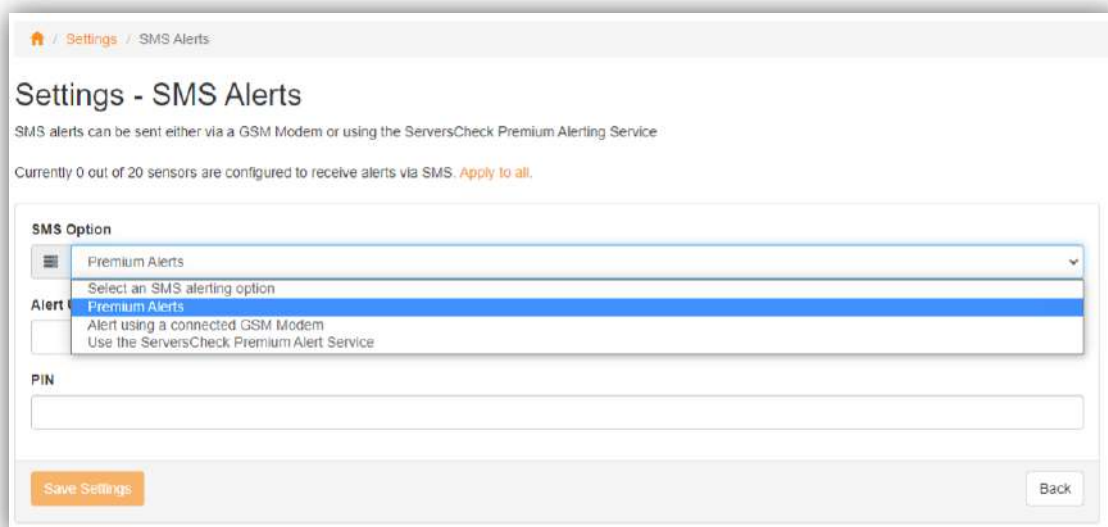
7. By now, you should be receiving a text message to the number you inputted and you need to simply go to the link provided on the text message to confirm and authenticate the phone number.



8. After adding and authenticating the phone number as your recipient. Copy the Alerts UID and PIN.

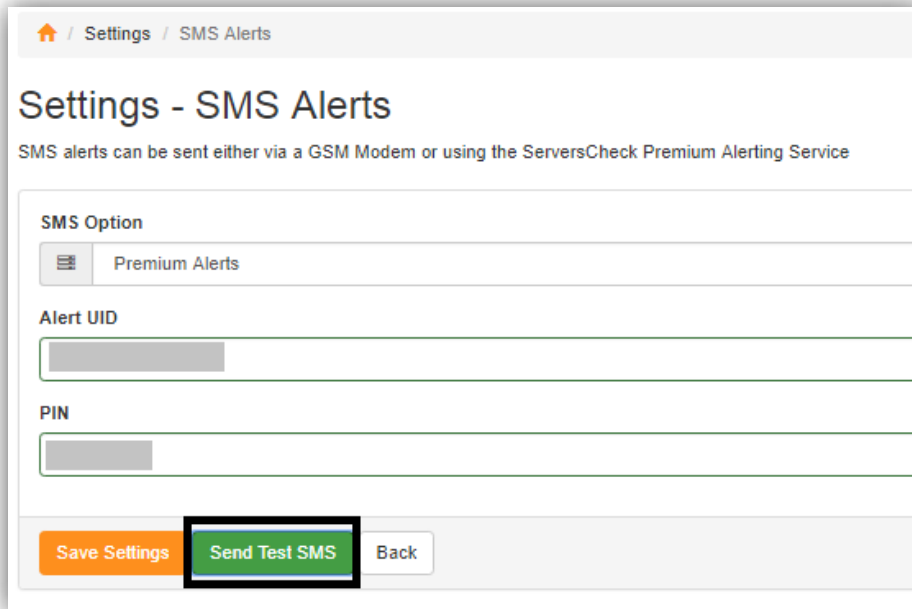


9. Now on the Monitoring Software, click Menu - Settings - SMS Alerts. Then select Use the ServersCheck Premium Alert Service.



10. Paste the **Alerts UID** and **PIN** you copied from your Premium Account under Alert UID and PIN on SMS alerts option of the Monitoring Software. Then Save Settings.

11. Send Test SMS.



Settings - SMS Alerts

SMS alerts can be sent either via a GSM Modem or using the ServersCheck Premium Alerting Service

SMS Option

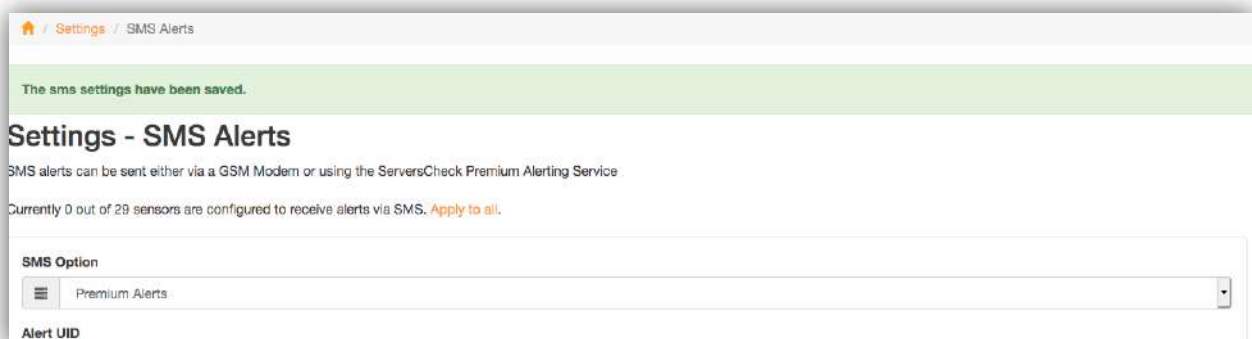
Premium Alerts

Alert UID

PIN

Save Settings Send Test SMS Back

12. You may opt to apply the settings to all your sensor by clicking on **apply to all**



Settings - SMS Alerts

The sms settings have been saved.

SMS alerts can be sent either via a GSM Modem or using the ServersCheck Premium Alerting Service

Currently 0 out of 29 sensors are configured to receive alerts via SMS. [Apply to all.](#)

SMS Option

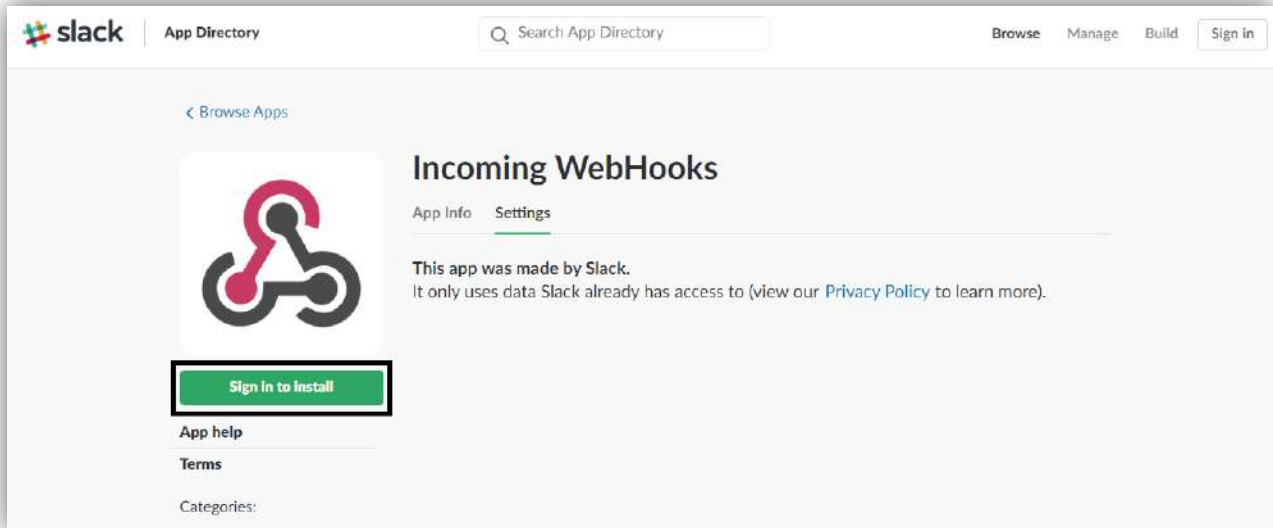
Premium Alerts

Alert UID

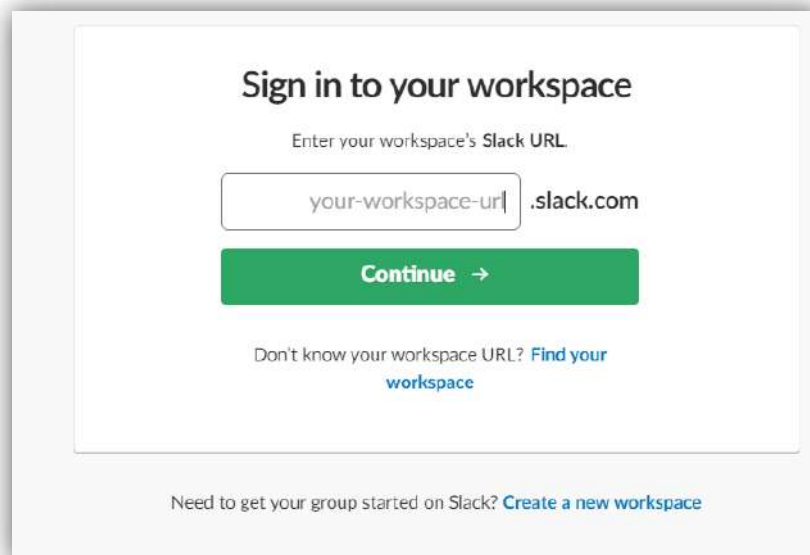
2.9. Setting Slack Alerts

These settings will be used for sending out alert notifications to your Slack channels.

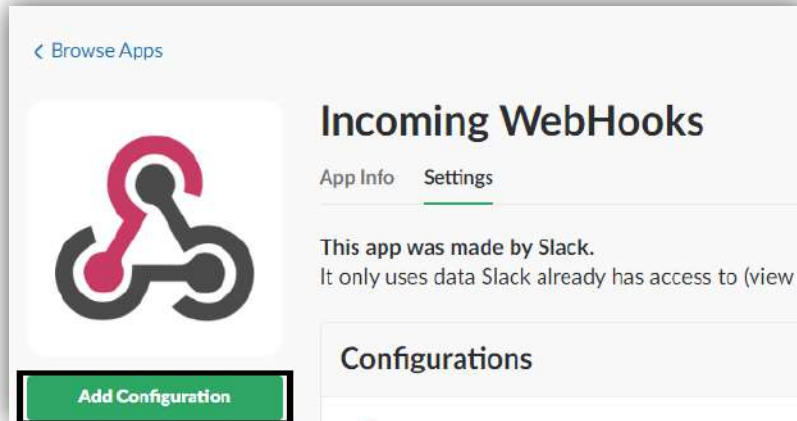
1. Go to the [Slack Incoming Webhooks App](https://slack.com/apps/A0F7XDUAZ-incoming-webhooks) and Click Sign in to Install.
You will be redirected to
<https://slack.com/apps/A0F7XDUAZ-incoming-webhooks?page=1>



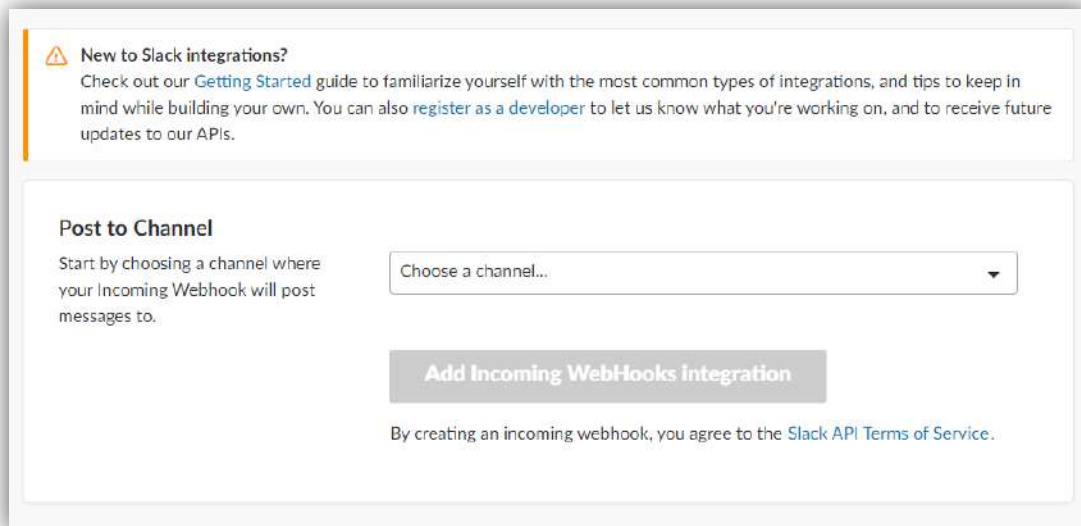
2. If you already have a Slack account, enter the name of your Slack URL. If you do not have an account yet, click Create a new workspace.



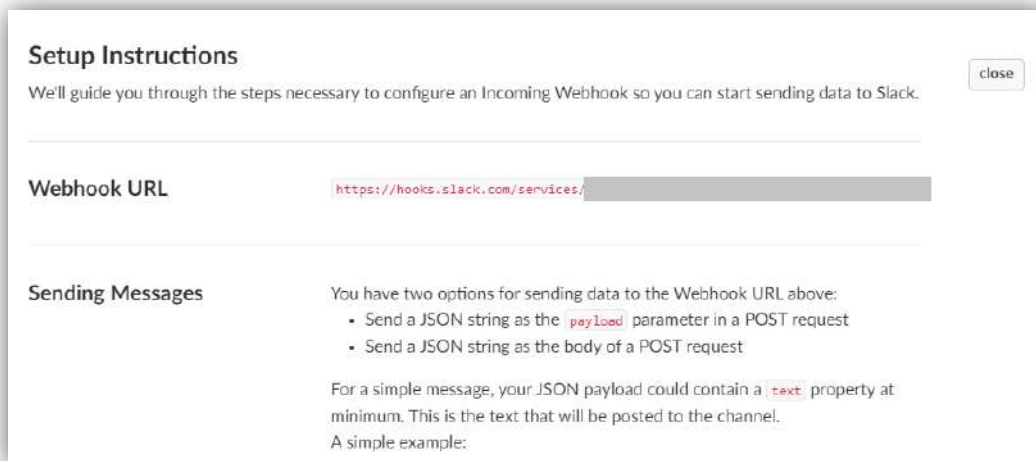
3. Click Add Configuration.



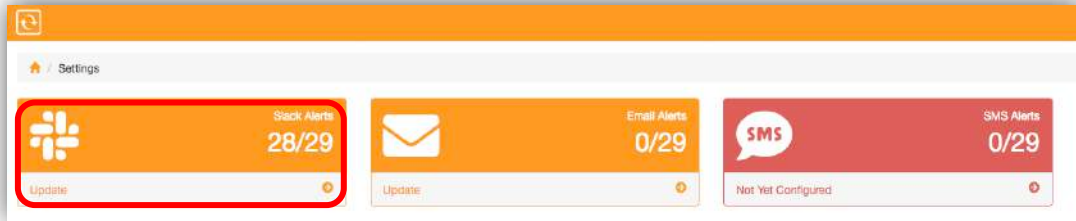
4. Select the Channel you want to send the alerts into from the drop down list. And click **Add Incoming Webhooks Integration**.



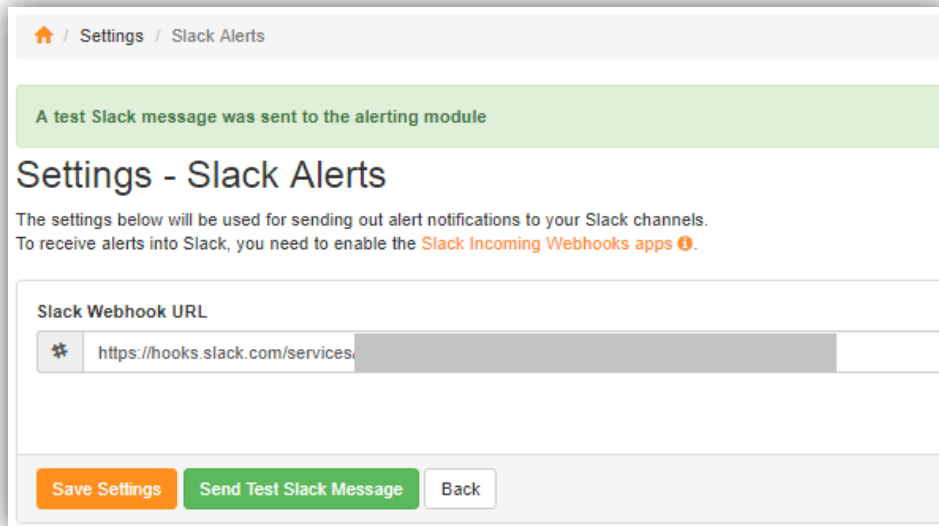
5. From the setup screen, copy the **Webhook URL**



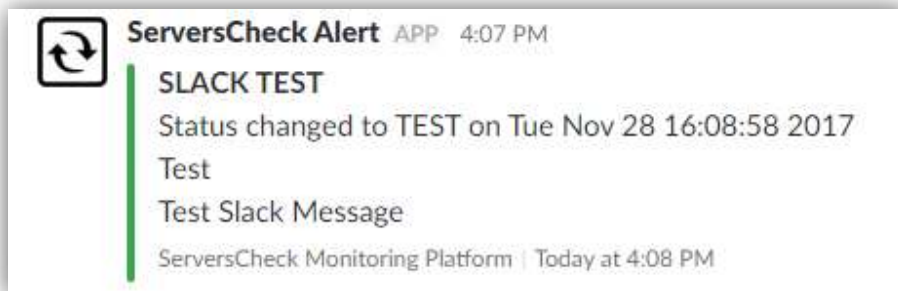
6. On the Monitoring Software, Click Menu then go to **Settings - Slack Alerts**.



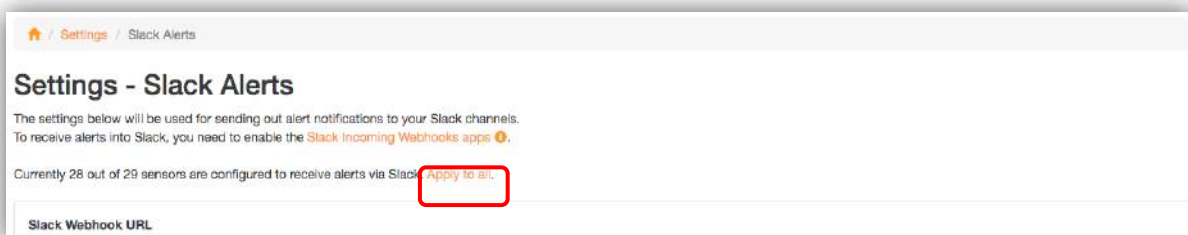
7. Paste the **Webhook URL** in the Settings - Slack Alerts Page of the Monitoring Software.



8. Save Setting and do a Send Test Slack Message. If successful, you should be receiving a similar message from your Slack account.



9. You may opt to apply your settings to all the sensors in your software



2.10. Setting up Username and Password

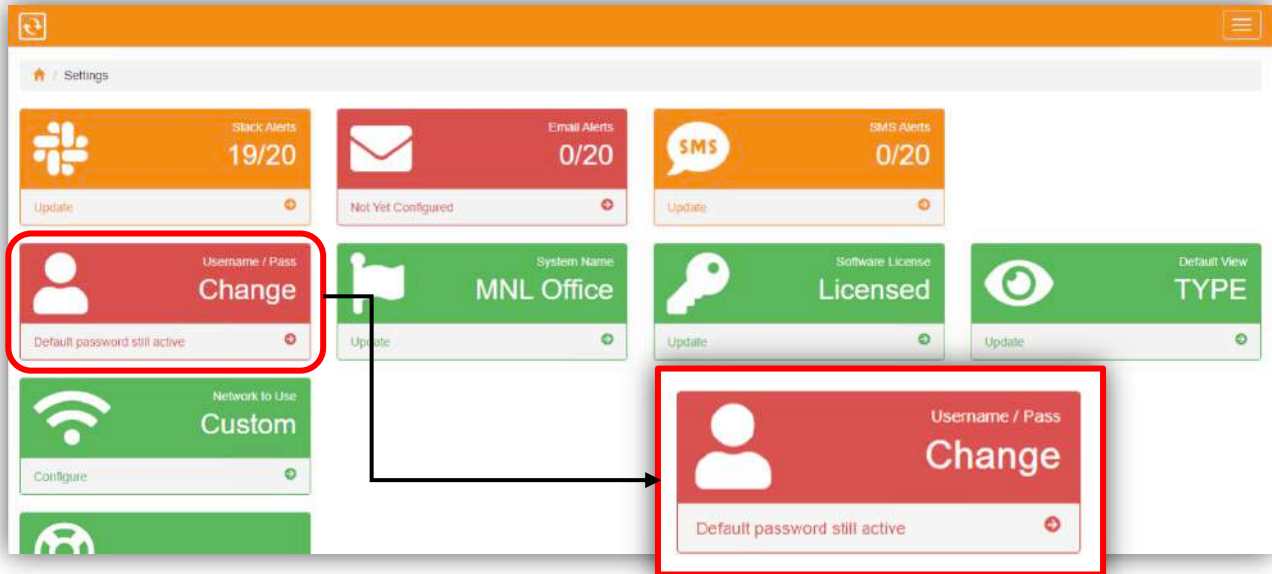
You need to setup a login Username and Password for the security of your Monitoring Software as it will be your credentials when you access the software on a separate computer.

Note: If accessing the software on a local host, it will not prompt for a Username and Password.

1. Click Menu and go to **Settings - Username & Password**.

Default Username - admin

Default Password - admin



2. Provide your new Username and Password and save settings.

Freeware version. Free for personal, private use only. Use by a for-profit or government organization requires a paid [license](#).

Settings / User Name & Password

Settings - User Name & Password

This is the username and password used for logging into this application.

User Name

Current Password

Enter the current password

New Password

Minimum of 6 characters

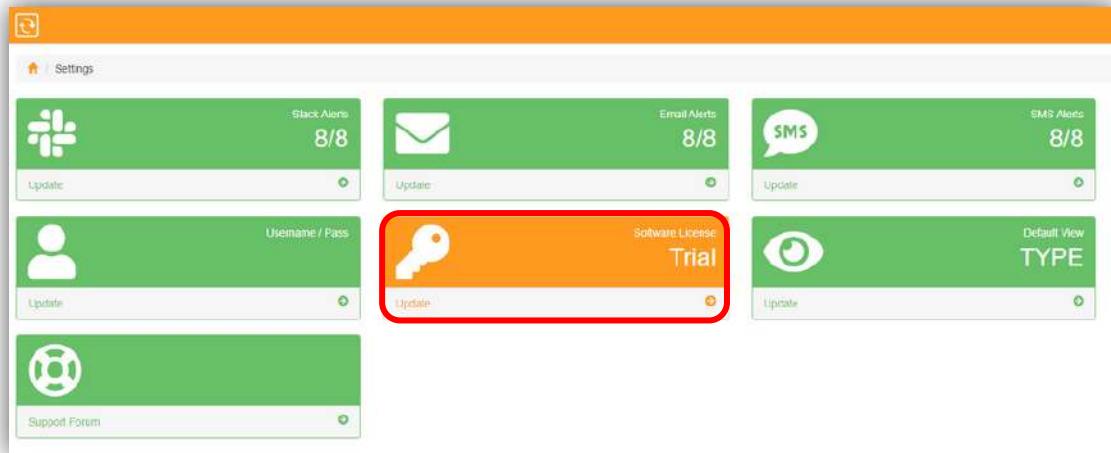
Username - use alphanumeric characters only

Password - minimum of 6 characters

2.11. Activating the License of your Software

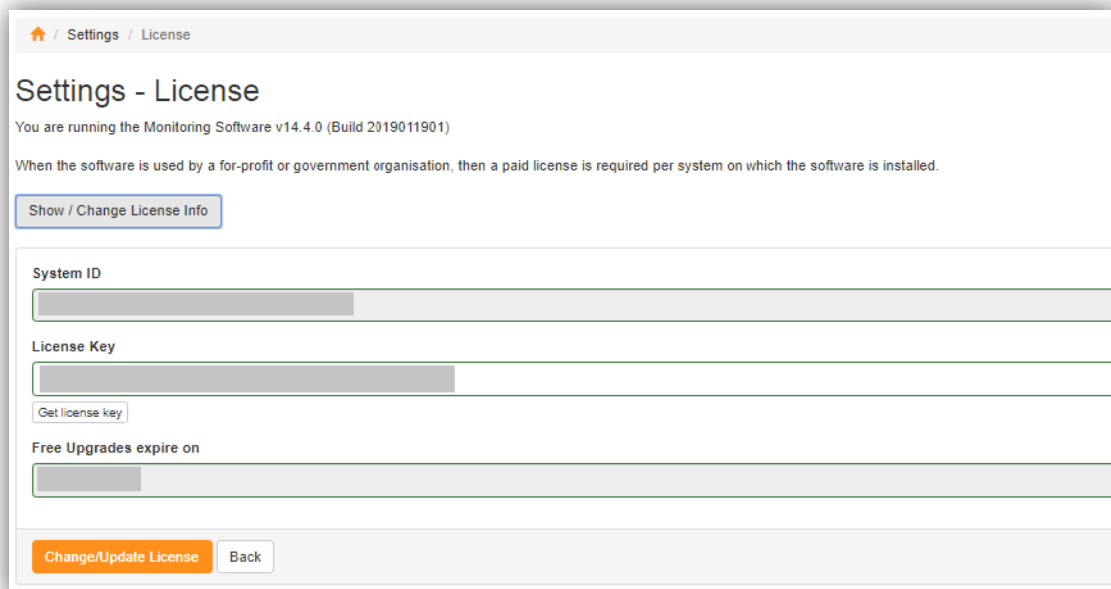
Freeware will be for personal and non-commercial use. For profit and government use, then you need to purchase a license. License is required per system on which the software is installed. You may contact any of our resellers or send an email to hello@ServersCheck.com for pricing.

1. Once you have purchased the license, you may activate it by clicking the **Menu - Settings - License**.

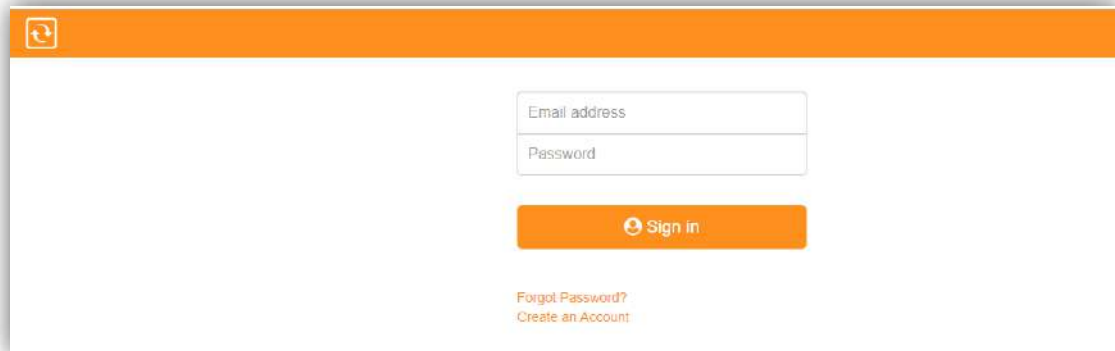


2. Click **Show/Change License Info**. A **System ID** will be generated with a unique identifier based on a specific Windows computer the software is installed.

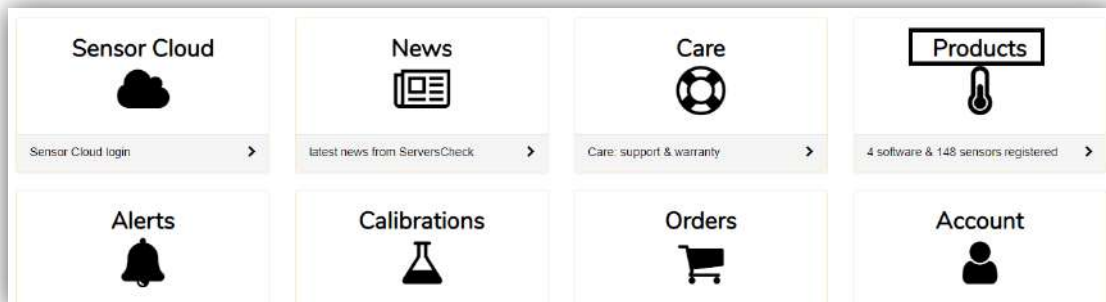
Note: The License Key only works on the computer it was issued for. Changing the installation of the software in another computer, requires a new license key.



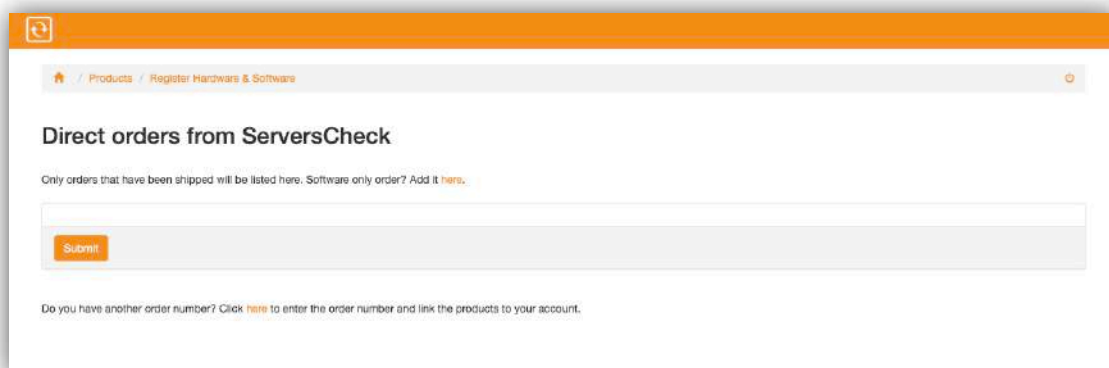
3. Clicking **Get License Key**, will redirect you to <https://my.infrasensing.com/> page. You need to Create an Account first if you do not have one yet, otherwise log in with your registered Email Address and Password.



4. Go to **Products** and register your purchases.



5. Register the software. You need to input the InfraSensing Order Number if you purchased directly from InfraSensing or from a Reseller.



6. After registering your Order, you need to Register your System ID to obtain an activation key. The System ID can be found in the Software's License Page.

Register System ID

As of version 14.4 a System ID is required to obtain a software activation key. The System ID can be found on the software's license page.

SKU
MON-APPLIANCE

System ID

Only alpha numeric characters and a dash character are allowed for the System ID. Length is 36 characters.

System Name

Close Save System ID

7. A license key will be generated in which you can copy and paste on the Software's License Page.

Product	Name	System ID	License Key	Support Until	Upgrades Until	Purchase Date
MON-APPLIANCE	Demo Appliance	BA304D	387c9a	2019-09-21	2019-09-21	2017-10-19

Note: Once the license is activated, you need to restart the software or the PC to apply the new license settings.

Additional Note: License Key can also be generated from your Order Page.

2.7.1. License Agreement

This document is a legal agreement between you (either an individual or a single entity), the "END USER," and ServersCheck BVBA, the "AUTHOR". By installing, copying or otherwise using the enclosed SOFTWARE you agree to be bound by the terms of this license agreement. As used in this License agreement, the term "SOFTWARE" means the SOFTWARE included on the CD, disk media, or otherwise electronically supplied SOFTWARE provided with this License Agreement. The term "SOFTWARE" does not include any SOFTWARE that is covered by a separate license offered or granted by a person other than the AUTHOR. This SOFTWARE product is licensed not sold.

This license agreement applies to versions 14.0.1 or higher of the SOFTWARE until replaced by another license.

IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, BEFORE INSTALLING OR EXECUTING, COPYING, OR OTHERWISE USING THE SOFTWARE, EITHER DESTROY OR RETURN, INTACT, THE SOFTWARE, CONTAINING THE CD OR DISK MEDIA, TOGETHER WITH THE OTHER COMPONENTS OF THE PRODUCT TO THE PLACE OF PURCHASE.

- 1. PROPRIETARY RIGHTS.** The SOFTWARE and any accompanying documentation are proprietary products of ServersCheck BVBA and are protected under European and U.S. copyright laws and international treaty provisions. You obtain no rights, title or other interests in or to the enclosed SOFTWARE or related documentation, including any copyright, patent, trade secret, trademark or other proprietary rights therein. Ownership of the SOFTWARE and all copies, modifications, and merged portions thereof shall at all times remain with ServersCheck BVBA. All copies of the enclosed SOFTWARE, in whole, or in part remain the intellectual property of ServersCheck BVBA unless otherwise specified.
- 2. GRANT OF LICENSE FOR SERVERSCHECK MONITORING SOFTWARE.** The SOFTWARE is licensed to you, which means you have the right to use the SOFTWARE only in accordance with this License Agreement. The SOFTWARE is considered in use on a computer when it is loaded into temporary memory, or installed into permanent memory. You may not sell, license, sublicense, transfer, assign, lease or rent (including via a timeshare arrangement) the SOFTWARE or the license granted by this Agreement.
- 3. NON PERMITTED USES.** Without the express permission of the AUTHOR, END USER may not (a) use, copy, modify, alter, or transfer, electronically or otherwise, the SOFTWARE or documentation except as expressly permitted in this License Agreement, or (b) translate, reverse program, disassemble, decompile, or otherwise reverse engineer the SOFTWARE, or (c) use, bundle or ship it as part of a service or a product for which the END USER receives a financial compensation.
- 4. TERM.** This license is effective from your date of purchase and shall remain in force until terminated. You may terminate the license and this License Agreement at any time by destroying the SOFTWARE and the accompanying documentation, together with all copies in any form. You agree to cease any and all further use of the SOFTWARE. This Agreement will terminate automatically if you breach any provision of this license agreement. Termination will have no effect on your obligation to safeguard proprietary rights of the AUTHOR under Section 1, or disclaimers under Section 8.
- 5. WARRANTIES AND LIABILITY.** The AUTHOR disclaims all warranties relating to this SOFTWARE. This SOFTWARE is distributed on an "AS IS" basis without warranties of any kind, whether expressed or implied, including without limitation any implied warranties of merchantability or fitness for any particular purpose. The AUTHOR or his suppliers assumes no liability for any damages, including but not limited to, special, incidental, consequential, indirect, loss of data, loss of profit, use of SOFTWARE or similar claims, or for any other reason. Even if the AUTHOR has specifically advised you of the possibility of such damage regardless of the form of the claim. The END USER bears all risk as to the quality and performance of the SOFTWARE. Should any other warranties be found to exist, such warranties shall be limited in duration to (90) days following the date of delivery to you. In no event will the AUTHOR's or his

suppliers' liability for any damages to you or any other person exceed the amount paid for the license to use the SOFTWARE.

6. HIGH RISK ACTIVITIES. The SOFTWARE is not fault-tolerant and is not designed, manufactured or intended for use or resale as on-line control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of the Software could lead directly to death, personal injury, or severe physical or environmental damage ("High Risk Activities"). ServersCheck BVBA and its suppliers specifically disclaim any express or implied warranty of fitness for High Risk Activities.

7. DISTRIBUTION & BUNDLING. The bundling of the SOFTWARE with other product(s) or service(s), or the distribution of the SOFTWARE in any form requires the purchase of Distribution and Bundling Agreement. Contact sales@ServersCheck.com for pricing information.

8. MARKETING. Unless END USER submits to the AUTHOR a written request that END USER's company and/or END USER's Web site cannot be used for marketing purposes, END USER hereby grants to AUTHOR the right to mention END USER's company and/or END USER's Web site as a customer site in its marketing materials, such as on AUTHOR's Web sites, in product brochures, or in other media. Such usage may include listing END USER's Web site, linking to END USER's Web site, and/or displaying END USER's company's logo as part of such listings or links.

9. FREE VERSION. The use of the free version of the SOFTWARE is only allowed when in use for personal, private use. Use by for profit organizations & government agencies requires a paid license.

10. This License Agreement constitutes the entire agreement between you and the AUTHOR pertaining to its subject matter. This License Agreement is governed by the laws of Belgium, and shall benefit the AUTHOR, his Successors and assigns. Any litigation arising from this license will be pursued only in the courts located in Leuven, Belgium.

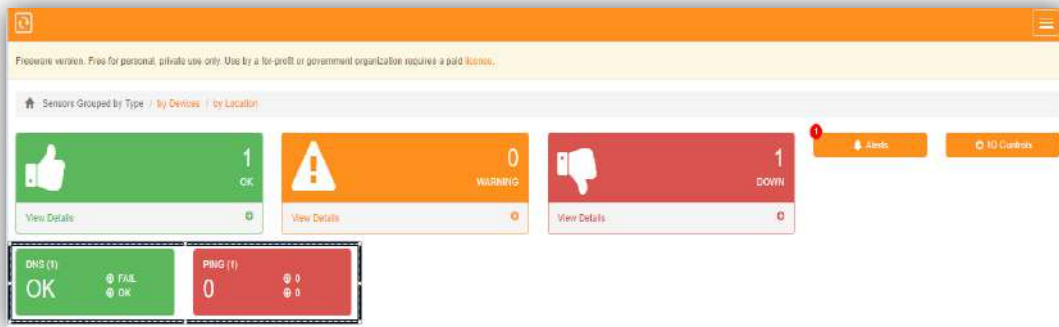
No responsibility is assumed by ServersCheck BVBA for the use or reliability of software.

For further information: Should you have any questions concerning this Agreement, or if you desire to contact the AUTHOR for any reason, please e-mail: hello@ServersCheck.com

Copyright 2003-2017 ServersCheck BVBA and 3rd parties.
All rights reserved.

3. Setting up Your First Checks

Upon installation of the software, it comes in with a default PING and DNS checks

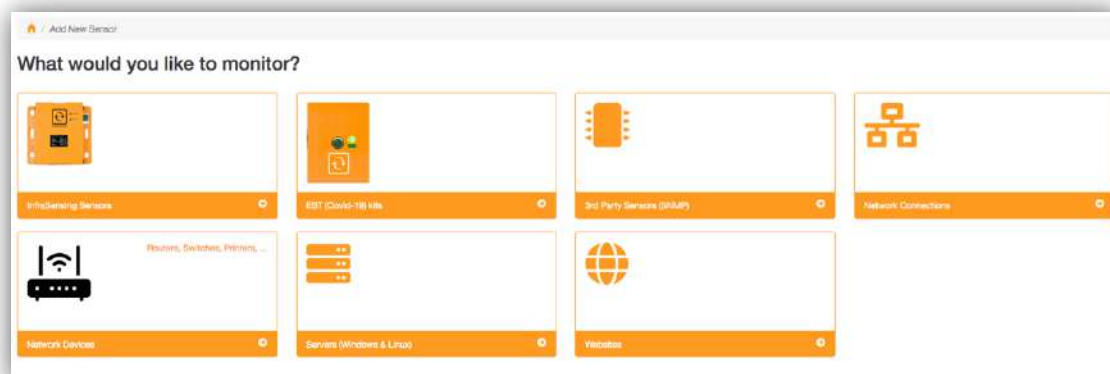


3.1. Adding ServersCheck Sensors (Environment, Power, Security, Industrial) & Controls

1. Click Menu and select Add New Sensor.



2. Select InfraSensing Sensors



3. Input the IP address of the SensorGateway as shown on the OLED display.

The screenshot shows a web interface for adding a new physical sensor. At the top, there is a breadcrumb trail: Home / Add New Sensor / Physical Sensor. The main heading is 'Add New Physical Sensor'. Below the heading, a message states: 'The system will scan your SensorGateway and detect any connected sensor to it.' The form contains several sections: 1. 'SensorGateway IP Address as shown on the OLED display' with a text input field containing '192.168.9.33'. 2. 'Use Default SNMP Connection Settings' with radio buttons for 'yes' (selected) and 'no, use custom settings'. 3. 'Control outputs on Sensorhub, IO Dry Contact or Multi-Sensor & Hub? Or do you have a Thermal Imaging Camera connected?' with radio buttons for 'yes' (selected) and 'no'. 4. 'SensorGateway's Username & Password' with a text input field for the username containing 'admin' and a password input field with masked characters '.....'. At the bottom of the form are two buttons: 'Submit' (orange) and 'Back' (white).

Use Default SNMP Connection Settings

If Yes,
default Community String - **public**
default Port - **161**

If No,
Use the Community String set under SNMP Settings of the Sensorgateway.

If your SensorGateway is connected to a Sensorhub, IO or Multisensor, select Yes. Then it prompts for the SensorGateway Username and Password.

Sensorgateway's Username & Password

Default Username - **admin**
Default Password - **admin**

If the Username and Password was changed on the Sensorgateway, input the new Username and Password to access the Sensorgateway.

4. The following sensors connected to the Sensorgateway should automatically be detected, and you can also modify Sensor Name and the Sensor Type. By default, all are selected. But you can only select which sensors you wish to monitor.

Note: If there are dry contacts connected, it will have to be monitored via SNMPTRAPS and will not show on the list

Monitor	Sensor Name	Sensor Type	Value
<input checked="" type="checkbox"/>	Int. Temp1	TEMPERATURE	29.92
<input checked="" type="checkbox"/>	Int. Ping1	PING	215.00
<input checked="" type="checkbox"/>	Airflow1	AIRFLOW	0.00
<input checked="" type="checkbox"/>	Dust Sensor1	DUST	0.02
<input checked="" type="checkbox"/>	Airflow1	AIRFLOW	0.00
<input checked="" type="checkbox"/>	PowerFail1	POWER FAILURE	PWR FAIL
<input checked="" type="checkbox"/>	Airflow1	AIRFLOW	0.00
<input checked="" type="checkbox"/>	Sound Meter1	SOUND	43.07
<input checked="" type="checkbox"/>	Dew Point1	DEW	-20.00
<input checked="" type="checkbox"/>	Ext. Temp1	TEMPERATURE	26.06
<input checked="" type="checkbox"/>	Humidity1	HUMIDITY	48.02
<input checked="" type="checkbox"/>	Dew Point1	DEW	15.67
<input checked="" type="checkbox"/>	Ext. Temp2	TEMPERATURE	26.81
<input checked="" type="checkbox"/>	Humidity2	HUMIDITY	84.31
<input checked="" type="checkbox"/>	Dew Point2	DEW	19.67

5. Next screen should appear if you have Output controls selected. You can modify the Control Name also.

[Home](#) / [Add New Sensor](#) / [Physical Sensor](#) / [Remote Controls](#)

Add Remote Control

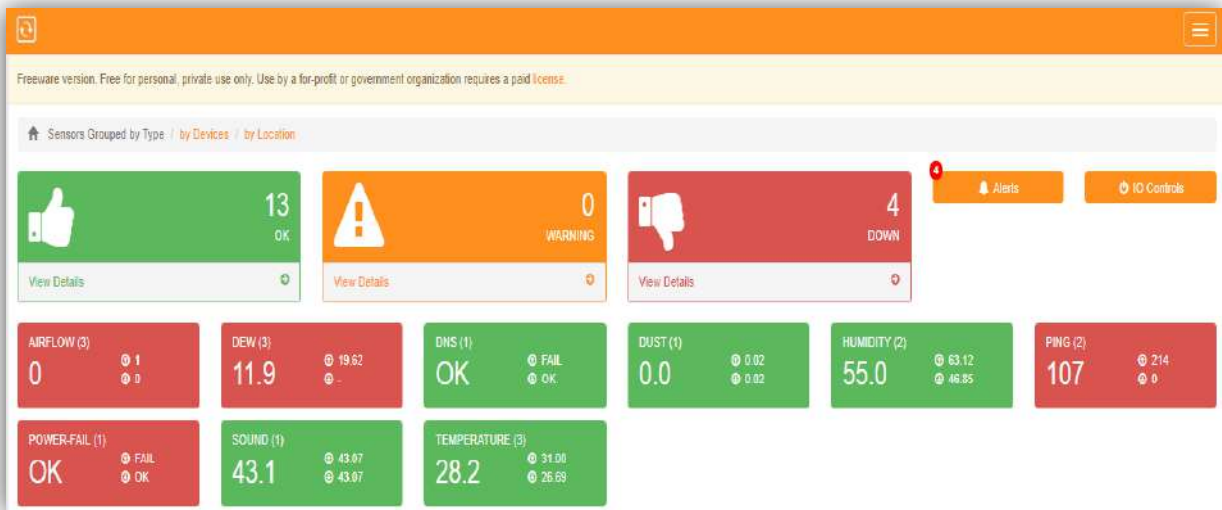
Output controls can be found on the SensorHub, IO Dry Contact sensor and the Multi-Sensor & Hub. While scanning your SensorGateway, we found following remote controls. You can change the name of the remote controls in this form or change it in the SensorGateway and then re-run this wizard.

Control ID	Control Name
0	Output1
1	Output2
2	Output3
3	Output4
4	Relay1
5	Relay2

- If successful, the device/sensors will then be added to the database.

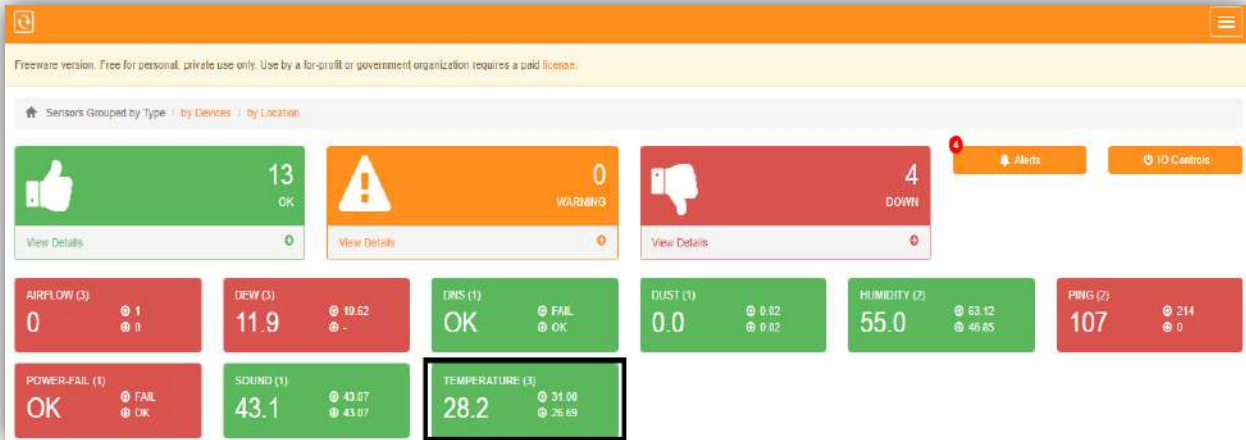


- After adding up the device and the sensors, you should be able to see it on the Dashboard.



3.2. Editing a Sensor/Check

1. By default on the dashboard, all sensors are grouped by Type. Click an individual Sensor Type. In this example, we selected Temperature.



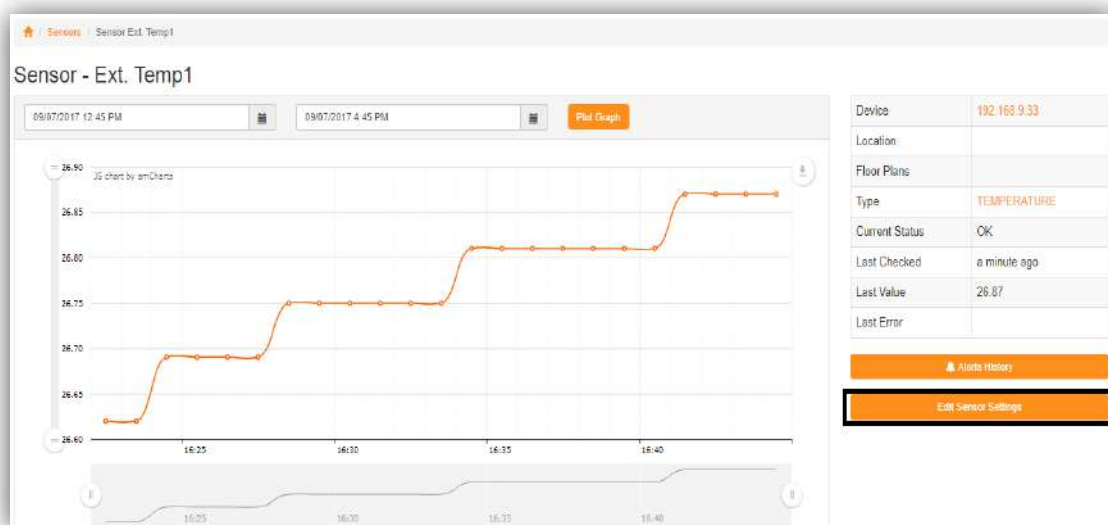
2. This gives you a list of all sensors with the same type.

The screenshot shows the "Sensors List" page for the TEMPERATURE type. It displays a table with the following data:

Sensor Type	Status	Name	Last Value	Last Check
TEMPERATURE	OK	Int. Temp1	31.57	a few seconds ago
TEMPERATURE	OK	Ext. Temp1	26.87	a few seconds ago
TEMPERATURE	OK	Ext. Temp2	25.94	a few seconds ago

The page also includes a search bar, a "Show 10 entries" dropdown, and "Previous" and "Next" navigation buttons.

3. Select an individual sensor to open up the sensor parameters. By clicking Edit Sensor Settings, you can then customize with several options that are further explained below.



4. General Tab

The screenshot shows the 'General' tab of the 'Sensor - Ext. Temp1' settings page. The breadcrumb trail is 'Sensors / Sensor Ext. Temp1 - Stats / Edit Sensor Settings'. The page title is 'Sensor - Ext. Temp1'. There are four tabs: 'General' (selected), 'Parameters', 'Alert Levels', and 'Alert Notifications'. The 'Sensor Name' field contains 'Ext. Temp1'. The 'Sensor Type' dropdown is set to 'TEMPERATURE'. The 'Device' dropdown is set to '192.168.9.33'. The 'Sensor Running' field has a play button icon. The 'Checking Interval (in seconds)' field contains '60'. At the bottom, there are 'Save', 'Back', and 'Delete Sensor' buttons.

Sensor Name - You can customize a name for that specific sensor.

Sensor Type - Will show what type of Sensor it is.

Device - List of individual devices to which that specific sensor will be grouped under.

Sensor Running - Able to Play or Pause the monitoring of the sensor.

Checking Interval (in seconds) - Number of seconds before it gets the current value of a sensor.
Minimum - 30 seconds
Default value - 60 seconds

Delete Sensor - If you want to delete the sensor completely from the list.

5. Parameters Tab

The screenshot shows the 'Parameters' tab of the 'Sensor - Ext. Temp1' settings page. The breadcrumb trail is 'Sensors / Sensor Ext. Temp1 - Stats / Edit Sensor Settings'. The page title is 'Sensor - Ext. Temp1'. There are four tabs: 'General', 'Parameters' (selected), 'Alert Levels', and 'Alert Notifications'. The 'IP Address' field contains '192.168.9.33'. The 'Community String' field contains 'public'. The 'Port' field contains '161'. The 'OID' field contains '1.3.6.1.4.1.17095.11.4.2.0'. At the bottom, there are 'Save' and 'Back' buttons.

IP address - Setting the IP address you set for that sensor.

Community String - Handshaking used for SNMP.
Default - public

Port - SNMP port.
Default - 161

OID - You can manually input the OID string.

6. Alert Levels Tab

The screenshot shows the 'Alert Levels' configuration page for 'Sensor - Ext. Temp1'. It features four tabs: 'General', 'Parameters', 'Alert Levels' (active), and 'Alert Notifications'. The page is divided into two main sections: 'Set sensor in WARNING state when' and 'Set sensor in DOWN state when'. Each section contains two rows of configuration. Row 1 includes a 'Sensor Value' input, a dropdown menu labeled 'A.', a text input labeled 'B.', and a dropdown menu with a question mark. Row 2 includes a dropdown menu labeled 'C.' and another dropdown menu with a question mark. Row 3 includes another 'Sensor Value' input, a dropdown menu labeled 'D.', a text input labeled 'E.', and another dropdown menu with a question mark. At the bottom, there are 'Save', 'Back', and 'Delete Sensor' buttons.

Setting up specific thresholds for Warning state and Down State.

Alert levels for both warning state and down state works by completing the statements:

- A. First threshold level. You may select if a certain sensor is : less than (<), greater than (>), equals (=), contains, ignore
- B. Input a value based on what you selected on (A).
- C. You can select AND or OR if you want to include another specific threshold level.
- D. Second threshold level. You may select if a certain sensor is : less than (<), greater than (>), equals (=), contains, ignore
- E. Input a value based on what you selected on (D).

Note: Example of a Warning state is if temperature value is at 44 deg C, Down state should be configured at 48 deg C with the same settings as explained above.

7. Alert Notifications Tab

The screenshot shows the 'Alert Notifications' configuration page for 'Sensor - Ext. Temp2'. It features four tabs: 'General', 'Parameters', 'Alert Levels', and 'Alert Notifications' (active). The page is divided into three main sections: 'Send Email Alerts', 'Send SMS Alerts', and 'Send Slack Alerts'. 'Send Email Alerts' has radio buttons for 'no', 'yes to the default email address(es)', and 'yes to this address(es)', with a text input field below. 'Send SMS Alerts' has radio buttons for 'no', 'yes to the default SMS number(s)', and 'yes to this number(s)', with a text input field below. 'Send Slack Alerts' has radio buttons for 'no' and 'yes to the default channel'. Below these is a 'Custom Alert Message' section with a text area. At the bottom, there are 'Save' and 'Back' buttons.

Able to send Email notifications, SMS notifications or Slack Alerts if the thresholds you set are met.

Send Email Alerts

no - If no email is to be sent

yes to default email address(es) - If to be sent to what you set under Section 2.4.

yes to this address(es) - If to be sent to specific email address(es).

Note: separator is a comma, no spaces.

Send SMS Alerts

no - If no SMS is to be sent.

yes to default SMS number(s) - If to be sent to what you set under Section 2.5.

yes to this number(s) - If to be sent to specific phone number(s).

Note: Use valid phone numbers (+ symbol and numbers only). For multiple numbers, use a comma as a separator. For example: +180075489, +334546545

Send Slack Alerts

no - if no Slack message is to be sent.

yes to the default channel - If to be sent to what you set under Section 2.6.

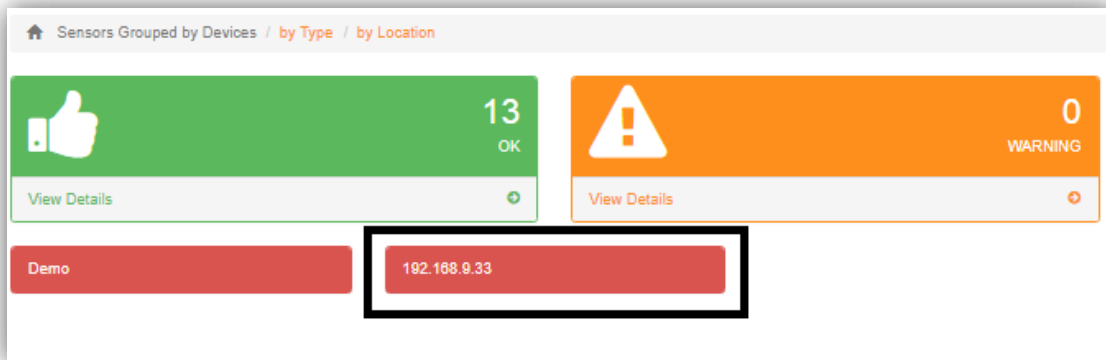
Custom Alert Message - Allows you to create your own customizable message to be sent when there is an alert.

3.3. Editing a Device and Adding Location

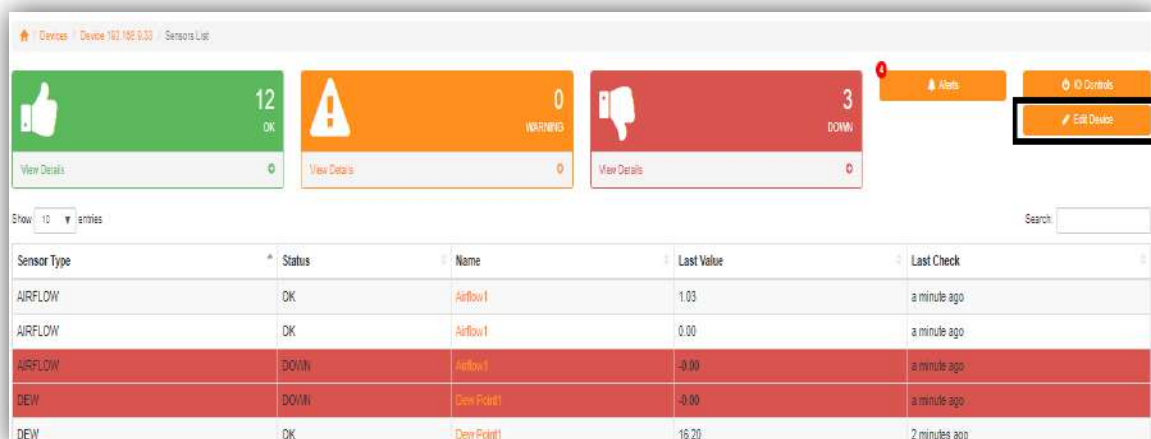
1. From the Dashboard screen, select Sensors Grouped by Devices.



2. Select a device you want to edit.



3. This screen shows you all sensors that are connected within the device. By clicking **Edit Device**, you can then customize with several options that are further explained below.



4. General Tab

The screenshot shows the configuration page for a device with IP 192.168.9.33. The 'General' tab is selected. The form includes fields for 'Device Name' (Demo Test), 'Device IP Address' (192.168.9.33), a 'Device Active' toggle (currently off), and a 'Locations' dropdown menu (Add a new location). At the bottom, there are 'Save', 'Back', and 'Delete Device' buttons.

Device Name - You can customize a name for the Device type.

Device IP address - Setting up/editing the IP address of the device.

Device Active - Able to Play or Pause the monitoring of the device.

Locations - Able to edit the location of the device to anywhere in the world.

Delete Device - Delete a device completely from the list.

4.1. Adding a Location > Select Add a New Location.

This screenshot is identical to the one above, but with a black rectangular box highlighting the 'Add a new location' button in the 'Locations' dropdown menu.

- 4.2. Input the details of the location. Then click Save Location. Once you have added the location, you can now then select the Location Name from the Dropdown menu on Locations.

Add a new location

new york

Find Address

Search results:

- [New York City, New York, United States of America](#)
- [New York, United States of America](#)
- [New York, New York City, New York, United States of America](#)
- [New York, Tyne and Wear, North East England, England, United Kingdom](#)
- [New York, Santa Rosa County, Florida, United States of America](#)

Location name

Give a name to this location

Latitude

40.7306458

Longitude

-73.9886136

Location address

New York City, New York, United States of America

Close Save location

Type in an address - Input specific address where the device is located to search. Search results lists all the addresses from the address you input.

Note: selecting from any of the search results will automatically provide the Latitude and Longitude of the address.

Location Name - Providing specific name of the location.

Latitude - You can manually input the latitude of the address.

Longitude - You can manually input the longitude of the address.

Location Address - You can input the specific address of the location.

Upon adding a location, this will enable you to set up a Floor Plan which will be explained further in Section 3.4 of the manual.

5. SNMP Tab

Home / Devices / [Devices 192.168.9.33 Sensors](#) / Edit Device 192.168.9.33 Sensors

Device - 192.168.9.33

<> General **SNMP** Web Credentials

Community String

public

Port

161

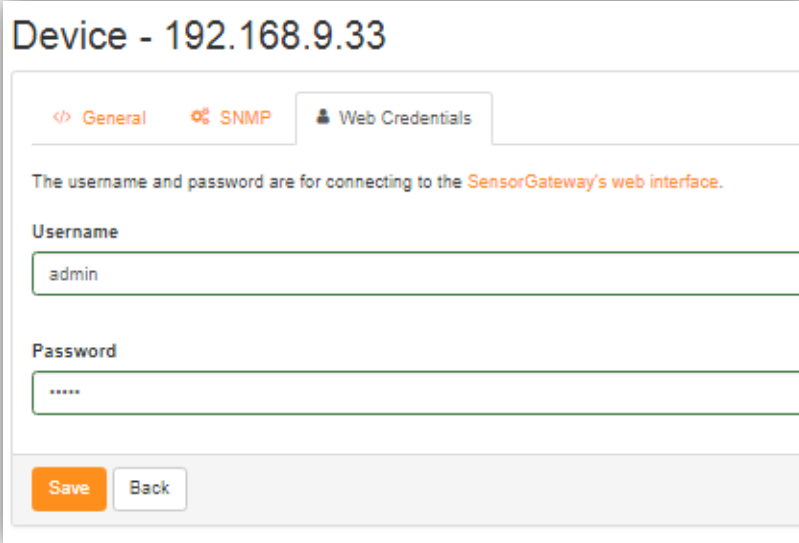
Save Back

Community String - The handshake for SNMP.
Default value - **public**

Port - Input the SNMP port.
Default - 161

6. Web Credentials Tab

This is for the username and password used to connect to the Sensorgateway's Web Interface.



Device - 192.168.9.33

<> General 🔌 SNMP 👤 Web Credentials

The username and password are for connecting to the **SensorGateway's web interface**.

Username

Password

Save Back

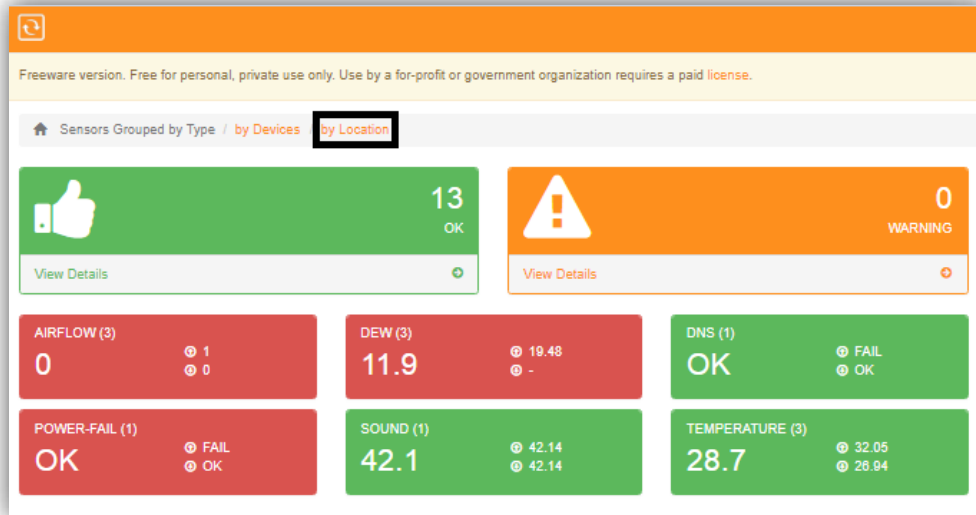
Username - The same username used to access the Sensorgateway's Web Interface.
Default - admin

Password - The same password used to access the Sensorgateway's Web Interface.
Default - admin

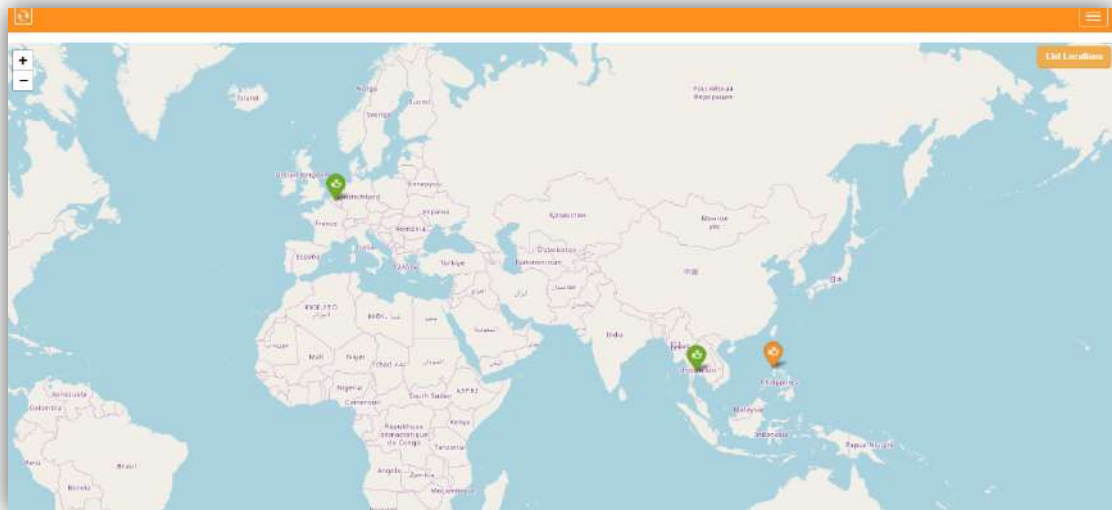
3.4. Adding a Floor Plan

Upon grouping your devices by location, you also have an option to upload a floor plan wherein you can place your sensors on that specified location.

1. From your Dashboard screen, group your devices by **Location**.



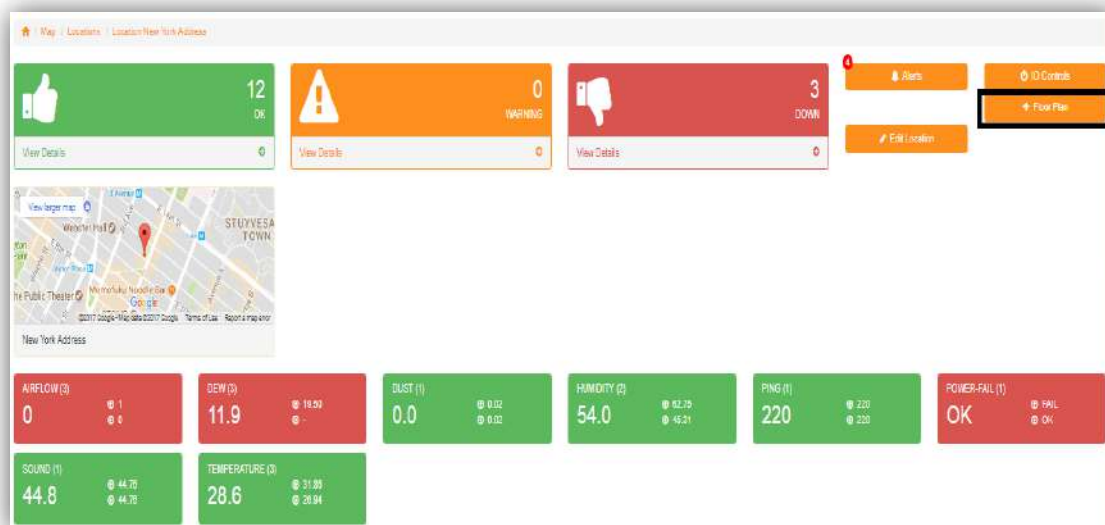
2. This opens up the world map where you see all of the devices set on different addresses.



3. Clicking View Details on each of the address will show all of the status of the devices which are normal, in warning, and down.



4. Click Add Floor Plan.



Save a copy of a floor plan design in PNG file format for **Temperature layer**, **Humidity Layer** and **Flooding Layer** or a single design for all.

Where to save the floor plan?

* Locate the directory where you saved the Monitoring Software.

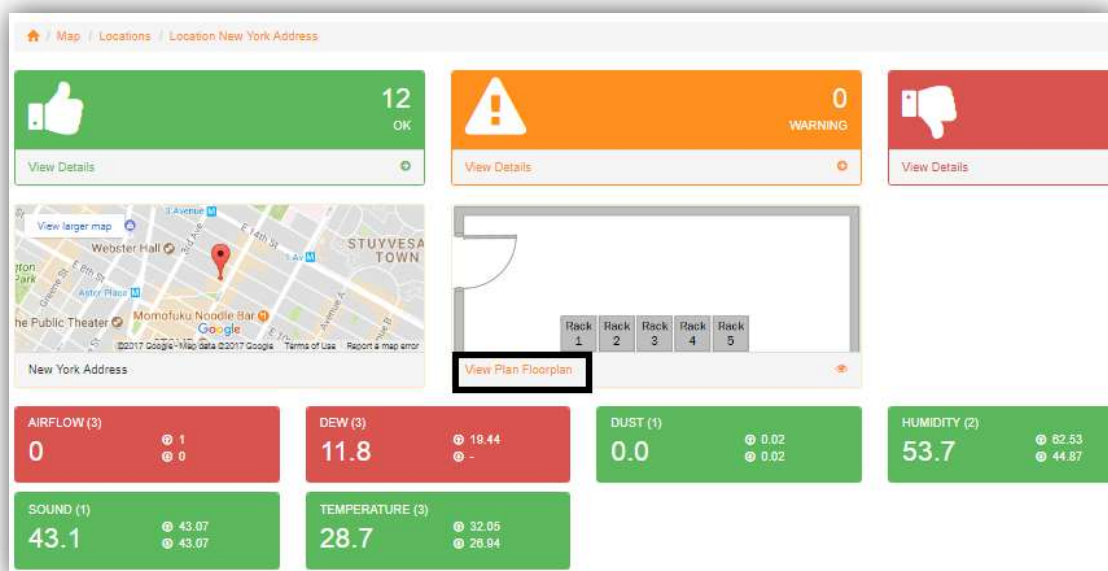
Copy the 2D floor plan in PNG format to the **/static/uploaded** subfolder of your main ServersCheck installation.

Once you have saved a floor plan, it should appear on a list of PNG files. Select one you wish to add by clicking on the one with the box as shown below.

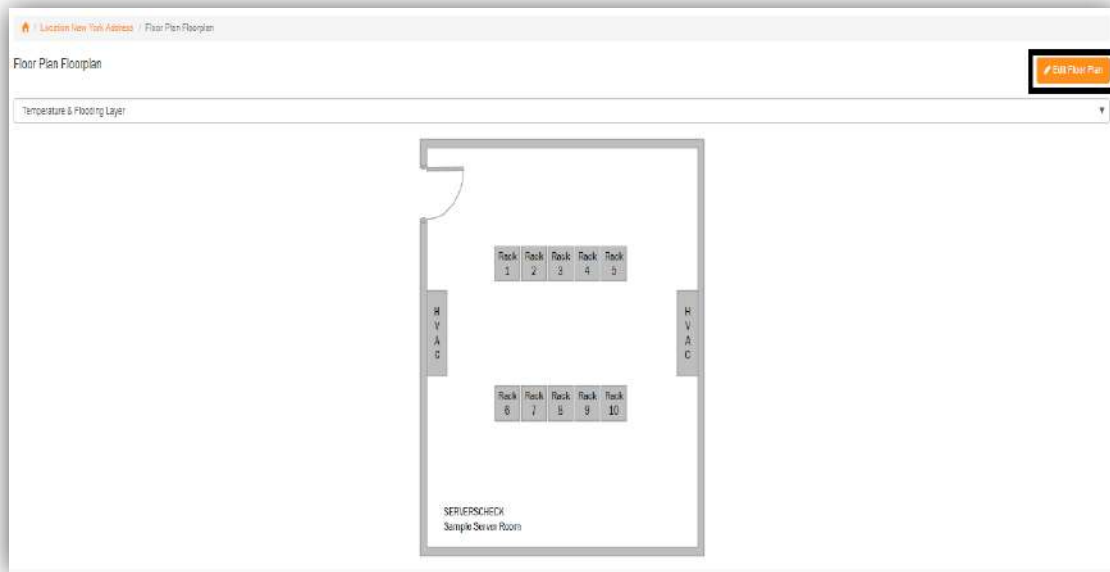


5. Adding your Sensors to your Floor Plan

- Click **View Floor Plan**.



- Click **Edit Floor Plan**.



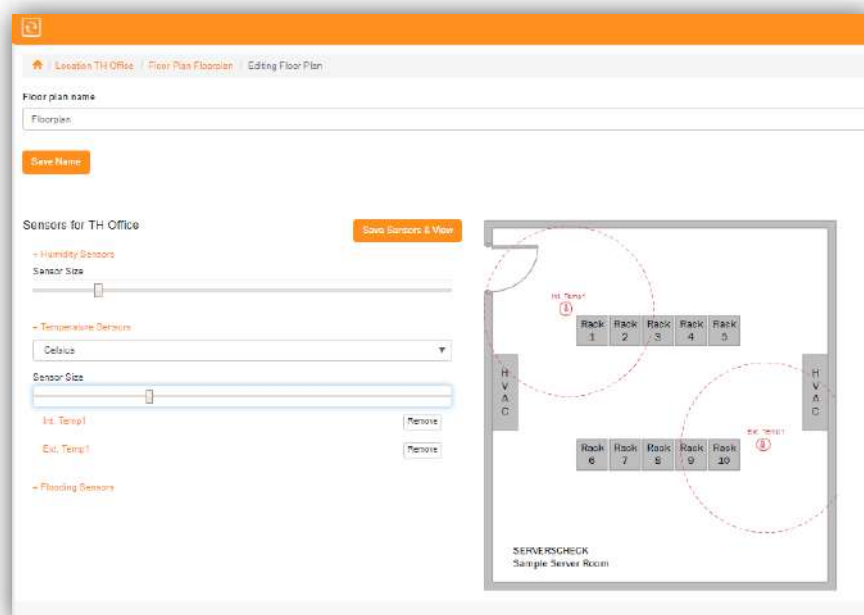
- Place your sensors to the Floor Plan.

Floor Plan Name - you can rename the Floor plan name.

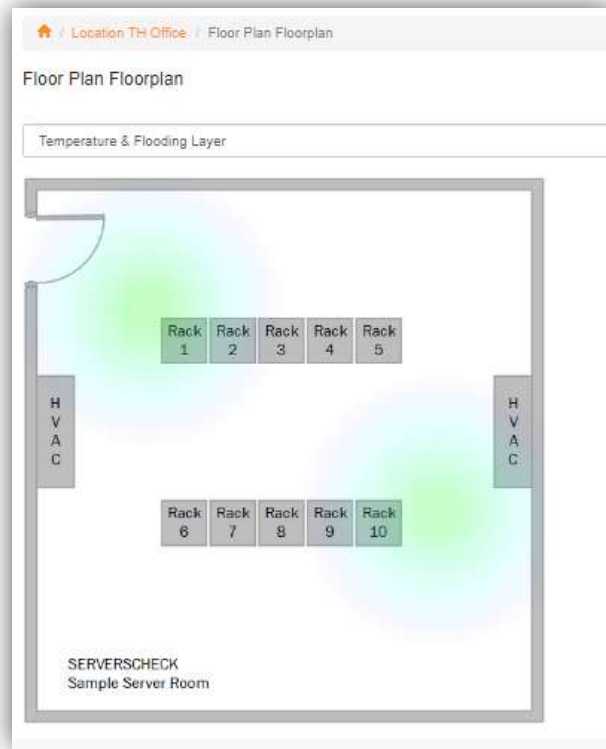
You do have options to place sensors on the Floor Plan. If you have a list of Humidity, Temperature and Flooding Sensors, you will be able to place it on the floor plan.

- Move or place the sensors to the specific location of the floor plan.
- You can adjust the Sensor size with respect to the scale of the floor plan.
- Able to change Celsius or Fahrenheit temperature unit as the software will automatically adjust the color zones.
- The archived maps are stored in the respective archive subfolders. For temperature, this is **/heatmaps/temperature/archive**

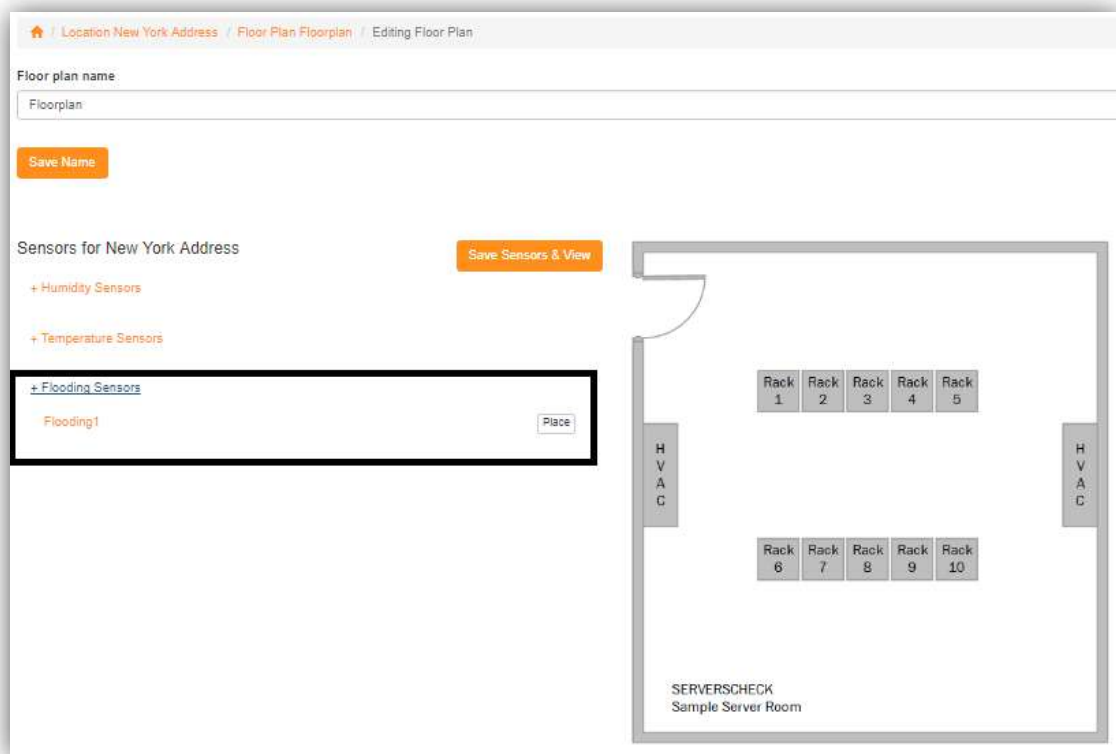
Then click **Save Sensors & View**.



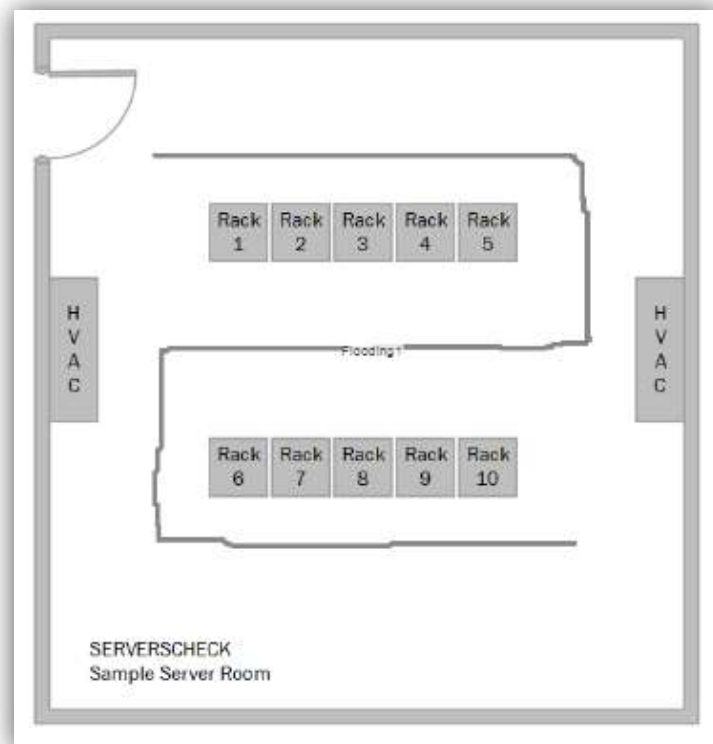
This should show similar as the one below.



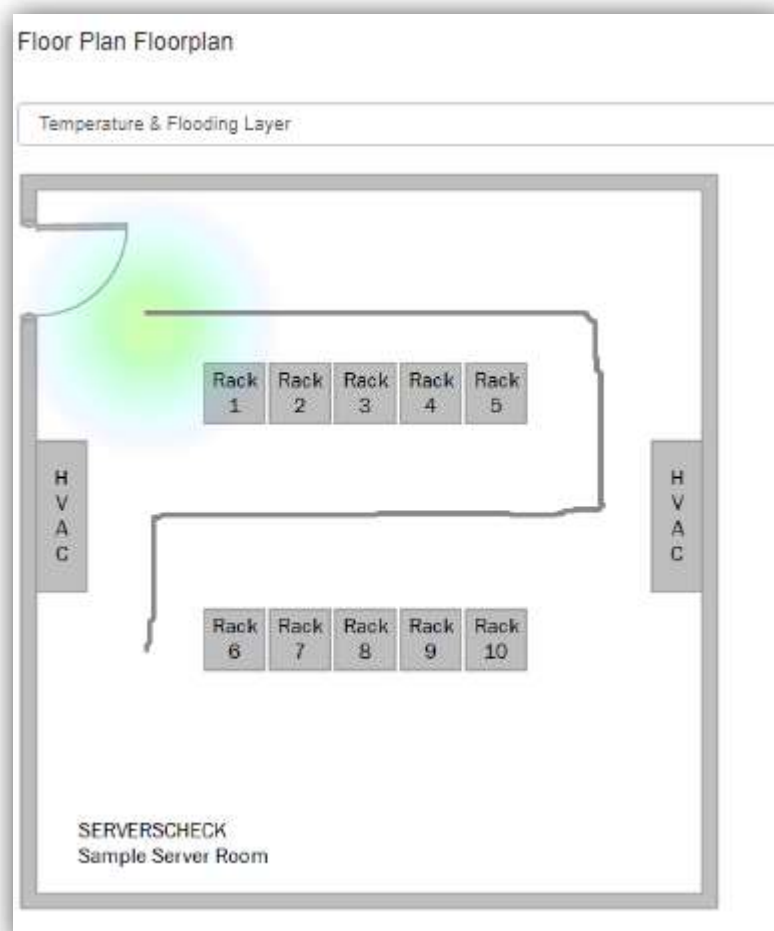
If you have a Leak sensor added, it will also let you place the Leak Detection Cable on the floor plan.



You can then draw the section of the Leak sensor on the floor plan.



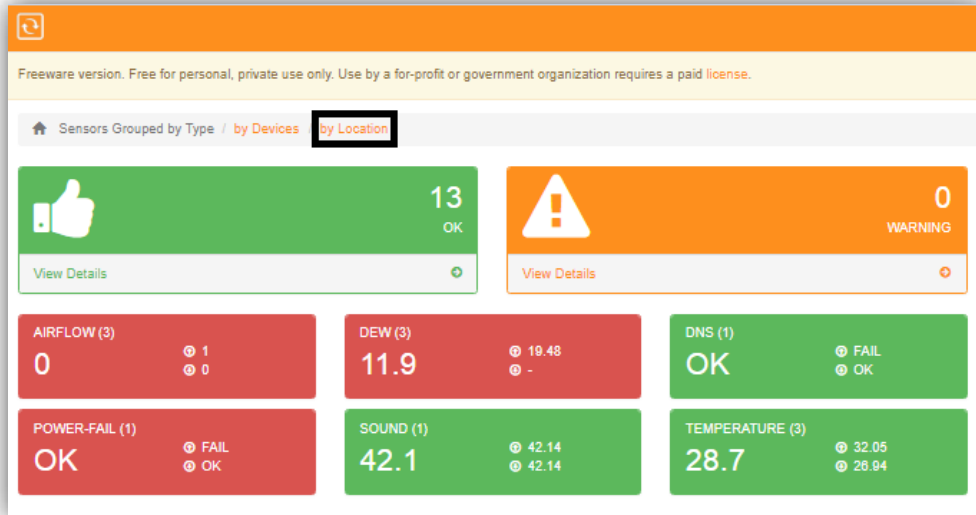
This should show similar to the image below.



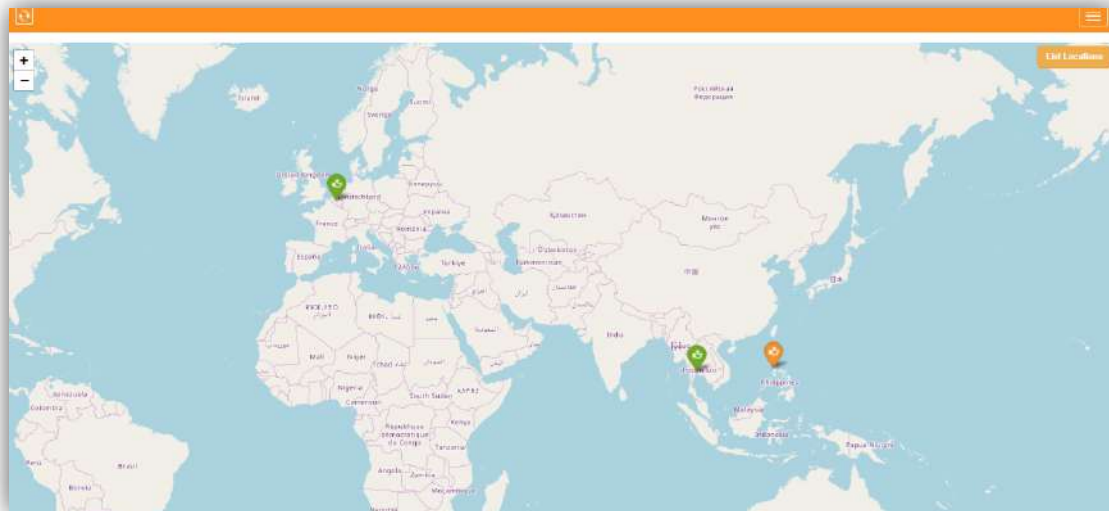
3.5. Adding a Thermal Image

If you have a Sensorgateway connected with a Thermal Imaging Camera, once you have added it as shown in Section 3.1. It should be detected to show on the dashboard when you group devices by location.

1. From your Dashboard screen, group your devices by Location.



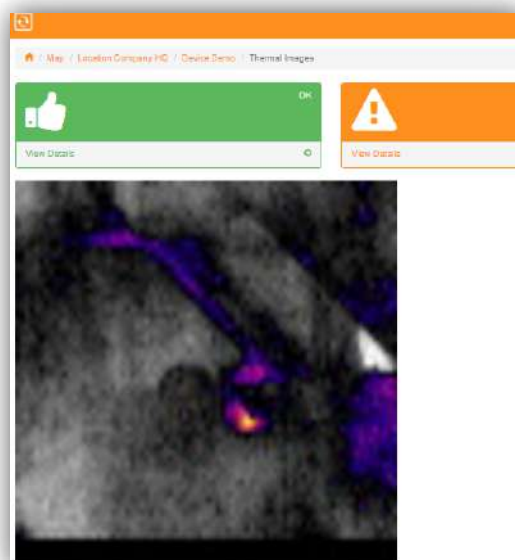
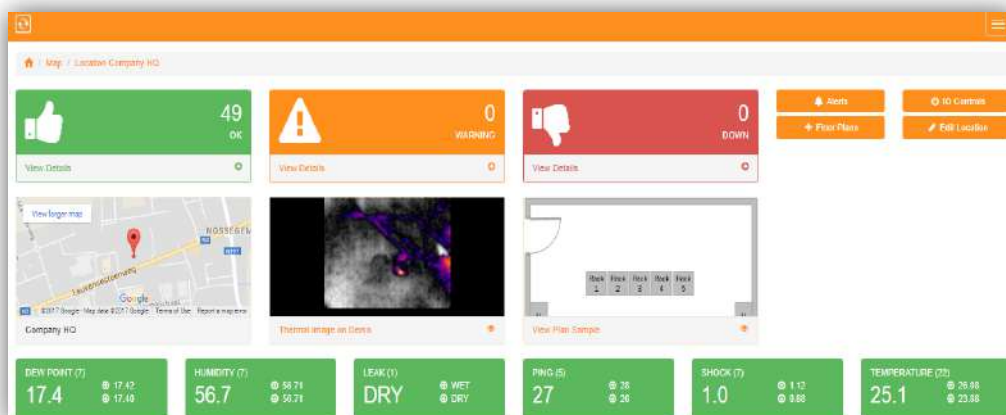
2. This opens up the world map where you see all of the devices set on different addresses.



3. Clicking View Details on each of the address will show all of the status of the devices which are normal, in warning, and down.



4. It should show as similar to the images below

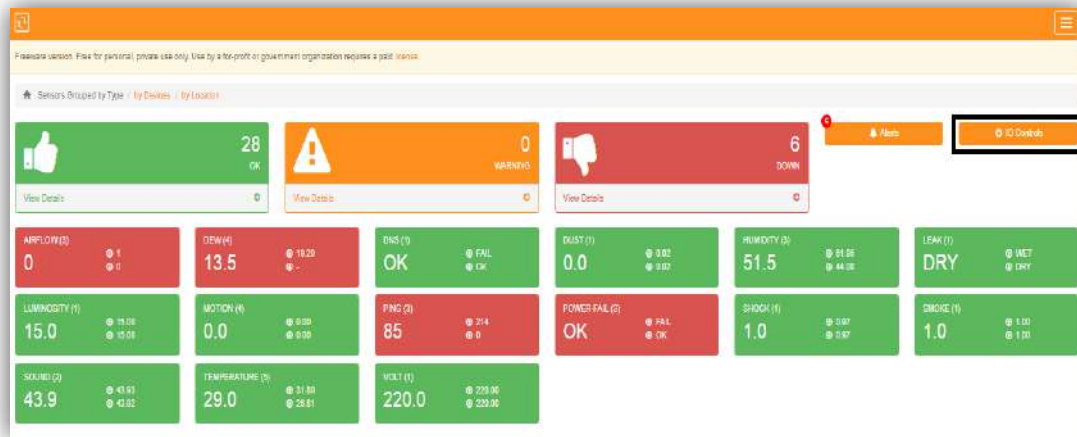


3.6. Controlling Outputs and Relays

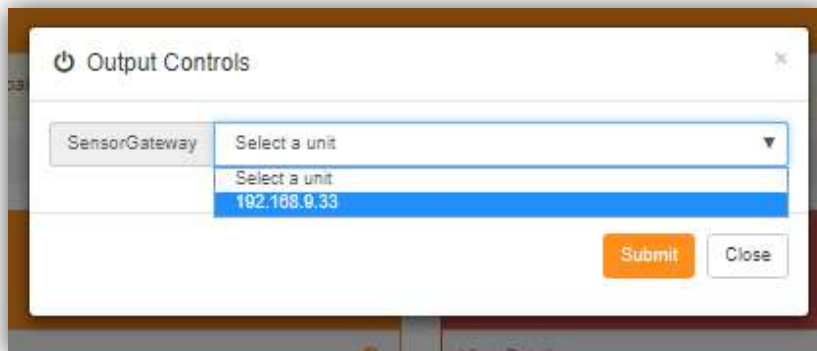
After adding ServersCheck sensors shown in Section 3.1, it does gives you an option to include I/O controls if your device has a Sensorhub, IO Dry Contact Sensor or Multi-Sensor & Hub.

Section 3.1, number 5 gives you a full list of IO sensors. Once added, it should appear on the Dashboard option of the software.

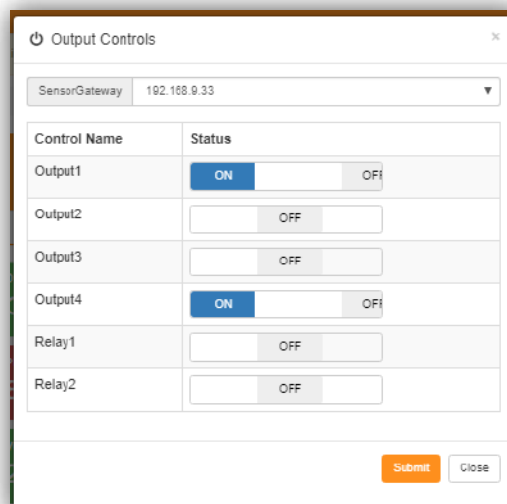
1. From the Dashboard screen, select **IO Controls**.



2. You will see a drop down list of all Sensorgateway devices that you have added that has IO sensors.



3. Select to one of the Sensorgateway that you want to control the Outputs. Choose an output or relay you wish to override.

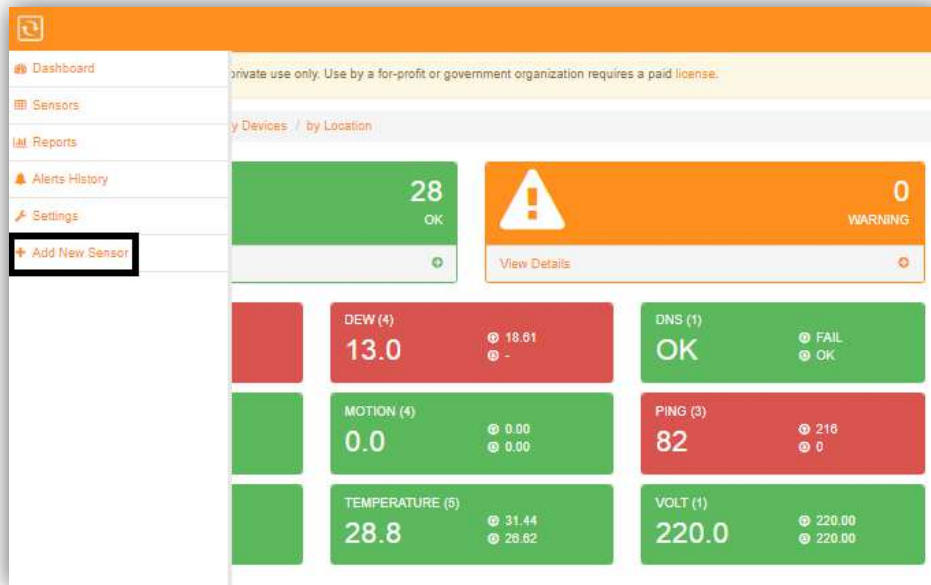


4. Setting up Other Check Type

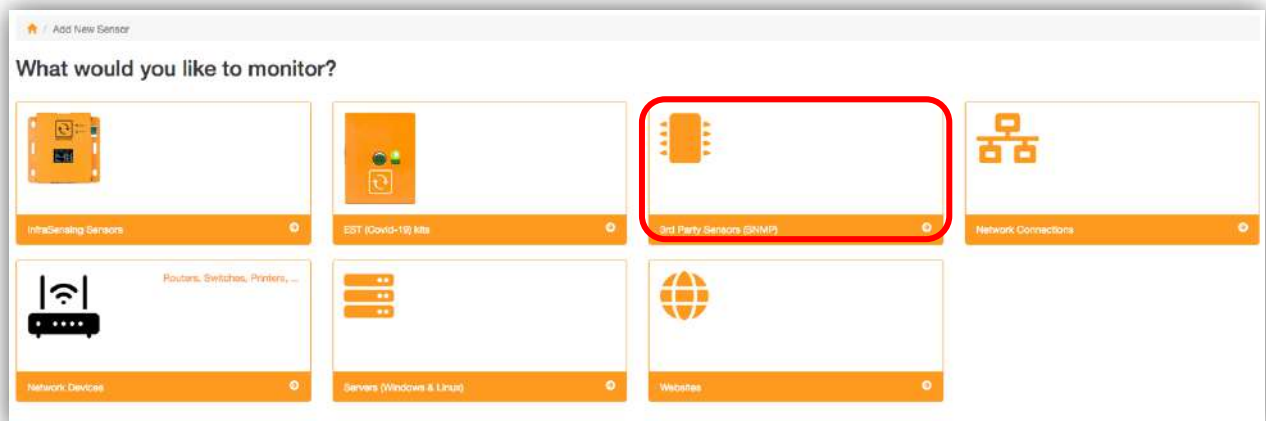
4.1. Adding Checks for 3rd Party Sensors (SNMP)

This check will allow you to monitor other 3rd party SNMP sensors. Only SNMP capable devices will be able to be added under this check.

1. Access **Menu** and Click **Add New Sensor**.



2. Select **3rd Party Sensors (SNMP)**.

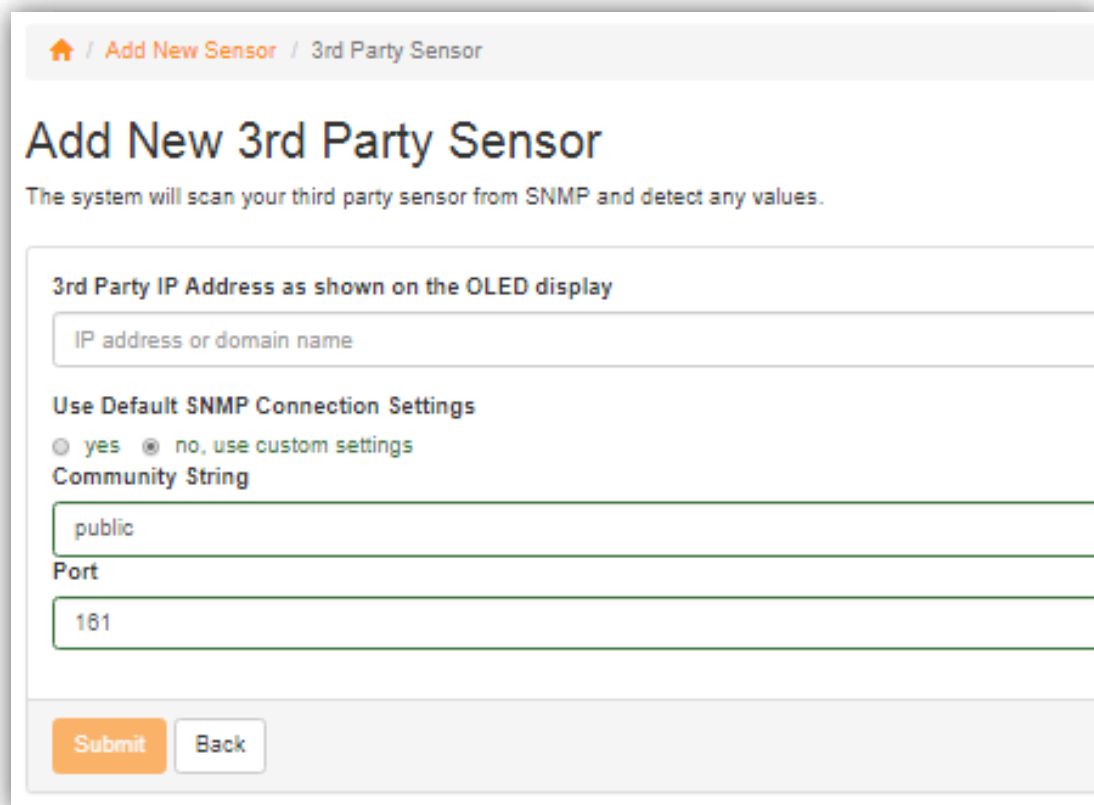


3. Input the IP address or Domain Name of the 3rd party sensor you want to monitor.

Use Default SNMP Connection Settings

If Yes,
default Community String used for the 3rd party device.
default Port used for the 3rd party device

If No, use custom settings
Use the Community String and port set for the 3rd party device.



The screenshot shows a web interface for adding a new 3rd party sensor. The breadcrumb trail at the top reads: Home / Add New Sensor / 3rd Party Sensor. The main heading is "Add New 3rd Party Sensor". Below the heading is a sub-heading: "The system will scan your third party sensor from SNMP and detect any values." The form contains the following fields and options:

- 3rd Party IP Address as shown on the OLED display**: A text input field containing "IP address or domain name".
- Use Default SNMP Connection Settings**: Two radio buttons. The first is labeled "yes" and is unselected. The second is labeled "no, use custom settings" and is selected.
- Community String**: A text input field containing "public".
- Port**: A text input field containing "161".

At the bottom of the form are two buttons: "Submit" (orange) and "Back" (white).

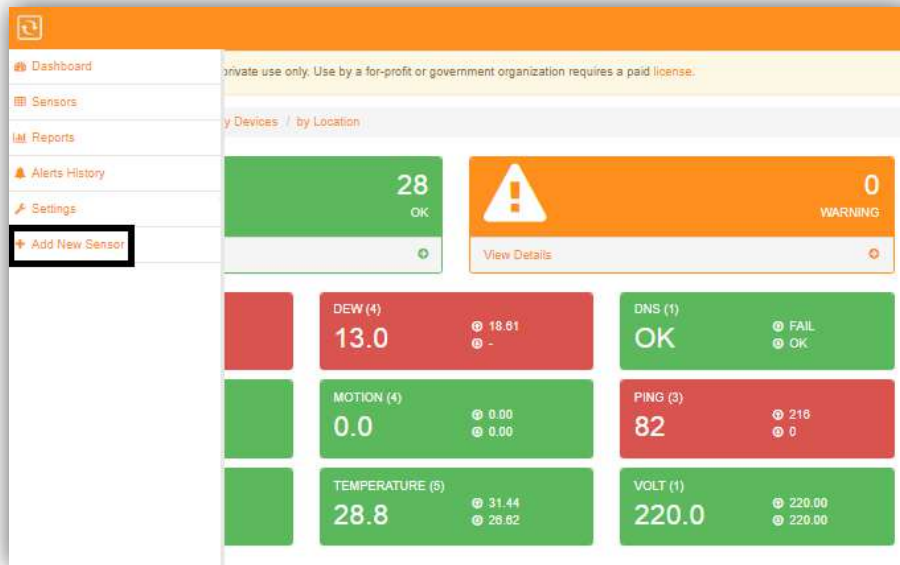
4.2. Adding Checks for Network Connections

ServersCheck Software monitors your network performance and capability.

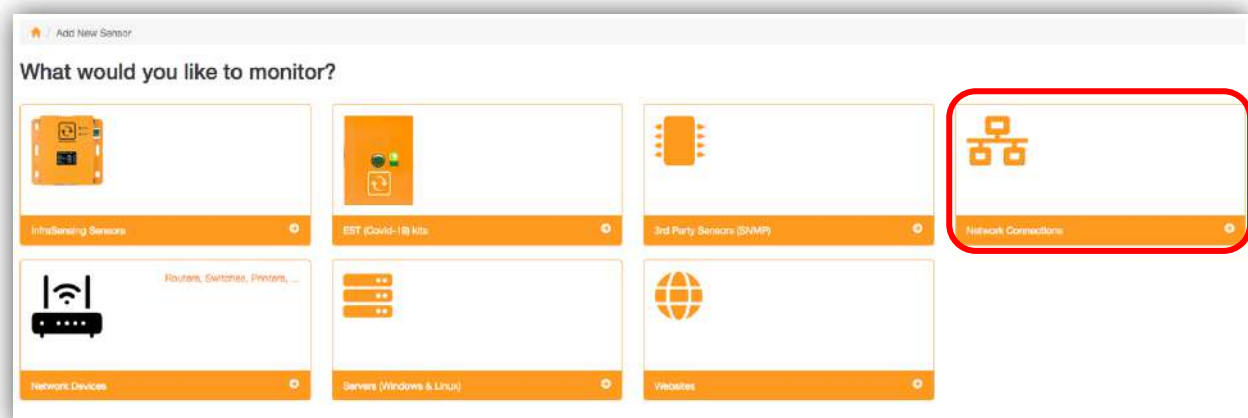
4.2.1. Adding Ping Check

This check will perform an ICMP ping to the destination server to check if server is available for connection. This check will send a ping command to a destination server and will retrieve the response time.

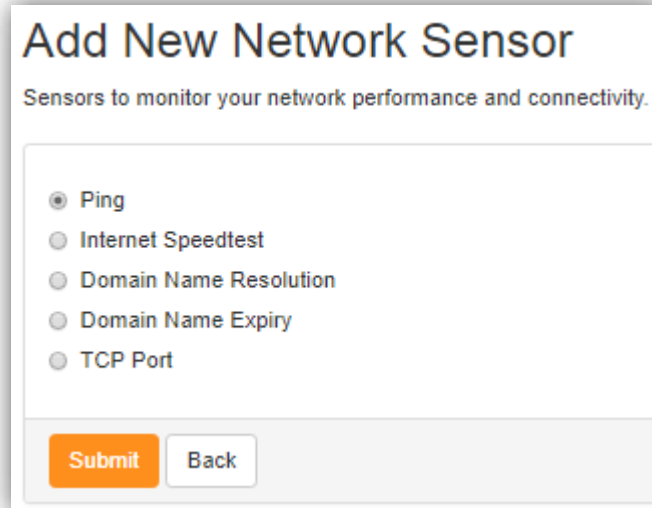
1. Access **Menu** and Click **Add New Sensor**.



2. Select **Network Connections**.



3. Select PING.

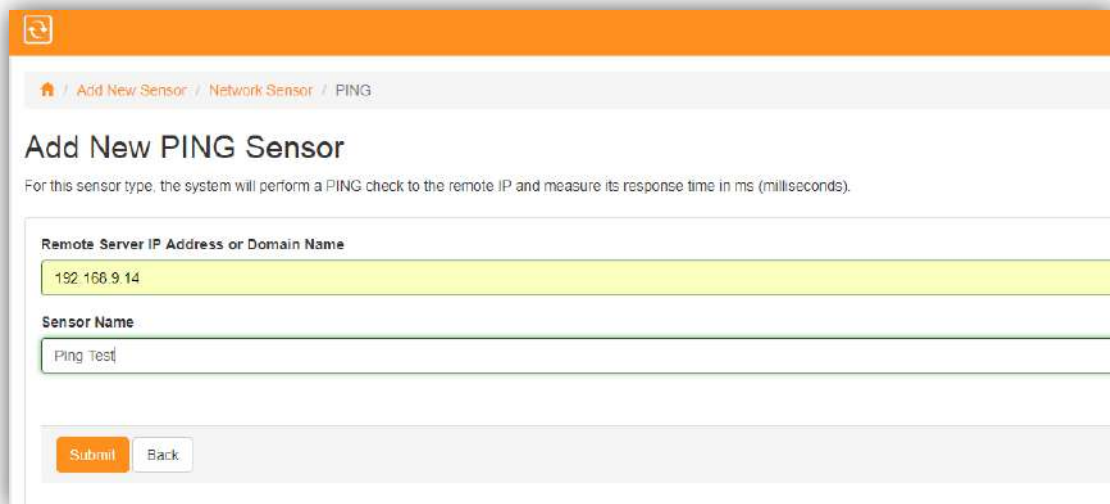


Add New Network Sensor
Sensors to monitor your network performance and connectivity.

- Ping
- Internet Speedtest
- Domain Name Resolution
- Domain Name Expiry
- TCP Port

Submit **Back**

4. Input the IP address or Domain Name you want to monitor and put a Sensor Name. This Sensor Name will be the name that should appear on the Dashboard.



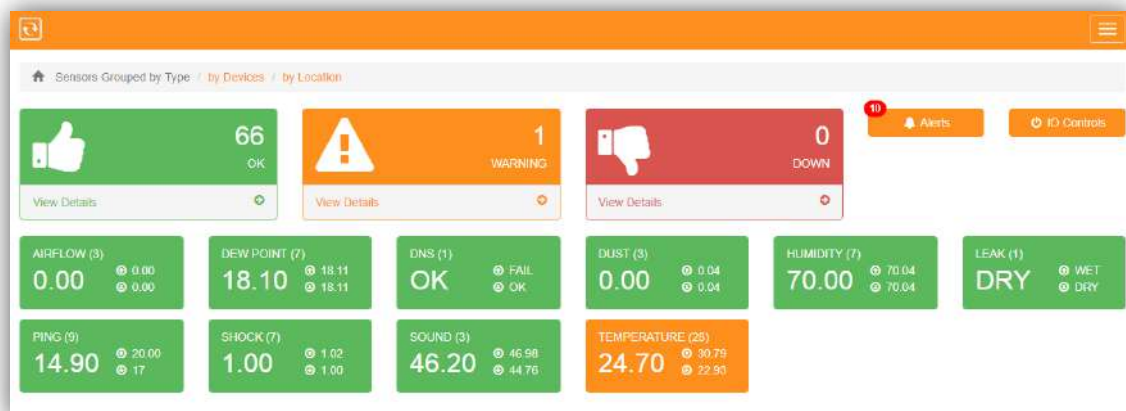
Add New PING Sensor
For this sensor type, the system will perform a PING check to the remote IP and measure its response time in ms (milliseconds).

Remote Server IP Address or Domain Name
192.168.9.14

Sensor Name
Ping Test

Submit **Back**

5. Once done, it should appear as one of the monitored checks on the Dashboard.



Sensors Grouped by Type / by Devices / by Location

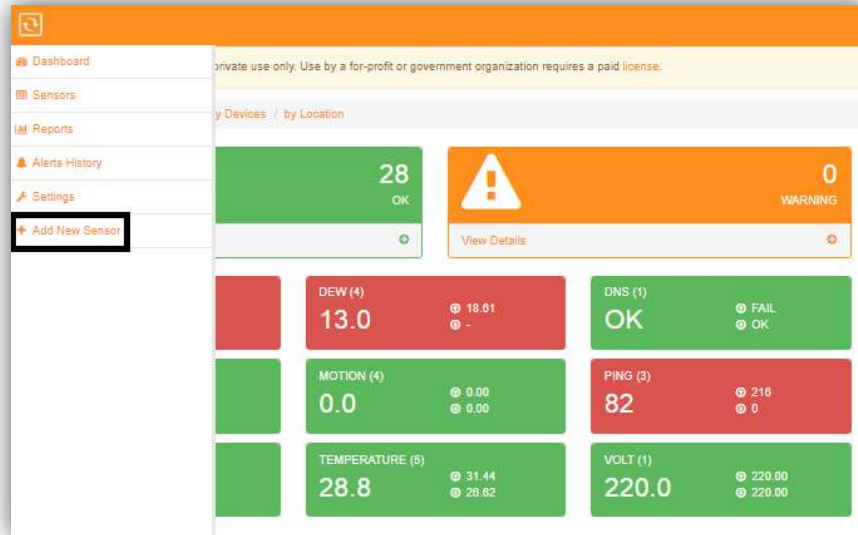
OK 66
WARNING 1
DOWN 0

AIRFLOW (3) 0.00
DEW POINT (7) 18.10
DNS (1) OK
DUST (3) 0.00
HUMIDITY (7) 70.00
LEAK (1) DRY
PING (9) 14.90
SHOCK (7) 1.00
SOUND (3) 46.20
TEMPERATURE (28) 24.70

4.2.2. Adding Internet Speed test Check

Internet Speed test will check the performance of your internet connection. It performs it by doing a download and upload test against the closest and fastest server. 2 sensors will then be created: Download and Upload, both reporting as Mbps.

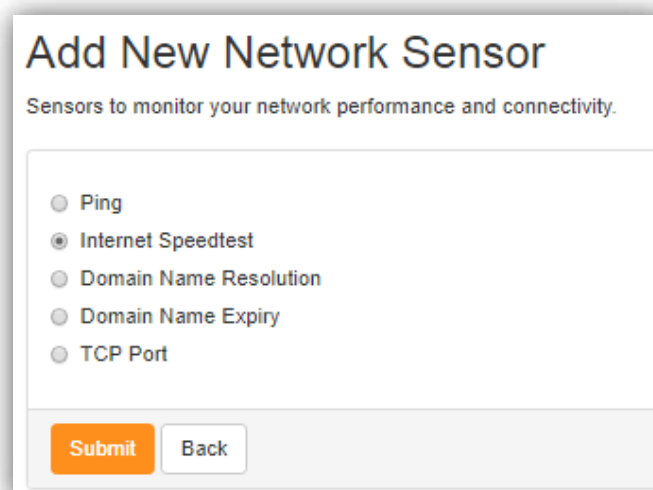
1. Access **Menu** and Click **Add New Sensor**.



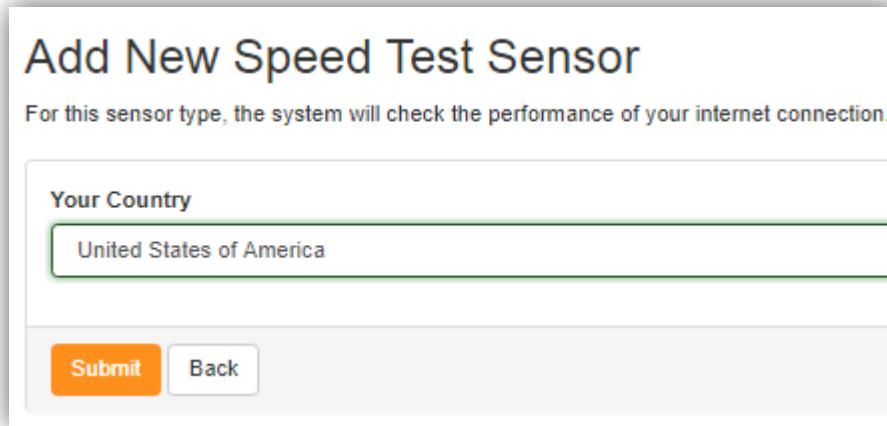
2. Select **Network Connections**.



3. Select **Internet Speed test**.



4. Select a country from which to check the speed of your internet connection.



Add New Speed Test Sensor

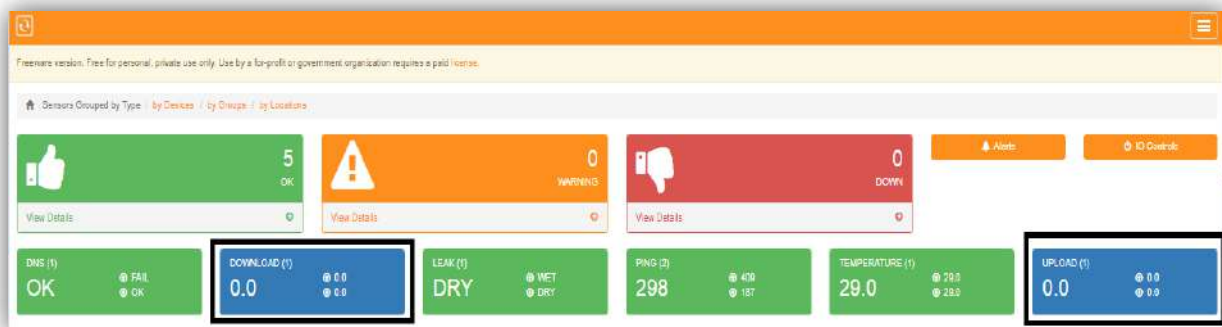
For this sensor type, the system will check the performance of your internet connection.

Your Country

United States of America

Submit **Back**

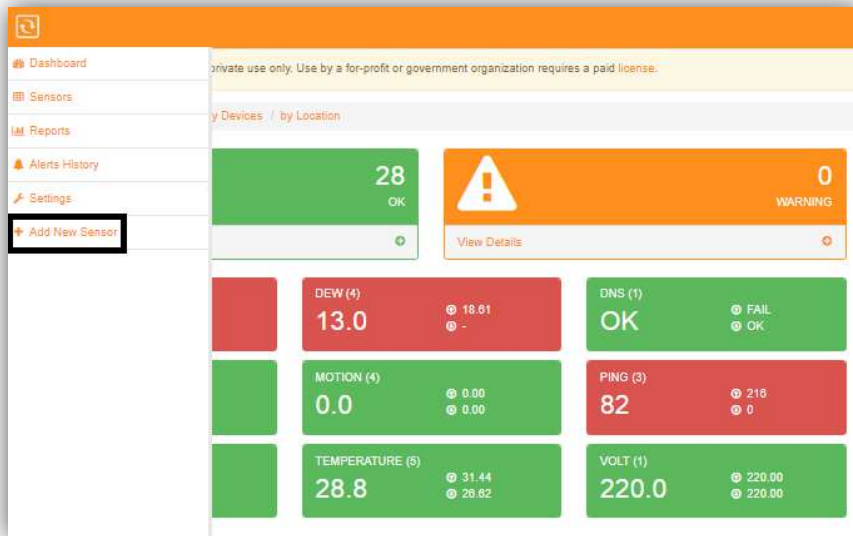
5. Once done, it should appear as one of the monitored checks on the Dashboard. 2 sensor checks will be created, Upload and Download.



4.2.3. Adding Domain Name Resolution Check

Each web server and any host connected to the internet has a unique IP address in textual form, translating it to an IP address. The system will perform a DNS resolution for the given domain name, record type and against the default or specified DNS server.

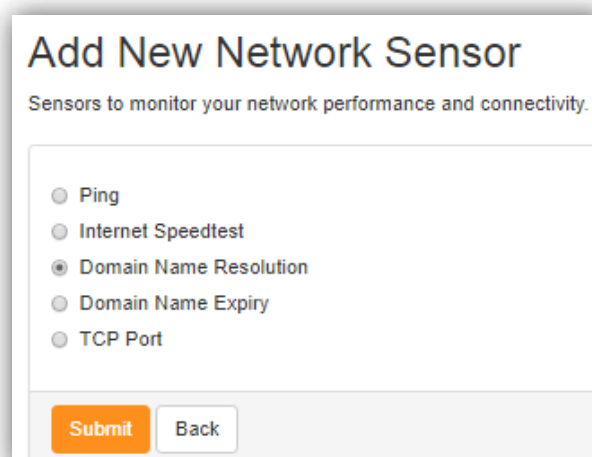
1. Access **Menu** and Click **Add New Sensor**.



2. Select **Network Connections**.



3. Select **Domain Name Resolution**.



4. Provide the Settings for the DNS Sensor.

Domain Name to Resolve - Input the Domain name you intend to check. Only alphanumeric characters, hyphen and dot symbols are allowed.

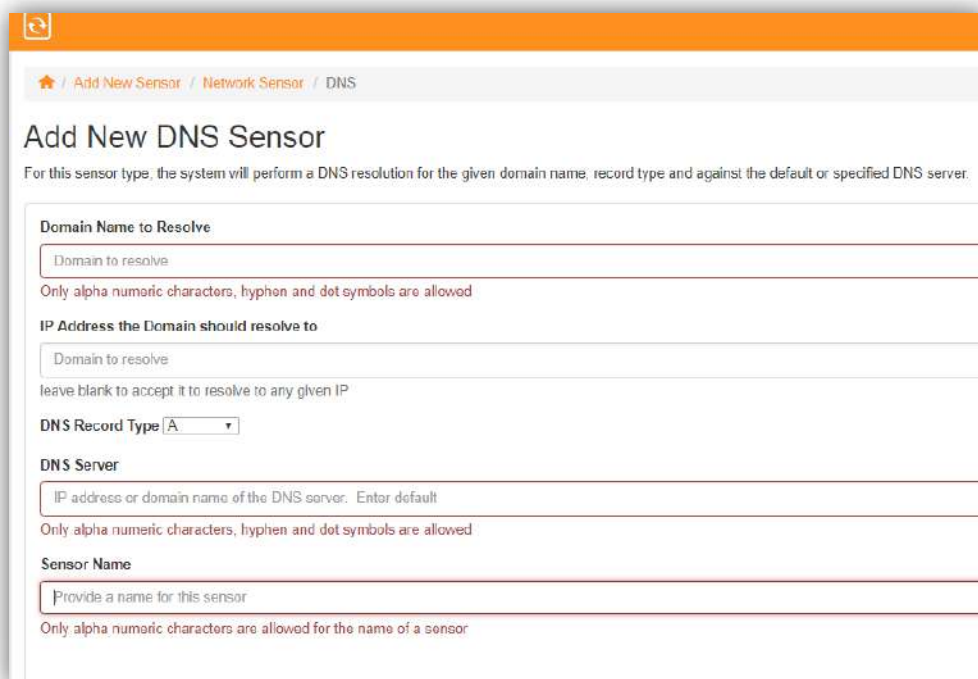
IP address the Domain should resolve to - You may provide the specific IP address you want the domain to resolve. Or if left blank, it will resolve to any given IP.

DNS Record Type - Select on the dropdown menu for options : A, MX, CNAME, PTR or NS

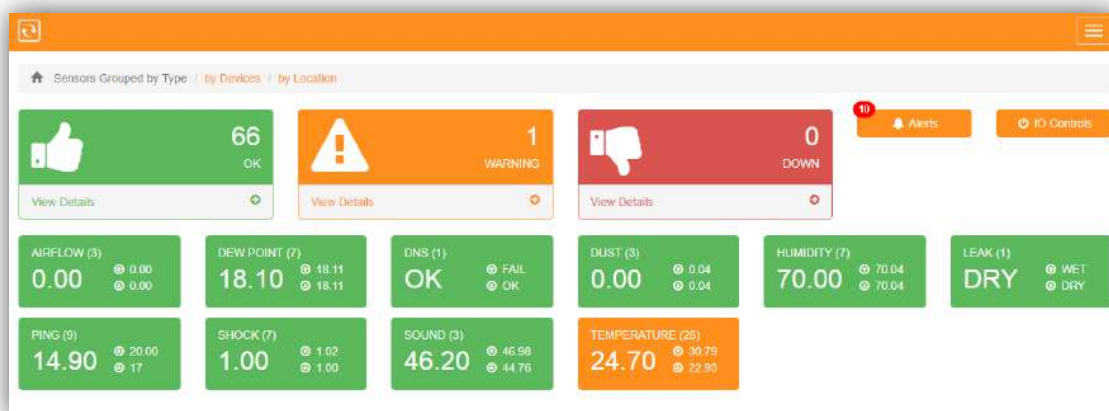
DNS Server - Enter the IP address or domain name of the DNS server. Only alphanumeric characters, hyphen, and dot symbols are allowed.

Sensor Name - Provide a name of the sensor. This Sensor Name will be the name that should appear on the Dashboard.

Note: Only alphanumeric characters are allowed.



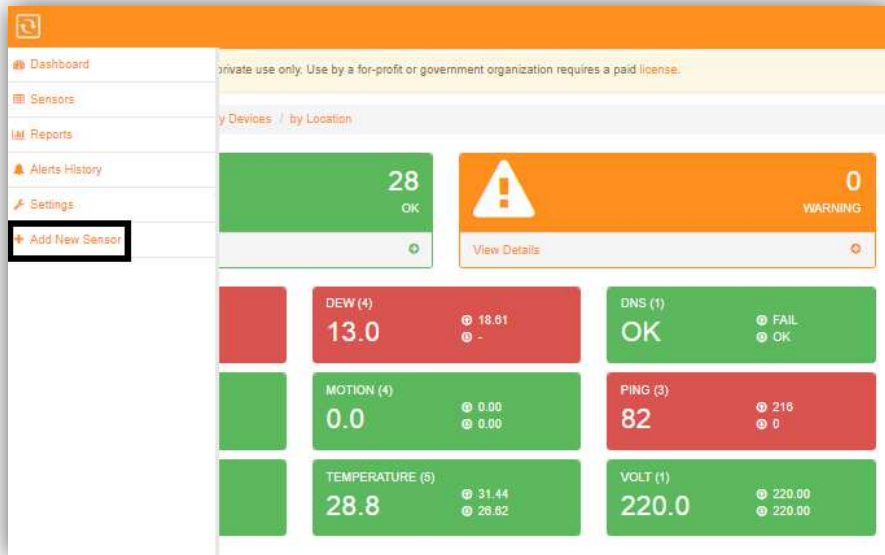
5. Once done, it should appear as one of the monitored checks on the Dashboard.



4.2.4. Adding Domain Name Expiry Check

For this sensor type, the software will check if the given domain name is about to expire or has expired. It starts warning if it is within 7 days of expiry. Multiple domain names can be entered (one per row).

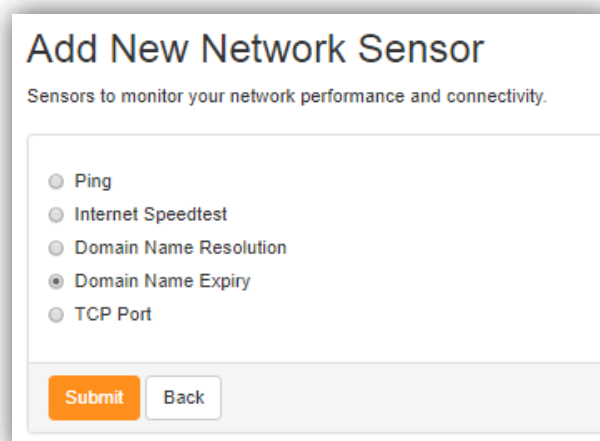
1. Access **Menu** and Click **Add New Sensor**.



2. Select **Network Connections**.



3. Select **Domain Name Expiry**.



4. Provide the Domain Name and a Sensor Name for identification.

Domain Names - provide the IP address or the Domain Name you want to check.

Note: Multiple Domain Names can be entered (one per row)

Sensor Name - provide a specific name for the sensor for identification.

Add New Domain Name Expiry Sensor

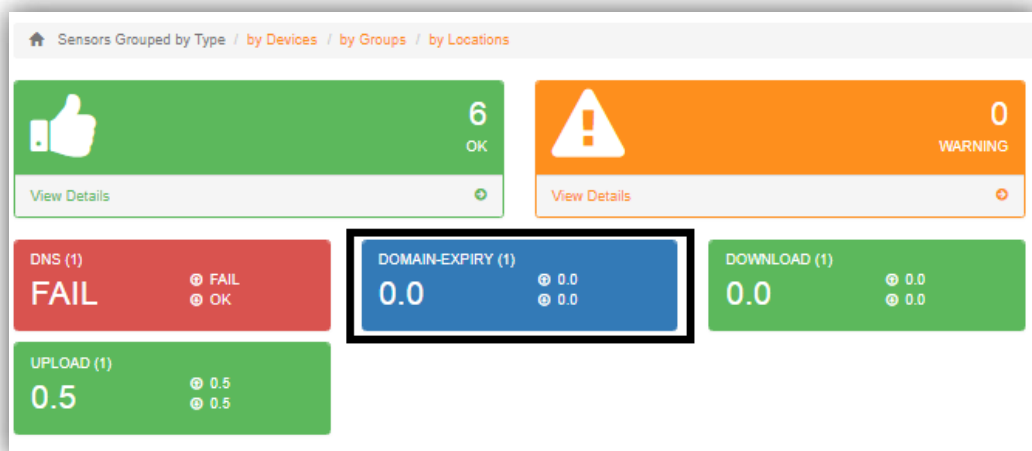
For this sensor type, the software will check if the given domain name is about to expire or has expired.

Domain names

192.168.9.14
www.yahoo.com
www.google.com

Submit **Back**

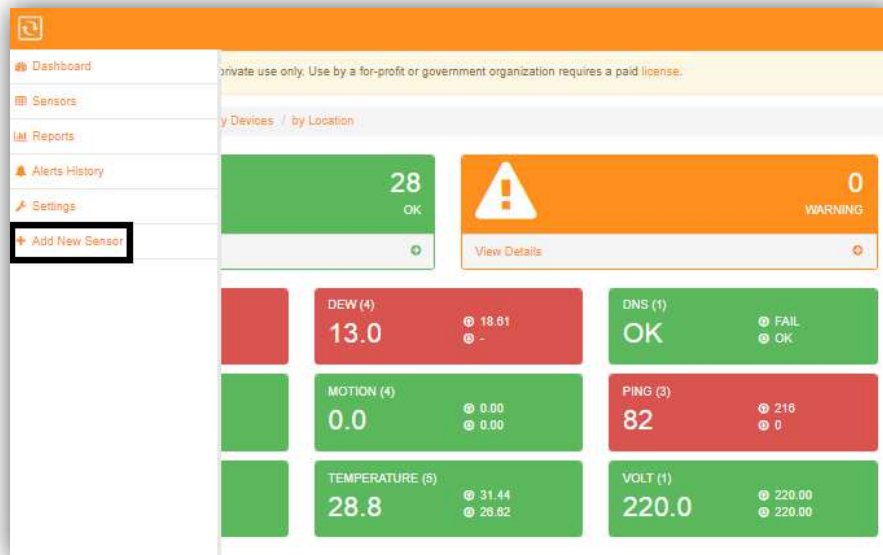
5. Once done, it should appear as one of the monitored checks on the Dashboard.



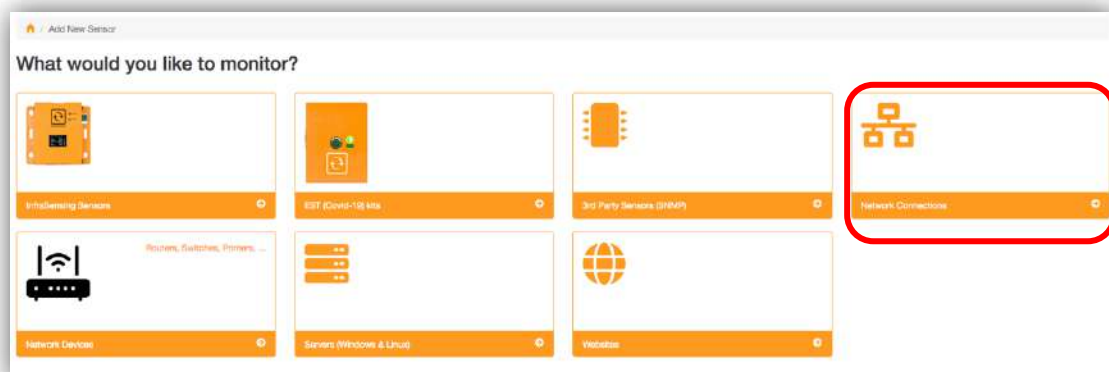
4.2.5. Adding TCP Port Check

This sensor type will check if a server responds on a specified TCP port.

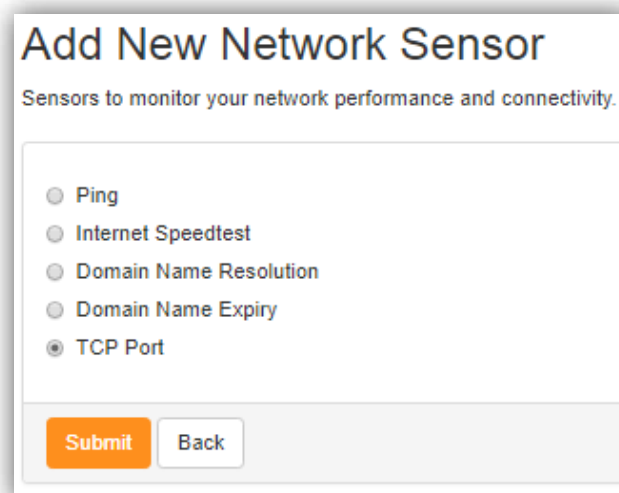
1. Access **Menu** and Click **Add New Sensor**.



2. Select **Network Connections**.



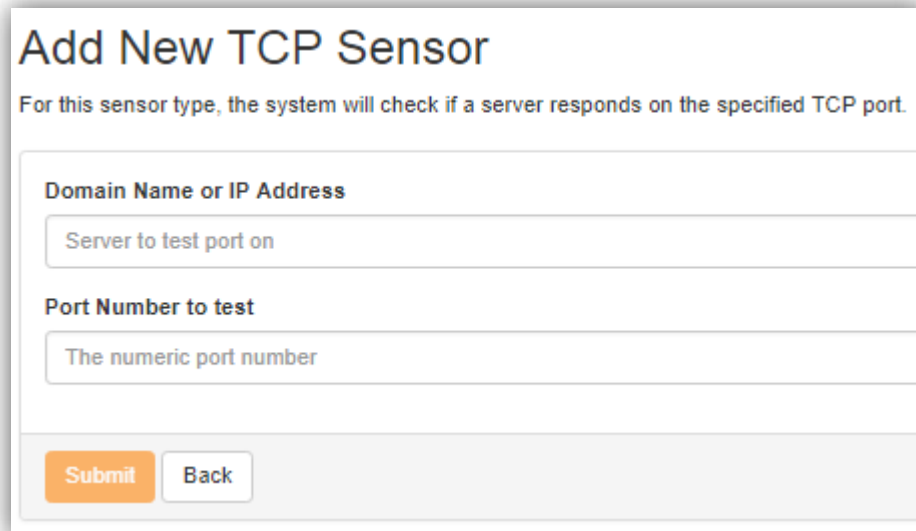
3. Select **TCP Port**.



4. Provide the details for the TCP port check.

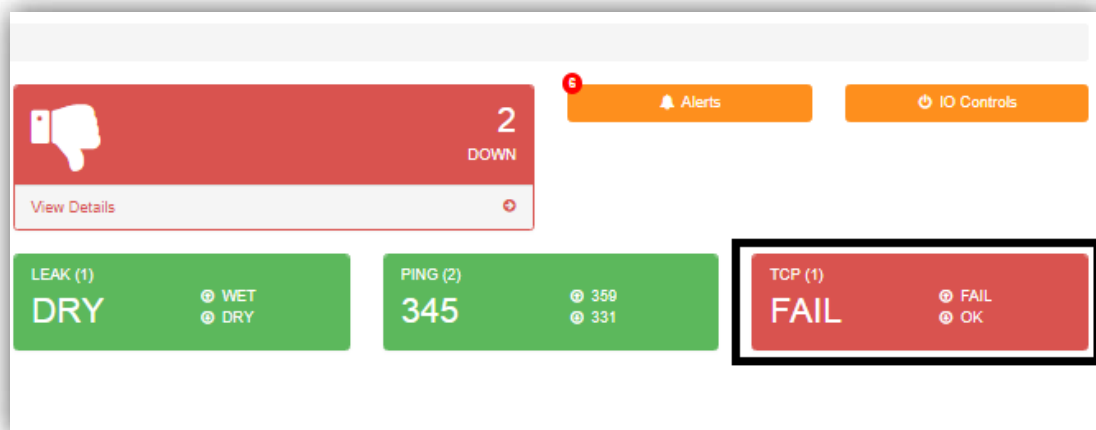
Domain Name or IP address - This is the server to test the port on.

Port Number to Test - Input the numeric port number.



The screenshot shows a web form titled "Add New TCP Sensor". Below the title is a subtitle: "For this sensor type, the system will check if a server responds on the specified TCP port." The form contains two input fields: "Domain Name or IP Address" with the placeholder text "Server to test port on", and "Port Number to test" with the placeholder text "The numeric port number". At the bottom of the form are two buttons: "Submit" (orange) and "Back" (white with grey border).

5. Once done, it should appear as one of the monitored checks on the Dashboard.



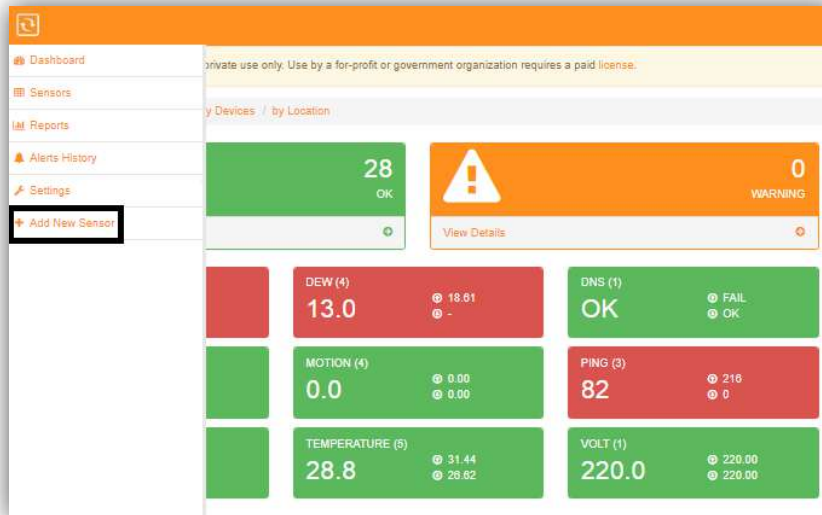
4.3. Adding Checks for Network Devices (Routers, Switches, Printers)

This gives you option to monitor any network devices on your network. Such as Routers, Switches, Printers, etc.

4.3.1. Adding Network Devices via Ping Check

For this sensor type, the system will perform a PING check to the remote IP and measure its response time in ms (milliseconds).

1. Access **Menu** and Click **Add New Sensor**.



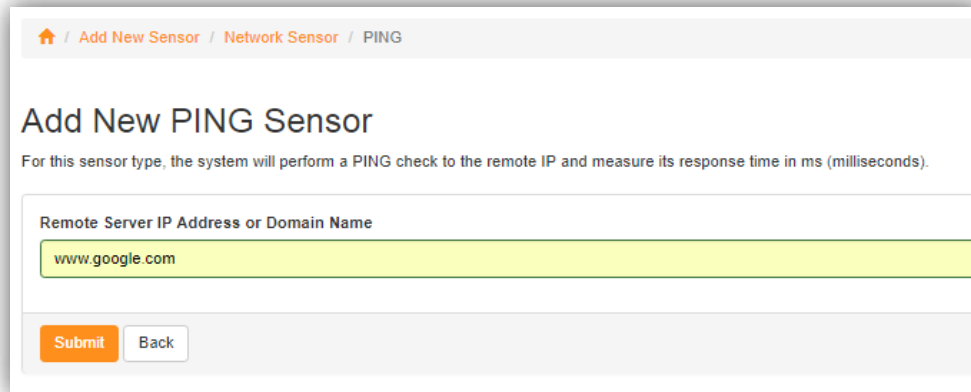
2. Select Network Devices.



3. Select PING.



4. Input the Remote Server IP address or Domain Name you want to check.



Home / Add New Sensor / Network Sensor / PING

Add New PING Sensor

For this sensor type, the system will perform a PING check to the remote IP and measure its response time in ms (milliseconds).

Remote Server IP Address or Domain Name

www.google.com

Submit Back

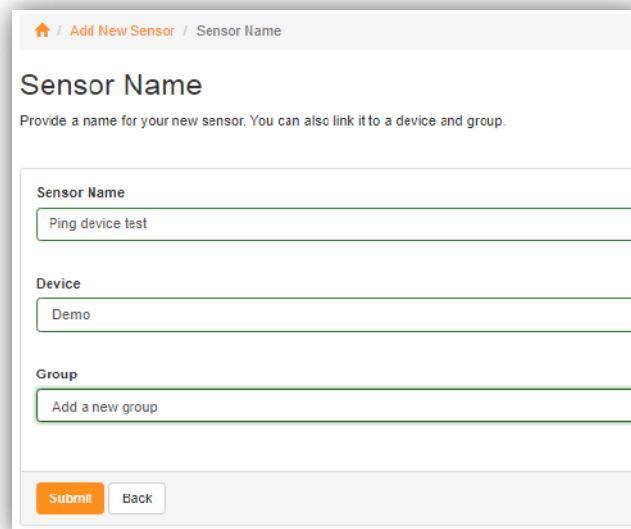
5. You can then provide a Sensor Name and link it to a specific device or group.

Sensor Name - Provide a name for the sensor.

Note: Only alpha numeric characters are allowed for the name of the sensor.

Device - You can select from the drop-down option of which device you want to group the sensor.

Group - You can select from a group name from the drop-down options or you can add a new group.



Home / Add New Sensor / Sensor Name

Sensor Name

Provide a name for your new sensor. You can also link it to a device and group.

Sensor Name

Ping device test

Device

Demo

Group

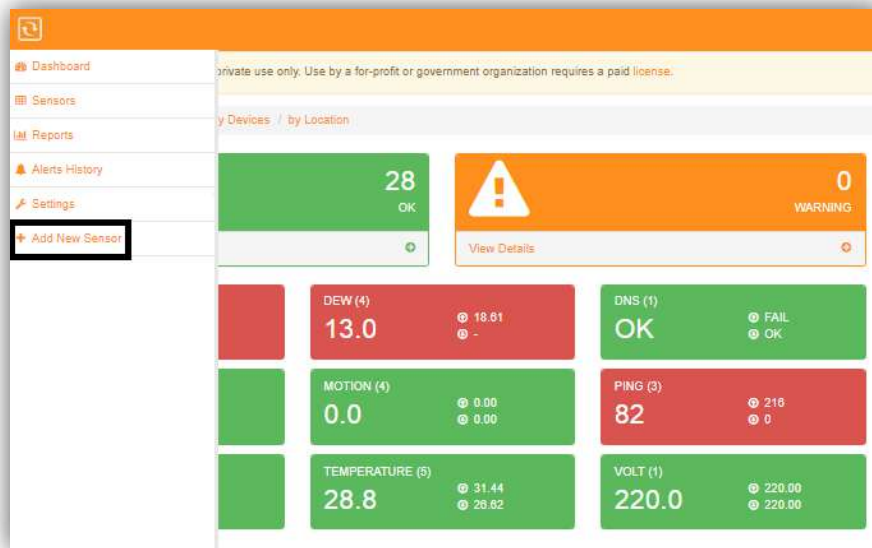
Add a new group

Submit Back

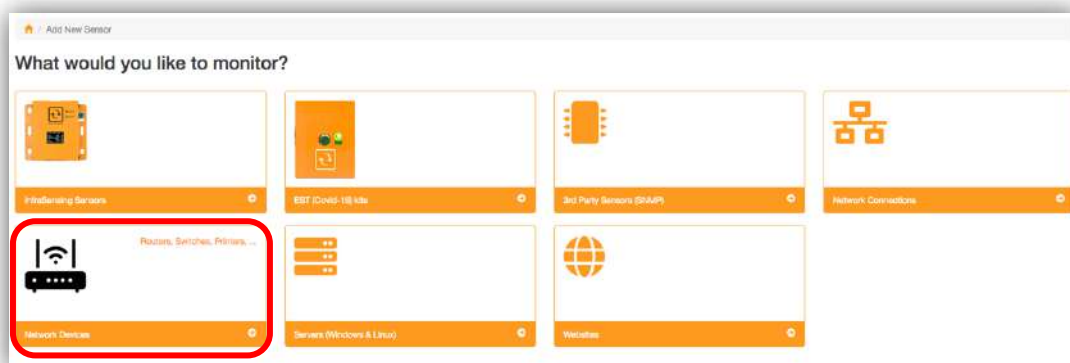
4.3.2. Adding Network Devices via TCP Port Check

For this sensor type, the system will check if a server responds to the specified TCP port.

1. Access **Menu** and Click **Add New Sensor**.



2. Select **Network Devices**.



3. Select **TCP Port**.



4. Input the Domain Name or IP address and the Port Number to test.

Domain Name or IP address - Server address to test the port on.

Note - Only alpha numeric characters, hyphens and dot symbols are allowed.

Port Number to Test - Numeric port number from which to test the server.

Home / Add New Sensor / Network Sensor / TCP

Add New TCP Sensor

For this sensor type, the system will check if a server responds on the specified TCP port.

Domain Name or IP Address

Server to test port on

Only alpha numeric characters, hyphen and dot symbols are allowed

Port Number to test

The numeric port number

Submit Back

5. You can then provide a Sensor Name and link it to a specific device or group.

Sensor Name - Provide a name for the sensor.

Note: Only alpha numeric characters are allowed for the name of the sensor.

Device - You can select from the drop-down option of which device you want to group the sensor.

Group - You can select from a group name from the drop-down options or you can add a new group.

Sensor Name

Provide a name for your new sensor. You can also link it to a device and group.

Sensor Name

TCP check on port 25

Device

192.168.9.33

Group

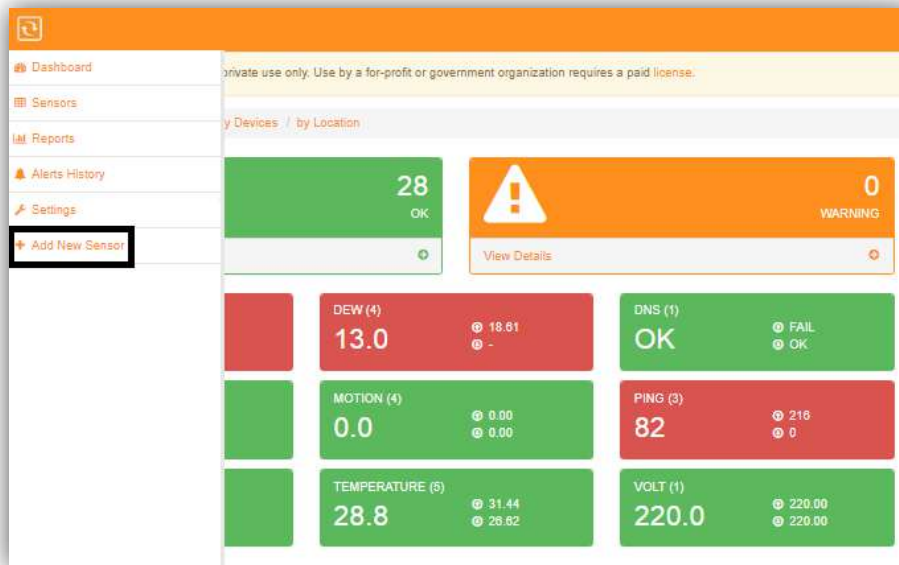
Select a Group

Submit Back

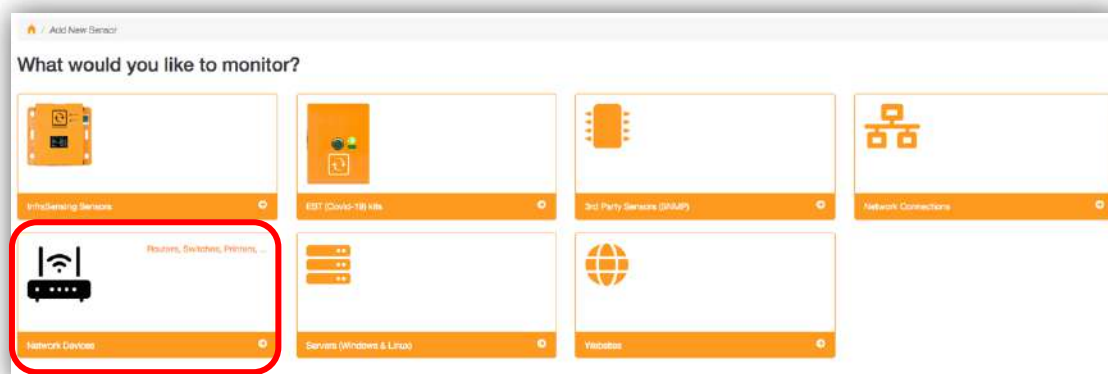
4.3.3. Adding Network Devices via SNMP Check

The system will scan your device using SNMP and detect any numeric values.

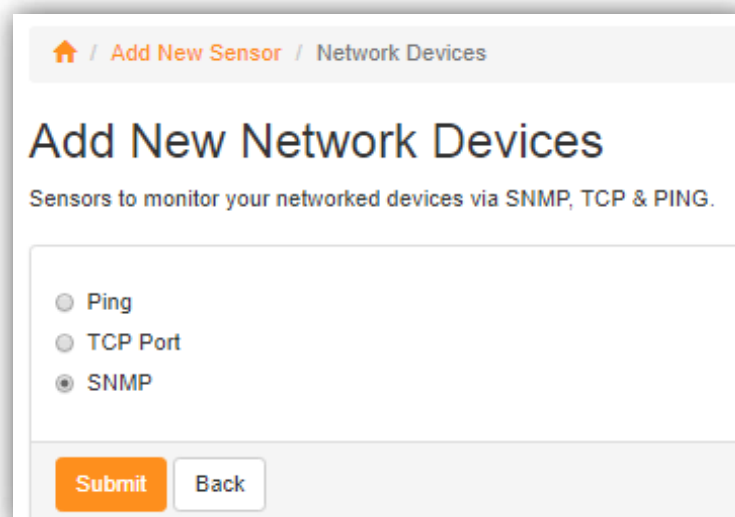
1. Access **Menu** and Click **Add New Sensor**.



2. Select **Network Devices**.



3. Select **SNMP**.



- Input the IP address and the SNMP settings.

3rd Party IP address - IP address or Domain Name of the device

Use Default SNMP Connection Settings

If Yes, it uses the default setting.

If No, input the customized Community String and Port.

Add New Numeric SNMP Sensor
The system will scan your device using SNMP and detect any numeric values.

3rd Party IP Address as shown on the OLED display
192.168.9.33

Use Default SNMP Connection Settings
 yes no, use custom settings

Community String
public

Port
161

Submit **Back**

- You can provide a sensor name and select which OID or sensor type to monitor.

Scanned Device
Following numeric values were found on the system. Click the checkbox if you want a sensor to be monitored.

Sensor List

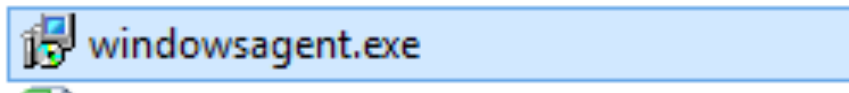
Monitor	Sensor Name	OID	Sensor Type	Value
<input type="checkbox"/>		1.3.6.1.4.1.17096.11.1.2.0	Select the sensor type	0.96
<input type="checkbox"/>		1.3.6.1.4.1.17096.11.13.2.0	Select the sensor type	1.88
<input checked="" type="checkbox"/>	Sound Dll	1.3.6.1.4.1.17096.11.22.2.0	Select the sensor type	42.14
<input type="checkbox"/>		1.3.6.1.4.1.17096.11.7.2.0	Select the sensor type	0.03
<input type="checkbox"/>		1.3.6.1.4.1.17096.3.2.0	Select the sensor type	30.11
<input type="checkbox"/>		1.3.6.1.4.1.17096.3.6.0	Select the sensor type	1000.00
<input type="checkbox"/>		1.3.6.1.4.1.17096.5.1.6.0	Select the sensor type	0

4.4. Adding Checks for Servers (Windows & Linux)

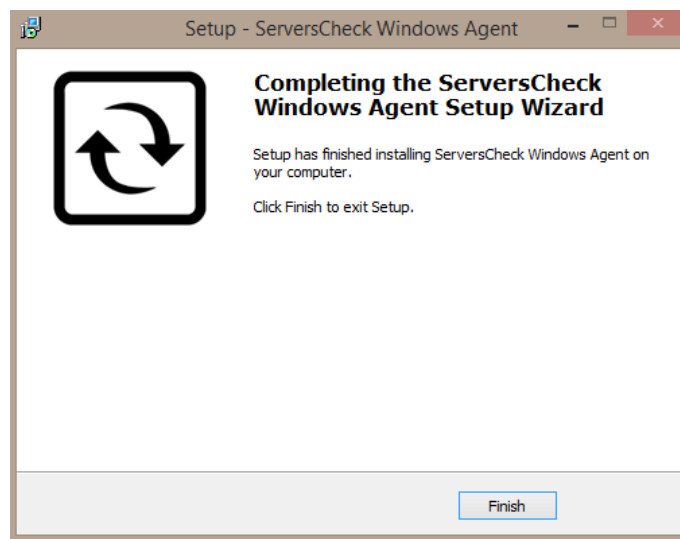
You can have sensors to monitor your network performance and connectivity.

Installing the Windows Agent on a Windows Remote System

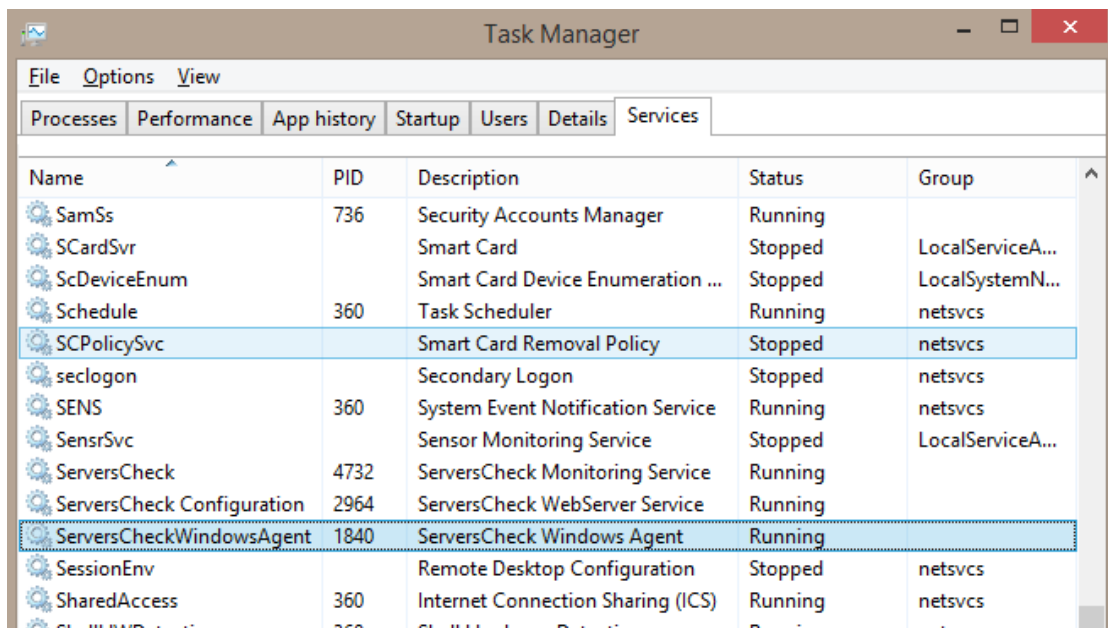
- a. Download the Windows Agent from the link
<https://ServersCheck.com/support/downloads.asp>
- b. Run the windowsagent.exe and Install. You need to have administrative privilege on the system you will install the agent.



- c. Accept the License Agreement. And finish the installation.



- d. Go to Task Manager and Run the ServersCheck Windows Agent to run the service on the background.



Installing the Linux Agent on a Linux Remote System

- a. Download the Linux Agent from the link
<https://ServersCheck.com/support/downloads.asp>
- b. Unzip the linuxsagent.zip file.



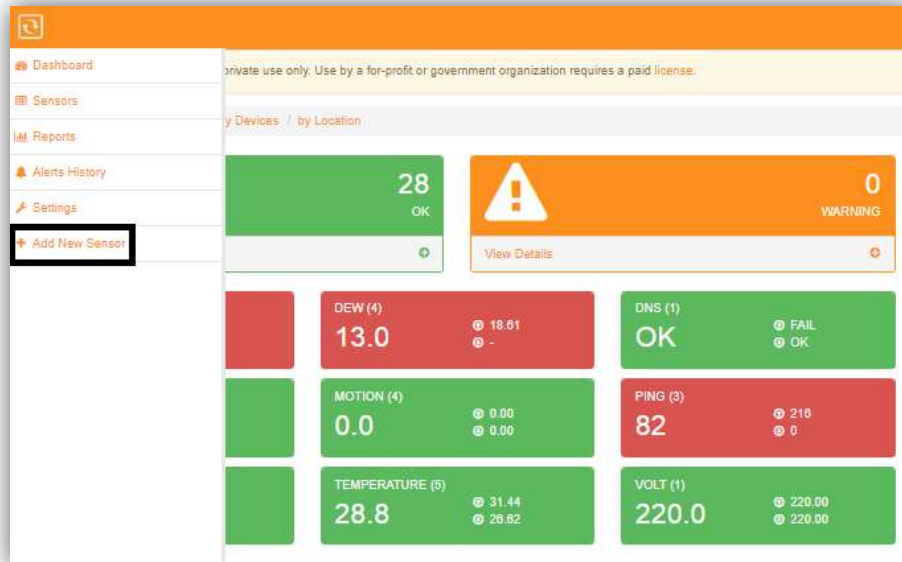
- c. You can change the port and default password in conf.cfg file.
Default Port - 30711
Default Password - passServersCheck
- d. Compile the ServersCheck.c file.
- e. Linux Agent should run as a service on the background.

4.4.1. Adding Checks for Windows Servers

This check type requires the free Windows Agent to be installed on the remote system being monitored. The Windows Agent can be downloaded from this link - <https://ServersCheck.com/support/downloads.asp>

The check will monitor CPU, Memory, Disk Space, Processes, Services or Event Logs.

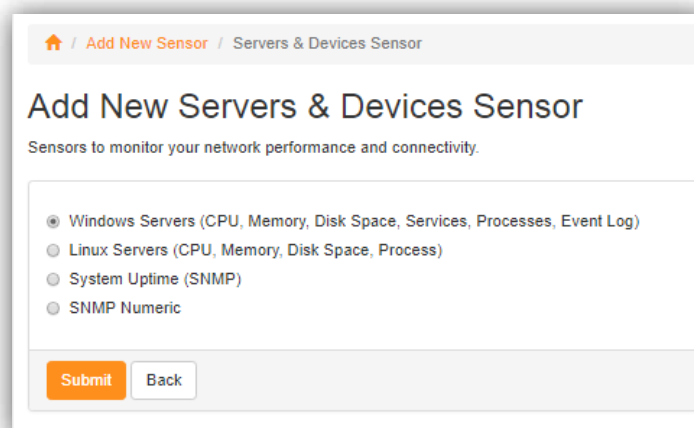
1. Access Menu and Click Add New Sensor.



2. Select Servers.



3. Select Windows Servers.



4. Input the parameters you want to monitor for the Windows Server.

Domain Name or IP Address of Windows Server - Server to monitor.

Agent Port Number - Numeric Port number you want to monitor.

Default Port - 30711

Agent Password - default is pass ServersCheck

Metric - You can select from the drop down options for the items you will monitor.

- * CPU Load in %
- * Free Memory in %
- * Free Diskspace in % (lowest of all disks returned)
- * Windows Services
- * Windows Processes
- * Event Log

Add New Windows Agent Sensor

This check type requires the free Windows Agent to be installed on the remote system being monitored. [Download the agent.](#)
The check will monitor CPU, Memory, Disk Space, Processes, Services or Event Logs.

Domain Name or IP Address of Windows Server
Server to monitor

Agent Port Number
30711

Agent Password
The default agent password

Metric

- Free Diskspace in % (lowest of all disks returned)
- CPU load in %
- Free Memory in %
- Free Diskspace in % (lowest of all disks returned)**
- Windows Services
- Windows Processes
- Event Log

5. You can then provide a Sensor Name and link it to a specific device or group.

Sensor Name - Provide a name for the sensor.

Note: Only alpha numeric characters are allowed for the name of the sensor.

Device - You can select from the drop-down option of which device you want to group the sensor.

Group - You can select from a group name from the drop-down options or you can add a new group.

Sensor Name

Provide a name for your new sensor. You can also link it to a device and group.

Sensor Name
DISK-SPACE of 192.168.9.33

Device
Demo

Group
Select a Group

Submit **Back**

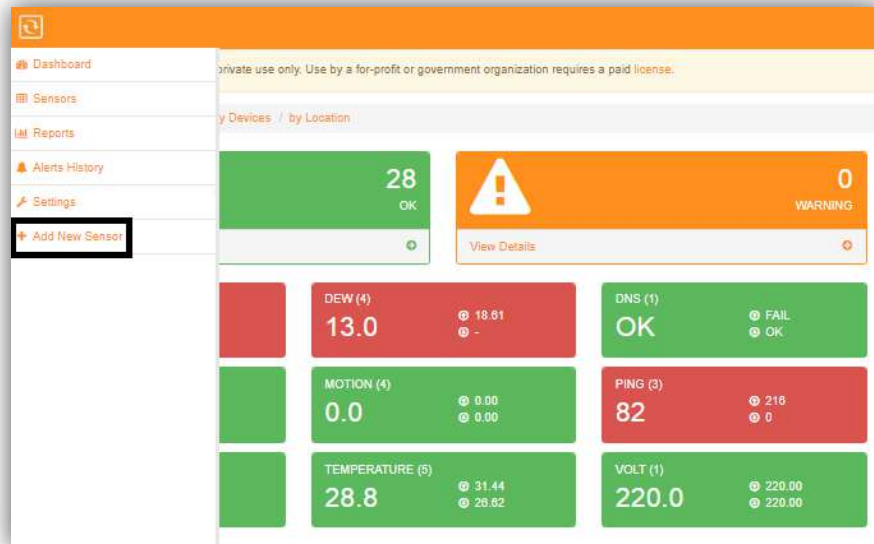
4.4.2. Adding Checks for Linux Servers

This check type requires the free Linux Agent to be installed on the remote system being monitored.

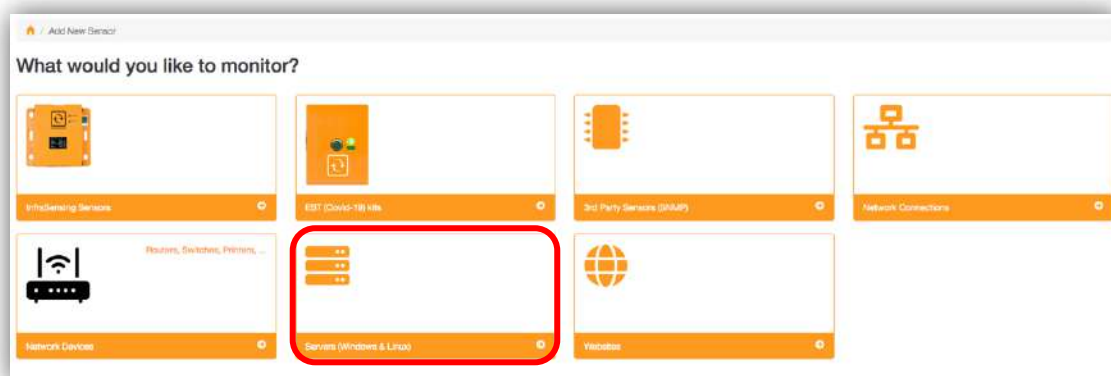
The Linux Agent can be downloaded from this link - <https://ServersCheck.com/support/downloads.asp>

The check will monitor CPU, Memory, Disk Space or Processes state.

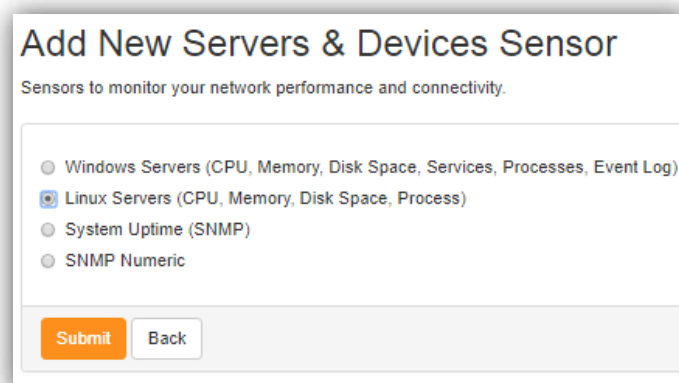
1. Access **Menu** and Click **Add New Sensor**.



2. Select Servers.



3. Select Linux Servers.



4. Input the parameters you want to monitor for the Linux Server.

Domain Name or IP Address of Windows Server - Server to monitor.

Agent Port Number - Numeric Port number you want to monitor.

Agent Password - default is pass ServersCheck

Metric - You can select from the drop down options for the items you will monitor.

* CPU Load in %

* Free Memory in %

* Free Diskspace in % (lowest of all disks returned)

* Linux Processes

Add New Linux Agent Sensor

This check type requires the free Linux Agent to be installed on the remote system being monitored. [Download the agent.](#)
The check will monitor CPU, Memory, Disk Space or Processes state.

Domain Name or IP Address of Linux Server
192.168.9.14

Agent Port Number
30711

Agent Password
The default agent password

Metric
CPU load in %
Free Memory in %
Free Diskspace in % (lowest of all disks returned)
Linux Processes

5. You can then provide a Sensor Name and link it to a specific device or group.

Sensor Name - Provide a name for the sensor.

Note: Only alpha numeric characters are allowed for the name of the sensor.

Device - You can select from the drop-down option of which device you want to group the sensor.

Group - You can select from a group name from the drop-down options or you can add a new group.

Sensor Name

Provide a name for your new sensor. You can also link it to a device and group.

Sensor Name
CPU of 192.168.9.14

Device
Demo

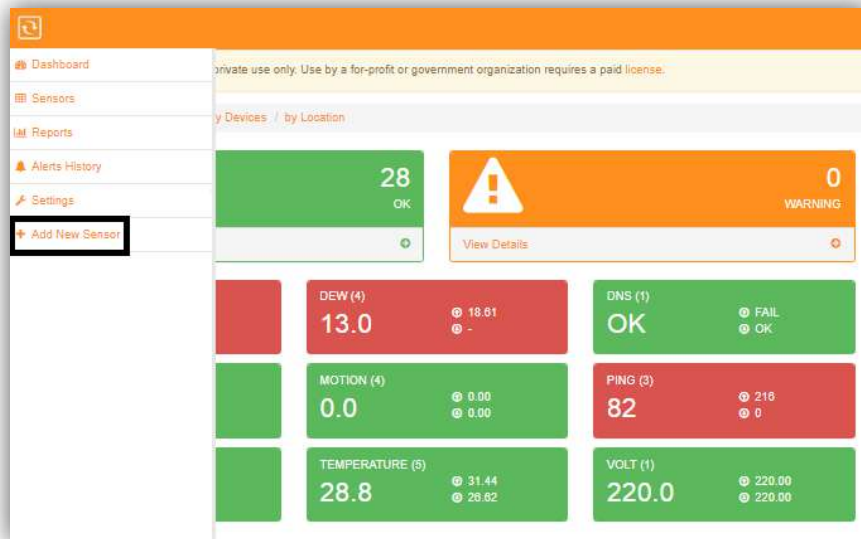
Group
None

Submit **Back**

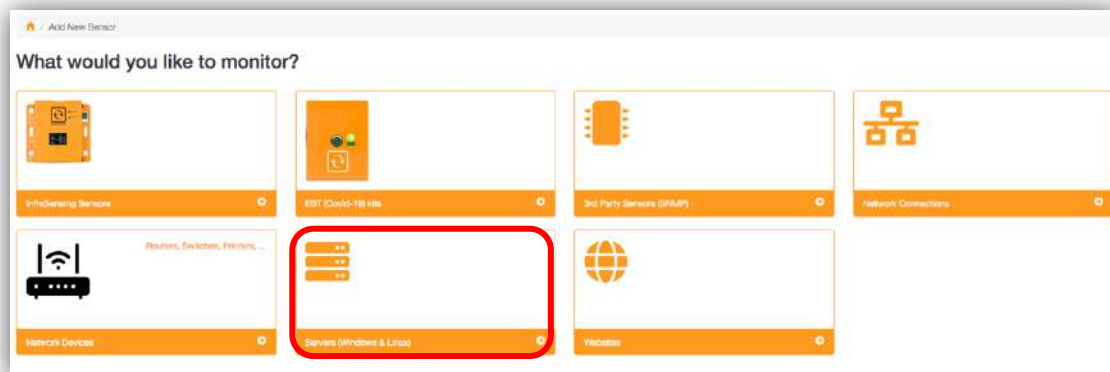
4.4.3. Adding Checks for System Uptime (SNMP)

This check type connects via SNMP to a device and queries its uptime in seconds.

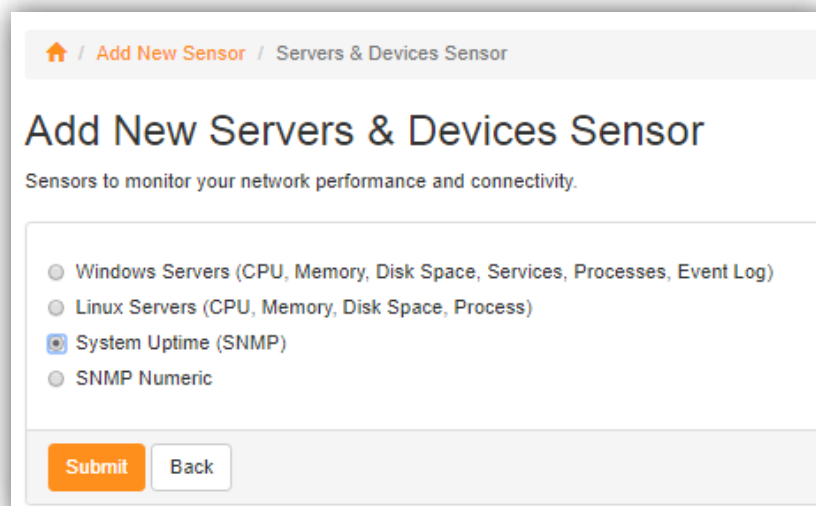
1. Access **Menu** and Click **Add New Sensor**.



2. Select Servers.



3. Select System Uptime (SNMP).



4. Input the SNMP settings of the IP address you wish to query.

IP Address - The IP address of the Server you wish to query via SNMP.

Note : Only Alpha numeric characters, hyphen and dot symbols are allowed.

Community String - the handshake for SNMP.

Port - SNMP Port

Typical SNMP port is 161

Home / Add New Sensor / Network Sensor / Sensor XY

Add New Uptime Sensor

This check type connects via SNMP to a device and queries its uptime in seconds.

IP Address
192.168.9.33

Community String
public

Port
161

Submit **Back**

5. You can then provide a Sensor Name and link it to a specific device or group.

Sensor Name - Provide a name for the sensor.

Note: Only alpha numeric characters are allowed for the name of the sensor.

Device - You can select from the drop-down option of which device you want to group the sensor.

Group - You can select from a group name from the drop-down options or you can add a new group.

Sensor Name

Provide a name for your new sensor. You can also link it to a device and group.

Sensor Name
Uptime in sec of 192.168.9.33

Device
Demo

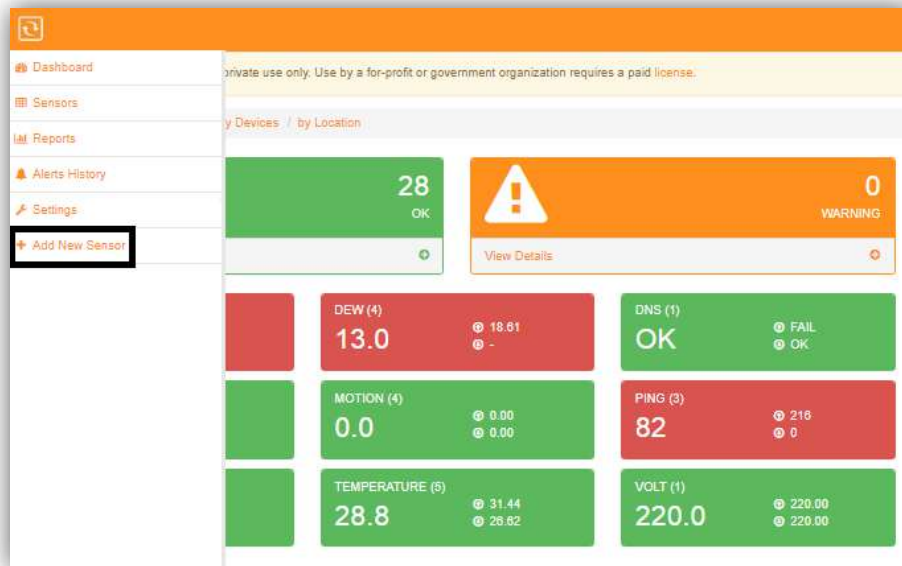
Group
None

Submit **Back**

4.4.4. Adding Checks for SNMP Numeric

The system will scan your device using SNMP and detect any numeric values.

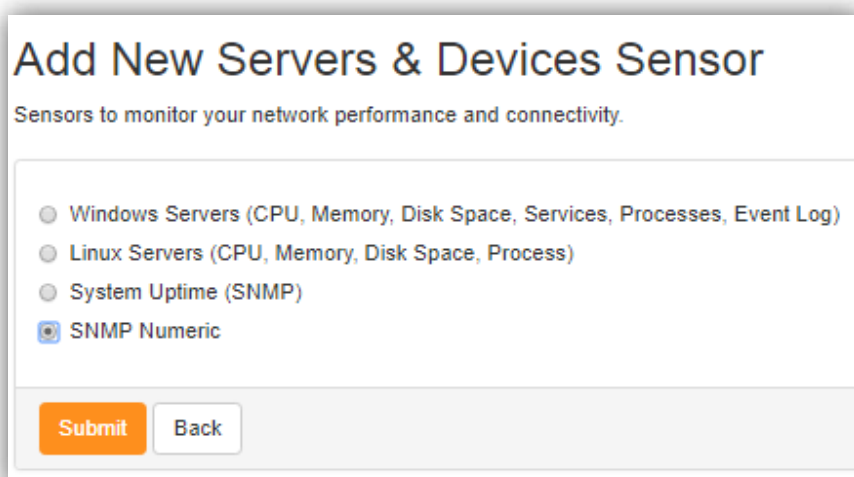
1. Access **Menu** and Click **Add New Sensor**.



2. Select Servers.



3. Select SNMP Numeric.



- Input the SNMP settings of system you want to scan.

3rd Party IP address - IP address or Domain Name of the device

Use Default SNMP Connection Settings

If Yes, it uses the default setting.

If No, input the customized Community String and Port.

Add New Numeric SNMP Sensor
The system will scan your device using SNMP and detect any numeric values.

3rd Party IP Address as shown on the OLED display
192.168.9.33

Use Default SNMP Connection Settings
 yes no, use custom settings

Community String
public

Port
161

Submit **Back**

- You can provide a sensor name and select which OID or sensor type to monitor.

Scanned Device
Following numeric values were found on the system. Click the checkbox if you want a sensor to be monitored.

Sensor List

Monitor	Sensor Name	OID	Sensor Type	Value
<input type="checkbox"/>		1.3.6.1.4.1.17095.11.1.2.0	Select the sensor type ▼	0.96
<input type="checkbox"/>		1.3.6.1.4.1.17095.11.13.2.0	Select the sensor type ▼	1.88
<input checked="" type="checkbox"/>	Sound DIT	1.3.6.1.4.1.17095.11.22.2.0	Select the sensor type ▼	42.14
<input type="checkbox"/>		1.3.6.1.4.1.17095.11.7.2.0	Select the sensor type ▼	0.03
<input type="checkbox"/>		1.3.6.1.4.1.17095.3.2.0	Select the sensor type ▼	30.11
<input type="checkbox"/>		1.3.6.1.4.1.17095.3.6.0	Select the sensor type ▼	1000.00
<input type="checkbox"/>		1.3.6.1.4.1.17095.5.1.6.0	Select the sensor type ▼	0

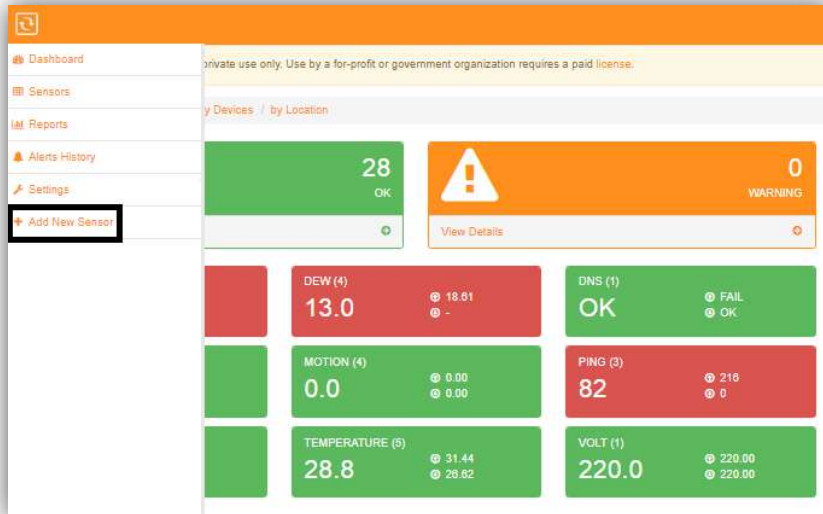
4.5. Adding Checks for Websites

You can have sensors to monitor your websites and web applications.

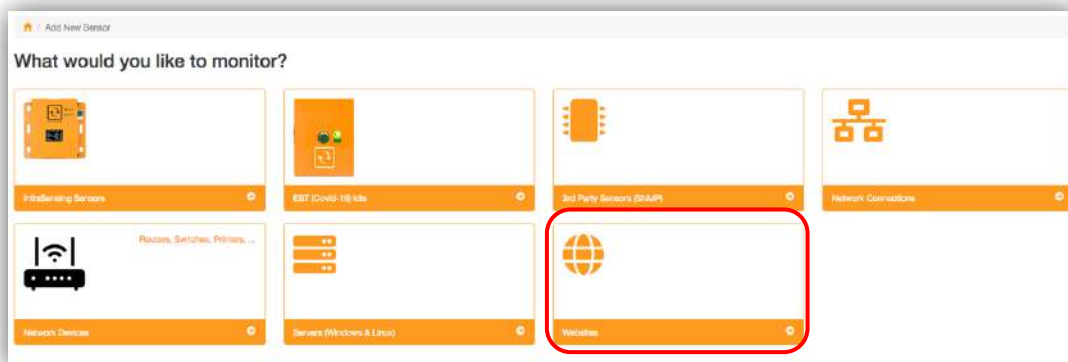
4.5.1. Adding SSL Certificate Validity Check

For this sensor type, the system will load the certificate for the given URL and checks its validity. If it expires within 45 days or it is expired, then an alert will be triggered.

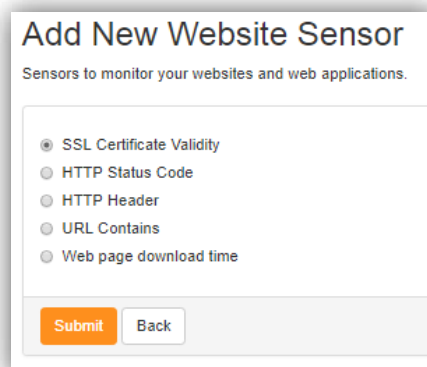
1. Access **Menu** and Click **Add New Sensor**.



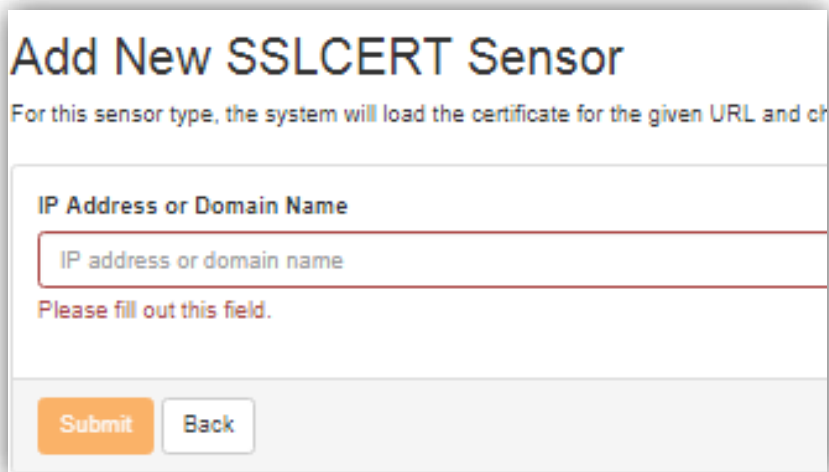
2. Select **Websites**.



3. Select **SSL Certificate Validity**.



4. Provide the IP address or Domain Name you want to check.



Add New SSLCERT Sensor

For this sensor type, the system will load the certificate for the given URL and ch

IP Address or Domain Name

IP address or domain name

Please fill out this field.

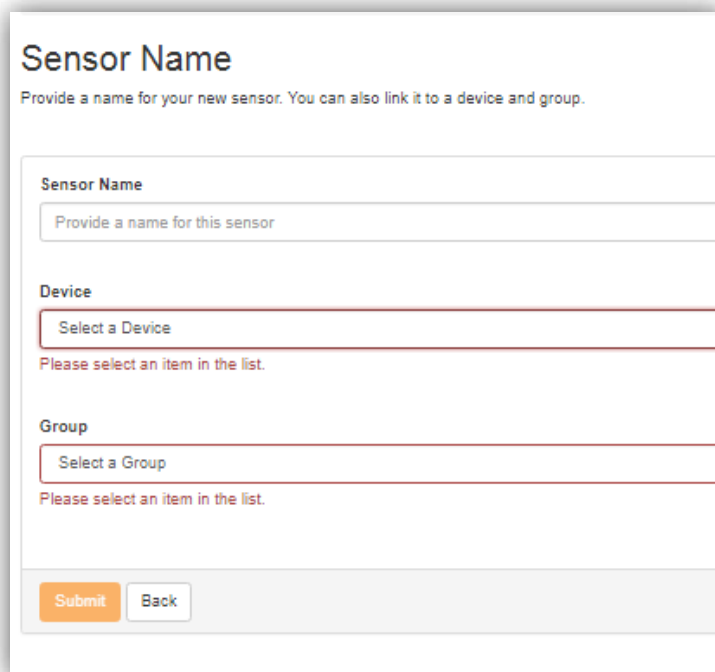
Submit **Back**

5. Provide a Sensor Name and link it to a device or group.

Sensor Name - Provide a name for the sensor.

Device - you may select to any device from the drop down list you have created.

Group - you may add to a certain group or you can add a new group.



Sensor Name

Provide a name for your new sensor. You can also link it to a device and group.

Sensor Name

Provide a name for this sensor

Device

Select a Device

Please select an item in the list.

Group

Select a Group

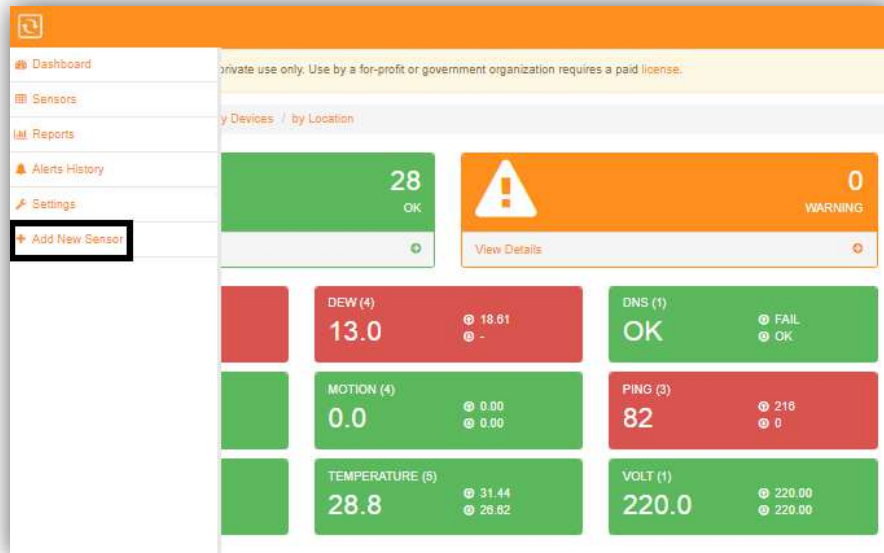
Please select an item in the list.

Submit **Back**

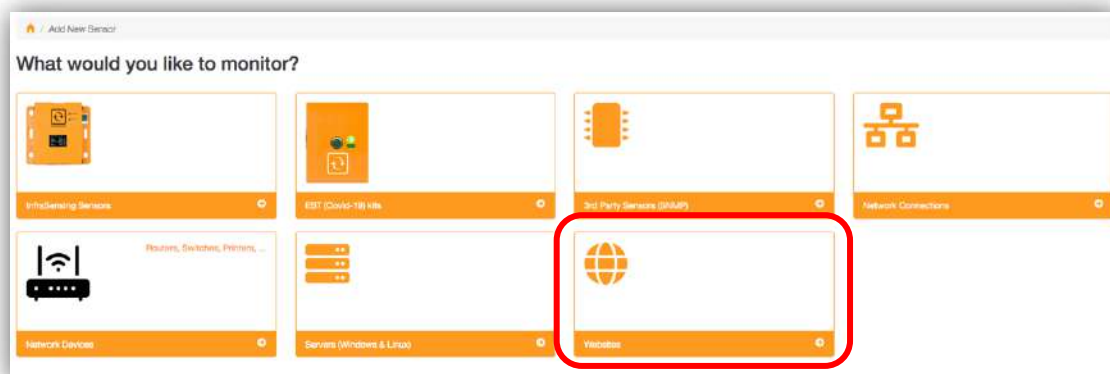
4.5.2. Adding HTTP Status Code Check

For this sensor type, the system will load the URL. The system checks the HTTP status code being returned and compares it to the expected status code.

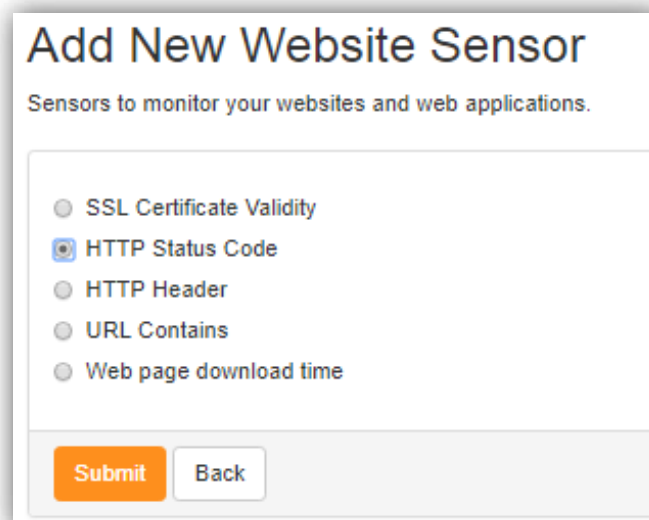
1. Access **Menu** and Click **Add New Sensor**.



2. Select **Websites**.



3. Select **HTTP Status Code**.



4. Provide the URL to be checked and select an Expected Status Code from the drop down list.

URL - Input the URL you want to check.

Expected Status Code - select a status code from the drop down list.

Add New HTTP-STATUS Sensor

For this sensor type, the system will load the URL. The system checks the HTTP Status co

URL

URL

Expected Status Code

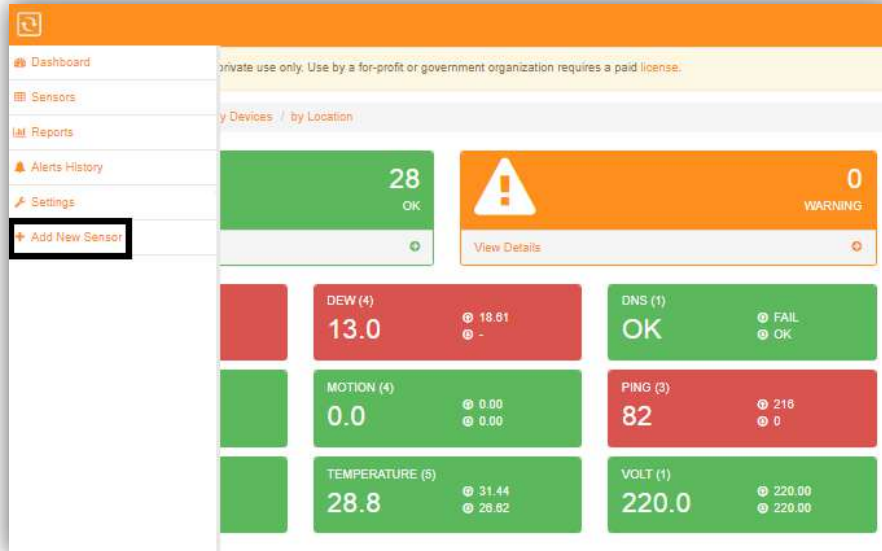
Select a status code

- Select a status code
- 200 OK
- 301 Moved Permanently
- 404 Not Found
- 500 Internal Server Error
- 100 Continue
- 101 Switching Protocols
- 102 Processing
- 200 OK
- 201 Created
- 202 Accepted
- 203 Non-authoritative Information
- 204 No Content
- 205 Reset Content
- 206 Partial Content
- 207 Multi-Status
- 208 Already Reported
- 300 Multiple Choices
- 301 Moved Permanently
- 302 Found

4.5.3. Adding HTTP Header Check

For this sensor type, the system will connect to the provided URL and load the HTTP Headers returned by the webserver. It will then see if the provided text can be found in the headers.

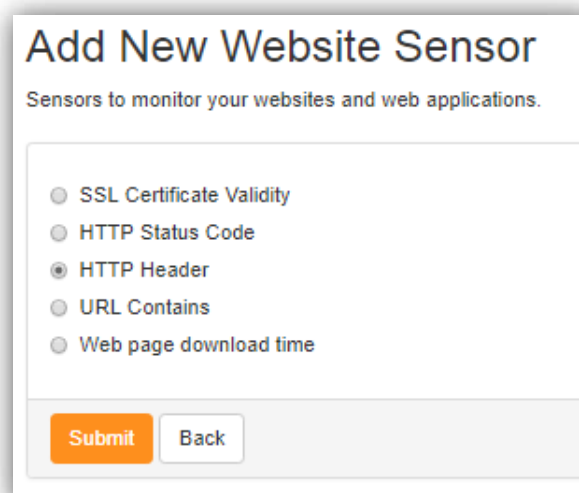
1. Access **Menu** and Click **Add New Sensor**.



2. Select **Websites**.



3. Select **HTTP Header**.



4. Provide the information needed to check for the HTTP Header.

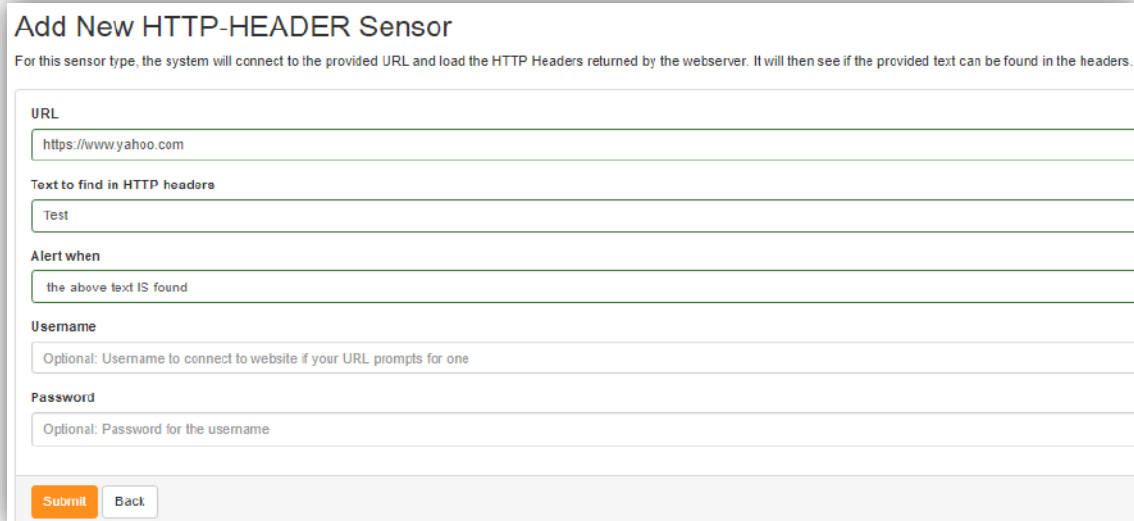
URL - Input the URL you want to check.

Text to Find in HTTP Header - Type in the text the system should find in the URL.

Alert when - choose between if above text is found or if above text is not found.

Username - Optional, if the website provided prompts for one.

Password - Optional, password for the username.



Add New HTTP-HEADER Sensor

For this sensor type, the system will connect to the provided URL and load the HTTP Headers returned by the webserver. It will then see if the provided text can be found in the headers.

URL
https://www.yahoo.com

Text to find in HTTP headers
Test

Alert when
the above text IS found

Username
Optional: Username to connect to website if your URL prompts for one

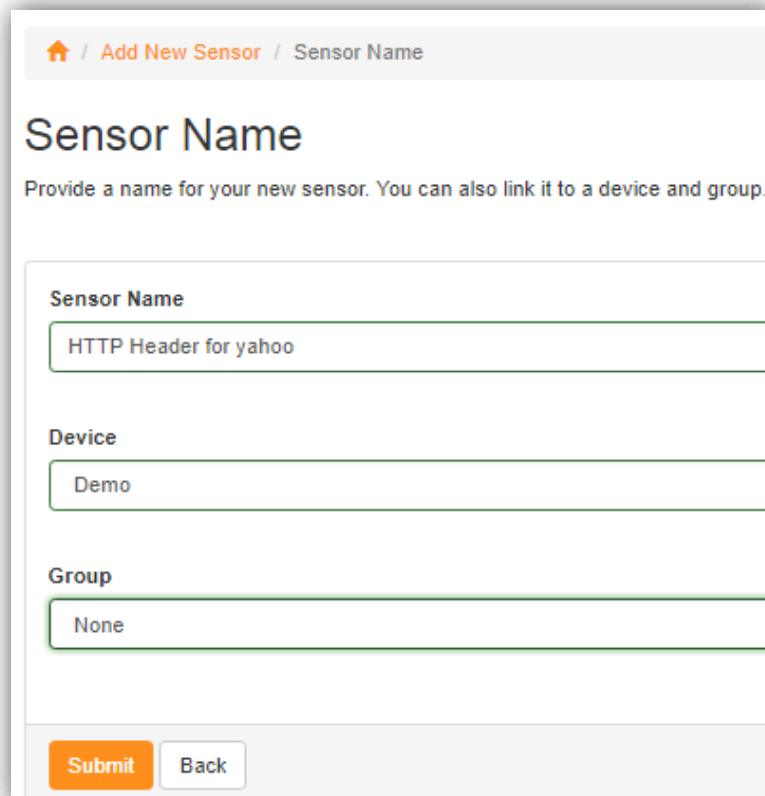
Password
Optional: Password for the username

5. Provide a Sensor Name and link it to a device or group.

Sensor Name - Provide a name for the sensor.

Device - you may select to any device from the drop down list you have created.

Group - you may add to a certain group or you can add a new group.



[Home](#) / [Add New Sensor](#) / [Sensor Name](#)

Sensor Name

Provide a name for your new sensor. You can also link it to a device and group.

Sensor Name
HTTP Header for yahoo

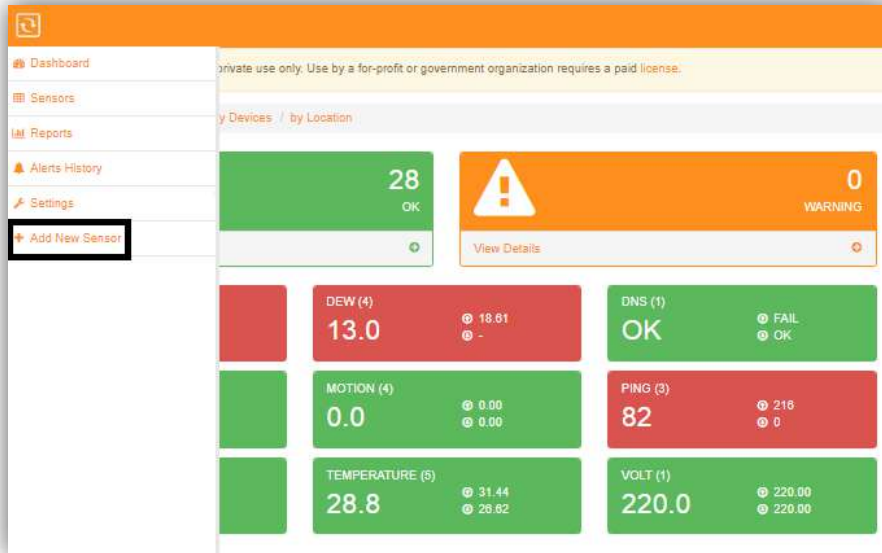
Device
Demo

Group
None

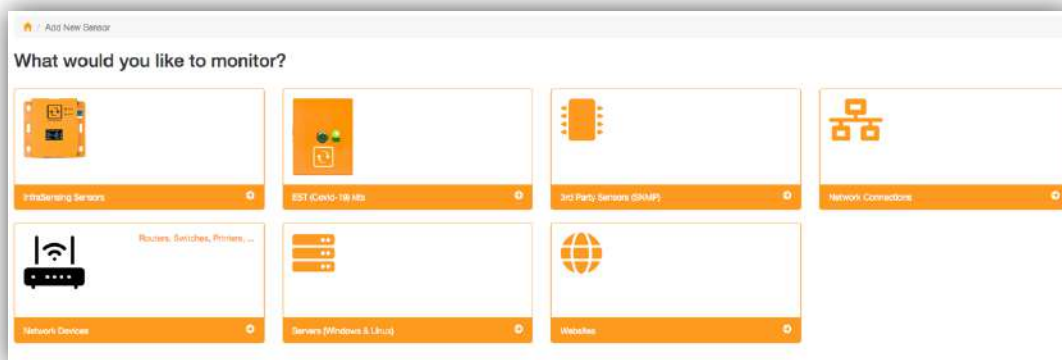
4.5.4. Adding URL Contains Check

For this sensor type, the system will load the URL. It will scan the page to see if the given text can be found or not.

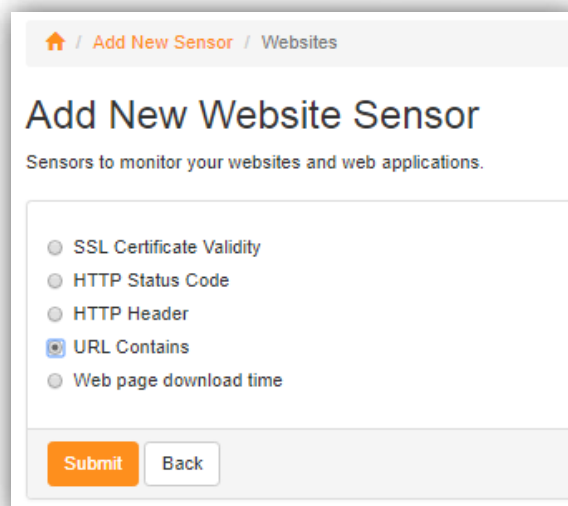
1. Access Menu and Click **Add New Sensor**.



2. Select Websites.



3. Select URL Contains.



4. Provide the information needed to check for the HTTP Header.

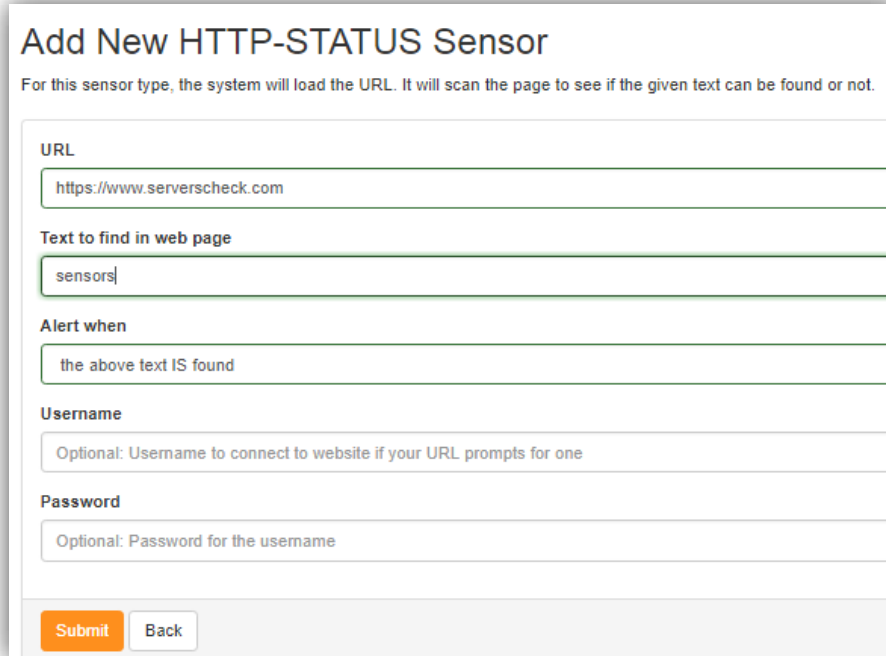
URL - Input the URL you want to check.

Text to Find in Web Page - Type in the text the system should find in the URL.

Alert when - choose between if above text is found or if above text is not found.

Username - Optional, if the website provided prompts for one.

Password - Optional, password for the username.



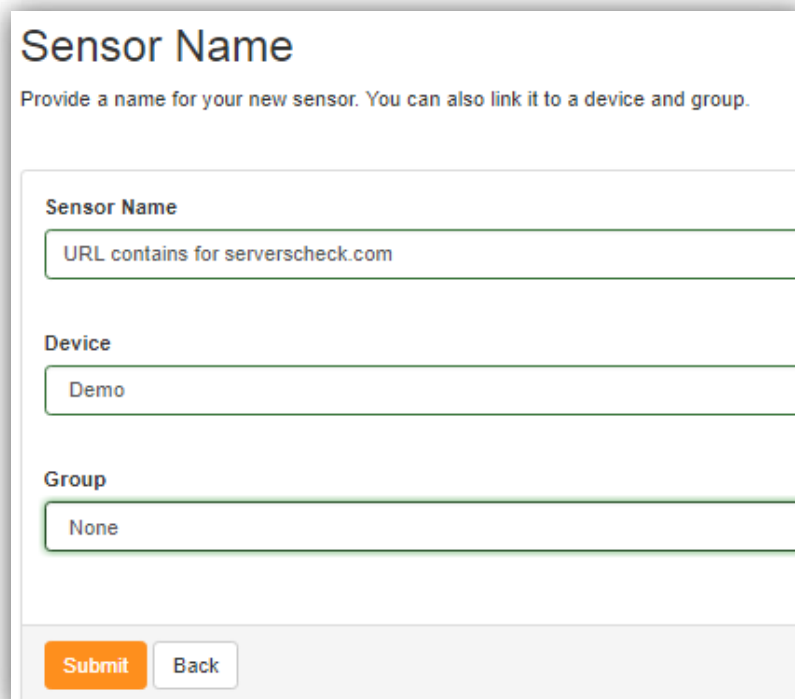
The screenshot shows a web form titled "Add New HTTP-STATUS Sensor". Below the title is a subtitle: "For this sensor type, the system will load the URL. It will scan the page to see if the given text can be found or not." The form contains several input fields: "URL" with the value "https://www.serverscheck.com", "Text to find in web page" with the value "sensors", "Alert when" with the value "the above text IS found", "Username" with the placeholder text "Optional: Username to connect to website if your URL prompts for one", and "Password" with the placeholder text "Optional: Password for the username". At the bottom of the form are two buttons: "Submit" (orange) and "Back" (white).

5. Provide a Sensor Name and link it to a device or group.

Sensor Name - Provide a name for the sensor.

Device - you may select to any device from the drop down list you have created.

Group - you may add to a certain group or you can add a new group.

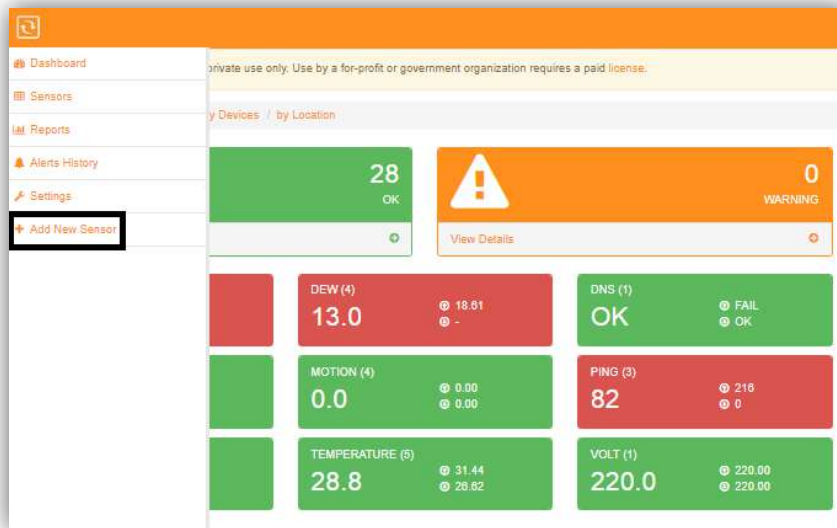


The screenshot shows a web form titled "Sensor Name". Below the title is a subtitle: "Provide a name for your new sensor. You can also link it to a device and group." The form contains three input fields: "Sensor Name" with the value "URL contains for serverscheck.com", "Device" with the value "Demo", and "Group" with the value "None". At the bottom of the form are two buttons: "Submit" (orange) and "Back" (white).

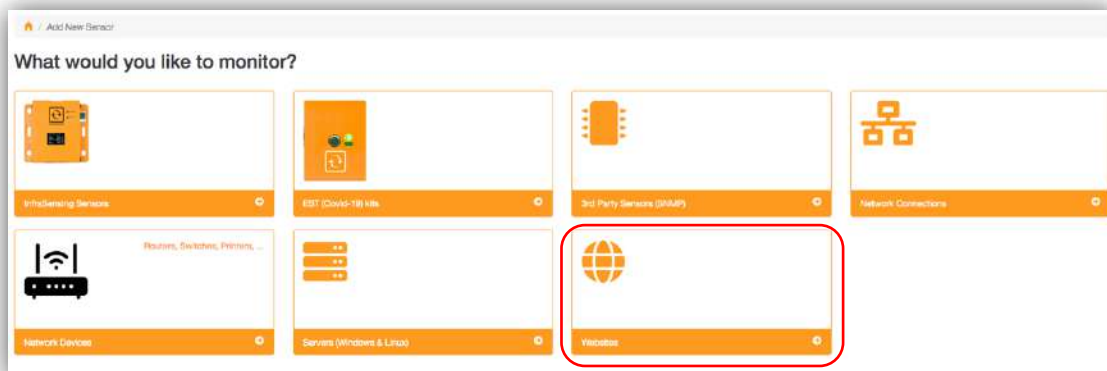
4.5.5. Adding URL Contains Check

For this sensor type, the system will download the webpage (HTML content only). Then it will report back the download time in ms.

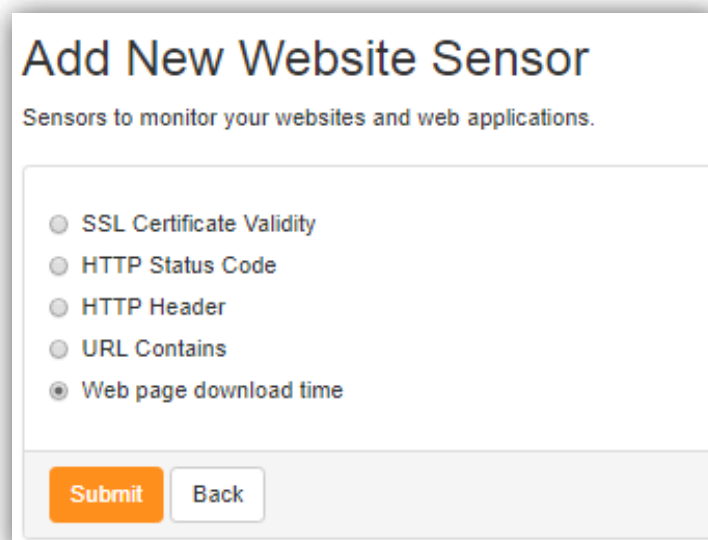
1. Access **Menu** and Click **Add New Sensor**.



2. Select Websites.



3. Select Web page download time.

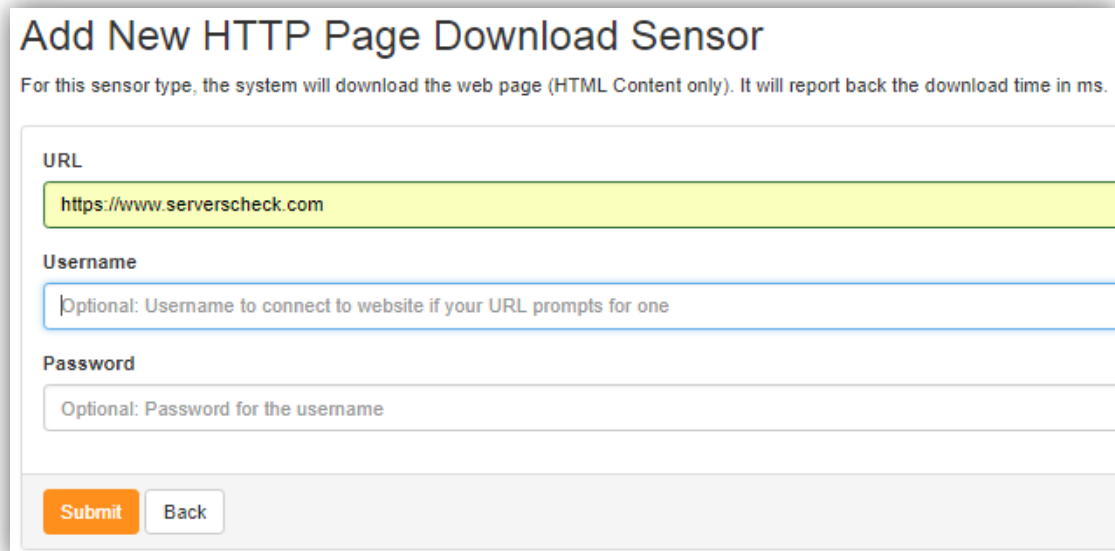


4. Provide the URL of the page you want to check the download time.

URL - Input the URL of the page.

Username - Optional, if the website provided prompts for one.

Password - Optional, password for the username.



Add New HTTP Page Download Sensor
For this sensor type, the system will download the web page (HTML Content only). It will report back the download time in ms.

URL
https://www.serverscheck.com

Username
Optional: Username to connect to website if your URL prompts for one

Password
Optional: Password for the username

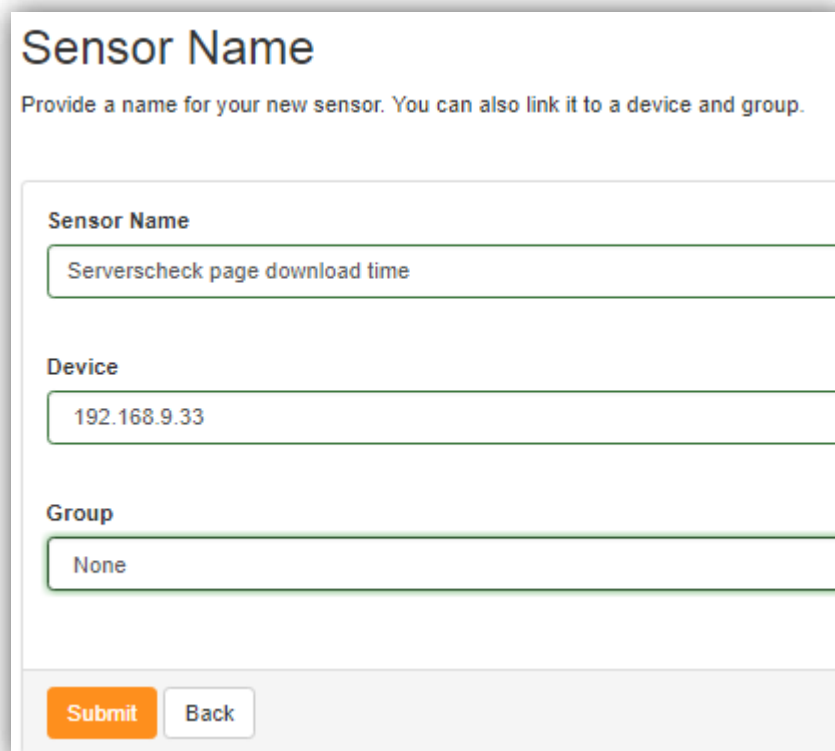
Submit **Back**

5. Provide a Sensor Name and link it to a device or group.

Sensor Name - Provide a name for the sensor.

Device - you may select to any device from the drop down list you have created.

Group - you may add to a certain group or you can add a new group.



Sensor Name
Provide a name for your new sensor. You can also link it to a device and group.

Sensor Name
Serverscheck page download time

Device
192.168.9.33

Group
None

Submit **Back**

5. Generating Reports

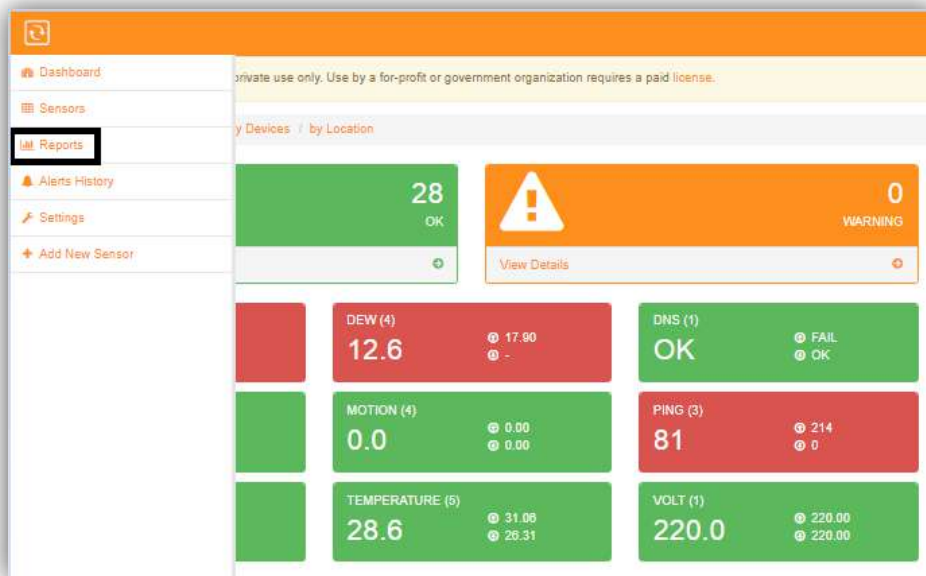
ServersCheck enables users to not only create custom graphs, but also schedule them to be refreshed at whatever rate needed.

Two ways to generate reports:

- by Sensor Names
- by Sensor Types

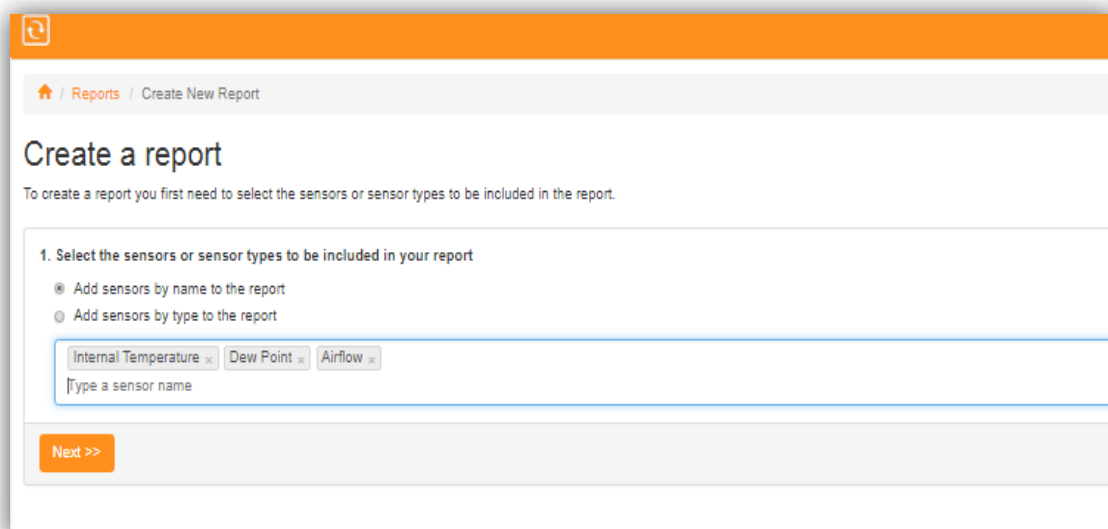
5.1. Generating By Sensor Names

1. Access Menu and go to Reports.



2. Click **Create Report** and select **Add Sensors by name to the report**. Type in the name of the sensor you want to create a report.

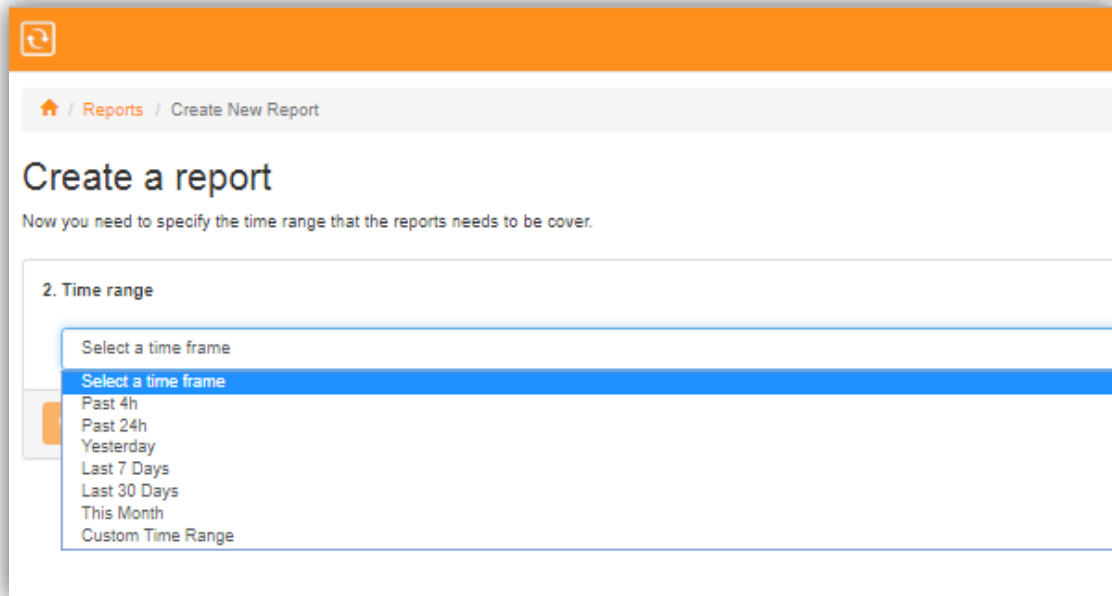
Note: You may input multiple sensor names to be included in your report.



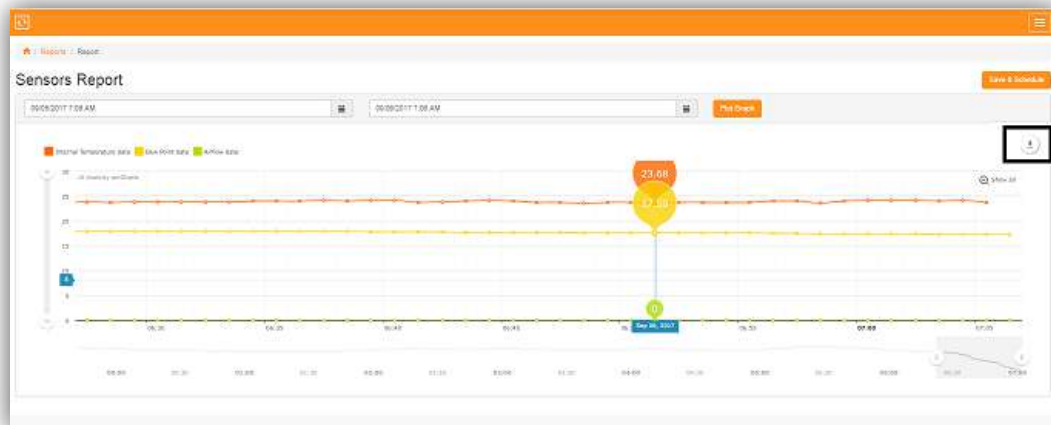
3. Select a Time Range for the report.

You may pre select time range for the report by:

- Past 4h
- Past 24h
- Yesterday
- Last 7 days
- Last 30 days
- This Month
- Custom Time Range



4. Click Generate Report. This will show you a graphical data of the sensors you've selected for reporting.



The image can be saved by clicking the arrow on the upper right hand side.

The image can be downloaded as **PNG, JPG, SVG** or **PDF**.

Or the output be saved as **CSV, XLSX**, or **JSON**.

You may also provide **Annotations** or you can directly **Print** it.

5. Saving & scheduling.

🏠 / Reports / Save & Schedule Report

Save Report

Fill in the form below to save the report. You can also have it automatically emailed to you.

Title of your report

Type the name of your report

Report scheduling

Schedule report to be sent periodically via email
 Run only when needed

Email to

Email addresses to send report to

Send report every

hours

Start sending report on

09/06/2017 1:28 PM

Save Report

Title of your Report - Specify the name of your report.

Report Scheduling:

: schedule report to be sent periodically via email.

Email to - Specify the email address you want the report to be sent.

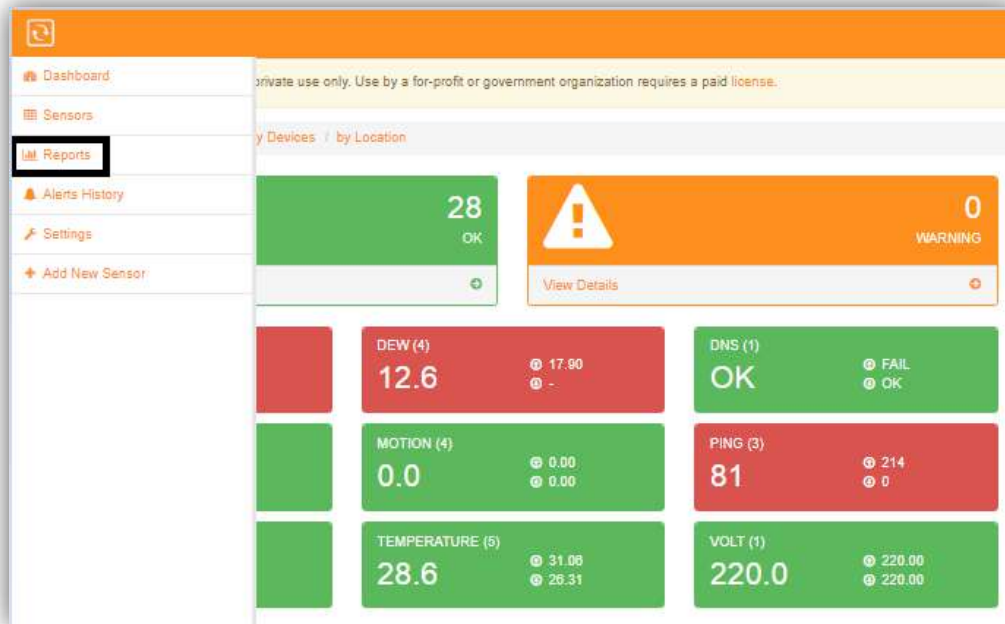
Send report every - Specify the number of hours or days for the report to be automatically be sent.

Start sending report on - You can select a date and time for when the report starts sending.

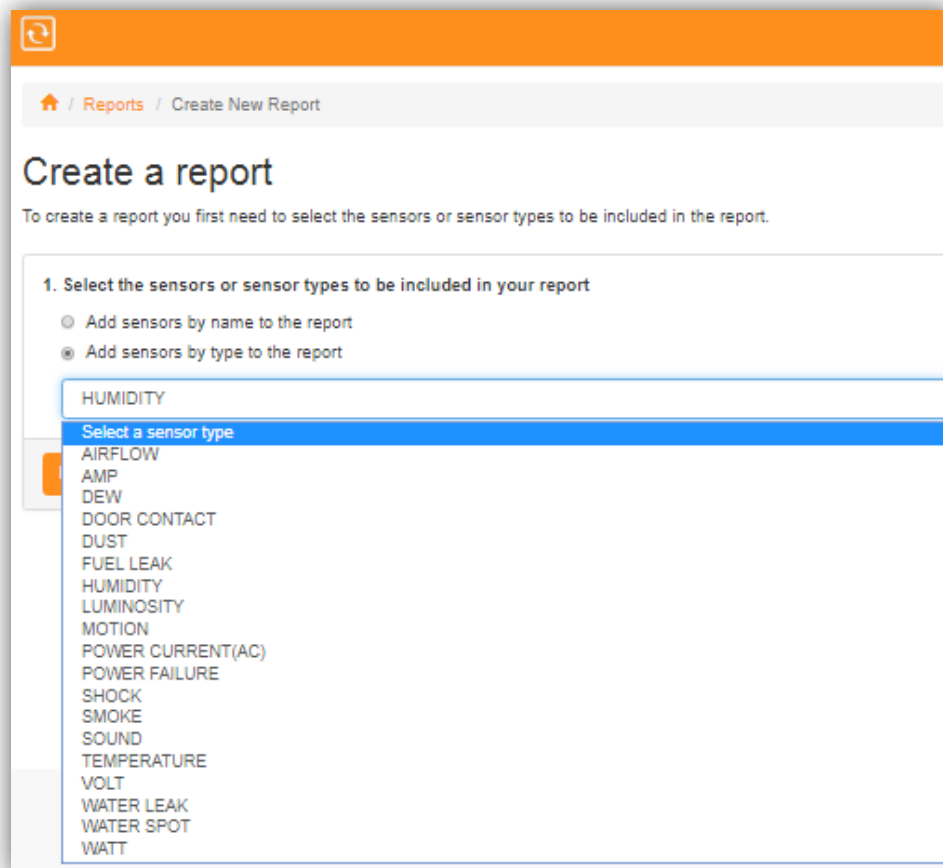
: Run only when needed - Will generate the report one time or only when you manually generate it.

5.2. Generating By Sensor Types

1. Access Menu and go to Reports



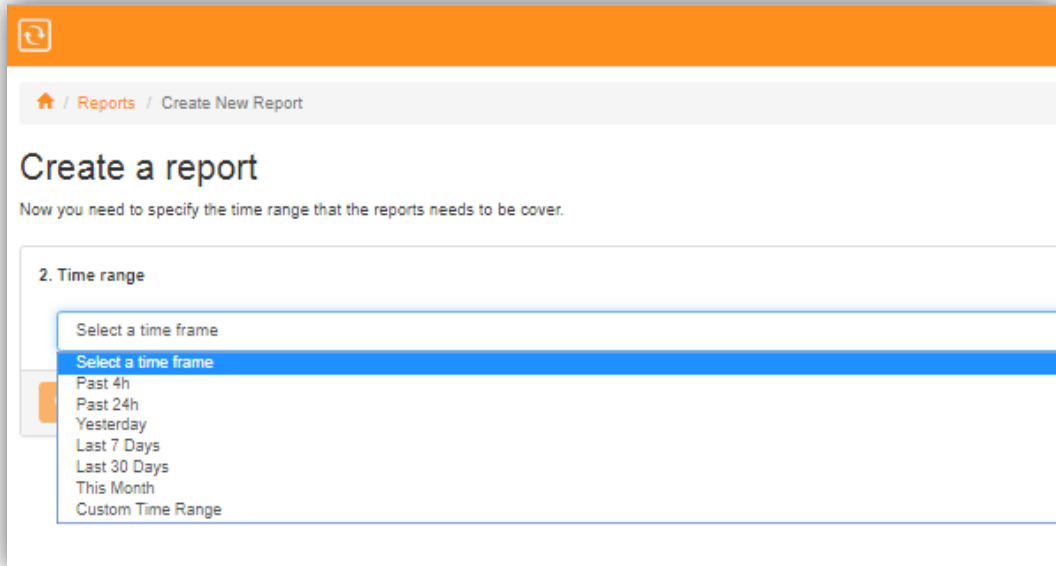
2. Click **Create Report** and select **Add Sensors by type to the report**. Select a sensor type from the drop down list.



3. Select a Time Range for the report.

You may pre select time range for the report by:

- Past 4h
- Past 24h
- Yesterday
- Last 7 days
- Last 30 days
- This Month
- Custom Time Range



4. Click Generate Report. This will show you a graphical data of all sensors that has the same Sensor Type. If you have multiple sensors with the same type, it should show on the graph.



The image can be saved by clicking the arrow on the upper right hand side.

The image can be downloaded as **PNG, JPG, SVG** or **PDF**.

Or the output be saved as **CSV, XLSX**, or **JSON**.

You may also provide **Annotations** or you can directly **Print** it.

5. Saving & scheduling

Home / Reports / Save & Schedule Report

Save Report

Fill in the form below to save the report. You can also have it automatically emailed to you.

Title of your report

Humidity Report

Report scheduling

Schedule report to be sent periodically via email
 Run only when needed

Email to

Email addresses to send report to

Send report every

hours

Start sending report on

09/08/2017 1:47 PM

Save Report

Title of your Report - Specify the name of your report.

Report Scheduling:

: schedule report to be sent periodically via email.

Email to - Specify the email address you want the report to be sent.

Send report every - Specify the number of hours or days for the report to be automatically be sent.

Start sending report on - You can select a date and time for when the report starts sending.

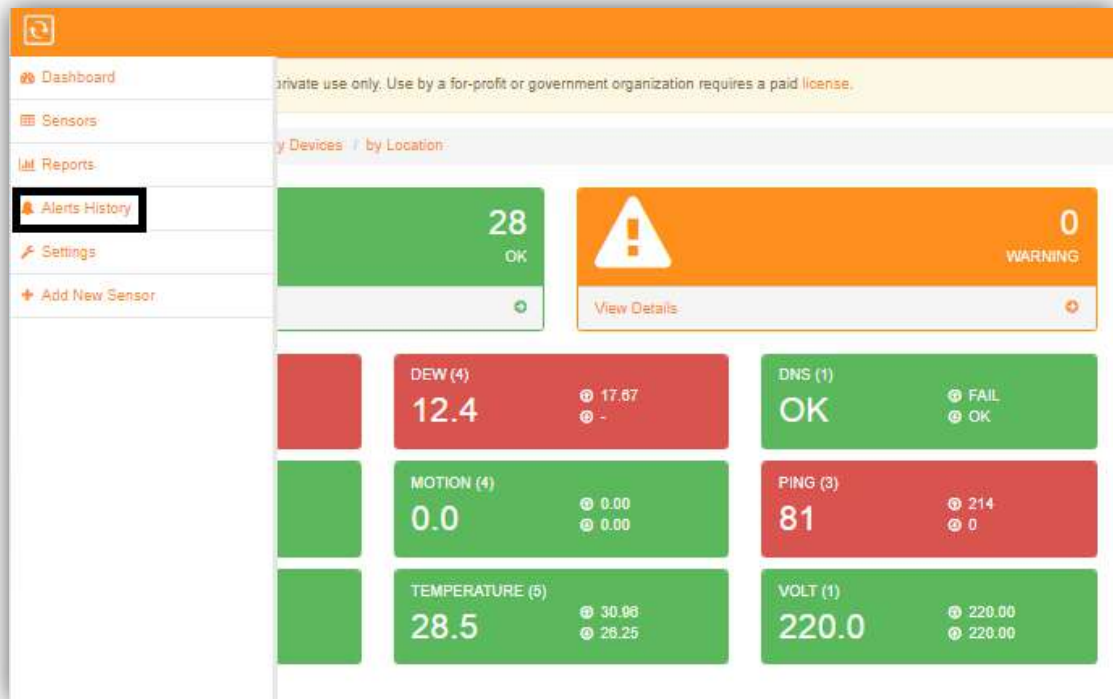
: Run only when needed - Will generate the report one time or only when you manually generate it.

Status	Name	Last Value	Last Check
OK	Airflow	0.00	2 days ago
OK	2Airflow1	0.00	2 days ago
OK	Airflow1	0.00	2 days ago
OK	Dew Point	18.11	2 days ago
OK	3Dew Point1	18.11	2 days ago

6. Alerts History

Alerts would show on a first in first out basis.

1. Click **Menu** and go to **Alerts History**.



2. This would open up a window that shows all historical alerts on any sensors/checks you have. This gives data of the time when the alerts occurred, the Sensor Name, the event type, the actual event that occurred, and the info.

Clicking on each of the Sensor Name would open up the graphical data of the Sensor.

The screenshot shows the 'Alerts History' page. It features a table with columns for ID, Time, Sensor Name, Event Type, Event, and Info. The table contains 10 entries, with the most recent alert occurring 8 hours ago. The table is paginated, showing 1 to 10 of 100 entries.

ID	Time	Sensor Name	Event Type	Event	Info
316	8 hours ago	Internal Temperature	Status Change	OK to WARNING	
315	2 days ago	Internal Temperature	Status Change	OK to WARNING	
314	2 days ago	Flooding ¹	Status Change	DOWN to OK	No numeric value returned (value was -)
313	2 days ago	Flooding ¹	Status Change	OK to DOWN	No numeric value returned (value was -)
312	3 days ago	Sound Sense	Status Change	DOWN to OK	
311	3 days ago	Sound Sense	Status Change	OK to DOWN	
310	3 days ago	Internal Temperature	Status Change	OK to WARNING	
309	4 days ago	Internal Temperature	Status Change	OK to WARNING	
308	4 days ago	Sound Sense	Status Change	OK to DOWN	No value returned
307	4 days ago	DNS resolution serverscheck.com	Status Change	OK to DOWN	Could not resolve host serverscheck.com

7. Adding Security to your Monitoring Software.

This section is for more advanced users to allow the software to be run on https instead of the default port of 1272.

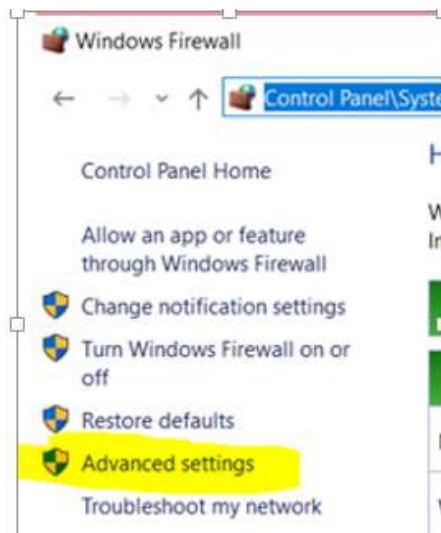
Default access to software is <http://192.x.x.x:1272> (IP is dependent on the address the Appliance gets)

1. First block the incoming connection on TCP port 1272 via Windows firewall.

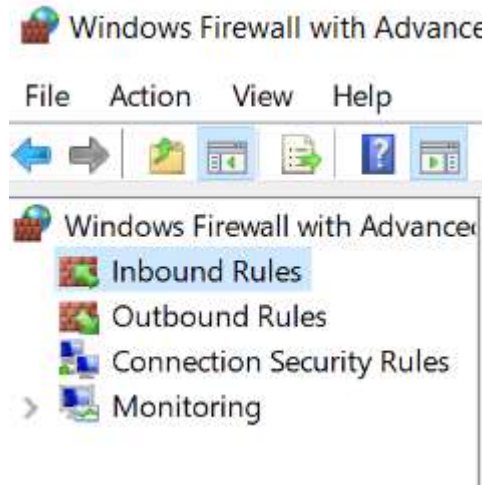
* To access the windows firewall open any folder on the address field type in Control Panel\System and Security\Windows Firewall.



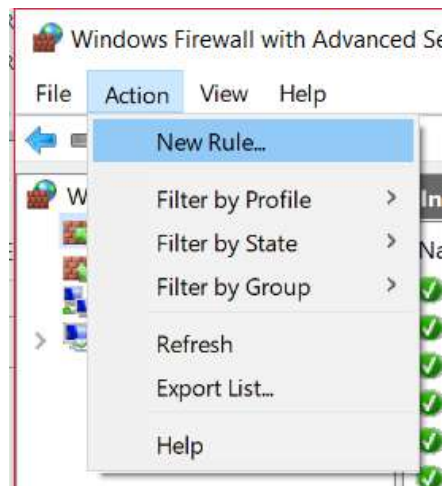
- * Choose "Advance settings" on the left panel.



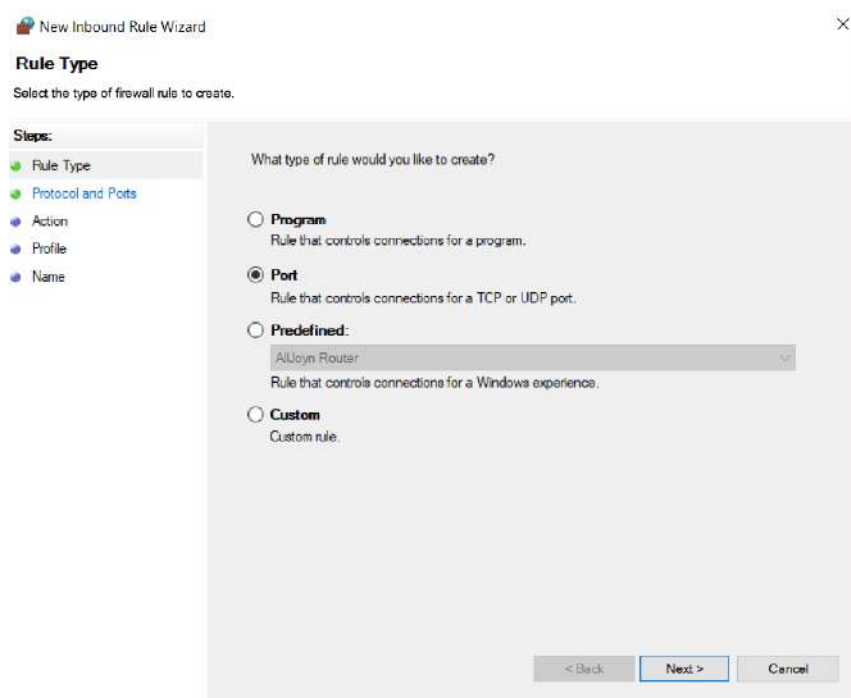
* Under firewall Advance Settings Highlight Inbound Rules.



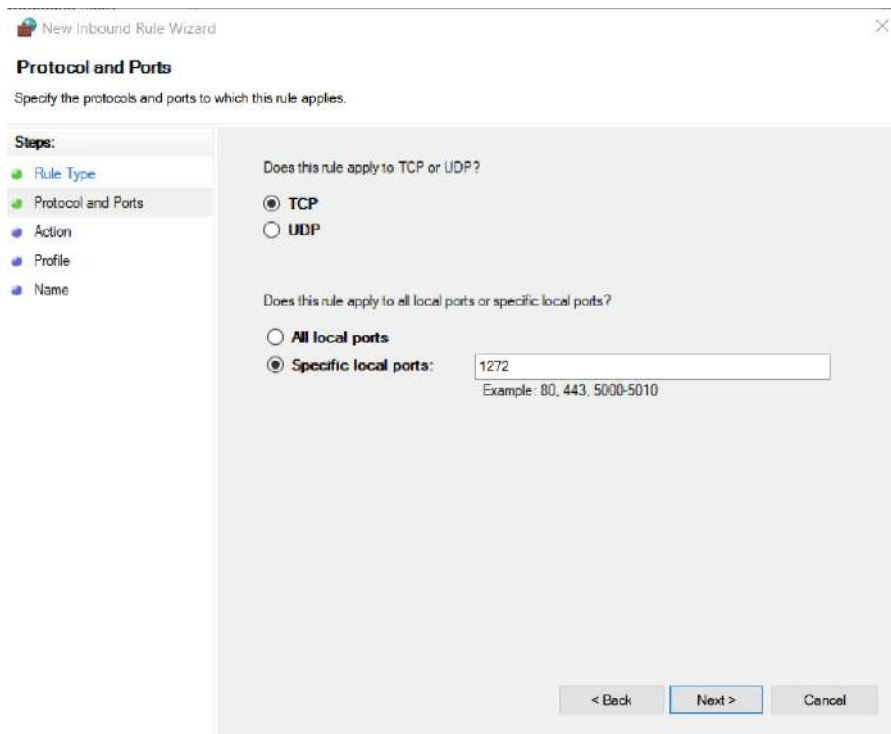
* Click on Action and then New Rule.



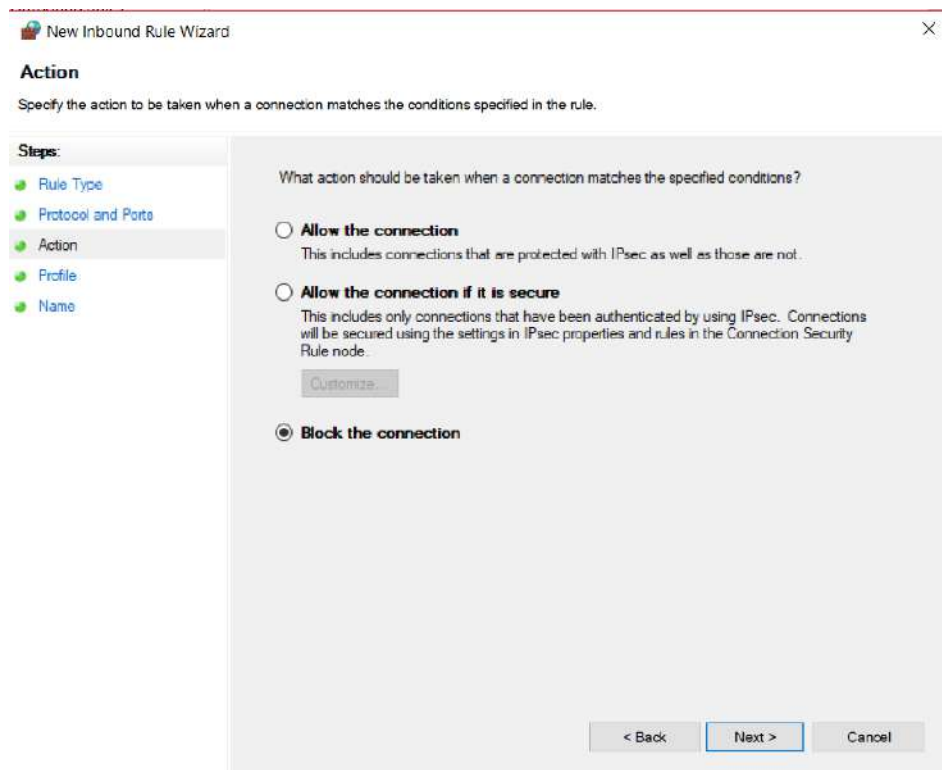
* On the next screen choose "PORT".



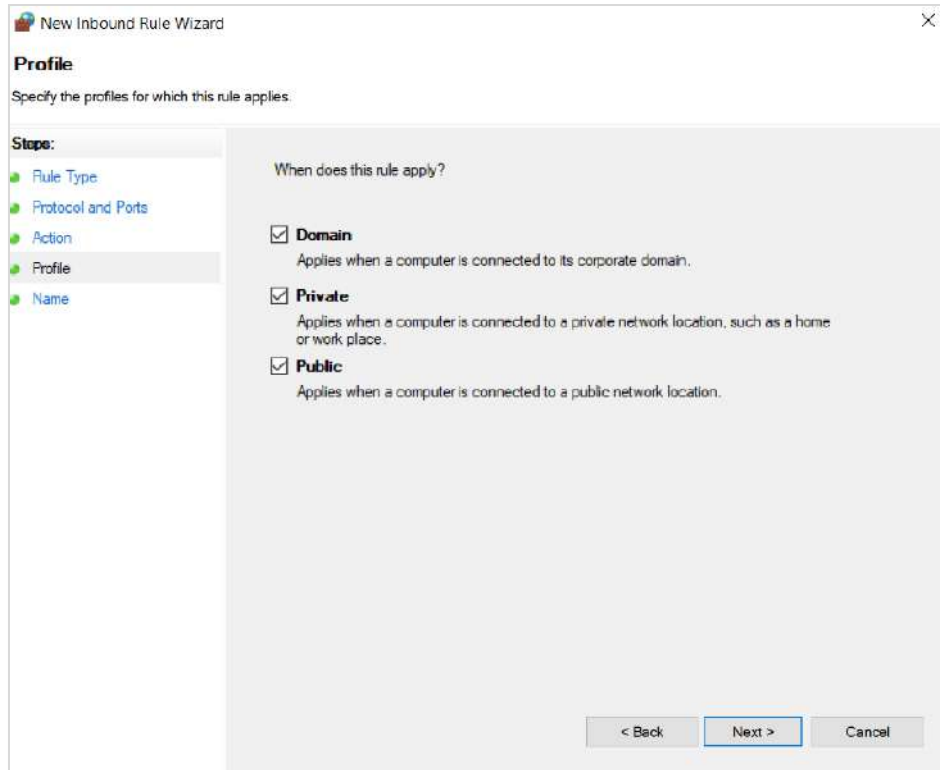
* Then “TCP” and then on the option below choose Specific Local Ports and then type in 1272 and click next.



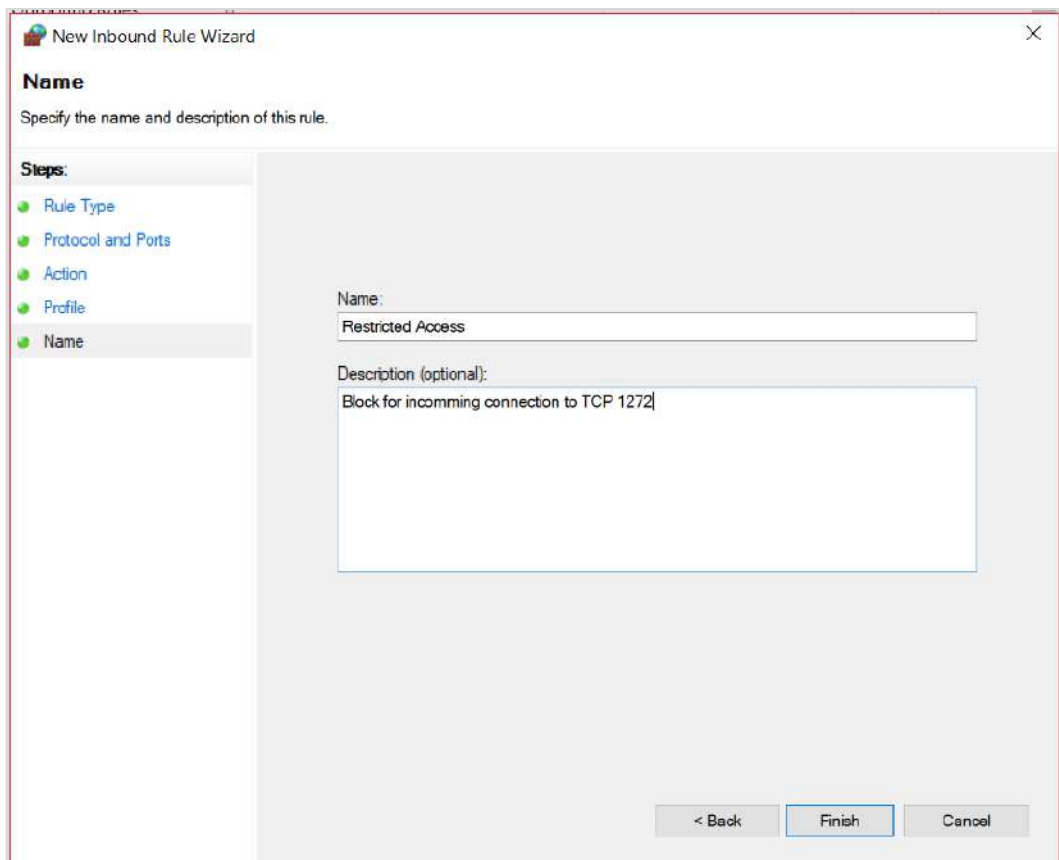
* Choose Block the Connection.



* Put a check mark on all.



* Create a label and finish set up.



After blocking the port 1272, users will no longer be able to access the software directly via port 1272. In which you will now need a reverse proxy server.

7.1. NGINX (reverse proxy server)

With the release of software version 15, we have integrated the NGINX technology into our software. NGINX is a web server, which can also be used as a reverse proxy, load balancer, mail proxy and HTTP cache. With NGINX, the security of the software has gone on to a higher level.

7.1.1. Configuring NGINX

You can access the configuration file on

C:\Program Files (x86)\ServersCheck_Monitoring\conf\nginx.conf

A default configuration is already made with the following feature

- website runs now on port 80 (no longer 1272)
- increased security as a lot of traffic filtering is done at the NGINX level
- static content is served by NGINX (better performance)
- ability to run it in SSL mode with custom certificates

NOTE: Advance users may configure NGINX at their own discretion, advance configuration is not supported. More information about NGINX here (<https://www.nginx.com/>)

7.2. Running the software on HTTPS mode

Advance users may apply certificates using NGINX by opening the configuration file then edit the server block as follows

By default it runs via http mode with the code “listen 80;”

To run HTTPS remove the # sign over the 3 lines mentioned below (HTTPS (SSL) mode on the configuration file).

```
listen          443 ssl;
ssl_certificate /conf/nginx.crt;
ssl_certificate_key /conf/nginx.key;
```

Place your certificate and key in C:\Program Files (x86)\ServersCheck_Monitoring\conf and then replace nginx with the name of the certificate.

Save your work, close all opened browsers, go to C:\Program Files (x86)\ServersCheck_Monitoring and click on the NGINX application to apply your settings.

8. Running on Debug Mode

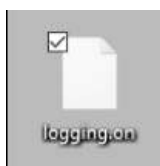
By running the software in debug mode we will be creating log files, log files will show the software activities and will help in resolving issues.

8.1. Steps to run in Debug Mode

1. Since the software folder is secured, lets create the file we require on your desktop, We do this by pressing the right click and then choosing the option "NEW" and then we click on "Text Document".



2. Next we have to rename the newly created document into "logging.on", initially after creating a file you can rename it right away otherwise hover your mouse over the file and then press right click, then choose "Rename". For comparison the file we created initially was named "New Text Document.txt" and we have to rename that into "logging.on".



3. After creating the file, copy or move it over to the directory path C:\Program Files (x86)\ServersCheck_Monitoring\logs

Name	Date modified	Type	Size
access.log	9/21/2020 9:01 AM	Text Document	311,405 KB
error.log	7/29/2020 11:21 AM	Text Document	22,438 KB
logging.on	10/5/2020 9:55 AM	ON File	0 KB
nginx.pid	9/21/2020 9:02 AM	PID File	1 KB

4. Restart the computer and then re open the software.
5. Go back to the directory path C:\Program Files (x86)\ServersCheck_Monitoring\logs, you will notice 3 text files created.

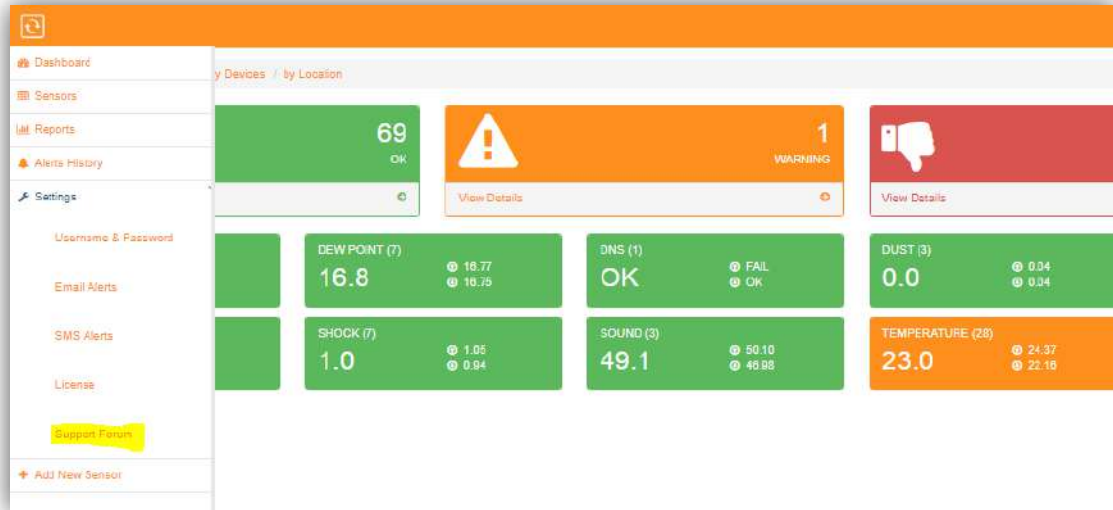
Name	Date modified	Type	Size
access.log	10/5/2020 9:42 AM	Text Document	350,124 KB
error.log	7/29/2020 11:21 AM	Text Document	22,438 KB
log_alerts.txt	10/5/2020 10:43 AM	Text Document	1 KB
log_thread2.txt	10/5/2020 10:44 AM	Text Document	8 KB
log_watcher.txt	10/5/2020 10:44 AM	Text Document	2 KB
logging.on	10/5/2020 9:55 AM	ON File	0 KB
nginx.pid	10/5/2020 10:36 AM	PID File	1 KB

9. Support Forum

You will be redirected to our online community forum which is managed by our Engineers and from other users using ServersCheck products -

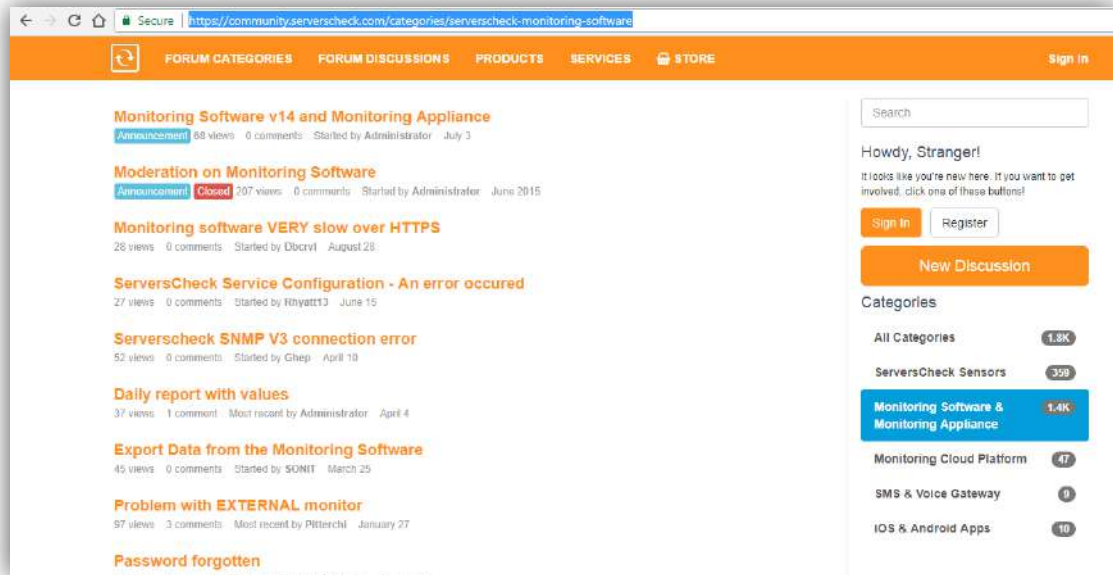
<https://community.ServersCheck.com/categories/ServersCheck-monitoring-software>

1. Go



2. You will be redirected to

<https://community.ServersCheck.com/categories/ServersCheck-monitoring-software> wherein you can create an account and post in the discussions in the forums.



3. Clicking Sign In will redirect you to <https://my.ServersCheck.com/>. You need to have a my.ServersCheck account for you to post a discussion.



Tips:

When submitting a support ticket regarding software issues it is best to give the log files along with the software version you are using.

For monitoring issues it is best to look at log_thread2.txt, for alerting issues it is log_alertst.txt and for general stability issues it is best to look at log_watcher.txt.