SERVERSCHECK

www.serverscheck.com

ServersCheck Monitoring Software
And
Monitoring Appliance User Manual

Copyright:

Copyright © 2019 ServersCheck BVBA
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 ServersCheck.
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 ServersCheck.

ServersCheck provides this document “as is,” without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. ServersCheck 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.

ServersCheck has made this document to the best of its abilities. However ServersCheck 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://serverscheck.com/
OPENING SENSORGATEWAY OR EXTERNAL SENSOR PROBE VOIDS THE WARRANTY

Contents

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

1.1.1. What's New on version 14

This is the new version of the Serverscheck 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

- SMS alerting via GSM modem (Huawei USB GSM modems)

1.2. ServersCheck Monitoring Appliance

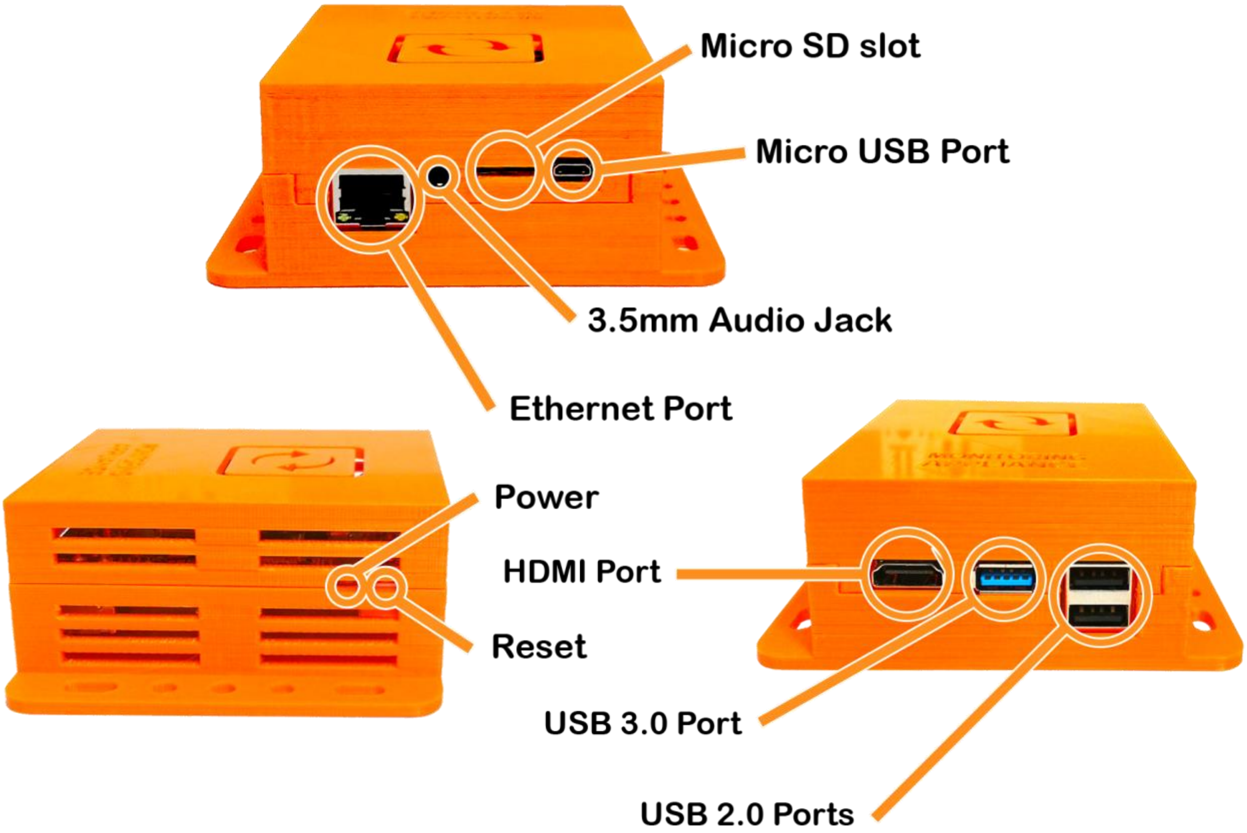
1.2.1. Overview of the Appliance

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.

1.2.2. Technical Specifications

- Processor: Intel Cherry Trail Z8300 Quad Core 1.8GHz
- Operation 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
- One USB3.0 port and two USB 2.0 ports
- WiFi and Bluetooth 4.0
- Video output: HDMI and MIPI-DSI
- Power: 5v/2A
- 3.5mm Audio Jack

1.2.3. Image and Parts of the Appliance



1.2.4. 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.

1.2.5. 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)

1.3. 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.

   * A GSM modem for SMS Alerting
```

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
that you use a USB GSM Modem or Purchase Premium Credits.

   * Requires Administrative privilege on the computer
```

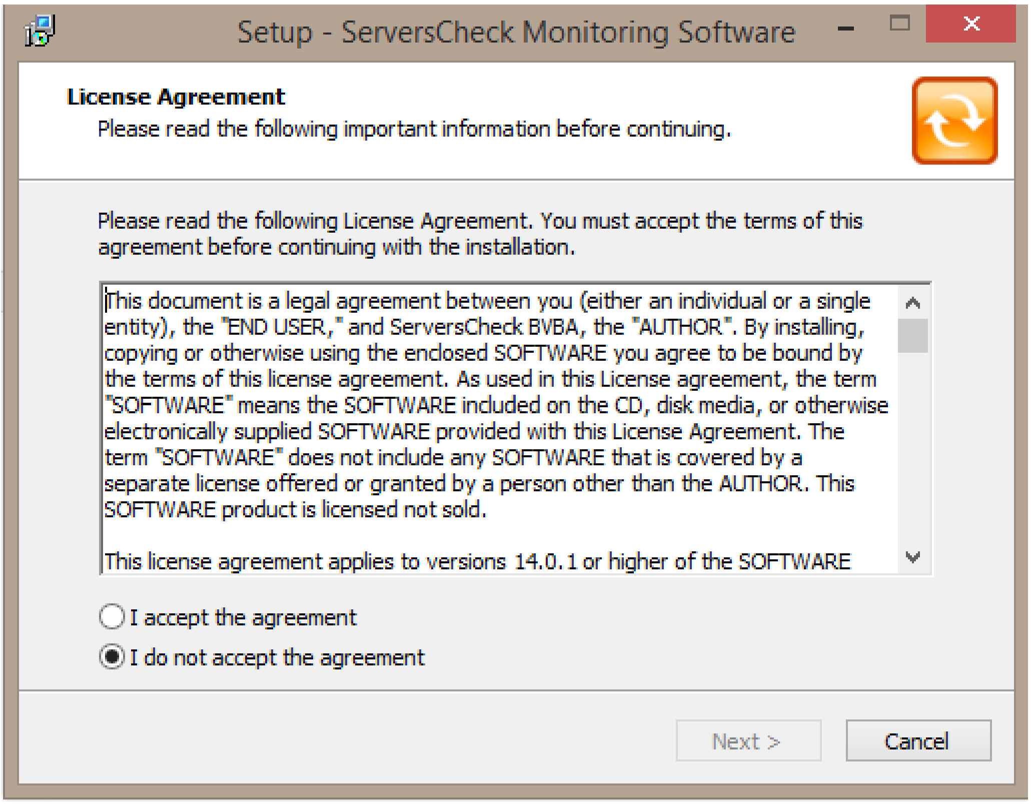
2. Getting Started

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 install.



License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

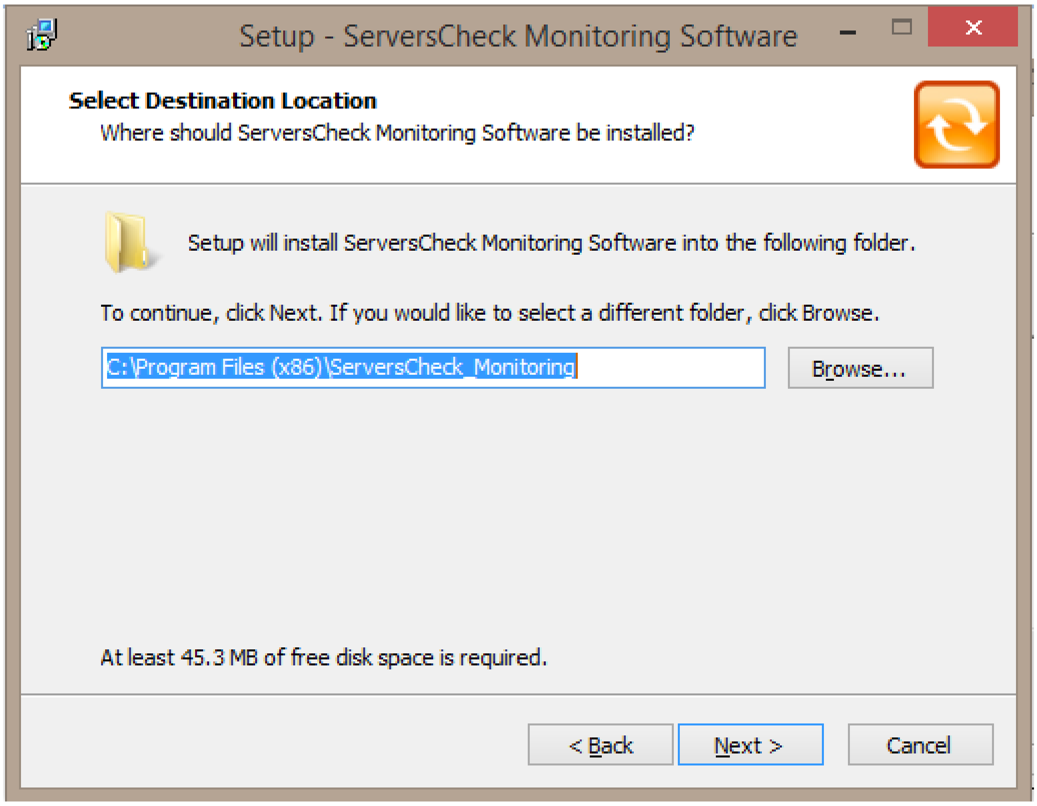
This document is a legal agreement between you (either an individual or a single entity), the "END USER," and ServersCheck BVBA, the "AUTHOR". By installing, copying or otherwise using the enclosed SOFTWARE you agree to be bound by the terms of this license agreement. As used in this License agreement, 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

○ I accept the agreement

● I do not accept the agreement

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



Select Destination Location

Where should ServersCheck Monitoring Software be installed?

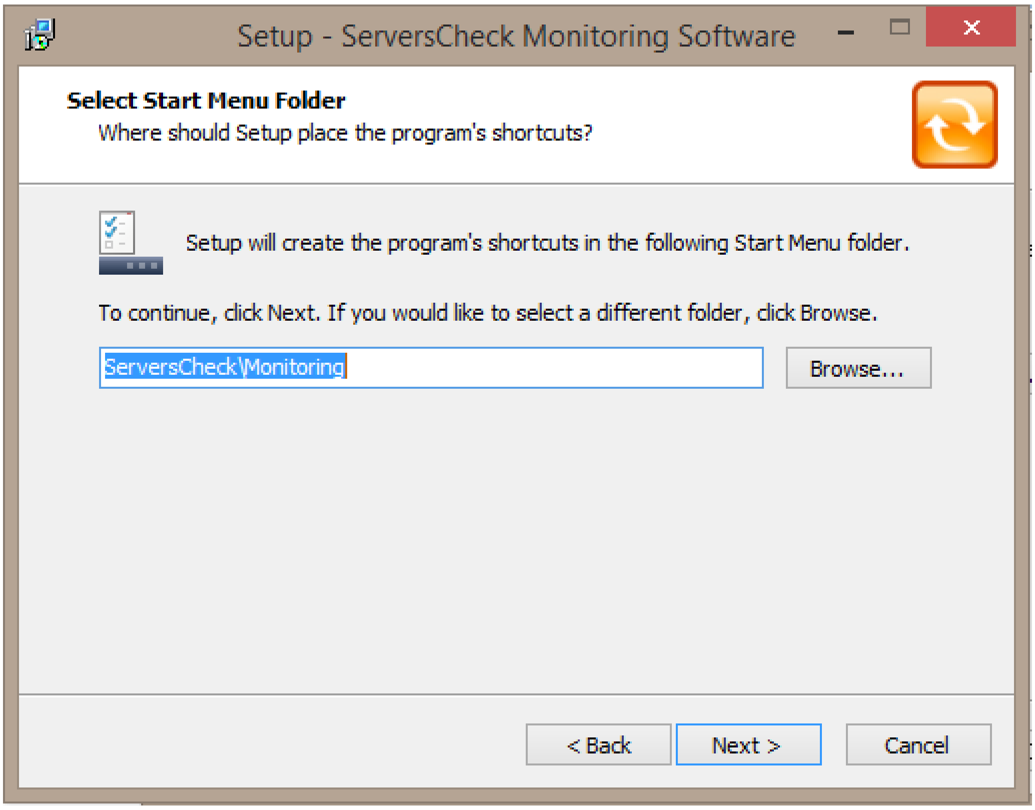
Setup will install ServersCheck Monitoring Software into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files (x86)\ServersCheck_Monitoring

At least 45.3 MB of free disk space is required.

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



Select Start Menu Folder

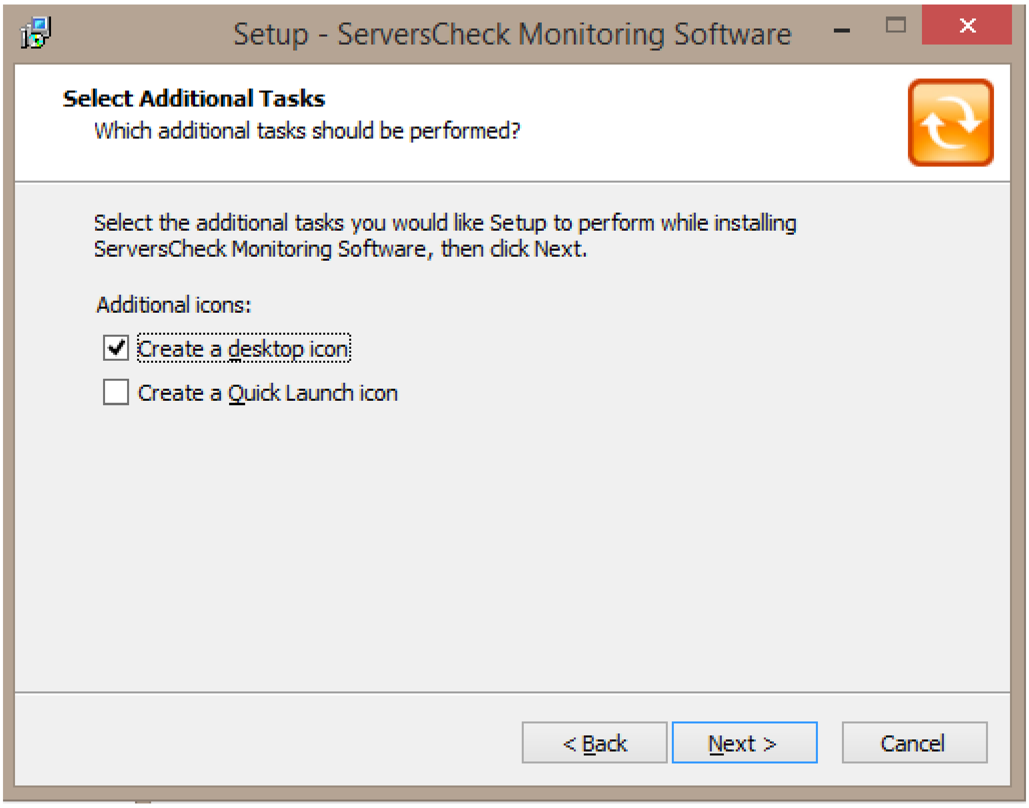
Where should Setup place the program's shortcuts?

Setup will create the program's shortcuts in the following Start Menu folder.

To continue, click Next. If you would like to select a different folder, click Browse.

ServersCheck\Monitoring

6. Additional options can be configured in this step.



Select Additional Tasks

Which additional tasks should be performed?

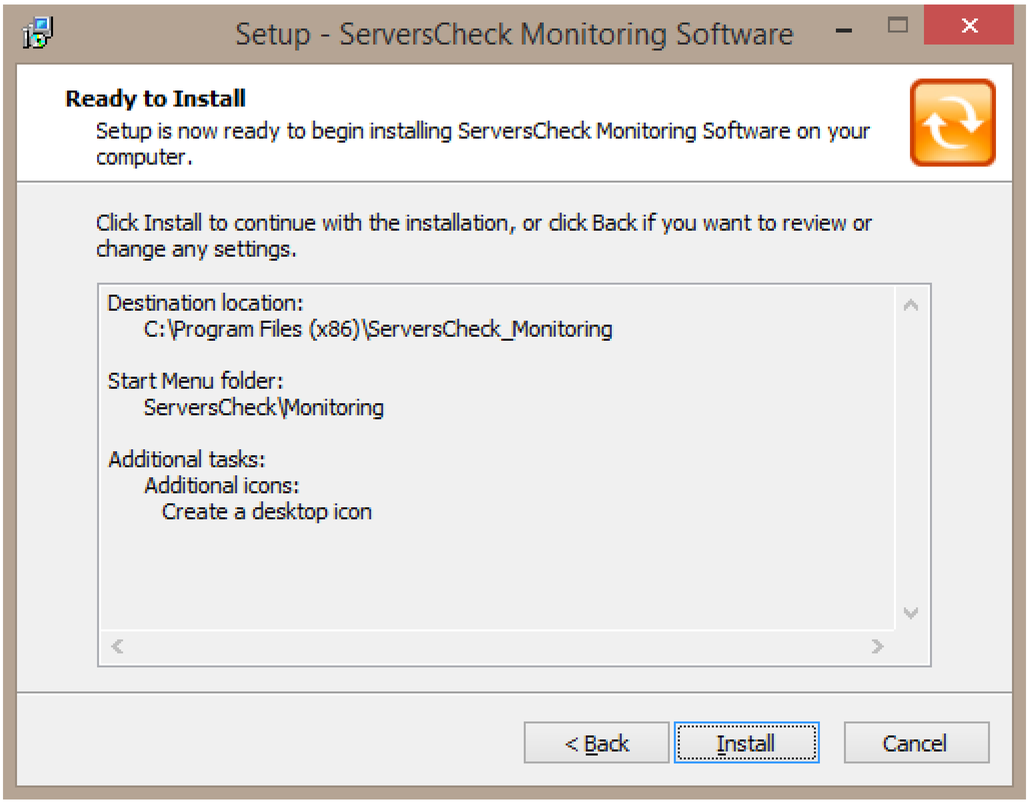
Select the additional tasks you would like Setup to perform while installing ServersCheck Monitoring Software, then click Next.

Additional icons:

☑ Create a desktop icon

□ Create a Quick Launch icon

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



Ready to Install

Setup is now ready to begin installing ServersCheck Monitoring Software on your computer.

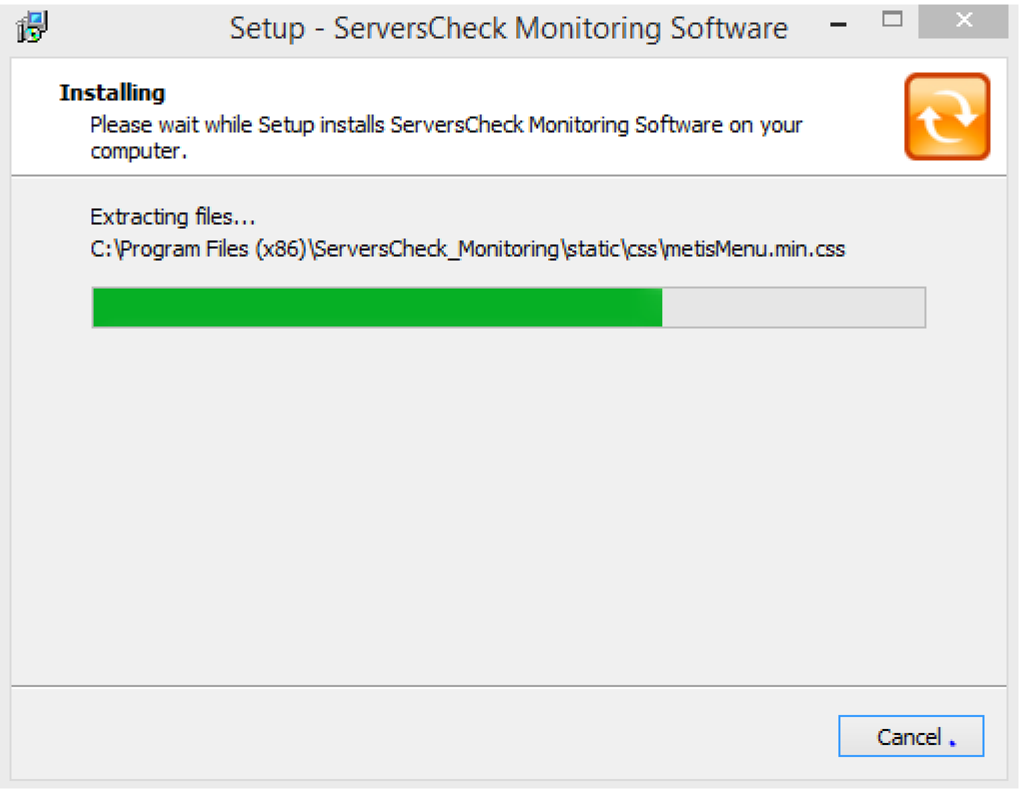
Click Install to continue with the installation, or click Back if you want to review or change any settings.

```
Destination location:
    C:\Program Files (x86)\ServersCheck_Monitoring

Start Menu folder:
    ServersCheck\Monitoring

Additional tasks:
    Additional icons:
      Create a desktop icon
```

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

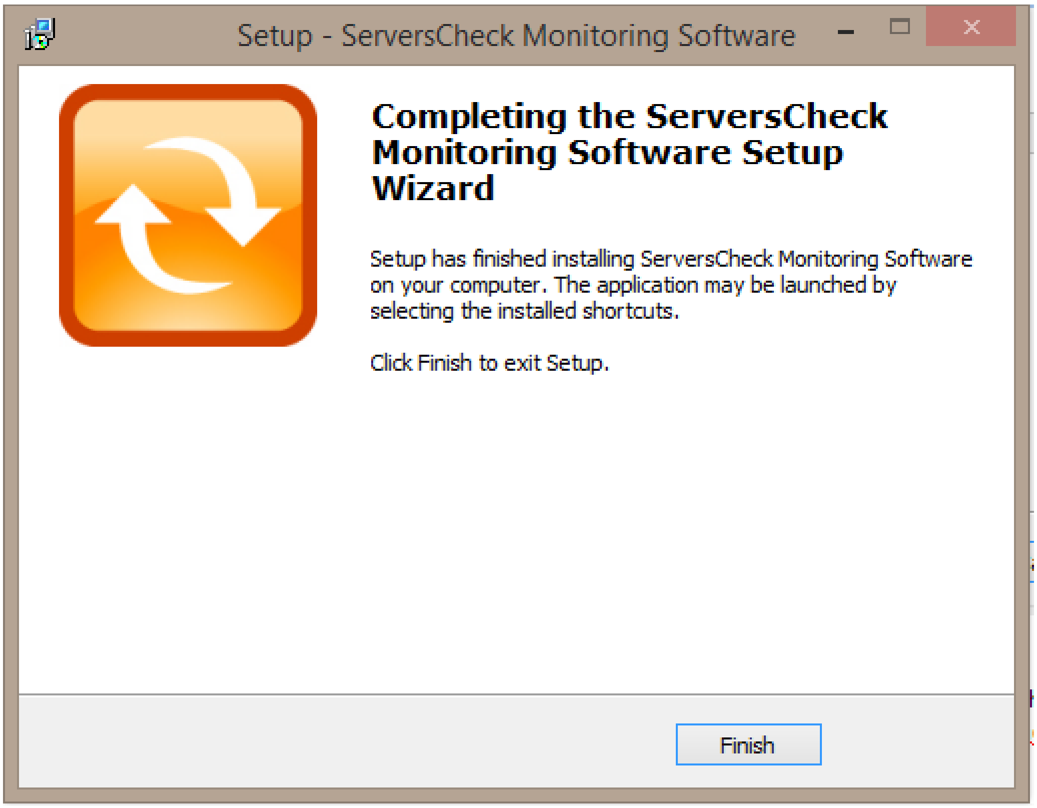


Installing

Please wait while Setup installs ServersCheck Monitoring Software on your computer.

Extracting files...
C:\Program Files (x86)\ServersCheck_Monitoring\static\css\metisMenu.min.css

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



Completing the ServersCheck Monitoring Software Setup Wizard

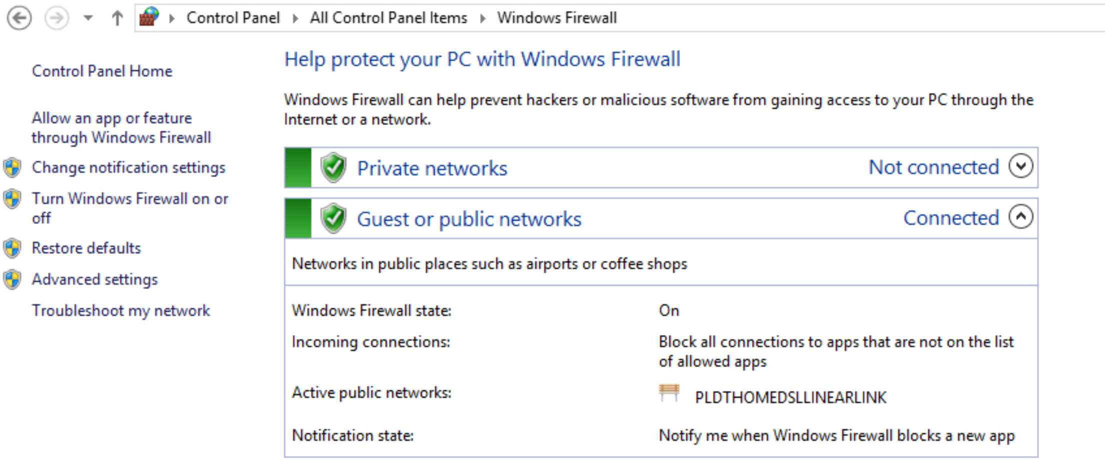
Setup has finished installing ServersCheck Monitoring Software on your computer. The application may be launched by selecting the installed shortcuts.

Click Finish to exit Setup.

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



Control Panel › All Control Panel Items › Windows Firewall

Control Panel Home

Allow an app or feature through Windows Firewall

Change notification settings

Turn Windows Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

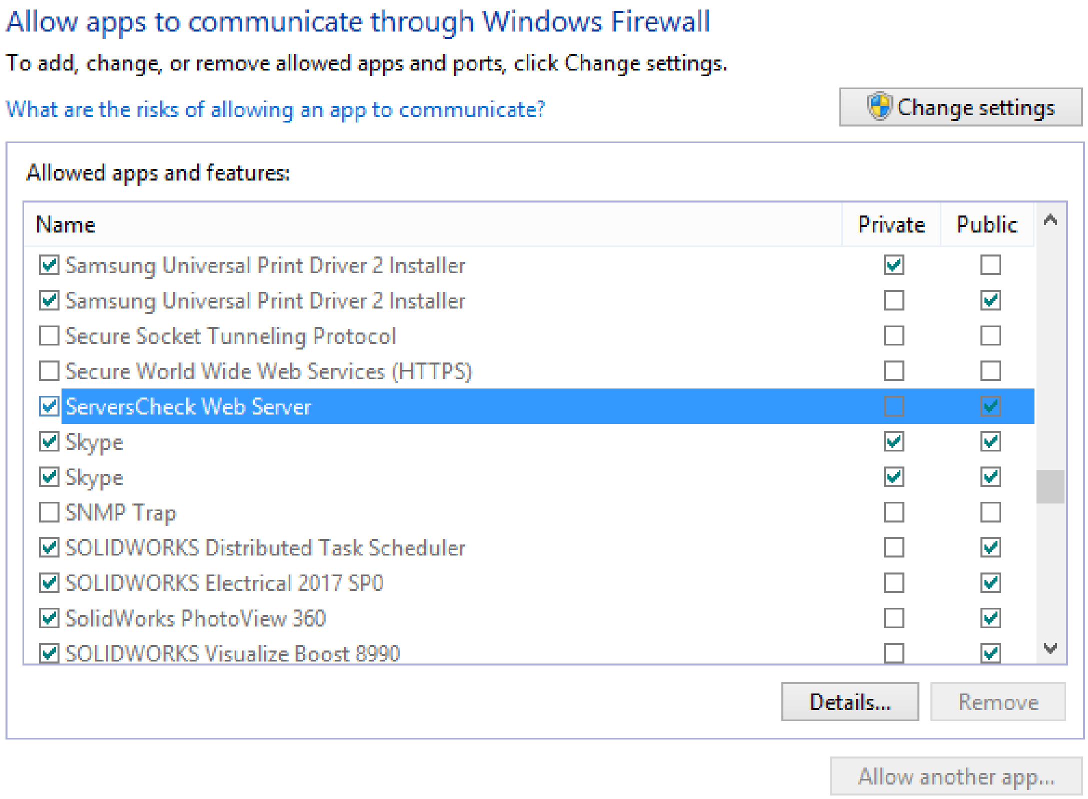
Private networks — Not connected

Guest or public networks — Connected

Networks in public places such as airports or coffee shops

Windows Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	PLDTHOMEDSLLINEARLINK
Notification state:	Notify me when Windows Firewall blocks a new app

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.



Allow apps to communicate through Windows Firewall

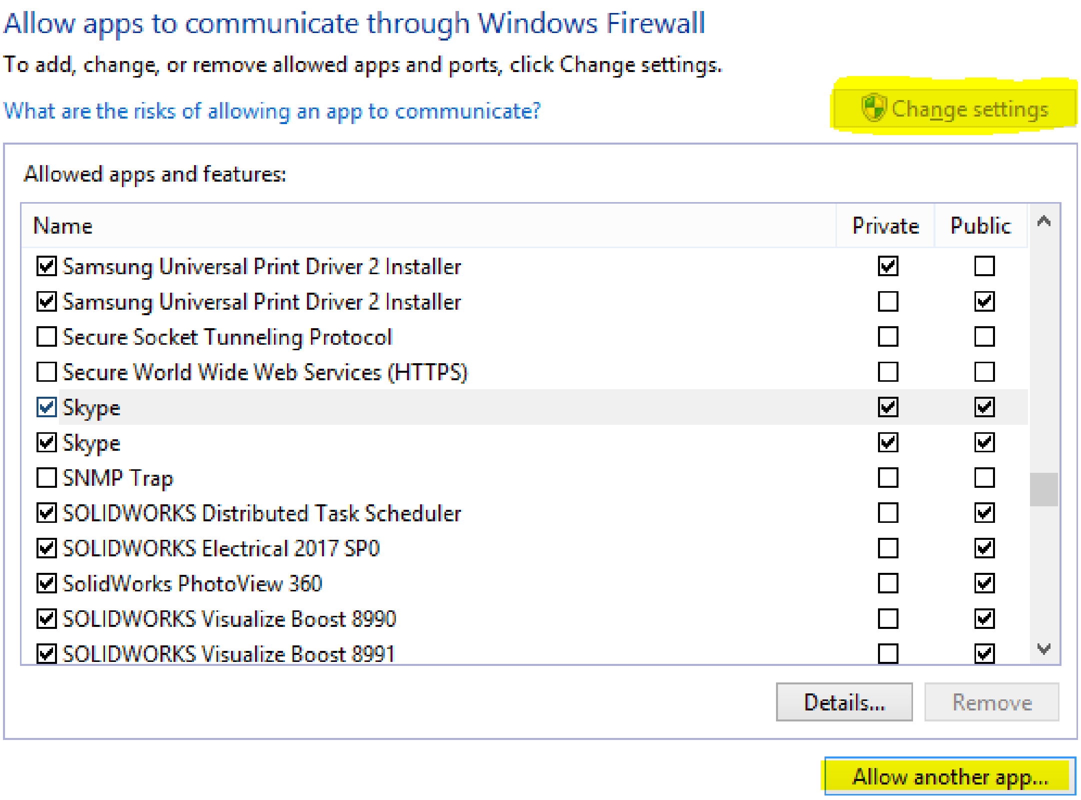
To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Allowed apps and features:

Name	Private	Public
☑ Samsung Universal Print Driver 2 Installer	☑	□
☑ Samsung Universal Print Driver 2 Installer	□	☑
□ Secure Socket Tunneling Protocol	□	□
□ Secure World Wide Web Services (HTTPS)	□	□
☑ ServersCheck Web Server	□	☑
☑ Skype	☑	☑
☑ Skype	☑	☑
□ SNMP Trap	□	□
☑ SOLIDWORKS Distributed Task Scheduler	□	☑
☑ SOLIDWORKS Electrical 2017 SP0	□	☑
☑ SolidWorks PhotoView 360	□	☑
☑ SOLIDWORKS Visualize Boost 8990	□	☑

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



Allow apps to communicate through Windows Firewall

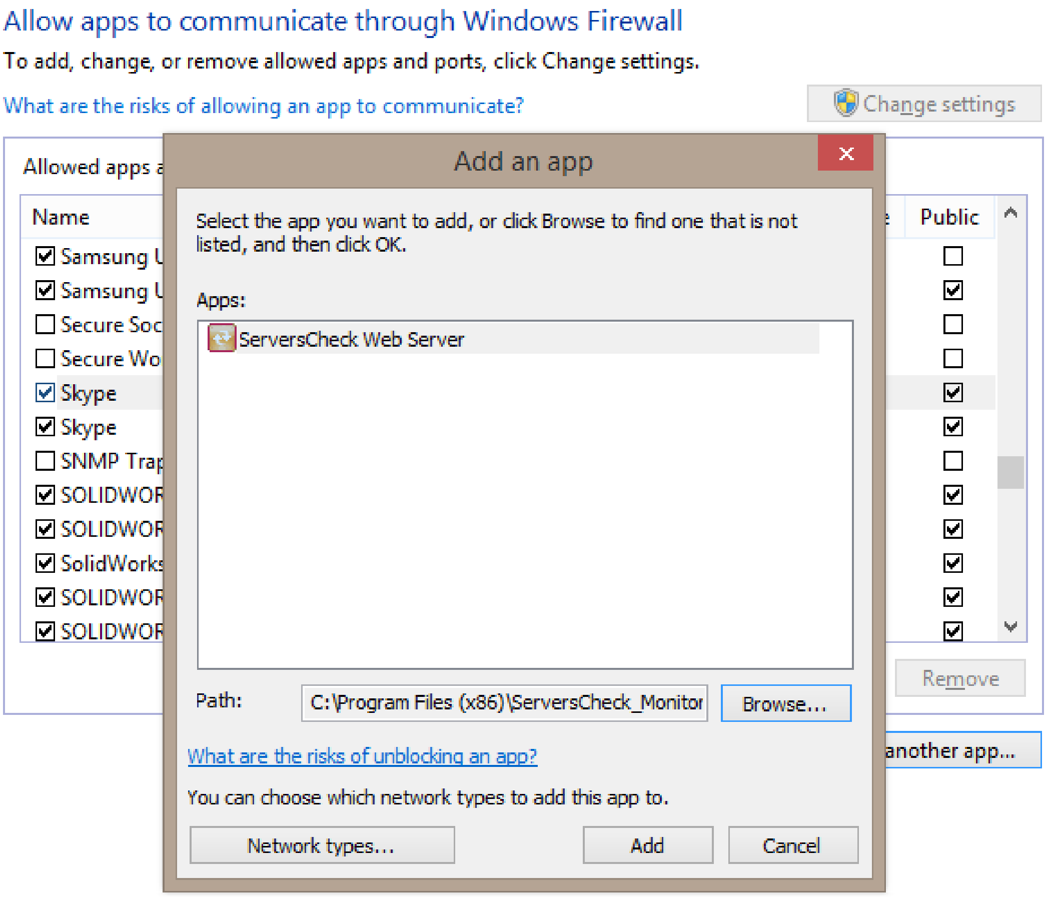
To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Allowed apps and features:

Name	Private	Public
☑ Samsung Universal Print Driver 2 Installer	☑	□
☑ Samsung Universal Print Driver 2 Installer	□	☑
□ Secure Socket Tunneling Protocol	□	□
□ Secure World Wide Web Services (HTTPS)	□	□
☑ Skype	☑	☑
☑ Skype	☑	☑
□ SNMP Trap	□	□
☑ SOLIDWORKS Distributed Task Scheduler	□	☑
☑ SOLIDWORKS Electrical 2017 SP0	□	☑
☑ SolidWorks PhotoView 360	□	☑
☑ SOLIDWORKS Visualize Boost 8990	□	☑
☑ SOLIDWORKS Visualize Boost 8991	□	☑

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.



Allow apps to communicate through Windows Firewall

To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Add an app

Select the app you want to add, or click Browse to find one that is not listed, and then click OK.

Apps:

ServersCheck Web Server

Path: C:\Program Files (x86)\ServersCheck_Monitor

What are the risks of unblocking an app?

You can choose which network types to add this app to.

2.3. 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.

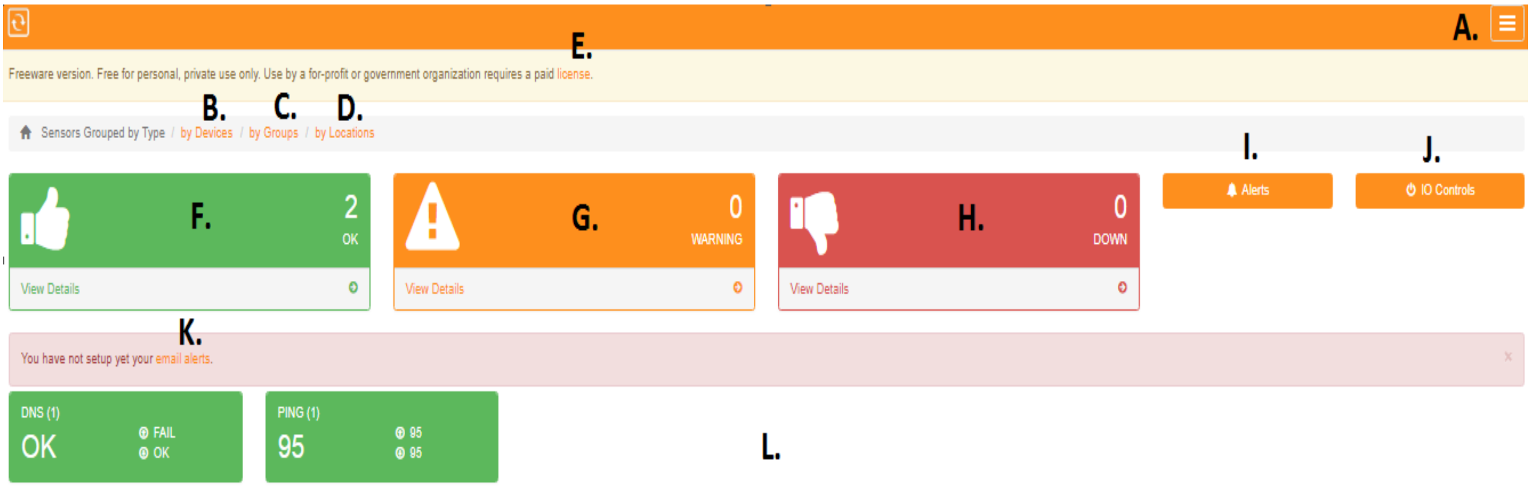
*** You may logon locally to the server using the pre-installed web browser. By default it will open the url http://localhost:1272. When the webserver is accessed locally, then no credentials are required.**

*** 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.

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.



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

You have not setup yet your email alerts.

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.

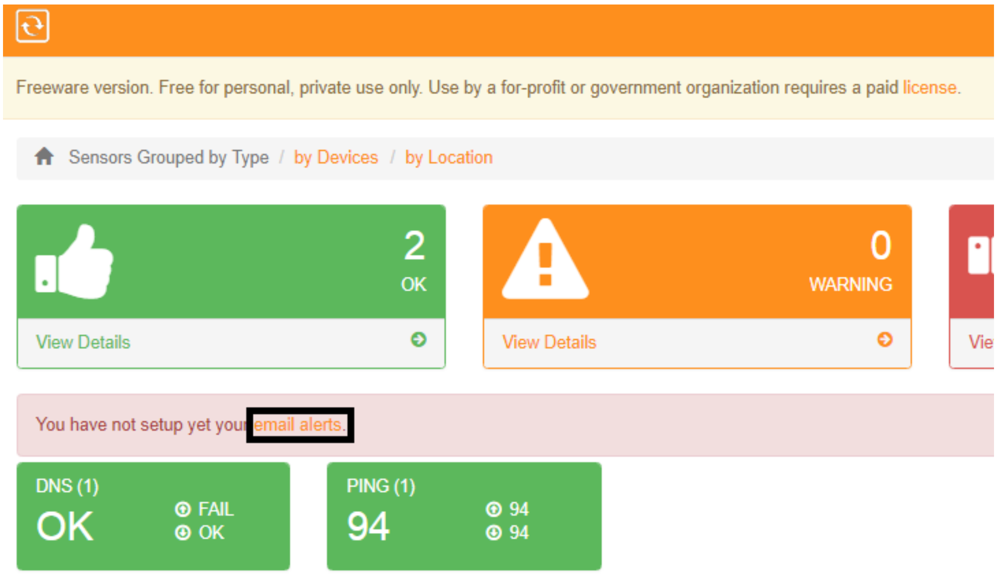
2.4. Setting up Email Alerts

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:

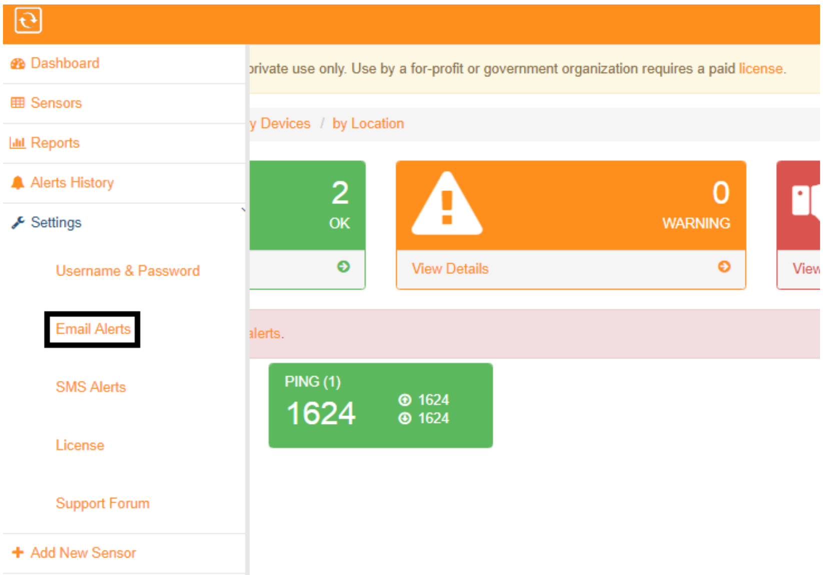
1. From the main Dashboard screen, click **Email Alerts** as shown in the image below.



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

You have not setup yet your email alerts.

2. Or access Menu - Settings - Email Alerts



rivate use only. Use by a for-profit or government organization requires a paid license.

lerts.

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

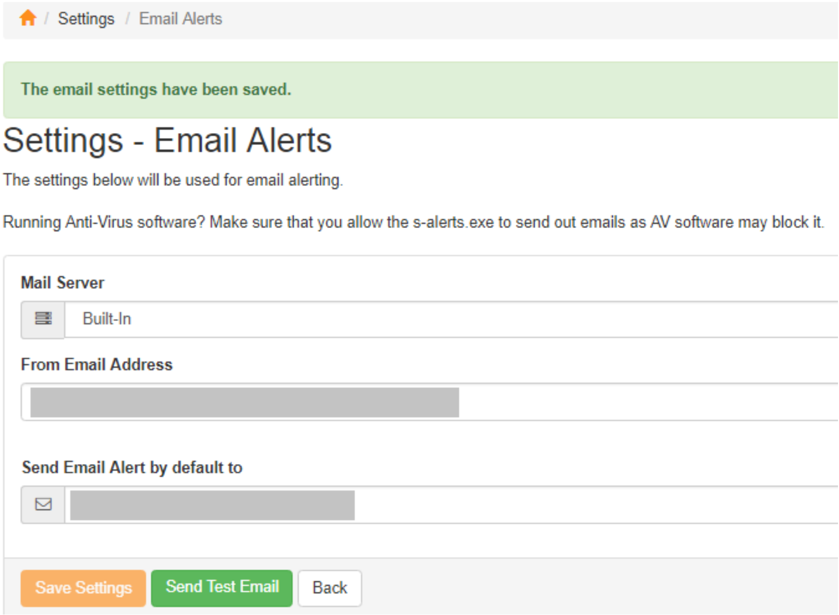
- IMAP Mail Server

- Gmail

2.4.1. Using The Built-In Mail Server

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

1. Select Built-In Mail Server.



The email settings have been saved.

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

[redacted]

Send Email Alert by default to

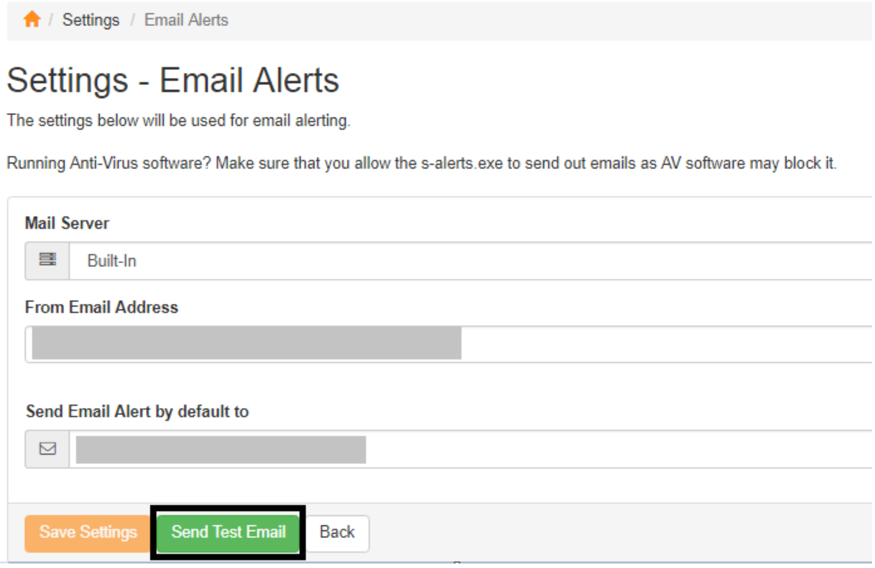
[redacted]

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.



Settings / Email Alerts

Settings - Email Alerts

The settings below will be used for email alerting.

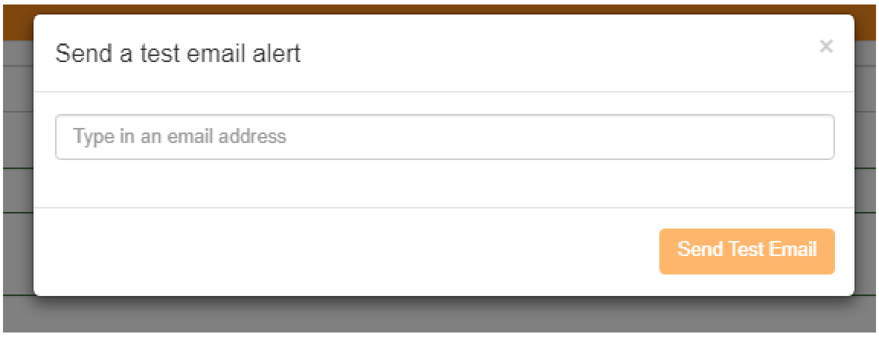
Running Anti-Virus software? Make sure that you allow the s-alerts.exe to send out emails as AV software may block it.

Mail Server: Built-In

From Email Address: [redacted]

Send Email Alert by default to: [redacted]

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



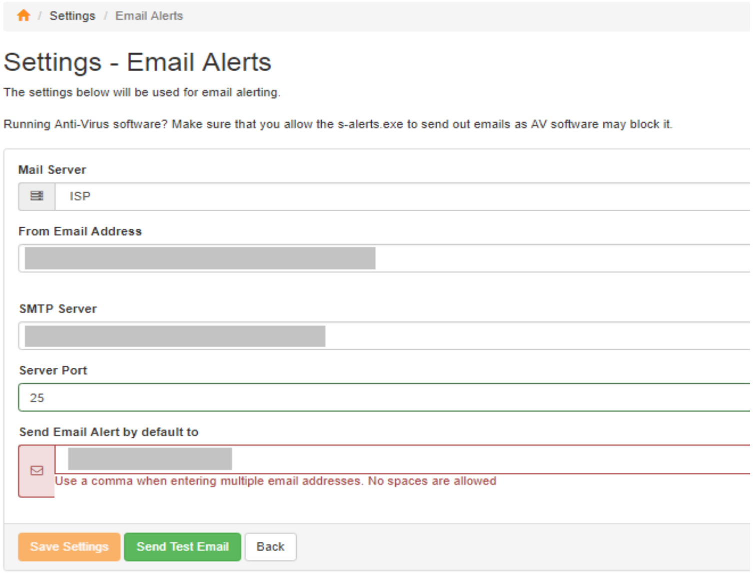
Send a test email alert

Type in an email address

2.4.2. 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.



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: ISP

From Email Address: [redacted]

SMTP Server: [redacted]

Server Port: 25

Send Email Alert by default to: [redacted]

Use a comma when entering multiple email addresses. No spaces are allowed

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.

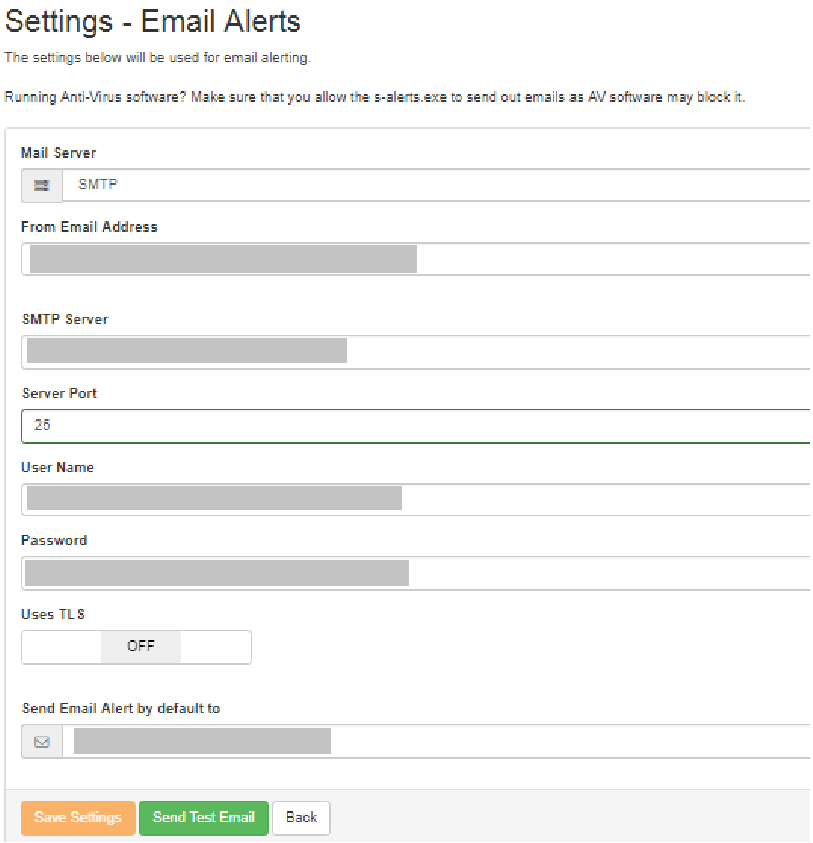
Send Email Alert by default to - Email address to where the email will be sent.

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

2.4.3 Using SMTP Server

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

1. Select SMTP 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.

Mail Server: SMTP

From Email Address: [redacted]

SMTP Server: [redacted]

Server Port: 25

User Name: [redacted]

Password: [redacted]

Uses TLS: OFF

Send Email Alert by default to: [redacted]

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.

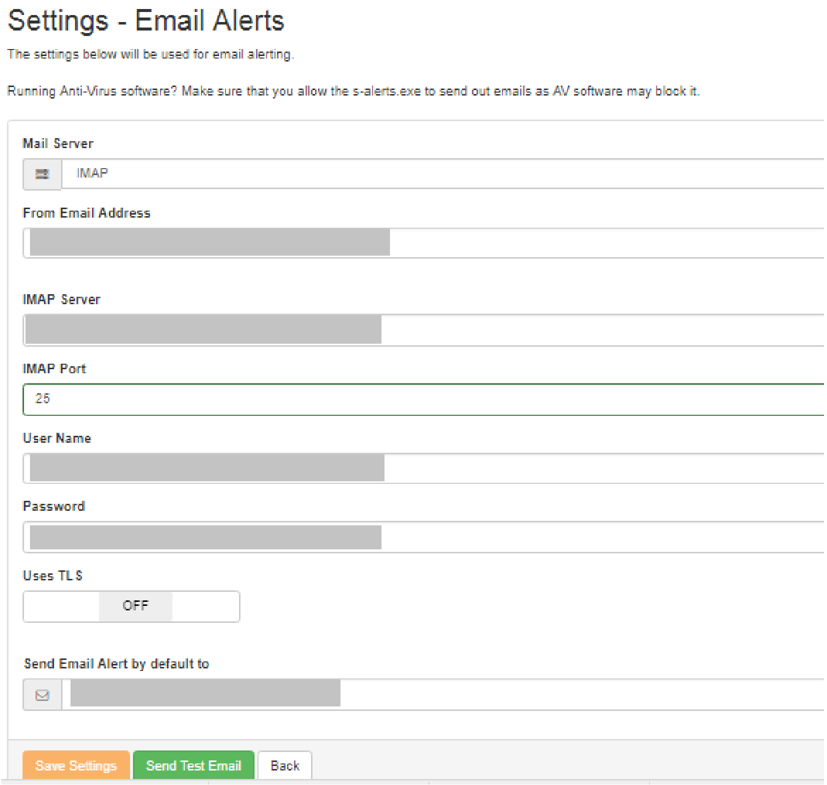
Send Email Alert by default to - Email address to where the email will be sent.

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

2.4.4 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.

Mail Server: IMAP

From Email Address: [redacted]

IMAP Server: [redacted]

IMAP Port: 25

User Name: [redacted]

Password: [redacted]

Uses TLS: OFF

Send Email Alert by default to: [redacted]

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.

2.4.5 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.

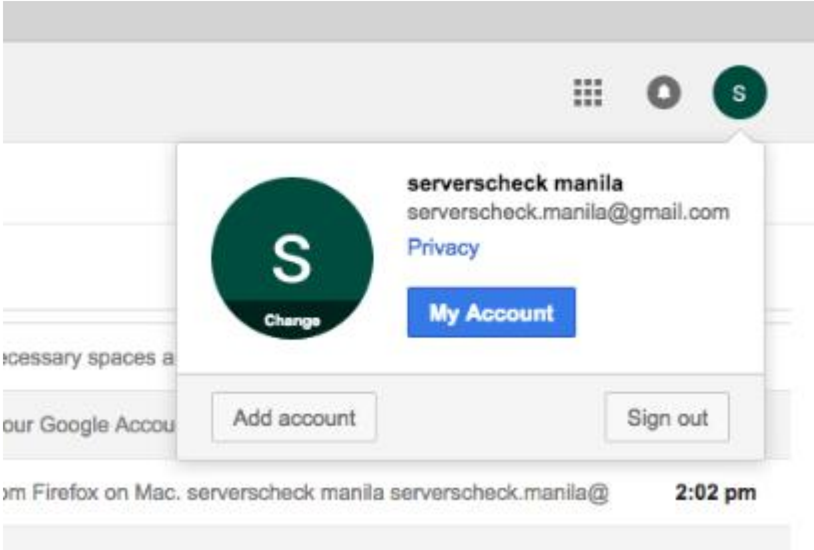
THINGS TO SET UP FOR GMAIL

*** Allowing Less Secured Apps**

Also make sure that your Gmail account is set to ON for **"allow less secured apps"**.

Below are the instructions on how to set it up.

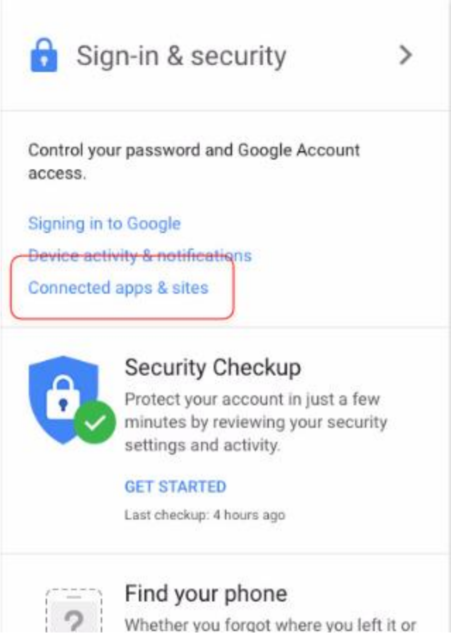
1. Log in to your Gmail Account and access **"My Account"**.



serverscheck manila
serverscheck.manila@gmail.com

cessary spaces a
our Google Accou
m Firefox on Mac. serverscheck manila serverscheck.manila@ 2:02 pm

2. Under Sign-In Security, click on **"Connected Apps & Sites"**.



Sign-in & security

Control your password and Google Account access.

Security Checkup

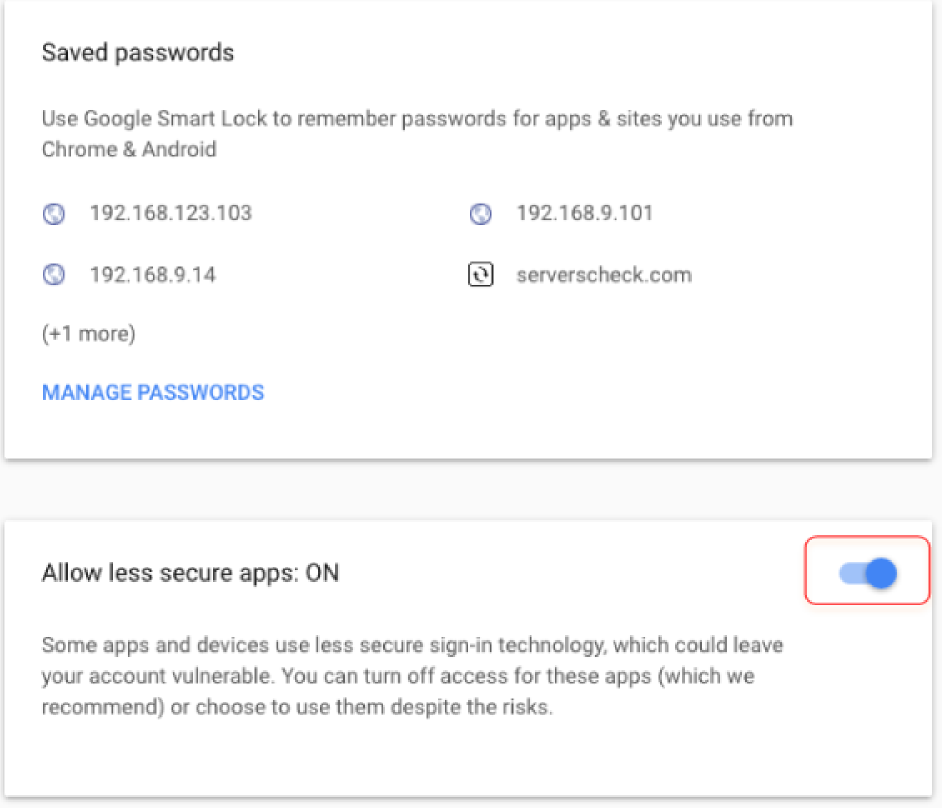
Protect your account in just a few minutes by reviewing your security settings and activity.

Last checkup: 4 hours ago

Find your phone

Whether you forgot where you left it or

3. Next page will allow you to activate **"allow less secure apps"**.



Saved passwords

Use Google Smart Lock to remember passwords for apps & sites you use from Chrome & Android

192.168.123.103

192.168.9.101

192.168.9.14

serverscheck.com

(+1 more)

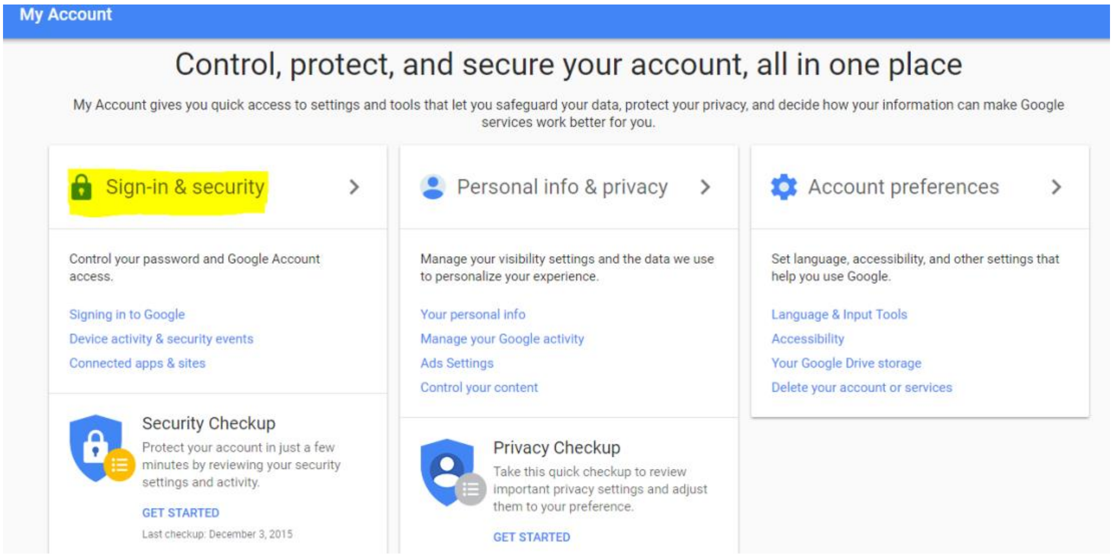
MANAGE PASSWORDS

Allow less secure apps: ON

Some apps and devices use less secure sign-in technology, which could leave your account vulnerable. You can turn off access for these apps (which we recommend) or choose to use them despite the risks.

*** How to turn off 2-factor authentication on your Gmail Account**

1. Log in to your Gmail account (https://mail.google.com)
2. Access (https://myaccount.google.com/)
3. Click Sign in & Security.



My Account

Control, protect, and secure your account, all in one place

My Account gives you quick access to settings and tools that let you safeguard your data, protect your privacy, and decide how your information can make Google services work better for you.

Sign-in & security

Control your password and Google Account access.

Signing in to Google
Device activity & security events
Connected apps & sites

Security Checkup

Protect your account in just a few minutes by reviewing your security settings and activity.

GET STARTED

Last checkup: December 3, 2015

Personal info & privacy

Manage your visibility settings and the data we use to personalize your experience.

Your personal info
Manage your Google activity
Ads Settings
Control your content

Privacy Checkup

Take this quick checkup to review important privacy settings and adjust them to your preference.

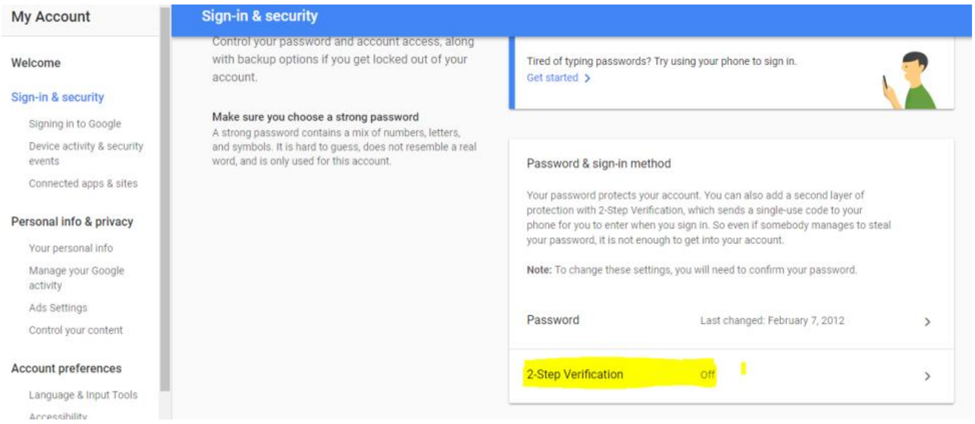
GET STARTED

Account preferences

Set language, accessibility, and other settings that help you use Google.

Language & Input Tools
Accessibility
Your Google Drive storage
Delete your account or services

4. Scroll down below under Password and Sign-in Method. See 2-step verification and make sure it is turned off.



Sign-in & security

Control your password and account access, along with backup options if you get locked out of your account.

Make sure you choose a strong password
A strong password contains a mix of numbers, letters, and symbols. It is hard to guess, does not resemble a real word, and is only used for this account.

Tired of typing passwords? Try using your phone to sign in.

Password & sign-in method

Your password protects your account. You can also add a second layer of protection with 2-Step Verification, which sends a single-use code to your phone for you to enter when you sign in. So even if somebody manages to steal your password, it is not enough to get into your account.

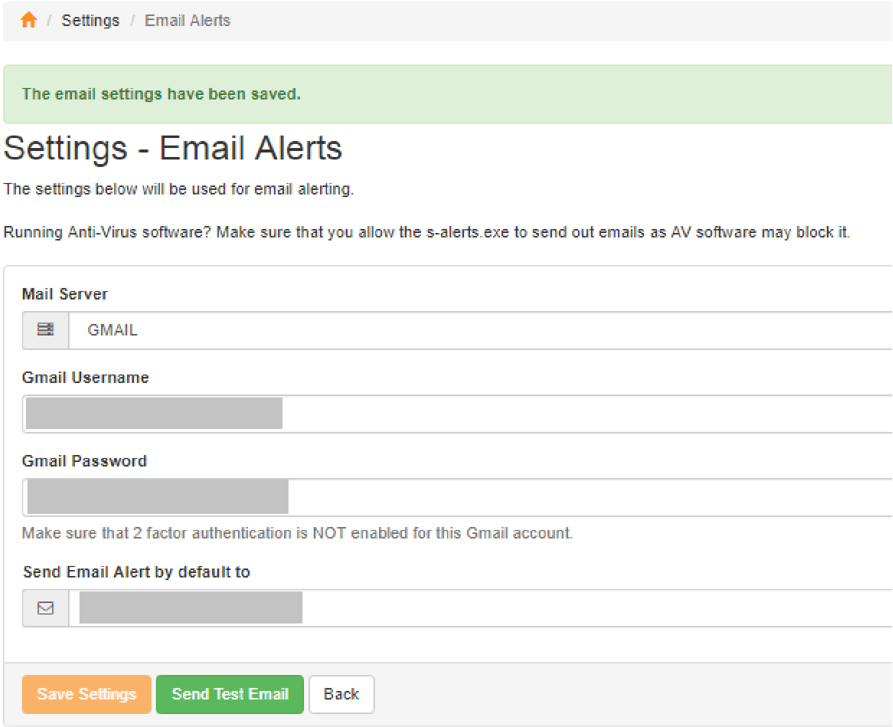
Note: To change these settings, you will need to confirm your password.

Password Last changed: February 7, 2012 >

2-Step Verification Off >

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

1. Select **GMAIL**.



The email settings have been saved.

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
GMAIL

Gmail Username
[redacted]

Gmail Password
[redacted]
Make sure that 2 factor authentication is NOT enabled for this Gmail account.

Send Email Alert by default to
[redacted]

Gmail Username - Username of your Gmail Account

Gmail Password - Password of your Gmail Account.

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.

2.5. Configuring SMS

Serverscheck Monitoring Appliance and Software can send SMS Alerts on 2 different options:

- optional USB GSM Modem Hardware (most USB modems that are vendor supported should be supported)

- Serverscheck Premium Alerts (https://premium.serverscheck.com/plans.asp?plan=alerts) - to be purchased with options of 100 credits or 500 credits.

2.5.1. Using an Optional USB GSM Modem Hardware

The software has been tested to work with USB GSM Modems manufactured by Huawei. Other modems may work.

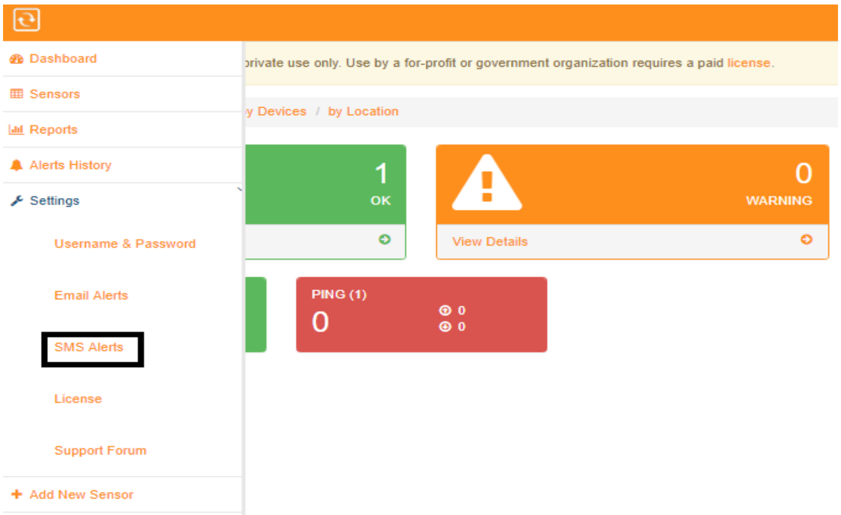
Note: AT&T and T-Mobile are recommended as a mobile operator in the US.

You may need to purchase a USB GSM Modem hardware first from your local Reseller or Distributor.

We have used Huawei GSM device here as an example.

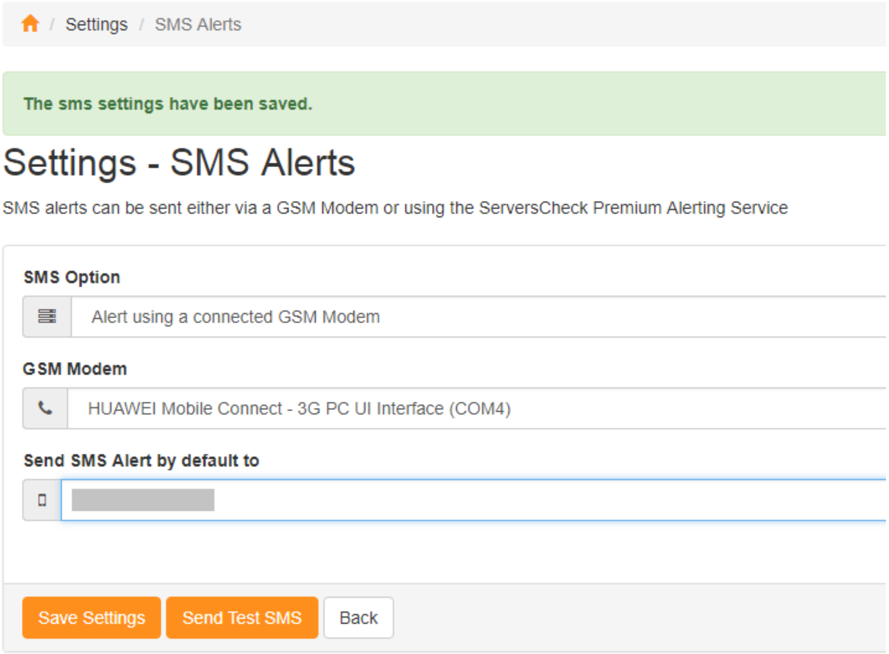
1. You need to install the USB GSM device first in your computer or on the Monitoring Appliance. For setup instructions, you can access it on https://www.manualslib.com/manual/851444/Huawei-E3276-4g-Lte.html#manual

2. Click Menu and go to Settings - SMS Alerts.



rivate use only. Use by a for-profit or government organization requires a paid license.

3. Select Alert using a connected GSM Modem.



The sms settings have been saved.

Settings - SMS Alerts

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

SMS Option: Alert using a connected GSM Modem

GSM Modem: HUAWEI Mobile Connect - 3G PC UI Interface (COM4)

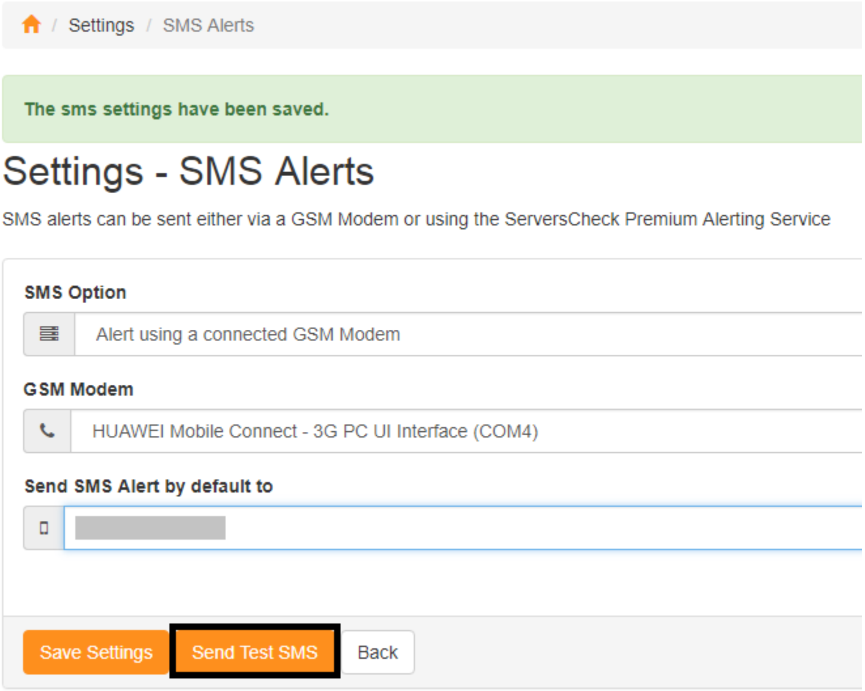
Send SMS Alert by default to: [redacted]

GSM Modem - Select the COM port of the GSM device.

Send SMS Alert by Default to - Phone number to where the SMS will be sent.

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

4. Send Test SMS.



The sms settings have been saved.

Settings - SMS Alerts

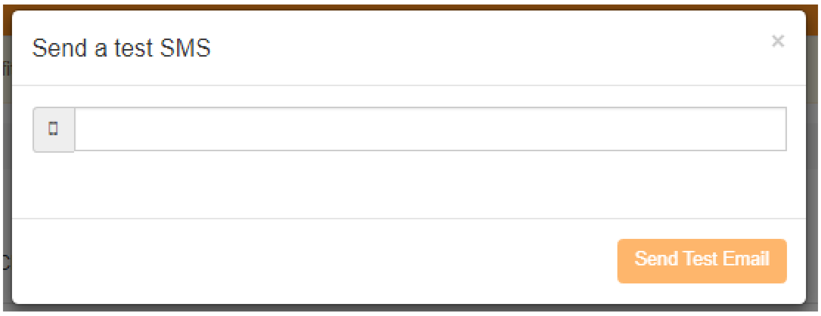
SMS alerts can be sent either via a GSM Modem or using the ServersCheck Premium Alerting Service

SMS Option: Alert using a connected GSM Modem

GSM Modem: HUAWEI Mobile Connect - 3G PC UI Interface (COM4)

Send SMS Alert by default to: [redacted]

Type in a phone number to which you want to send the test SMS.

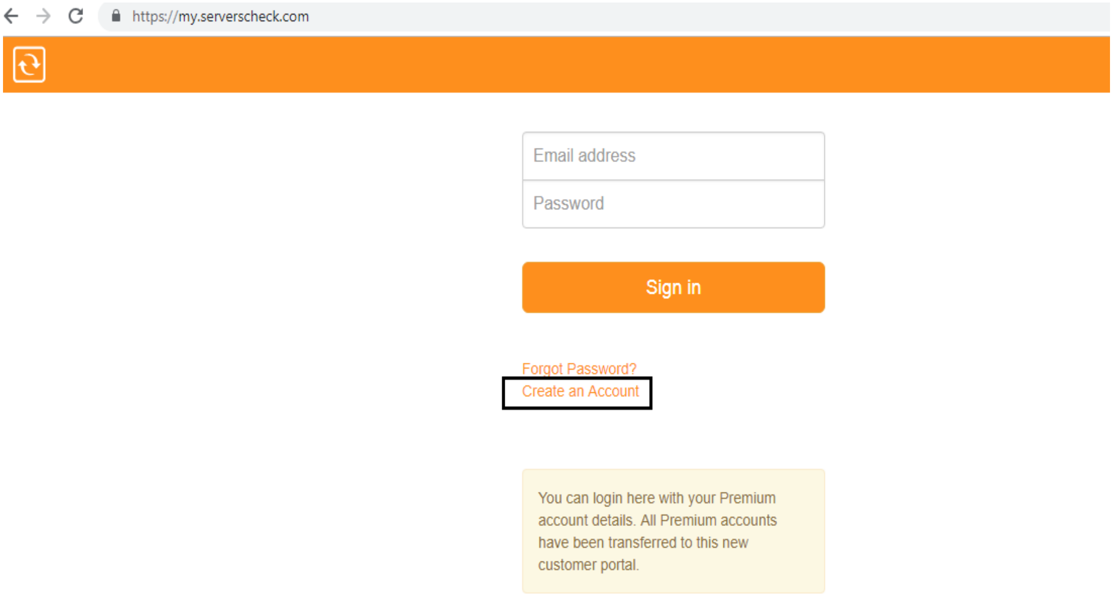


2.5.2. Using Serverscheck Premium Alerts (SMS & Voice Call Alerts)

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 my.serverscheck.com https://my.serverscheck.com/ with options of 100 or 500 credits.

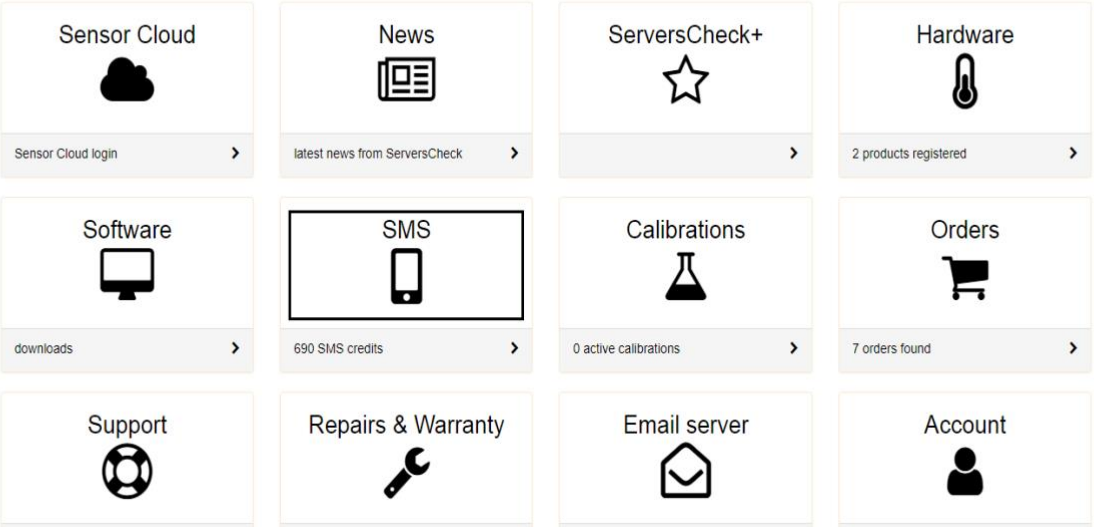
Here is also an instructional video on how our Premium Credits work.
https://serverscheck.com/video/?item=SMS

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.serverscheck.com/.

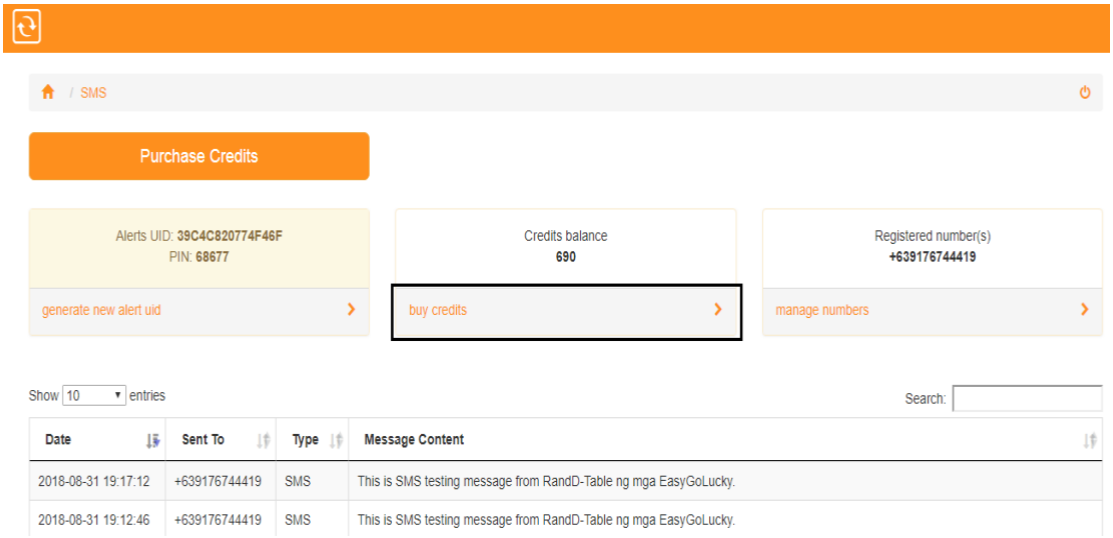


You can login here with your Premium account details. All Premium accounts have been transferred to this new customer portal.

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



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



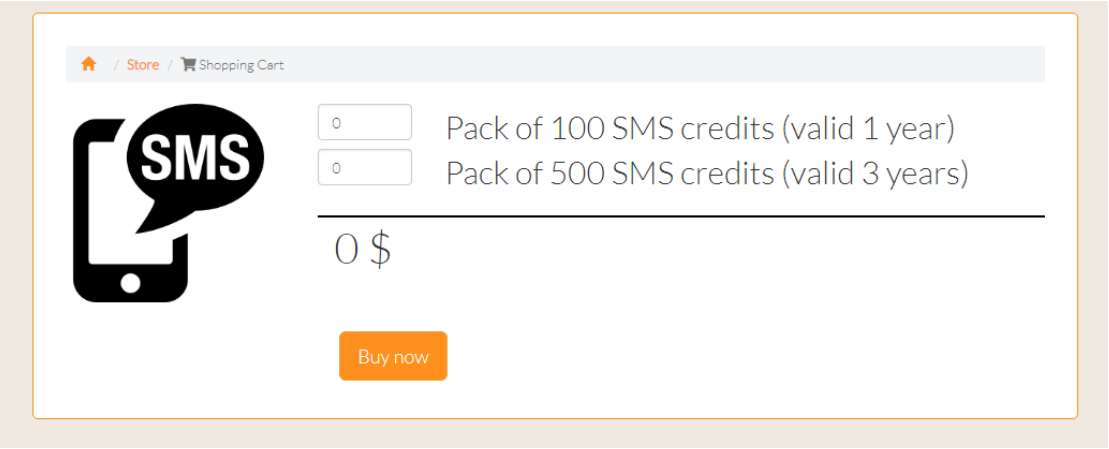
Alerts UID: **39C4C820774F46F**
PIN: **68677**

Credits balance
690

Registered number(s)
+639176744419

Date	Sent To	Type	Message Content
2018-08-31 19:17:12	+639176744419	SMS	This is SMS testing message from RandD-Table ng mga EasyGoLucky.
2018-08-31 19:12:46	+639176744419	SMS	This is SMS testing message from RandD-Table ng mga EasyGoLucky.

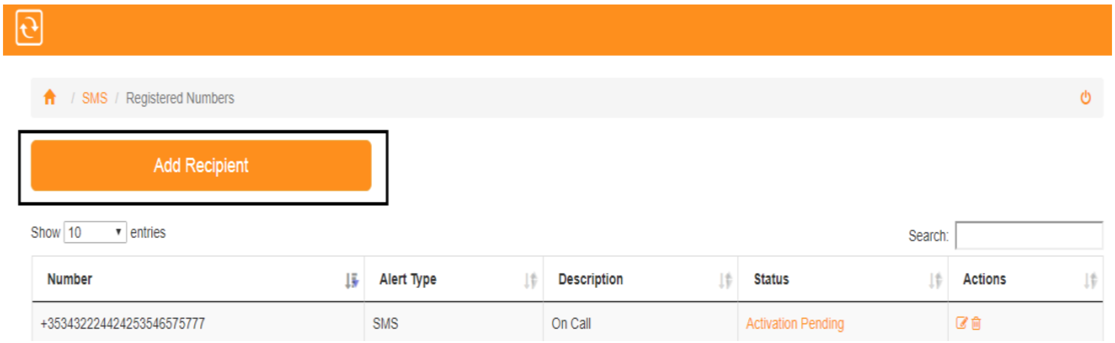
4. You can purchase option of 100 credits (valid for 1 year) or 500 credits (valid for 3 years). 1 credit per SMS, 3 credits per voice call.



0 Pack of 100 SMS credits (valid 1 year)
0 Pack of 500 SMS credits (valid 3 years)

0 $

5. Once you now have available credits, go to **Manage Numbers** to **Add Recipient**.

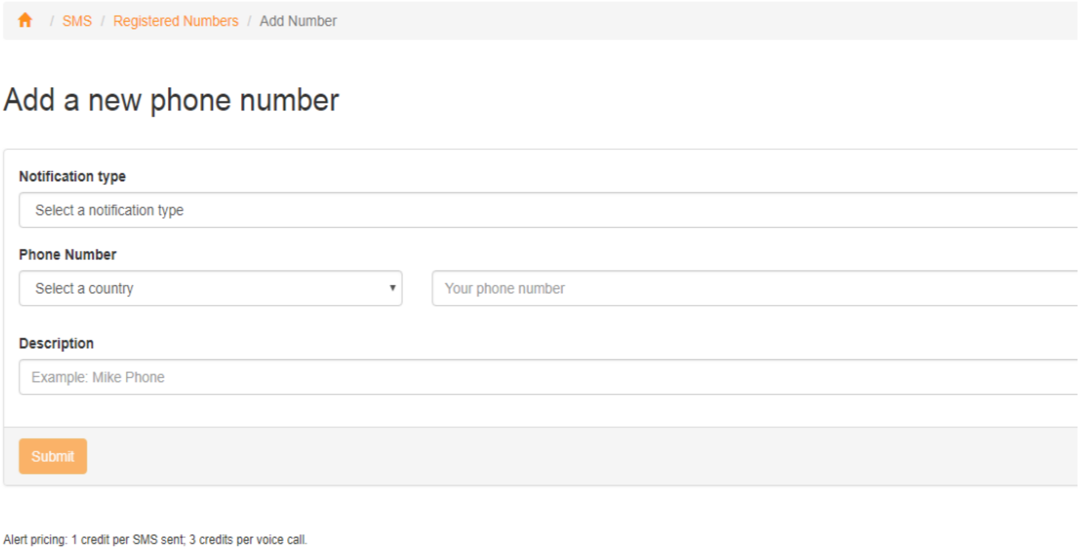


Number	Alert Type	Description	Status	Actions
+353432224424253546575777	SMS	On Call	Activation Pending	✎ 🗑

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

You may choose from the list of options:

- SMS only
- Voice only
- SMS + Voice



Add a new phone number

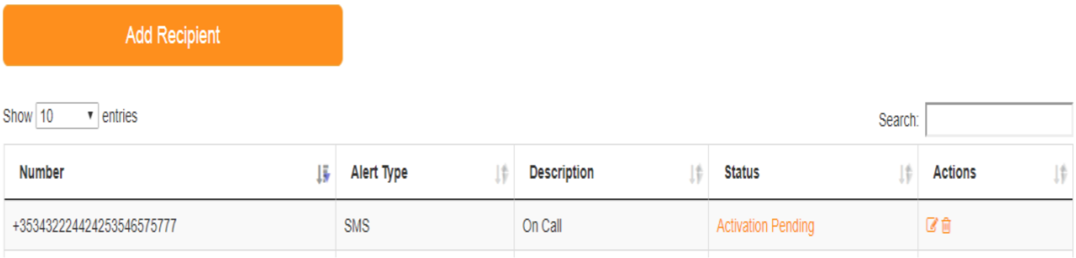
Notification type: Select a notification type

Phone Number: Select a country ▾ | Your phone number

Description: Example: Mike Phone

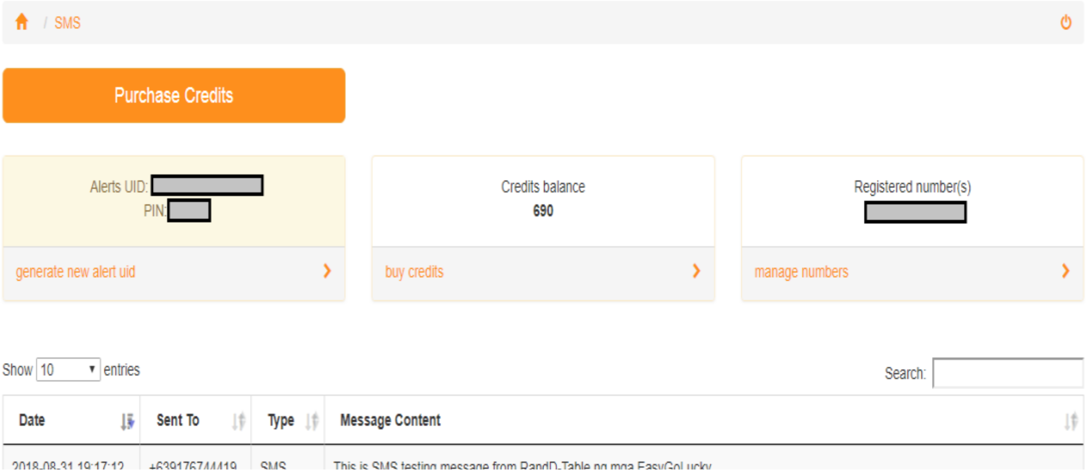
Alert pricing: 1 credit per SMS sent; 3 credits per voice call.

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.



Number	Alert Type	Description	Status	Actions
+353432224424253546575777	SMS	On Call	Activation Pending	✎ 🗑

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



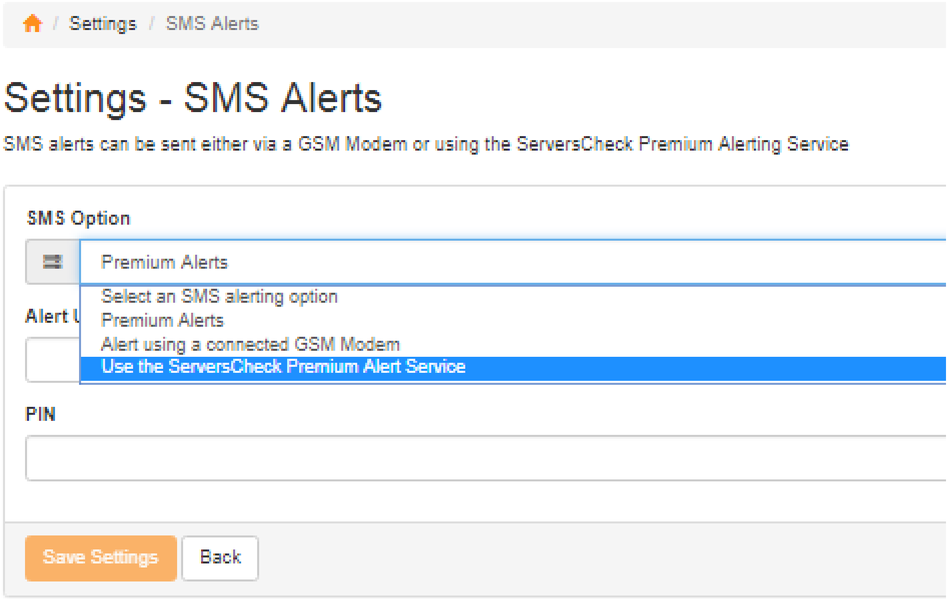
Alerts UID: [redacted]
PIN: [redacted]

Credits balance
690

Registered number(s)
[redacted]

Date	Sent To	Type	Message Content
2018-08-31 19:17:12	+639176744419	SMS	This is SMS testing message from RandD-Table ng mga EasyGoLucky

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



Settings - SMS Alerts

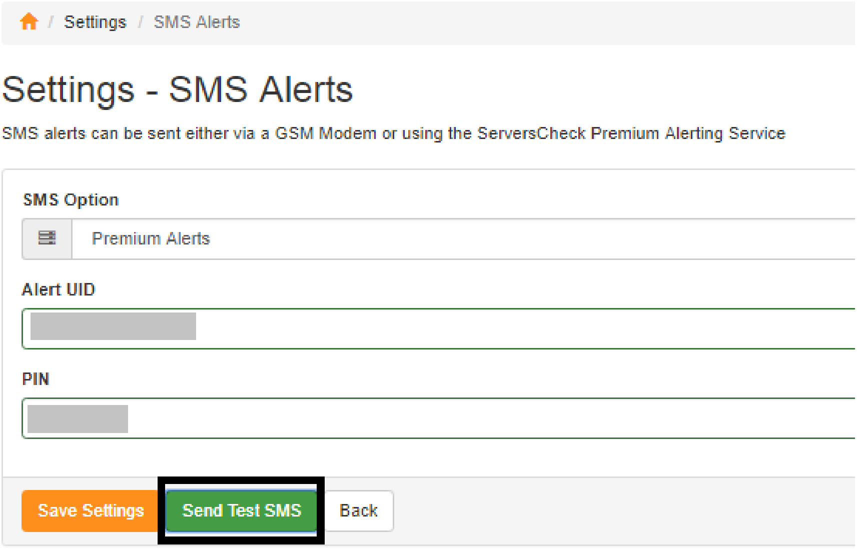
SMS alerts can be sent either via a GSM Modem or using the ServersCheck Premium Alerting Service

SMS Option: Premium Alerts

Select an SMS alerting option
Premium Alerts
Alert using a connected GSM Modem
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

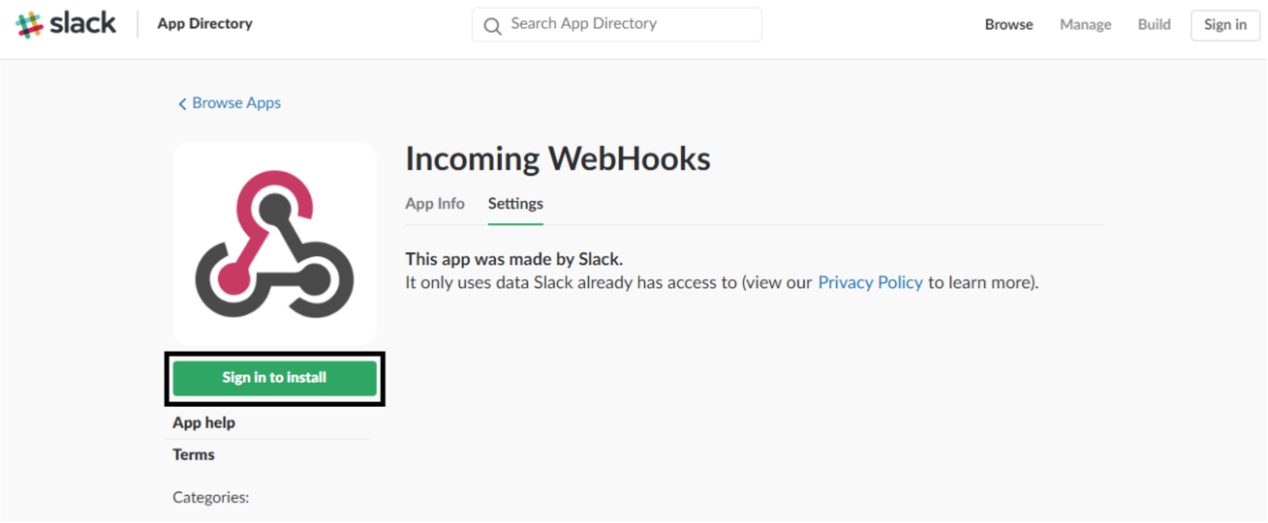
Alert UID: [redacted]

PIN: [redacted]

2.6. Setting Slack Alerts

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

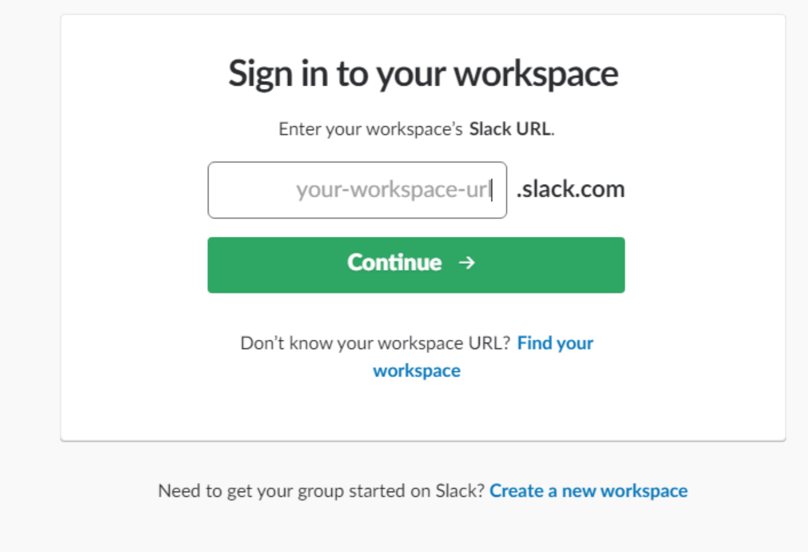
1. Go to the Slack Incoming Webhooks App and Click Sign in to Install.
   You will be redirected to
   https://slack.com/apps/A0F7XDUAZ-incoming-webhooks?page=1



Incoming WebHooks

This app was made by Slack.
It only uses data Slack already has access to (view our Privacy Policy to learn more).

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.



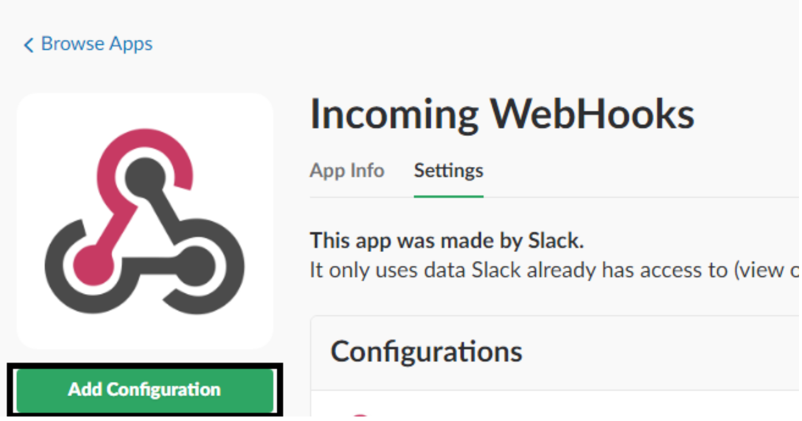
Sign in to your workspace

Enter your workspace's **Slack URL**.

Don't know your workspace URL? **Find your workspace**

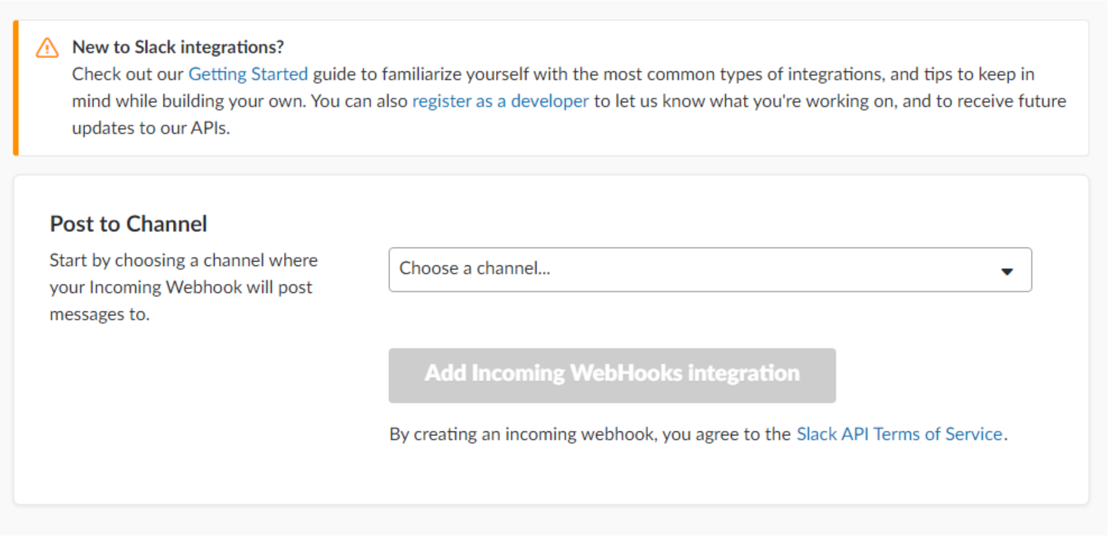
Need to get your group started on Slack? **Create a new workspace**

3. Click Add Configuration.



This app was made by Slack.
It only uses data Slack already has access to (view c

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



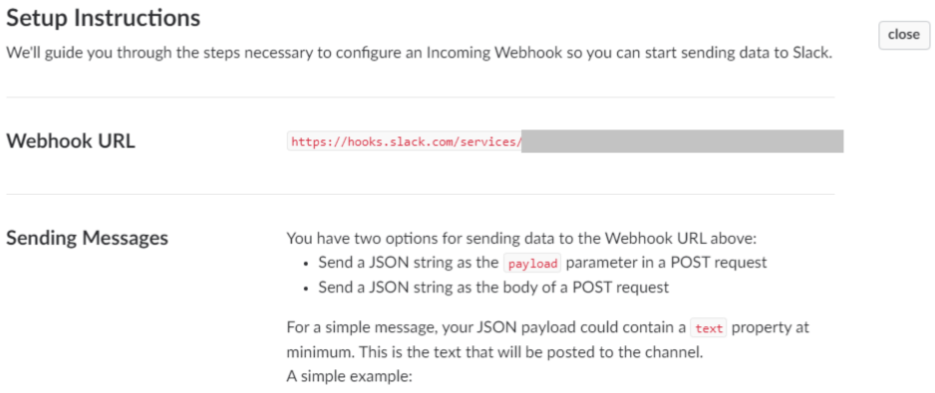
New to Slack integrations?
Check out our Getting Started guide to familiarize yourself with the most common types of integrations, and tips to keep in mind while building your own. You can also register as a developer to let us know what you're working on, and to receive future updates to our APIs.

Post to Channel

Start by choosing a channel where your Incoming Webhook will post messages to.

By creating an incoming webhook, you agree to the Slack API Terms of Service.

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



Setup Instructions

We'll guide you through the steps necessary to configure an Incoming Webhook so you can start sending data to Slack.

Webhook URL `https://hooks.slack.com/services/`[redacted]

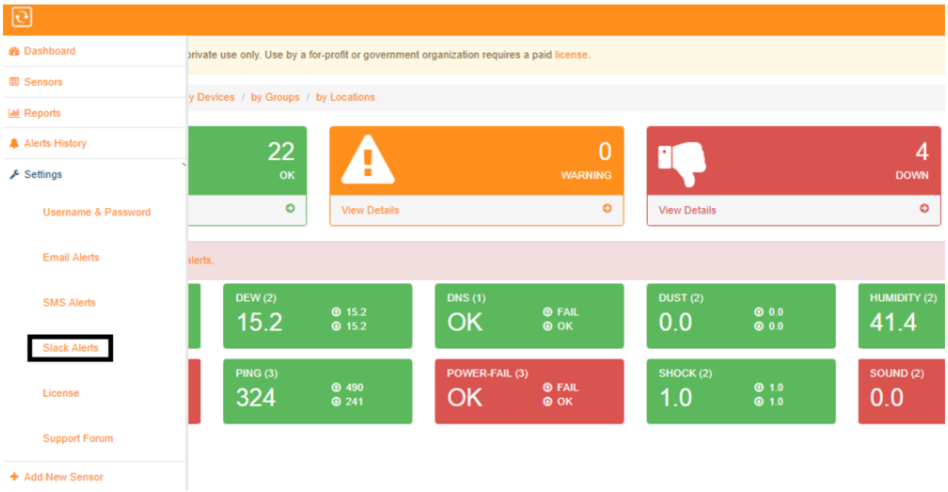
Sending Messages

You have two options for sending data to the Webhook URL above:

- Send a JSON string as the `payload` parameter in a POST request
- Send a JSON string as the body of a POST request

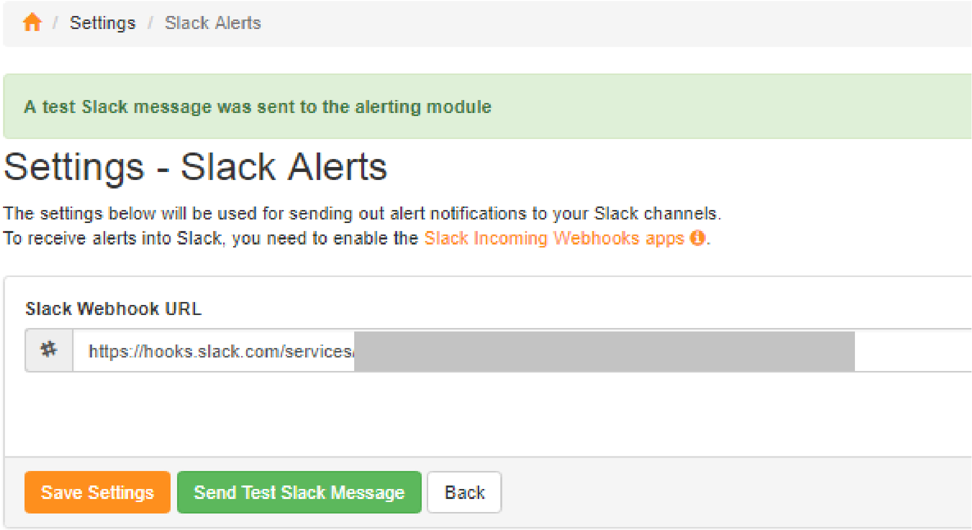
For a simple message, your JSON payload could contain a `text` property at minimum. This is the text that will be posted to the channel.
A simple example:

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



private use only. Use by a for-profit or government organization requires a paid license.

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



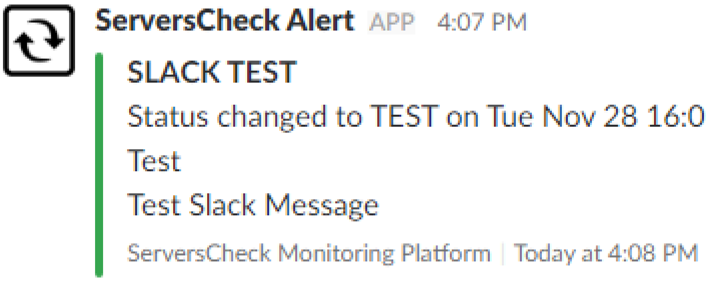
A test Slack message was sent to the alerting module

Settings - Slack Alerts

The settings below will be used for sending out alert notifications to your Slack channels.
To receive alerts into Slack, you need to enable the Slack Incoming Webhooks apps.

Slack Webhook URL: https://hooks.slack.com/services/[redacted]

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


ServersCheck Alert APP 4:07 PM

SLACK TEST

Status changed to TEST on Tue Nov 28 16:08:58 2017

Test

Test Slack Message

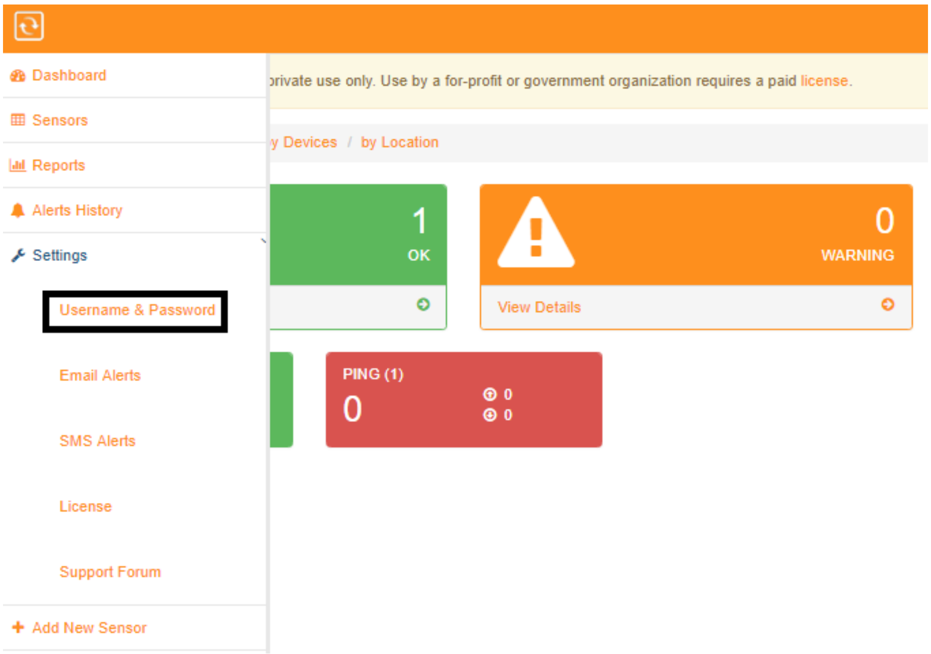
ServersCheck Monitoring Platform | Today at 4:08 PM

2.7. Setting up Username and Password

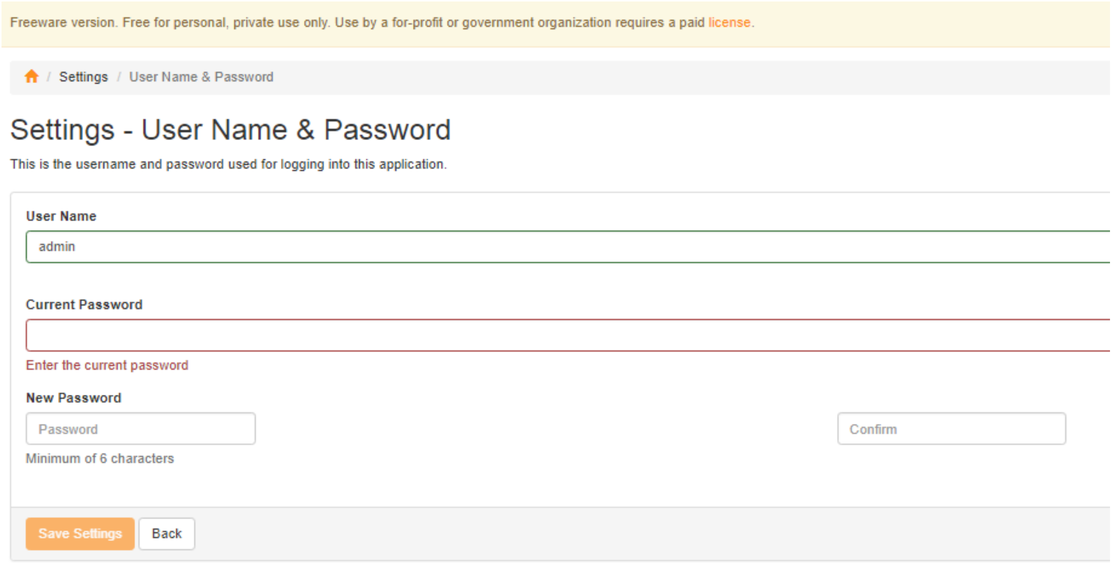
You need to setup a login Username and Password for the security of your Monitoring Software as it will be your credentials when you access the software on a separate computer.
Note: If accessing the software on a local host, it will not prompt for a Username and Password.

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

Default Username - admin
Default Password - admin


private use only. Use by a for-profit or government organization requires a paid license.

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

admin

Current Password

Enter the current password

New Password

Minimum of 6 characters

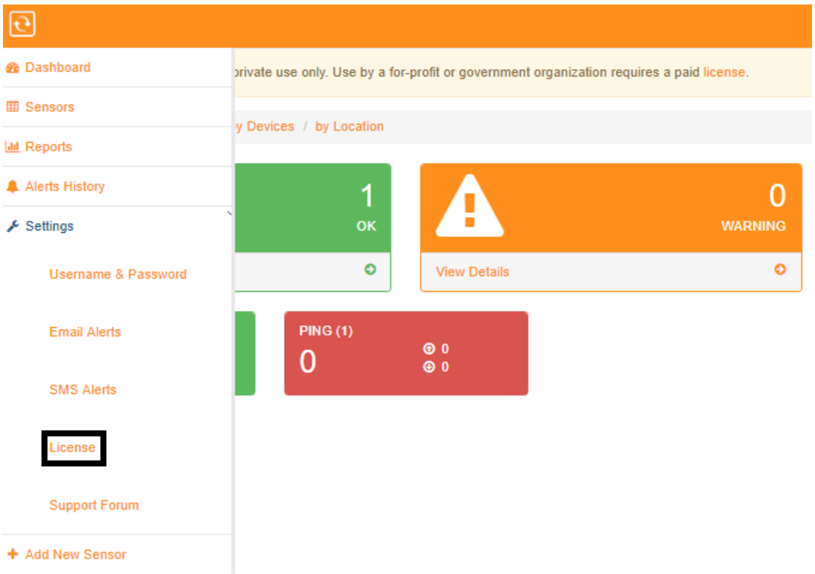
Username - use alphanumeric characters only

Password - minimum of 6 characters

2.8. 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.

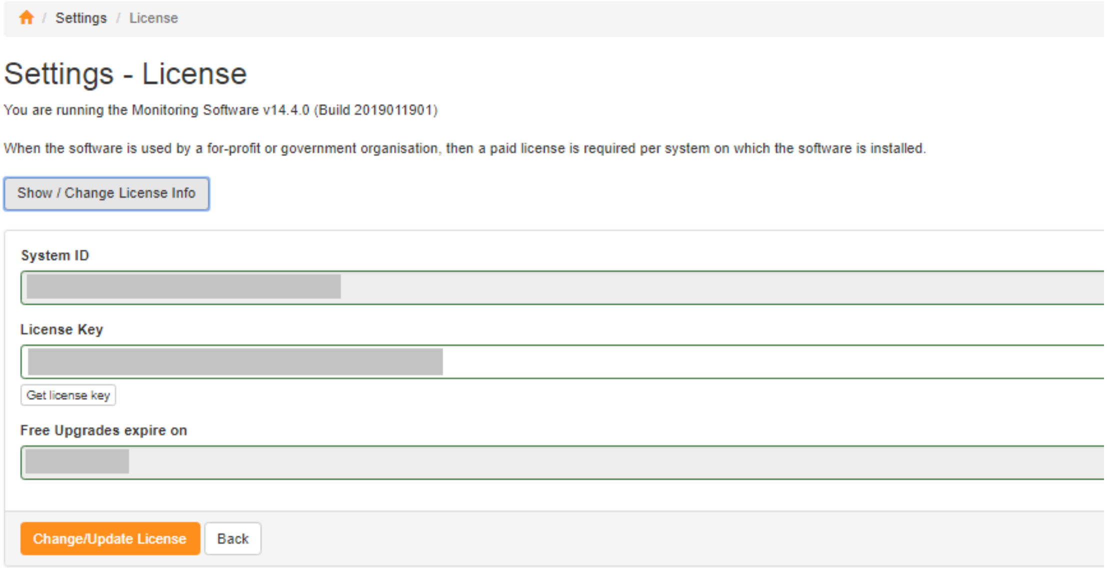
1. Once you have purchased the license, you may activate it by clicking the **Menu - Settings - License**.



rivate use only. Use by a for-profit or government organization requires a paid 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.



You are running the Monitoring Software v14.4.0 (Build 2019011901)

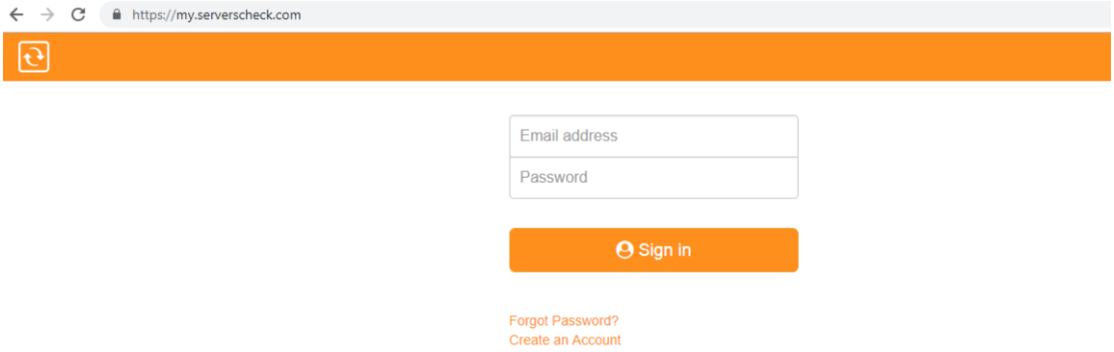
When the software is used by a for-profit or government organisation, then a paid license is required per system on which the software is installed.

System ID: [redacted]

License Key: [redacted]

Free Upgrades expire on: [redacted]

3. Clicking **Get License Key**, will redirect you to https://my.serverscheck.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.



https://my.serverscheck.com

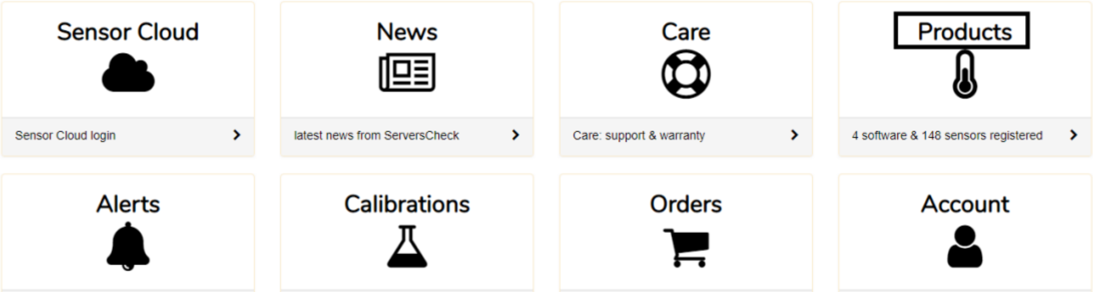
Email address

Password

Sign in

Forgot Password?
Create an Account

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



Sensor Cloud — Sensor Cloud login

News — latest news from ServersCheck

Care — Care: support & warranty

Products — 4 software & 148 sensors registered

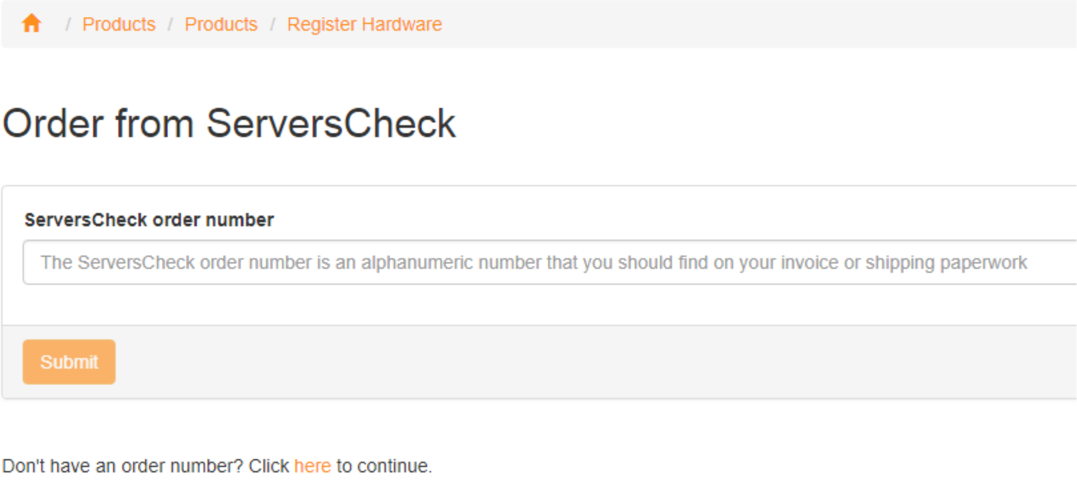
Alerts

Calibrations

Orders

Account

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



/ Products / Products / Register Hardware

Order from ServersCheck

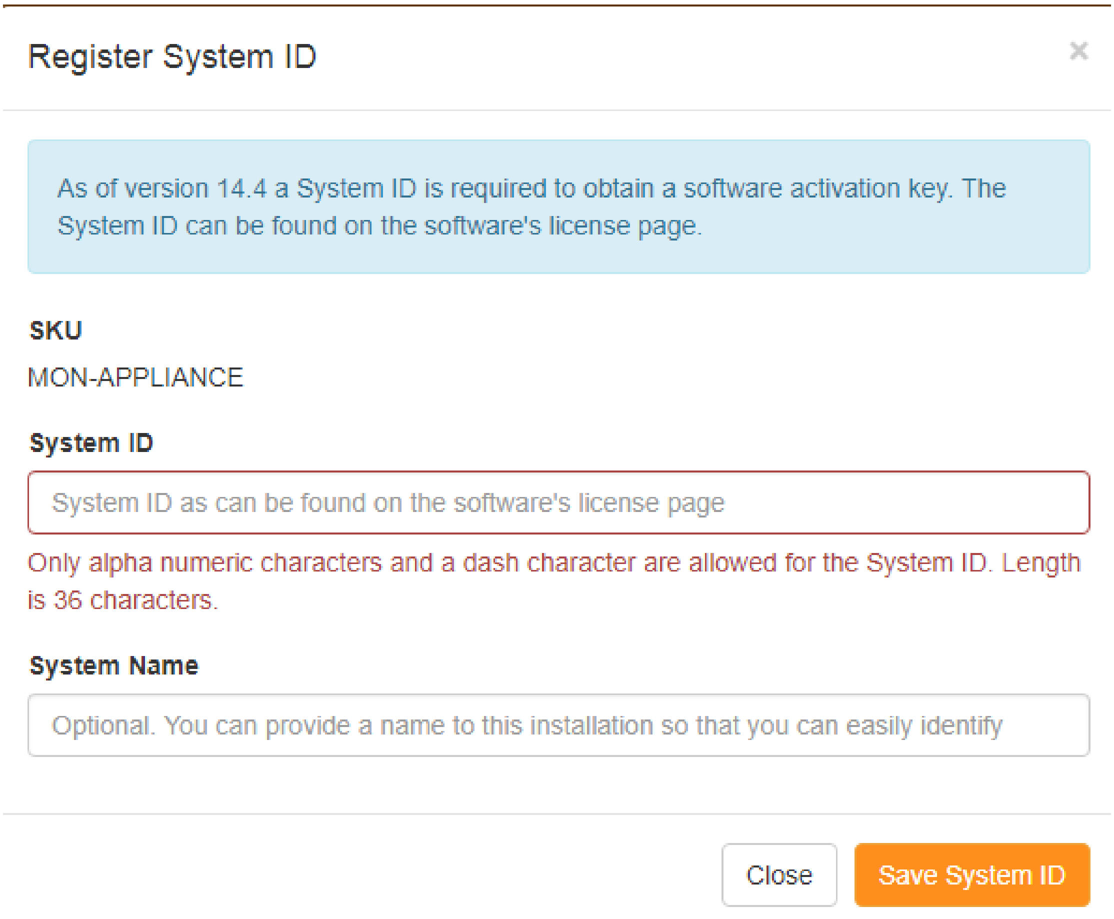
ServersCheck order number

The ServersCheck order number is an alphanumeric number that you should find on your invoice or shipping paperwork

Submit

Don't have an order number? Click here to continue.

6. After registering your Order, you need to Register your System ID to obtain an activation key. The System ID can be found 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

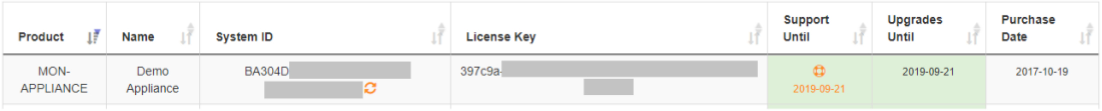
System ID as can be found on the software's license page

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

System Name

Optional. You can provide a name to this installation so that you can easily identify

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[redacted]	397c9a-[redacted]	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 SeversCheck 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.

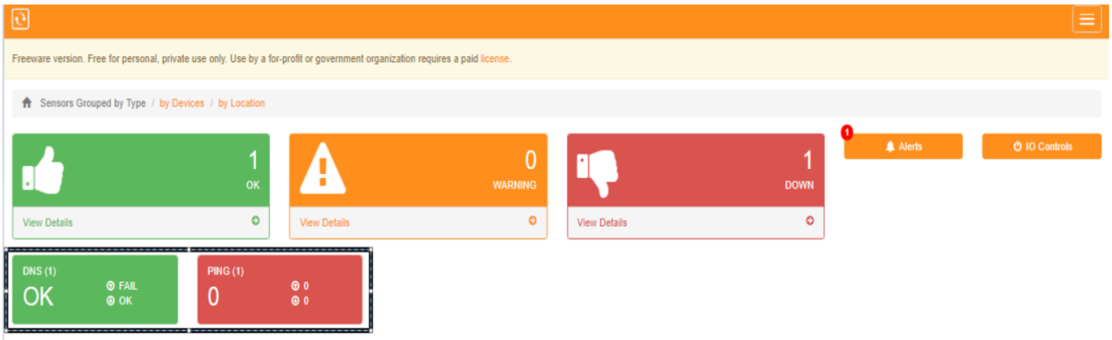
No responsibility is assumed by ServersCheck BVBA for the use or reliability of software.

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

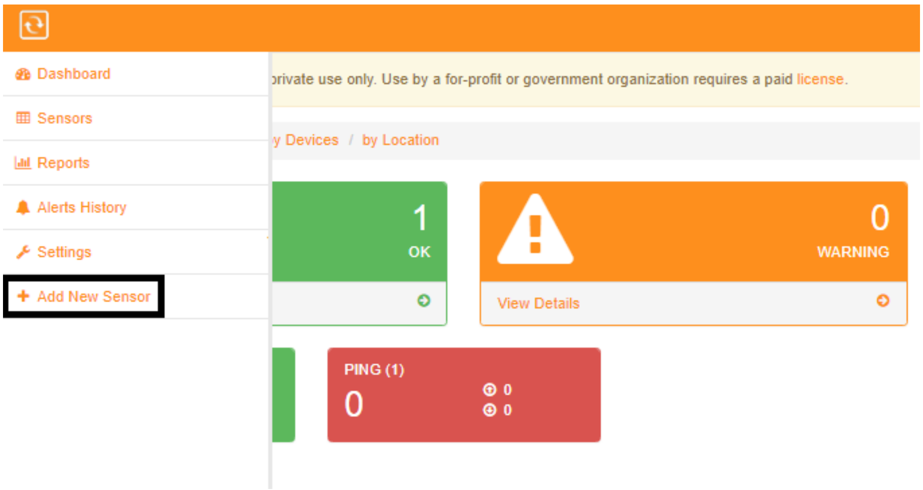
Upon installation of the software, it comes in with a default PING and DNS checks.



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

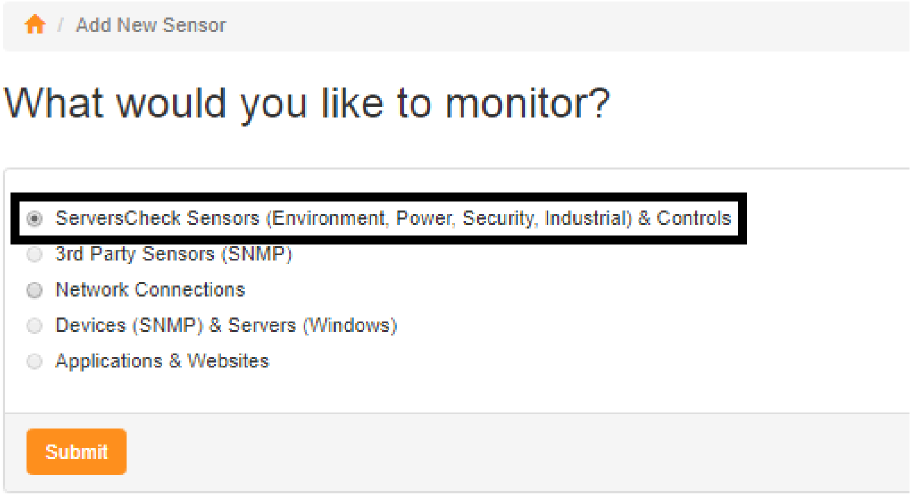
3.1. Adding Serverscheck Sensors (Environment, Power, Security, Industrial) & Controls

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



private use only. Use by a for-profit or government organization requires a paid license.

2. Select Serverscheck Sensors (Environment, Power, Security, Industrial) & Controls.

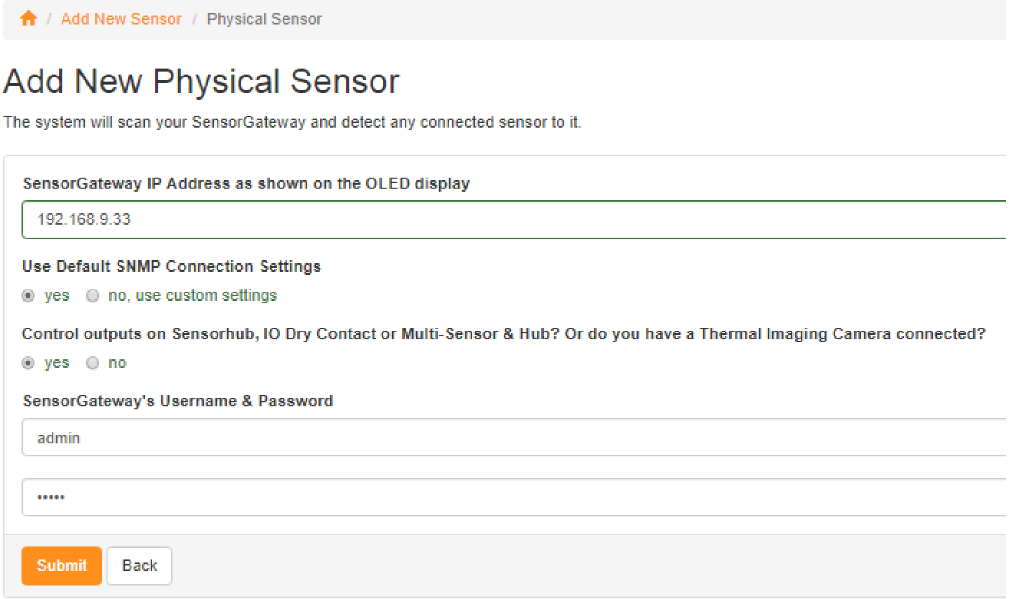


Add New Sensor

What would you like to monitor?

● ServersCheck Sensors (Environment, Power, Security, Industrial) & Controls
○ 3rd Party Sensors (SNMP)
○ Network Connections
○ Devices (SNMP) & Servers (Windows)
○ Applications & Websites

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



Add New Physical Sensor

The system will scan your SensorGateway and detect any connected sensor to it.

SensorGateway IP Address as shown on the OLED display: 192.168.9.33

Use Default SNMP Connection Settings: ● yes ○ no, use custom settings

Control outputs on Sensorhub, IO Dry Contact or Multi-Sensor & Hub? Or do you have a Thermal Imaging Camera connected? ● yes ○ no

SensorGateway's Username & Password: admin / •••••

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.

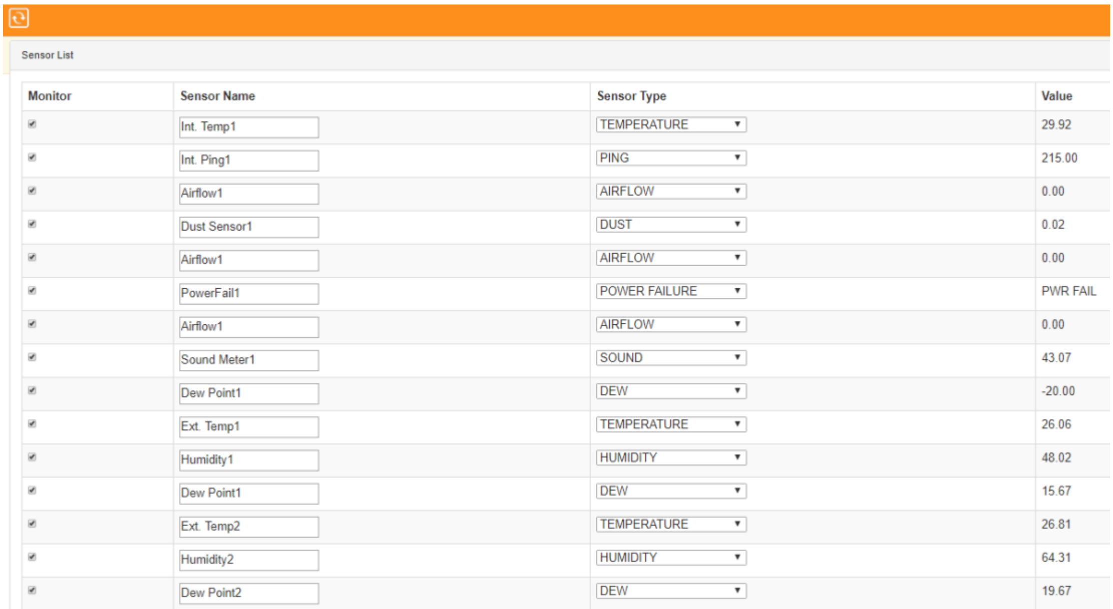
Sensorgateway's Username & Password

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.

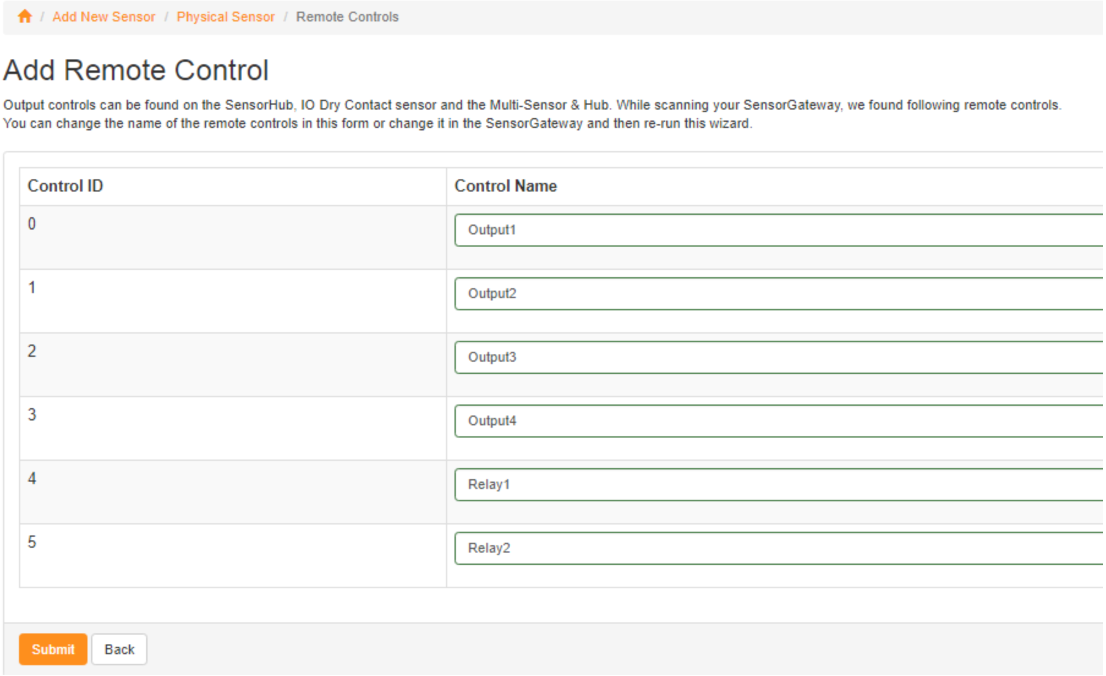
Note: If there are dry contacts connected, it will have to be monitored via SNMPTRAPS and will not shown on the list



Sensor List

Monitor	Sensor Name	Sensor Type	Value
☑	Int. Temp1	TEMPERATURE ▾	29.92
☑	Int. Ping1	PING ▾	215.00
☑	Airflow1	AIRFLOW ▾	0.00
☑	Dust Sensor1	DUST ▾	0.02
☑	Airflow1	AIRFLOW ▾	0.00
☑	PowerFail1	POWER FAILURE ▾	PWR FAIL
☑	Airflow1	AIRFLOW ▾	0.00
☑	Sound Meter1	SOUND ▾	43.07
☑	Dew Point1	DEW ▾	-20.00
☑	Ext. Temp1	TEMPERATURE ▾	26.06
☑	Humidity1	HUMIDITY ▾	48.02
☑	Dew Point1	DEW ▾	15.67
☑	Ext. Temp2	TEMPERATURE ▾	26.81
☑	Humidity2	HUMIDITY ▾	64.31
☑	Dew Point2	DEW ▾	19.67

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



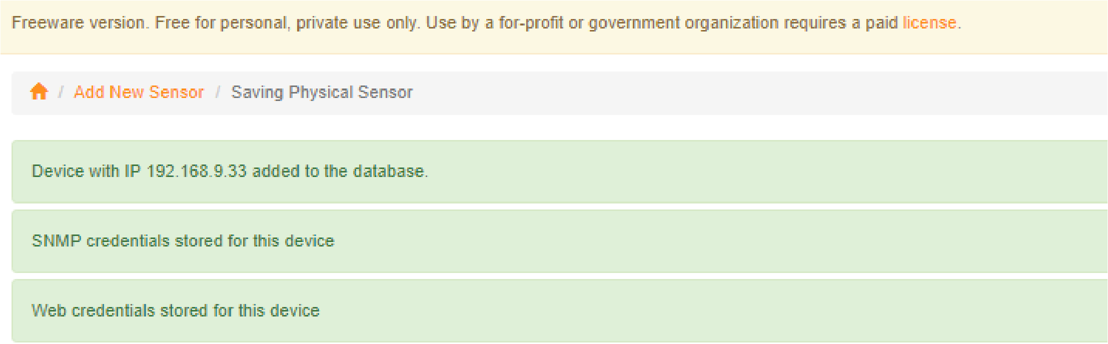
/ Add New Sensor / Physical Sensor / Remote Controls

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

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



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

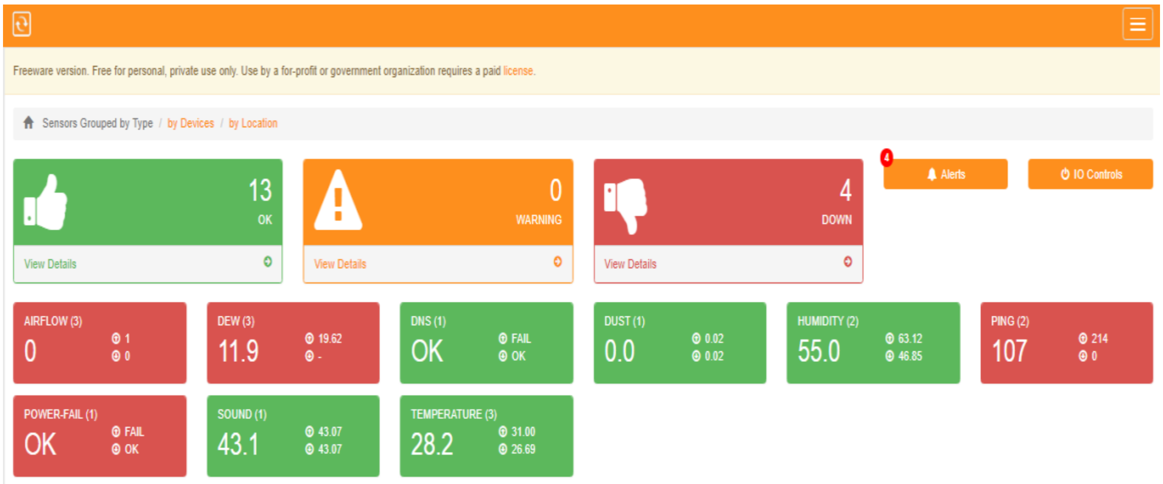
Add New Sensor / Saving Physical Sensor

Device with IP 192.168.9.33 added to the database.

SNMP credentials stored for this device

Web credentials stored for this device

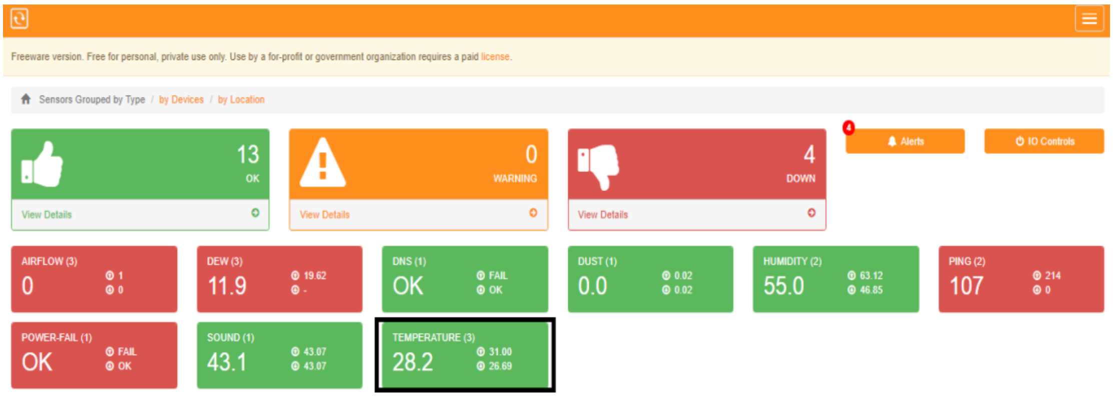
7. After adding up the device and the sensors, you should be able to see it on the Dashboard.



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

3.2. Editing a Sensor/Check

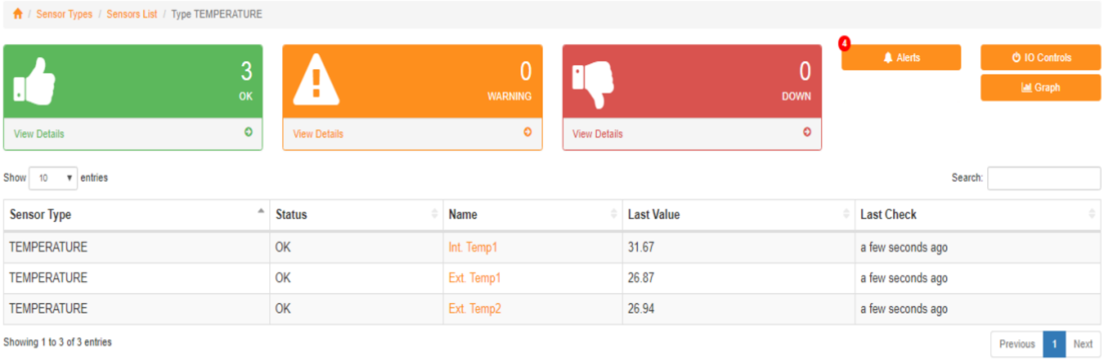
1. By default on the dashboard, all sensors are grouped by Type. Click an individual Sensor Type. In this example, we selected Temperature.



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

Sensors Grouped by Type / by Devices / by Location

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



Sensor Types / Sensors List / Type TEMPERATURE

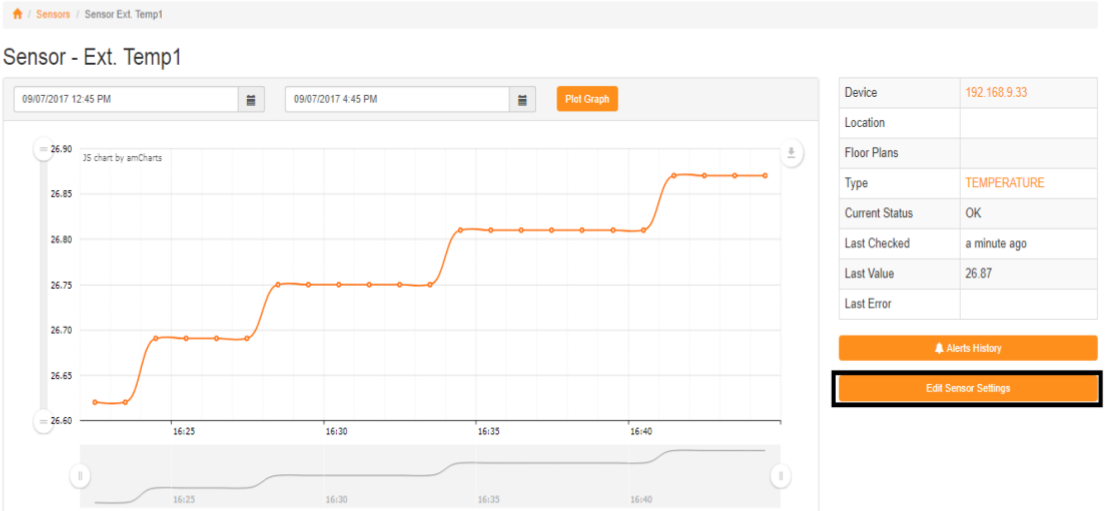
Show 10 entries

Search:

Sensor Type	Status	Name	Last Value	Last Check
TEMPERATURE	OK	Int. Temp1	31.67	a few seconds ago
TEMPERATURE	OK	Ext. Temp1	26.87	a few seconds ago
TEMPERATURE	OK	Ext. Temp2	26.94	a few seconds ago

Showing 1 to 3 of 3 entries

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.



Sensors / Sensor Ext. Temp1

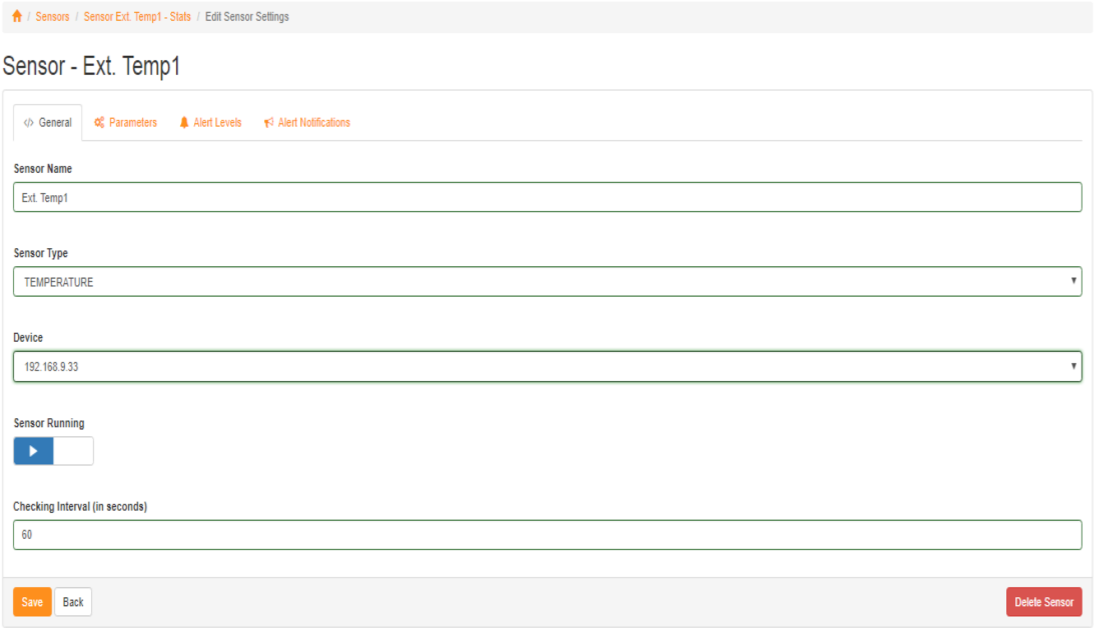
Sensor - Ext. Temp1

09/07/2017 12:45 PM

09/07/2017 4:45 PM

Device	192.168.9.33
Location	
Floor Plans	
Type	TEMPERATURE
Current Status	OK
Last Checked	a minute ago
Last Value	26.87
Last Error	

4. General Tab



Sensor - Ext. Temp1

Sensor Name: Ext. Temp1

Sensor Type: TEMPERATURE

Device: 192.168.9.33

Sensor Running

Checking Interval (in seconds): 60

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

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

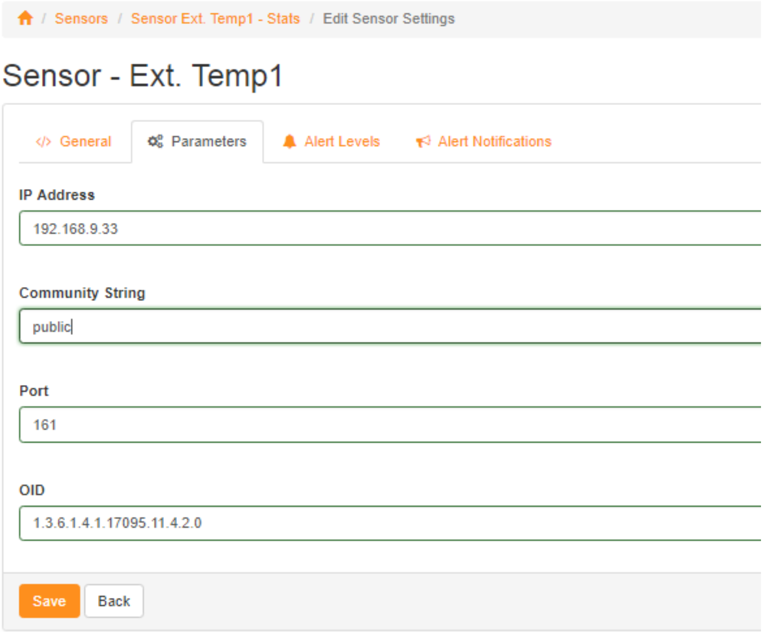
Device - List of individual devices to which that specific sensor will be grouped under.

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



Sensor - Ext. Temp1

IP Address: 192.168.9.33

Community String: public

Port: 161

OID: 1.3.6.1.4.1.17095.11.4.2.0

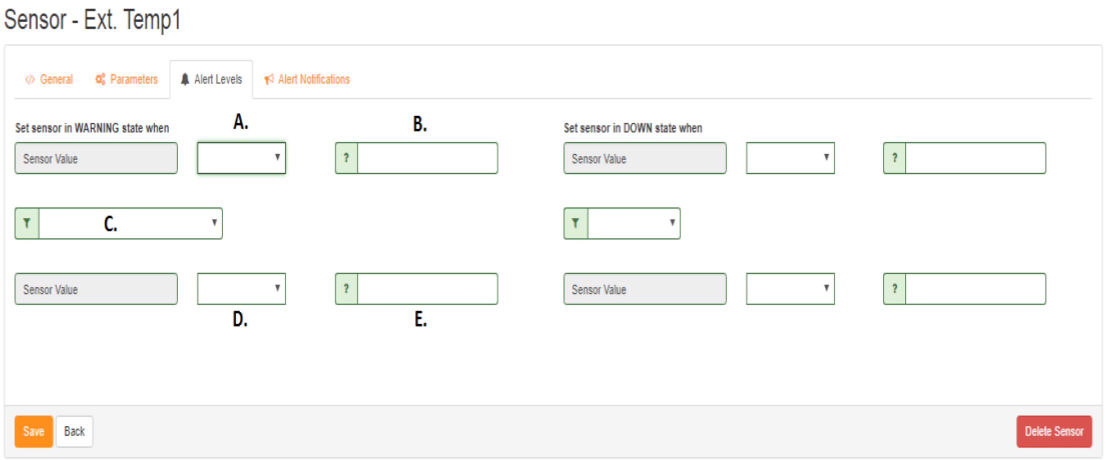
IP address - Setting the IP address you set for that sensor.

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**



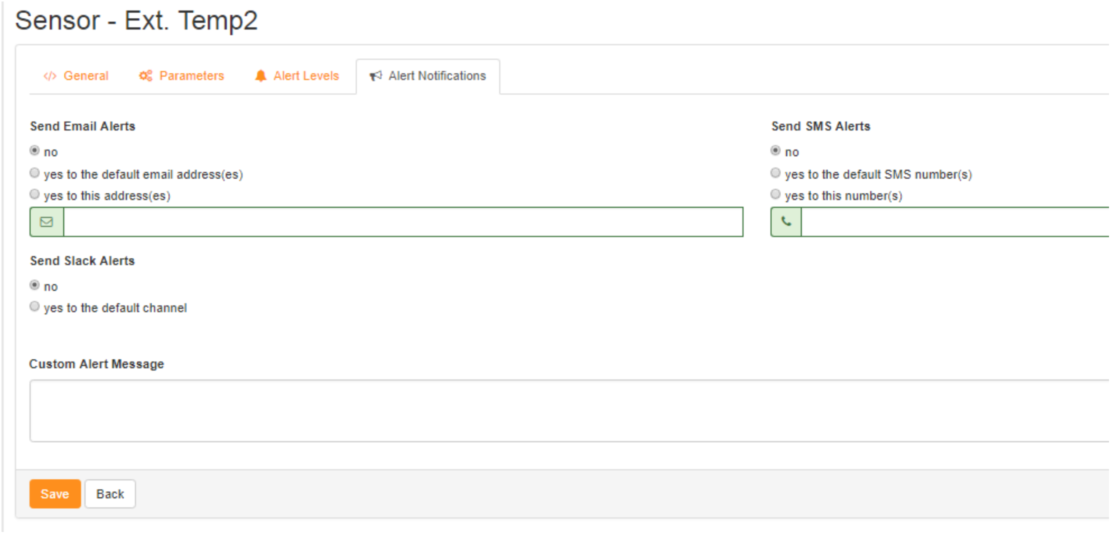
Setting up specific thresholds for Warning state and Down State.

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



Sensor - Ext. Temp2

Send Email Alerts

● no
○ yes to the default email address(es)
○ yes to this address(es)

Send SMS Alerts

● no
○ yes to the default SMS number(s)
○ yes to this number(s)

Send Slack Alerts

● no
○ yes to the default channel

Custom Alert Message

Able to sent 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.

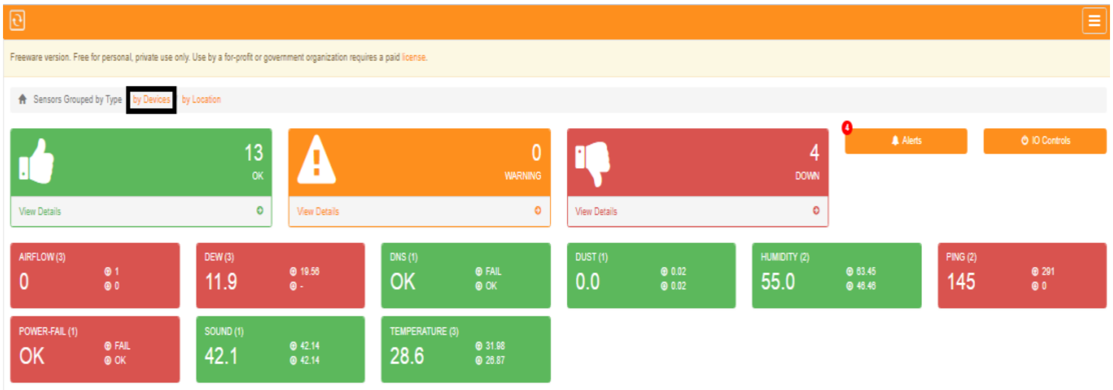
Send SMS Alerts
no - If no SMS is to be sent.
yes to default SMS number(s) - If to be sent to what you set under Section 2.5.
yes to this number(s) - If to be sent to specific phone number(s).
Note: Use valid phone numbers (+ symbol and numbers only). For multiple numbers, use a comma as a separator. 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.

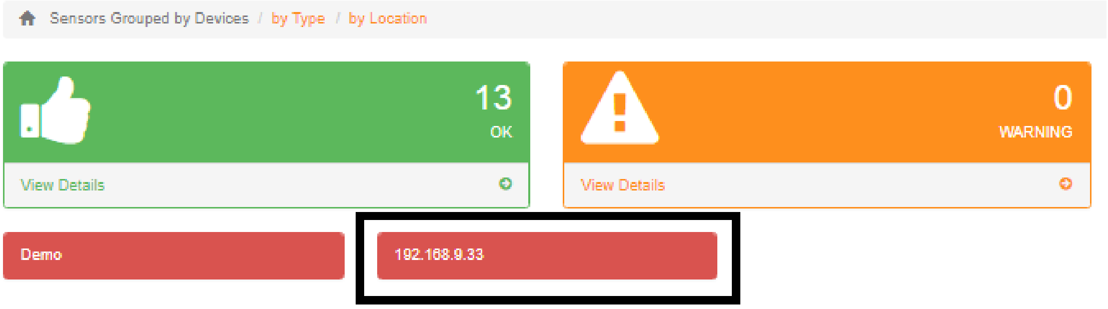
3.3. Editing a Device and Adding Location

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

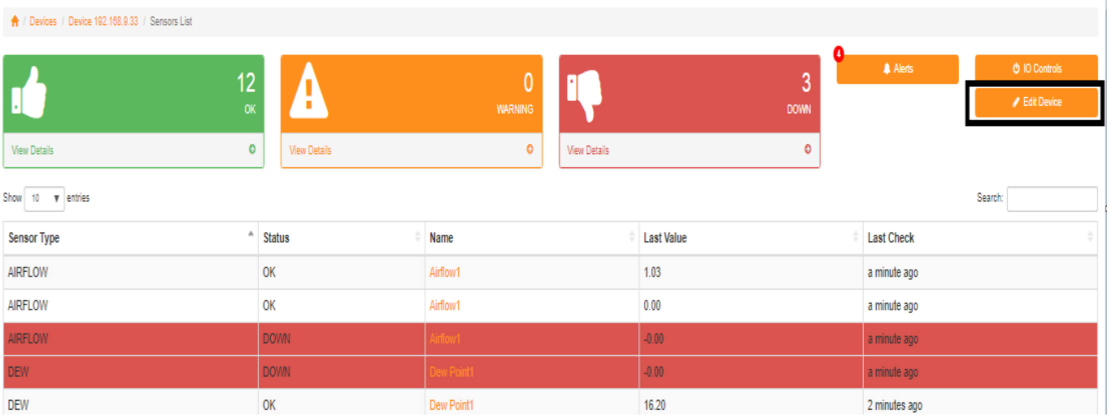


Freeware version. Free for personal, private use only. Use by a for-profit or government organization requires a paid license.

2. Select a device you want to edit.

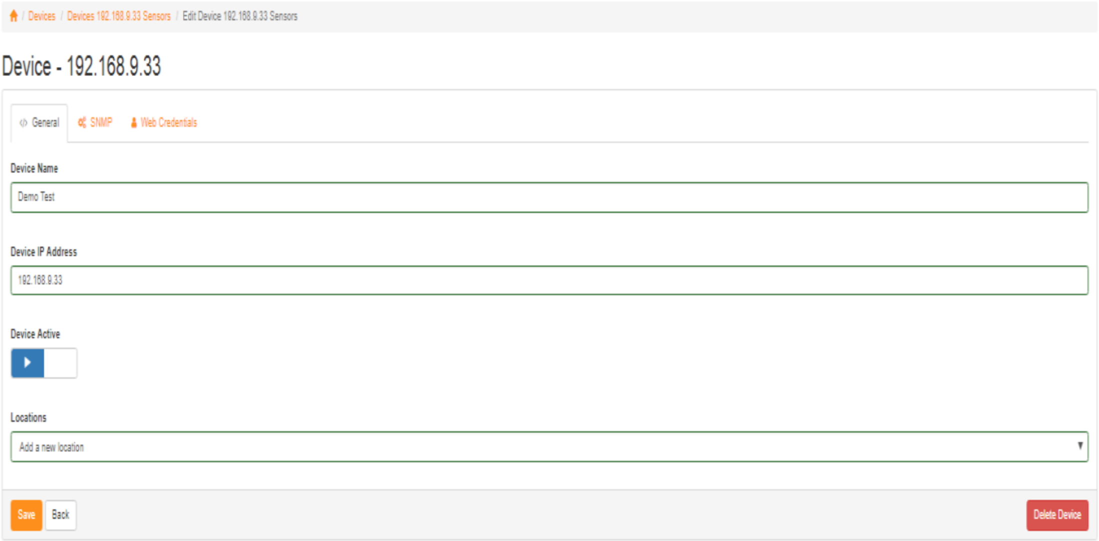


3. This screen shows you all sensors that are connected within the device. By clicking **Edit Device**, you can then customize with several options that are further explained below.



Sensor Type	Status	Name	Last Value	Last Check
AIRFLOW	OK	Airflow1	1.03	a minute ago
AIRFLOW	OK	Airflow1	0.00	a minute ago
AIRFLOW	DOWN	Airflow1	-0.00	a minute ago
DEW	DOWN	Dew Point1	-0.00	a minute ago
DEW	OK	Dew Point1	16.20	2 minutes ago

4. **General Tab**


Devices / Devices 192.168.9.33 Sensors / Edit Device 192.168.9.33 Sensors
General
SNMP
Web Credentials
Save
Back
Delete Device

Device - 192.168.9.33

Device Name: Demo Test

Device IP Address: 192.168.9.33

Device Active

Locations: Add a new location

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

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

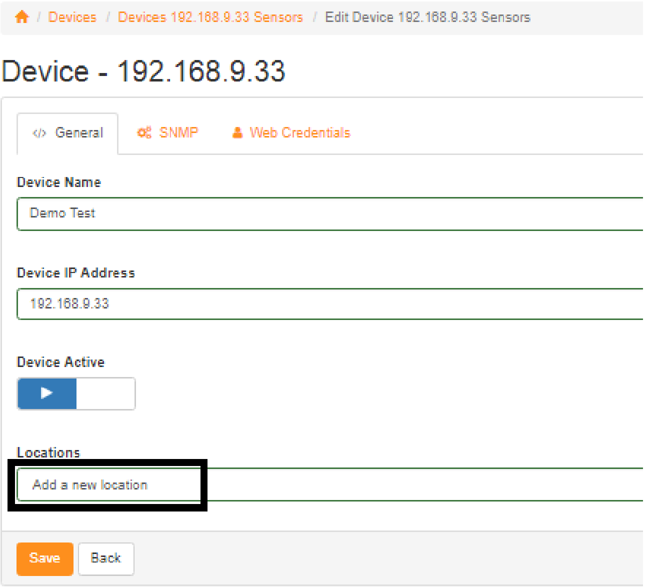
Device Active - Able to Play or Pause the monitoring of the device.

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

Delete Device - Delete a device completely from the list.

- **Adding a New Location**

4.1. Select **Add a New Location**.


Devices / Devices 192.168.9.33 Sensors / Edit Device 192.168.9.33 Sensors
General
SNMP
Web Credentials
Save
Back

Device - 192.168.9.33

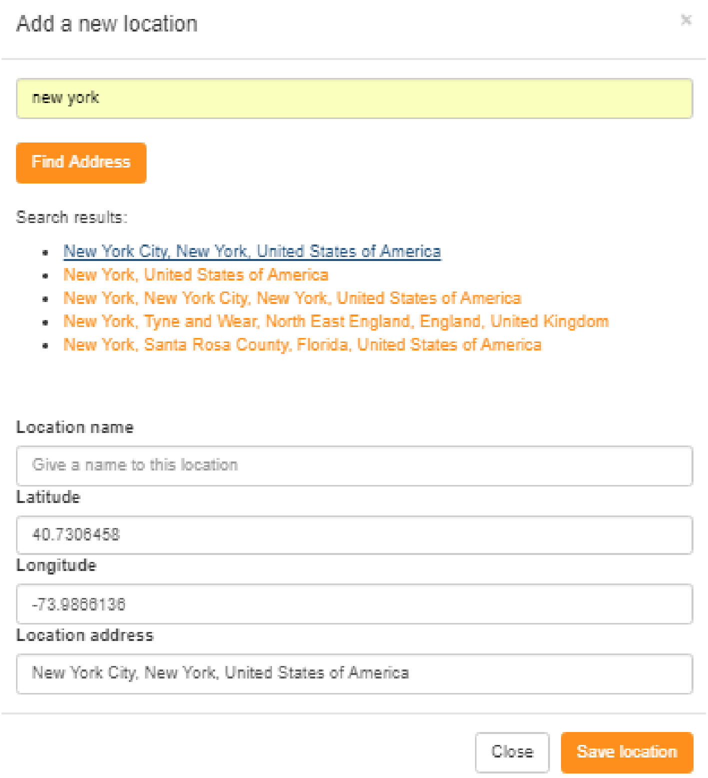
Device Name: Demo Test

Device IP Address: 192.168.9.33

Device Active

Locations: Add a new location

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

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: -73.9866136

Location address: New York City, New York, United States of America

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.

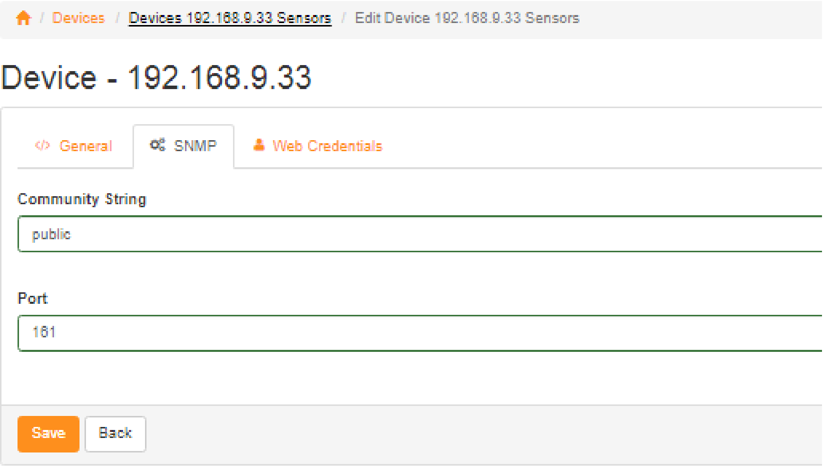
Latitude - You can manually input the latitude of the address.

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**


Devices / Devices 192.168.9.33 Sensors / Edit Device 192.168.9.33 Sensors
General
SNMP
Web Credentials
Save
Back

Device - 192.168.9.33

Community String
public

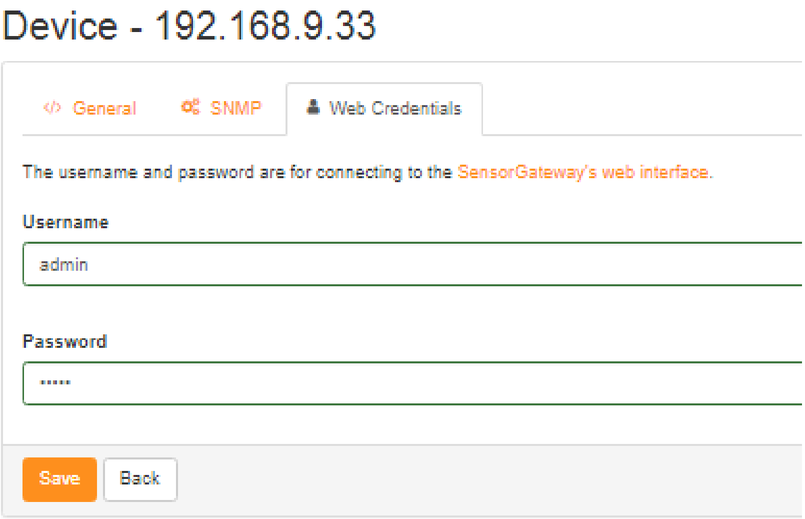
Port
161

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

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

Username
admin

Password
•••••

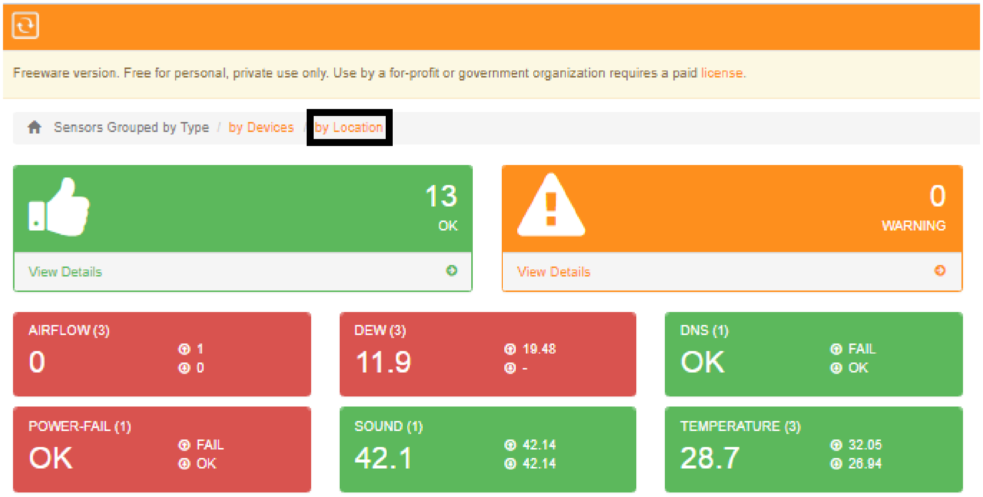
Username - The same username used to access the Sensorgateway's Web Interface.
Default - admin

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.



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

Sensors Grouped by Type / by Devices / by Location

13 OK — View Details

0 WARNING — View Details

AIRFLOW (3) 0 — 1 / 0

DEW (3) 11.9 — 19.48 / -

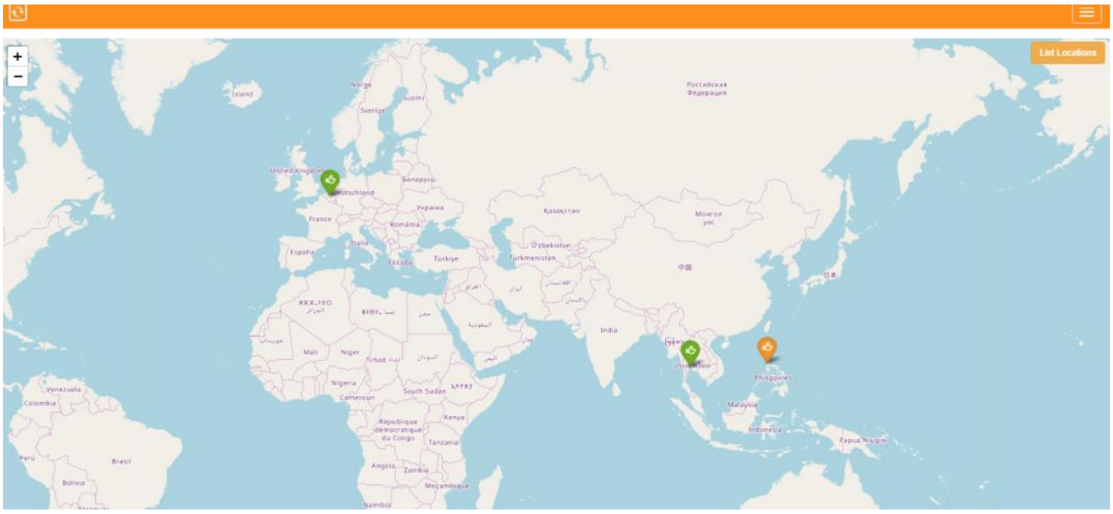
DNS (1) OK — FAIL / OK

POWER-FAIL (1) OK — FAIL / OK

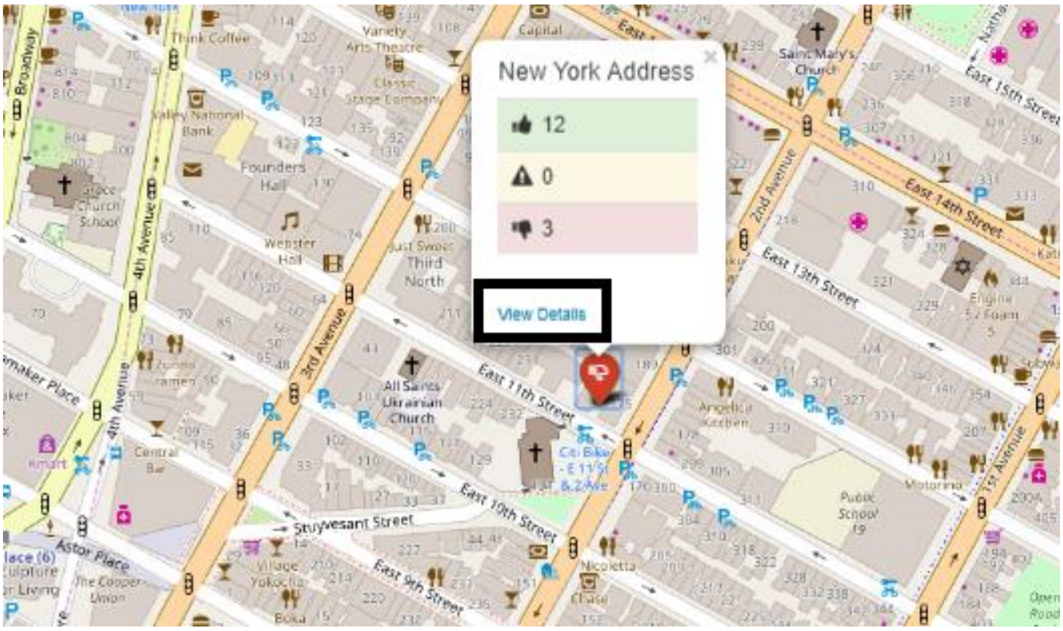
SOUND (1) 42.1 — 42.14 / 42.14

TEMPERATURE (3) 28.7 — 32.05 / 26.94

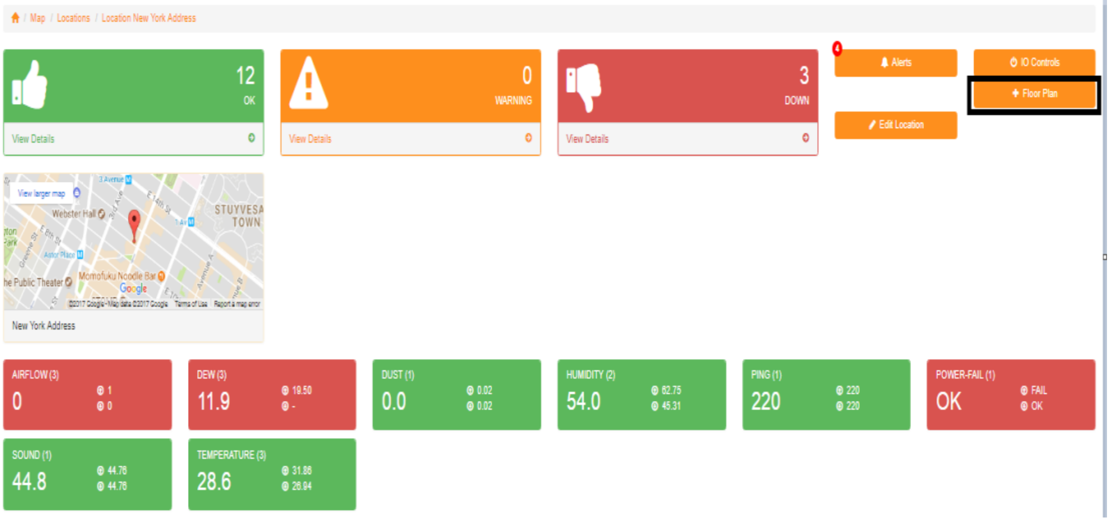
2. This opens up the world map where you see all of the devices set on different addresses.



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.

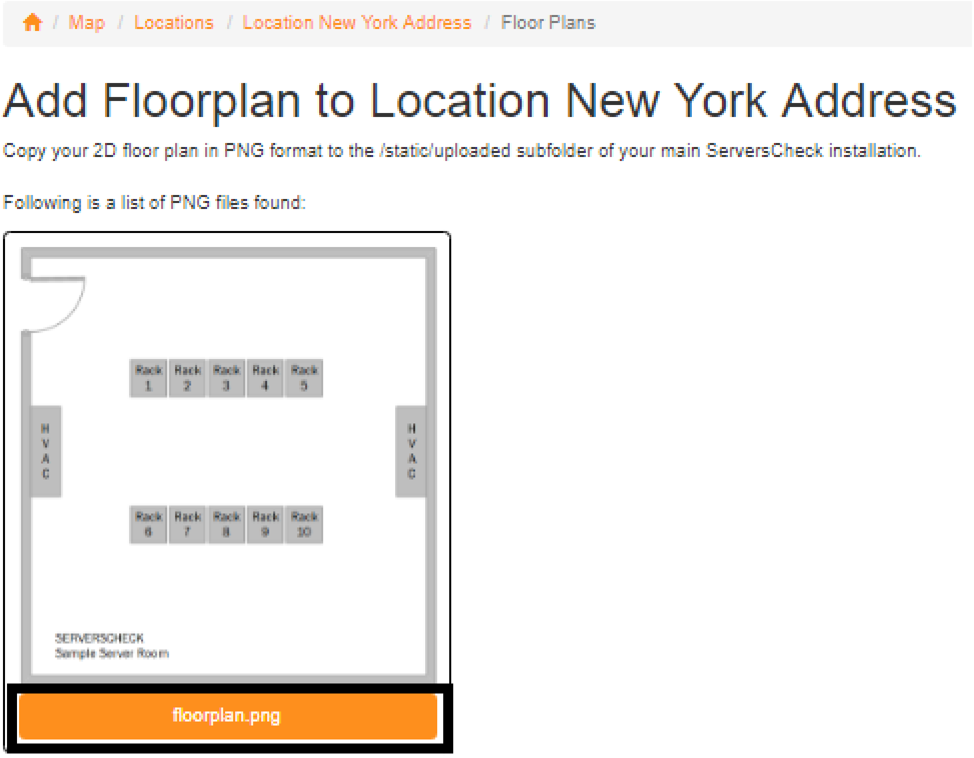


Save a copy of a floor plan design in PNG file format **for Temperature layer**, **Humidity Layer** and **Flooding Layer** or a single design for all.

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.



Map / Locations / Location New York Address / Floor Plans

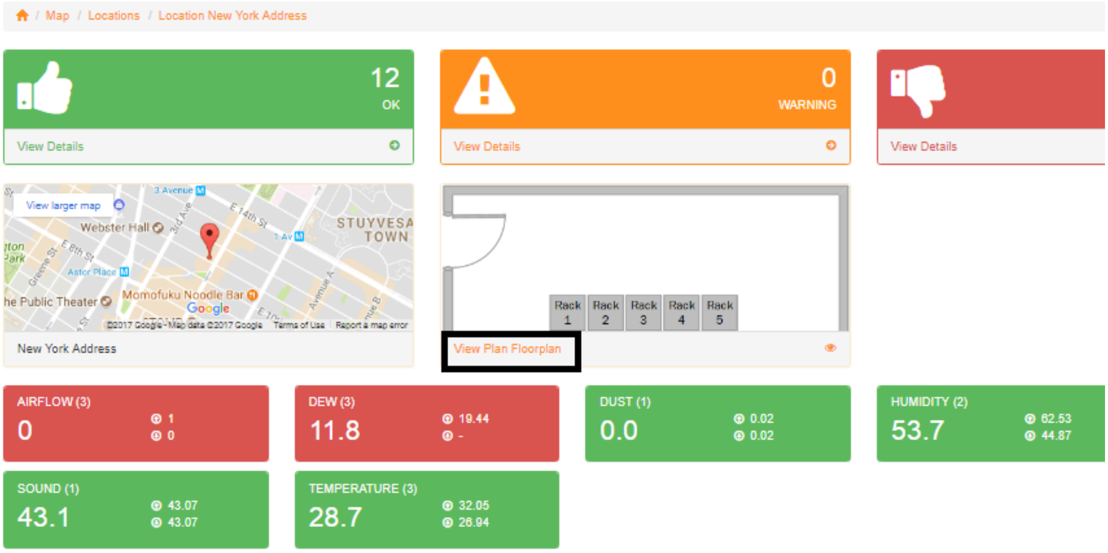
Add Floorplan to Location New York Address

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

Following is a list of PNG files found:

5. Adding your Sensors to your Floor Plan

- Click **View Floor Plan**.



Map / Locations / Location New York Address

12 OK — View Details

0 WARNING — View Details

View Details

New York Address

View Plan Floorplan

AIRFLOW (3) 0 — 1 / 0

DEW (3) 11.8 — 19.44 / -

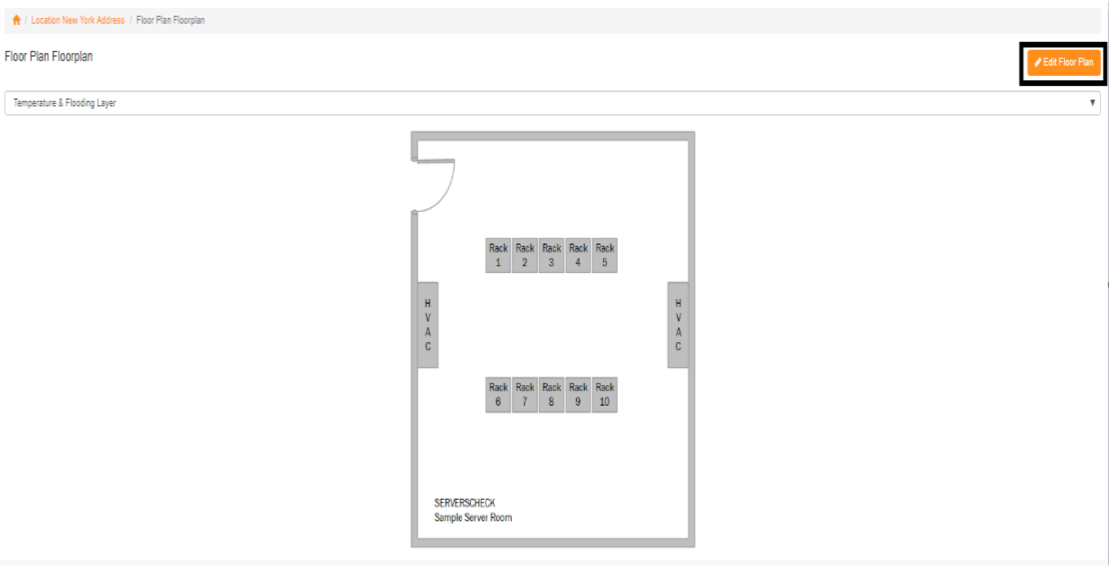
DUST (1) 0.0 — 0.02 / 0.02

HUMIDITY (2) 53.7 — 62.53 / 44.87

SOUND (1) 43.1 — 43.07 / 43.07

TEMPERATURE (3) 28.7 — 32.05 / 26.94

- Click **Edit Floor Plan**.



Location New York Address / Floor Plan Floorplan

Floor Plan Floorplan

Temperature & Flooding Layer

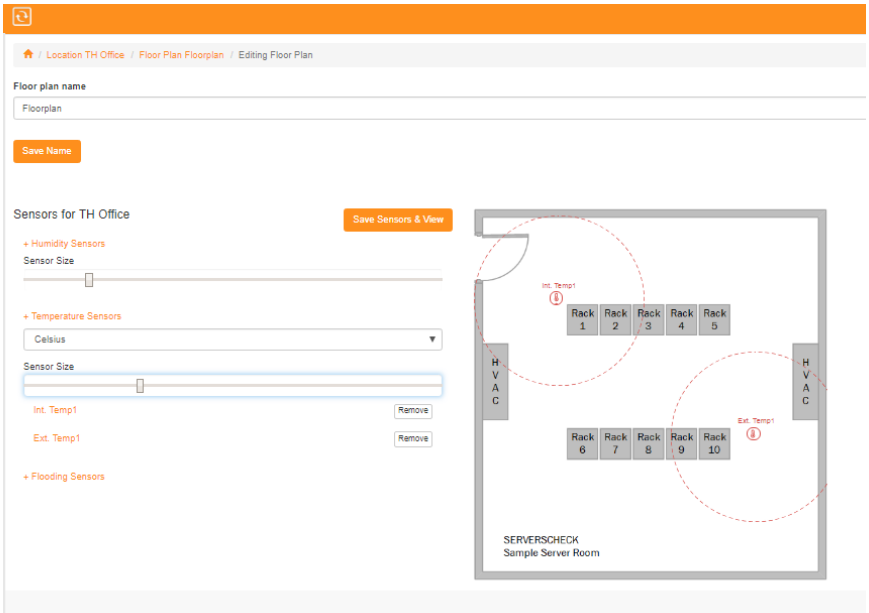
- Place your sensors to the Floor Plan.

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.



Location TH Office / Floor Plan Floorplan / Editing Floor Plan

Floor plan name: Floorplan

Sensors for TH Office

+ Humidity Sensors

Sensor Size

+ Temperature Sensors

Celsius

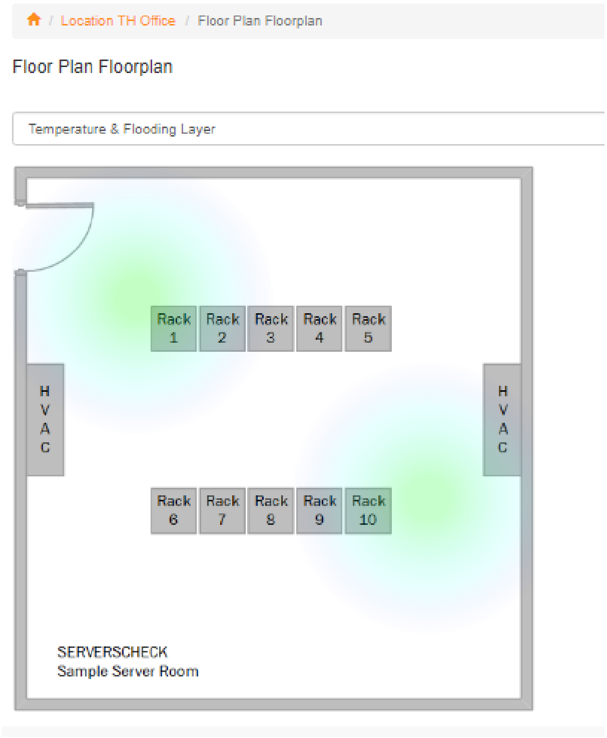
Sensor Size

Int. Temp1

Ext. Temp1

+ Flooding Sensors

This should show similar as the one below.

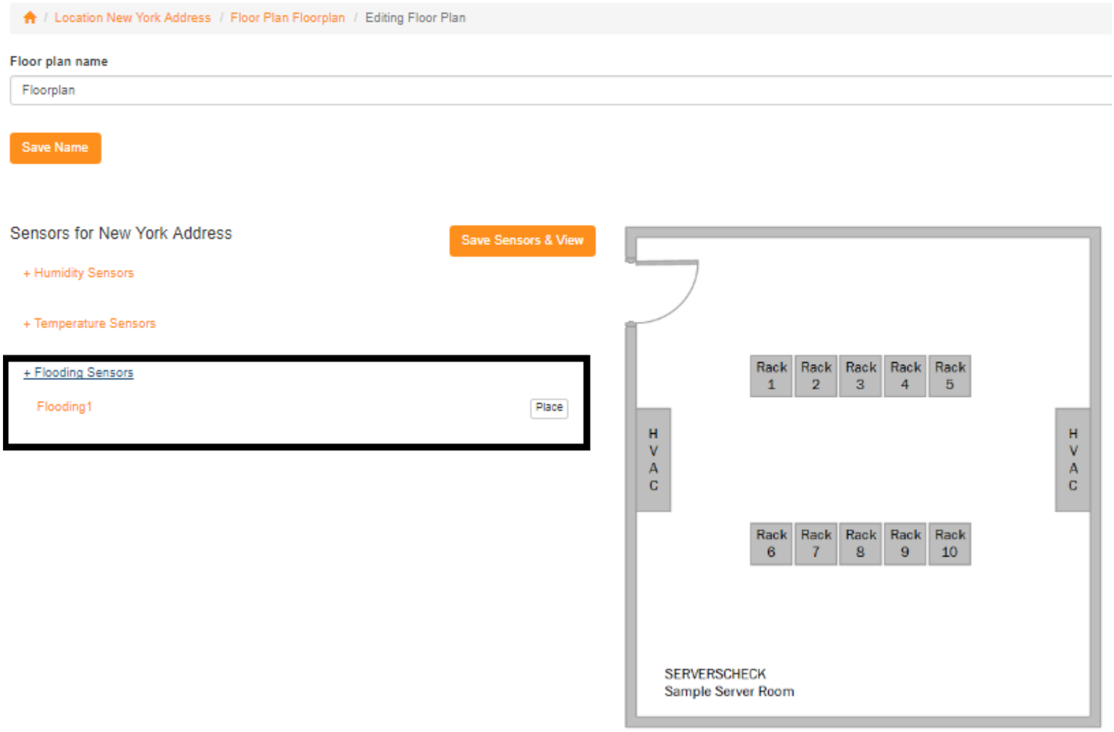


/ Location TH Office / Floor Plan Floorplan

Floor Plan Floorplan

Temperature & Flooding Layer

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



/ Location New York Address / Floor Plan Floorplan / Editing Floor Plan

Floor plan name

Floorplan

Save Name

Sensors for New York Address

Save Sensors & View

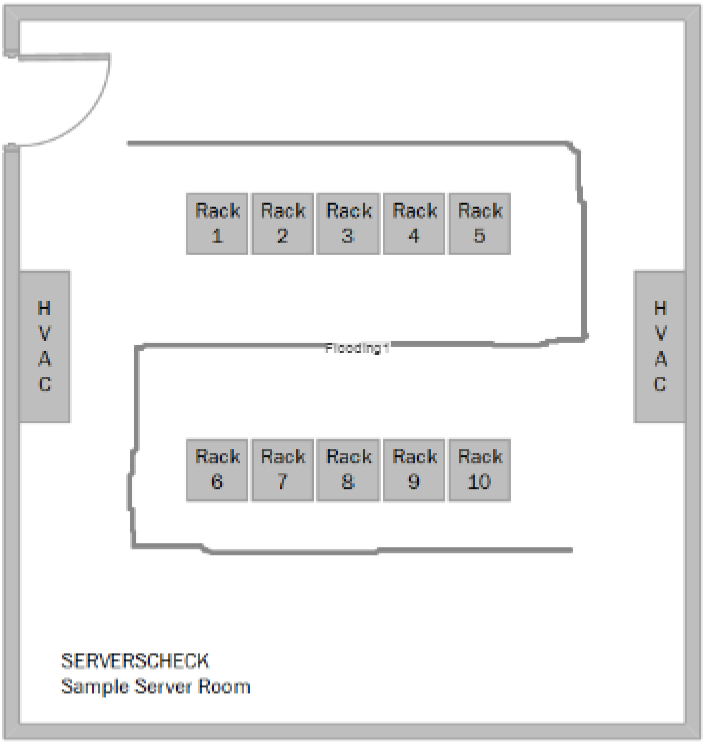
+ Humidity Sensors

+ Temperature Sensors

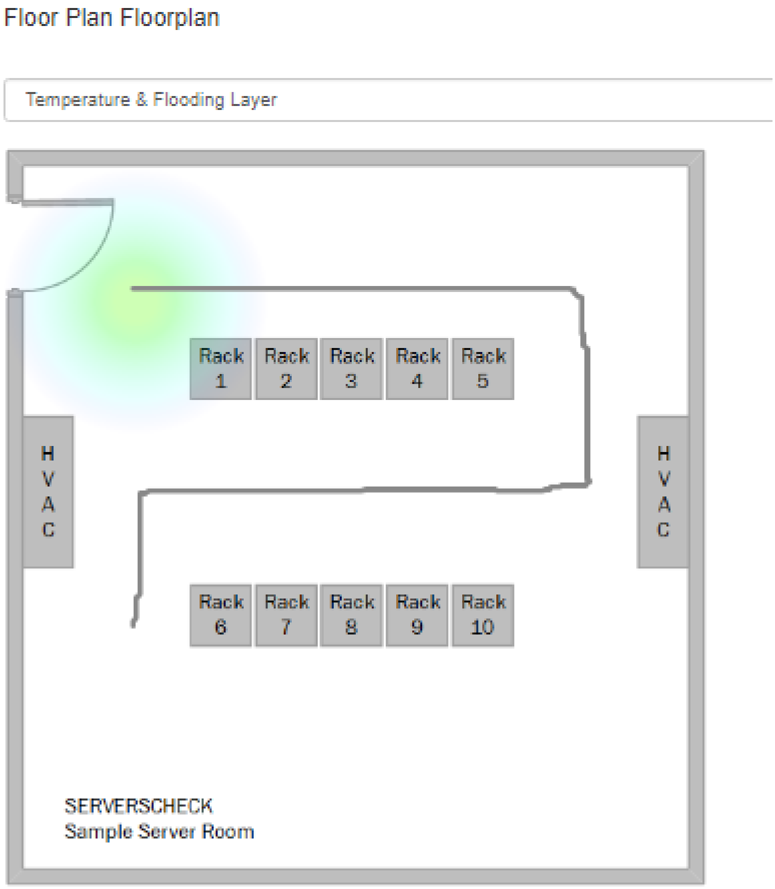
+ Flooding Sensors

Flooding1 Place

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



This should show similar to the image below.

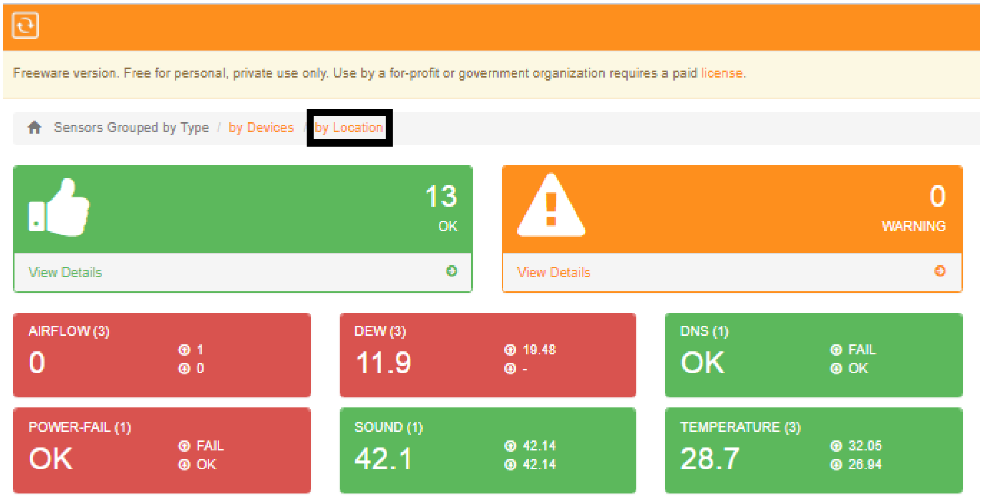

Floor Plan Floorplan

Temperature & Flooding Layer

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.



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

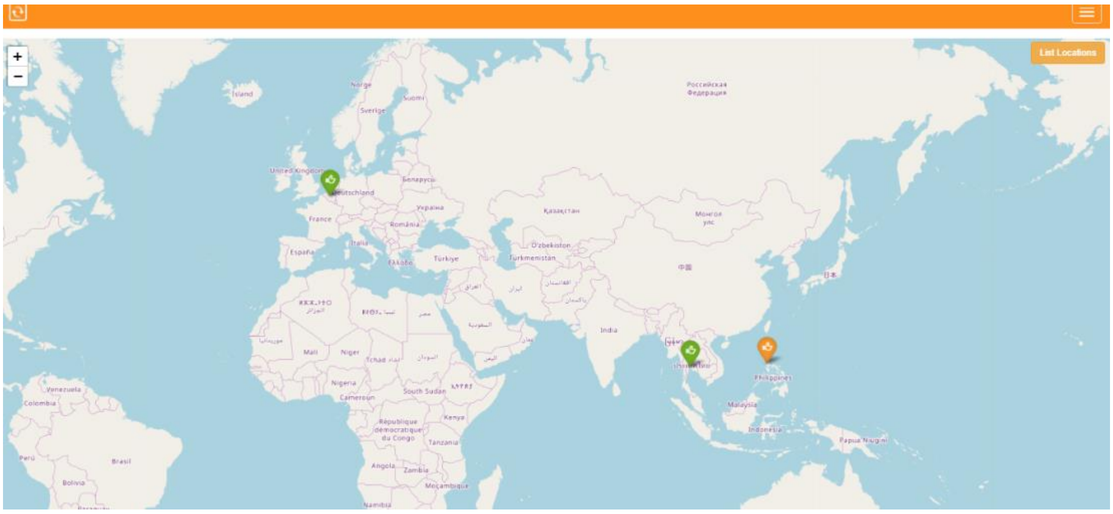
Sensors Grouped by Type / by Devices / by Location

13 OK — View Details

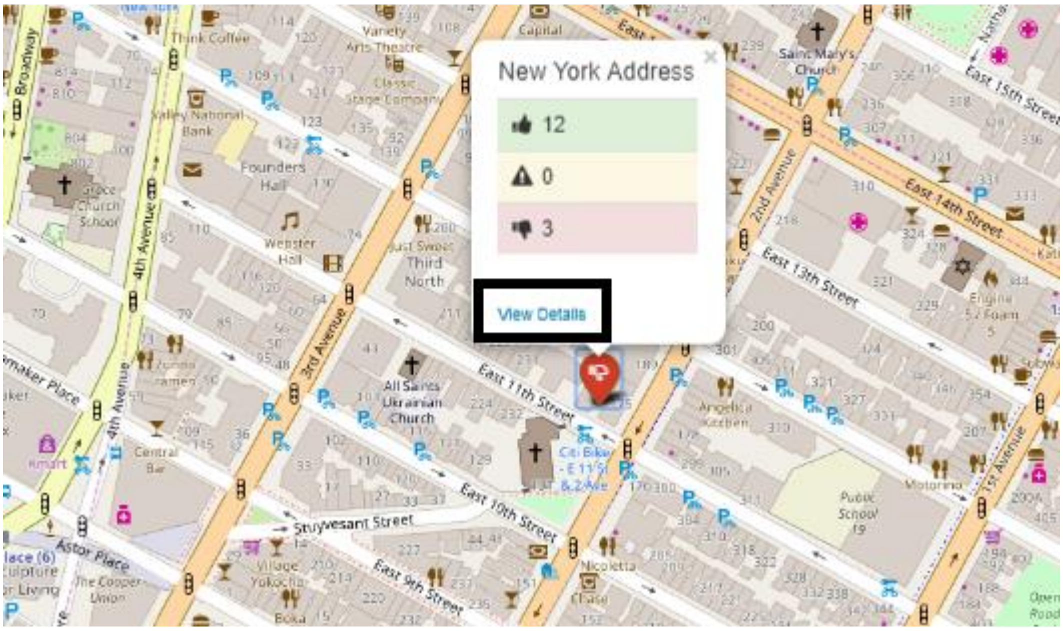
0 WARNING — View Details

AIRFLOW (3) 0 1 0	DEW (3) 11.9 19.48 -	DNS (1) OK FAIL OK
POWER-FAIL (1) OK FAIL OK	SOUND (1) 42.1 42.14 42.14	TEMPERATURE (3) 28.7 32.05 26.94

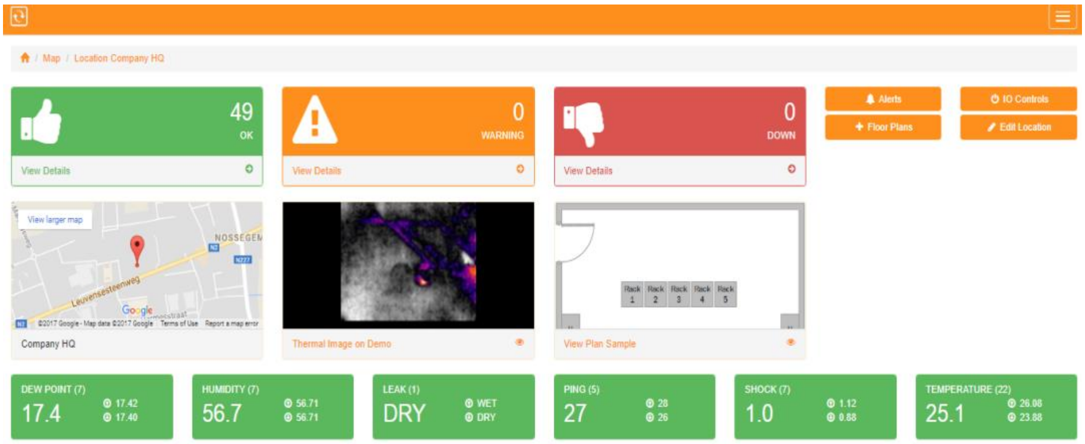
2. This opens up the world map where you see all of the devices set on different addresses.

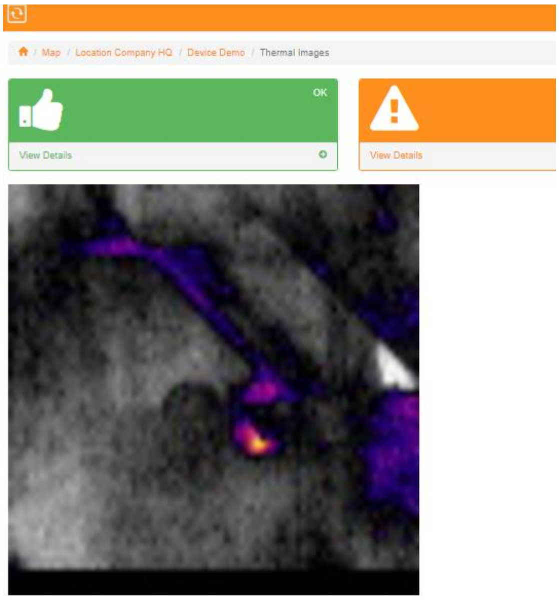


3. Clicking View Details on each of the address will show all of the status of the devices which are normal, in warning, and down.



4. It should show as similar to the images below.



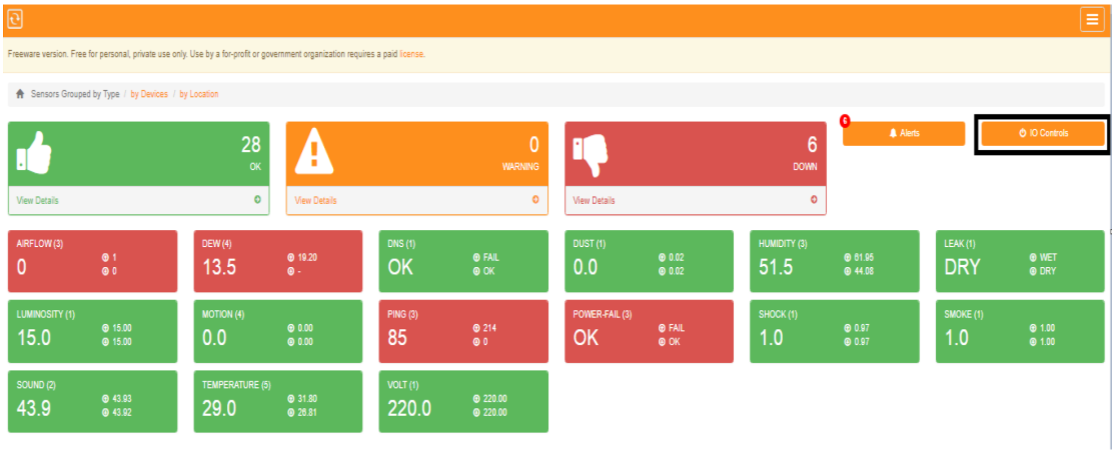


3.6. Controlling Outputs and Relays

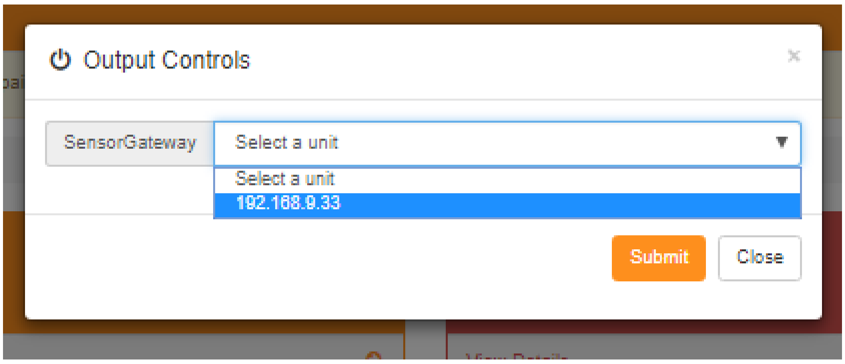
After adding Serverscheck sensors shown in Section 3.1, it does gives you an option to include I/O controls if your device has a Sensorhub, IO Dry Contact Sensor or Multi-Sensor & Hub.

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.

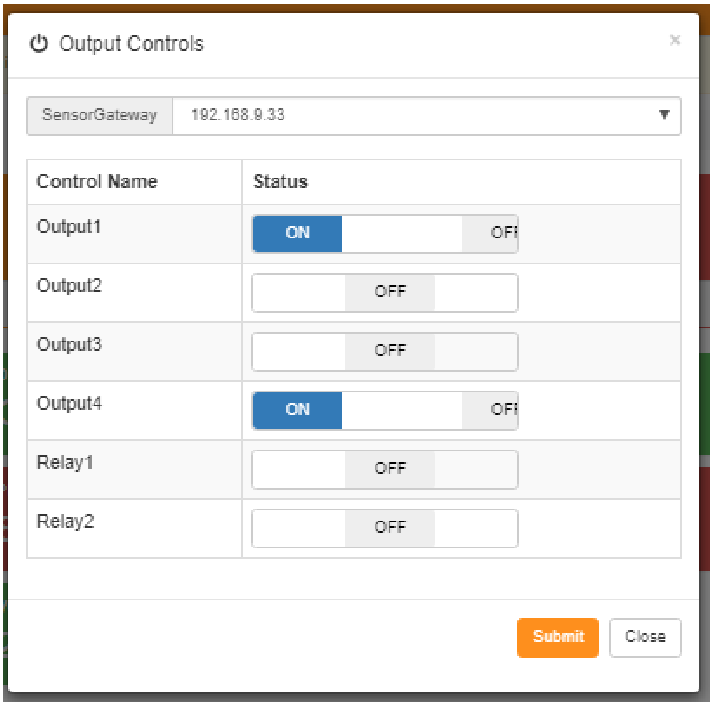
1. From the Dashboard screen, select **IO Controls**.


Freeware version. Free for personal, private use only. Use by a for-profit or government organization requires a paid license.
Sensors Grouped by Type / by Devices / by Location
28 OK
0 WARNING
6 DOWN
View Details
Alerts
IO Controls
AIRFLOW (3) 0 1 0
DEW (4) 13.5 19.20 -
DNS (1) OK FAIL OK
DUST (1) 0.0 0.02 0.02
HUMIDITY (3) 51.5 61.95 44.08
LEAK (1) DRY WET DRY
LUMINOSITY (1) 15.0 15.00 15.00
MOTION (4) 0.0 0.00 0.00
PING (3) 85 214 0
POWER-FAIL (3) OK FAIL OK
SHOCK (1) 1.0 0.97 0.97
SMOKE (1) 1.0 1.00 1.00
SOUND (2) 43.9 43.93 43.92
TEMPERATURE (5) 29.0 31.80 26.81
VOLT (1) 220.0 220.00 220.00

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.



SensorGateway 192.168.9.33 ▼

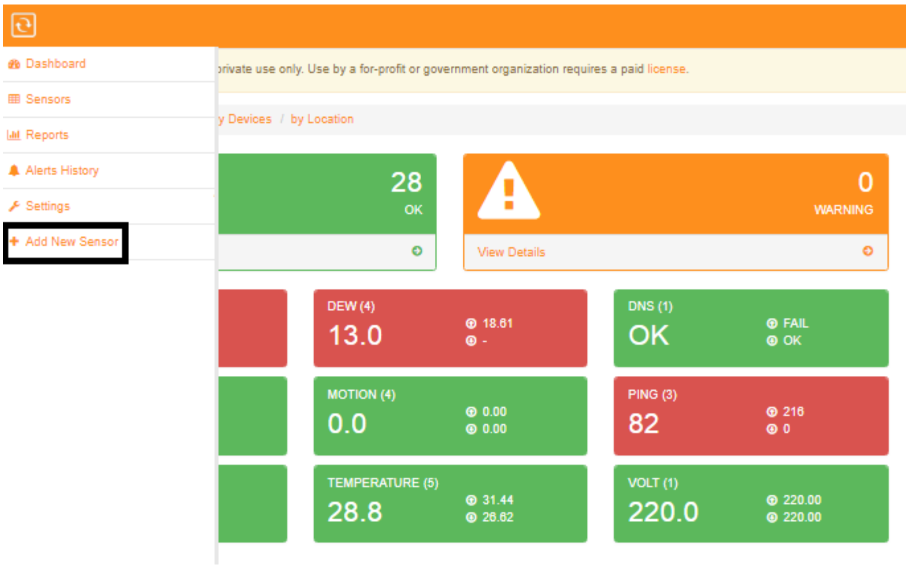
Control Name	Status
Output1	ON OFF
Output2	OFF
Output3	OFF
Output4	ON OFF
Relay1	OFF
Relay2	OFF

4. Setting up Other Check Types

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

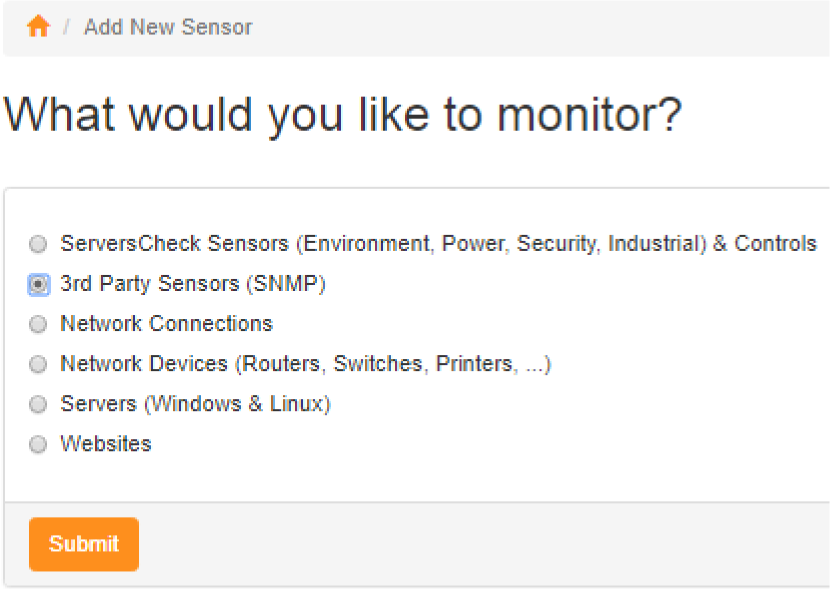
This check will allow you to monitor other 3rd party SNMP sensors. Only SNMP capable devices will be able to be added under this check.

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



rivate use only. Use by a for-profit or government organization requires a paid license.

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



Add New Sensor

What would you like to monitor?

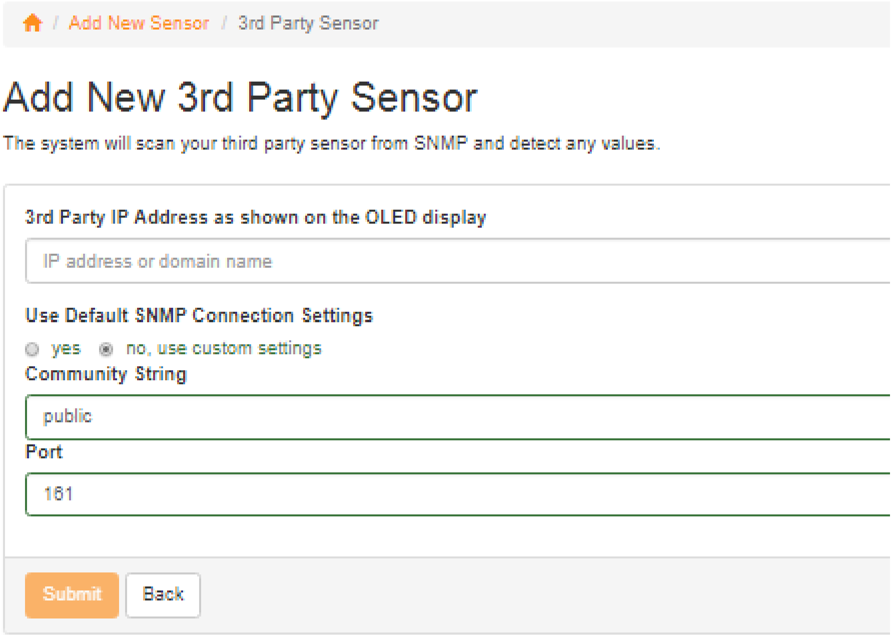
○ ServersCheck Sensors (Environment, Power, Security, Industrial) & Controls
● 3rd Party Sensors (SNMP)
○ Network Connections
○ Network Devices (Routers, Switches, Printers, ...)
○ Servers (Windows & Linux)
○ Websites

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.



Add New 3rd Party Sensor

The system will scan your third party sensor from SNMP and detect any values.

3rd Party IP Address as shown on the OLED display

IP address or domain name

Use Default SNMP Connection Settings

○ yes ● no, use custom settings

Community String

public

Port

161

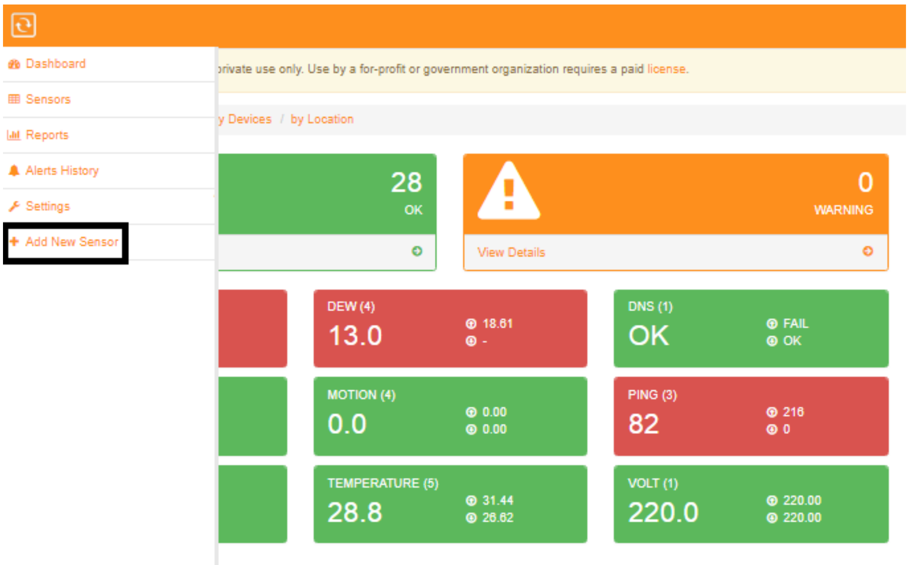
4.2. Adding Checks for Network Connections

Serverscheck Software monitors your network performance and capability.

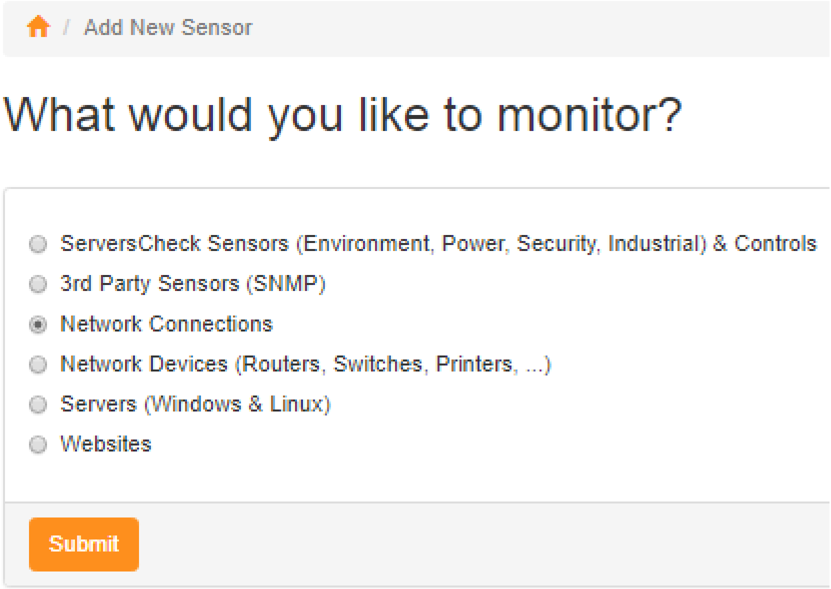
4.2.1. Adding Ping Check

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**.



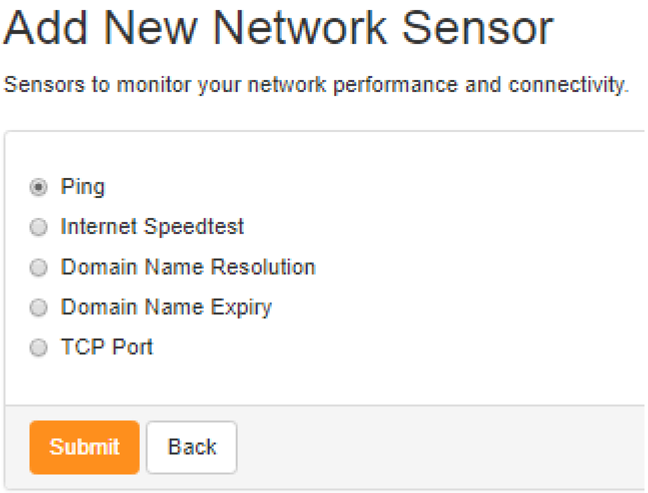
2. Select Network Connections.



What would you like to monitor?

○ ServersCheck Sensors (Environment, Power, Security, Industrial) & Controls
○ 3rd Party Sensors (SNMP)
● Network Connections
○ Network Devices (Routers, Switches, Printers, ...)
○ Servers (Windows & Linux)
○ Websites

3. Select PING.

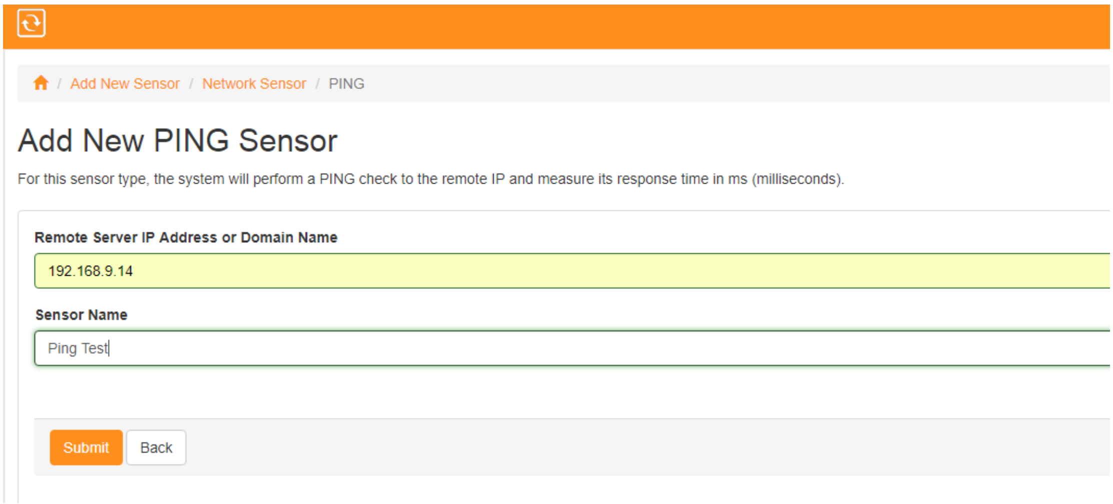


Add New Network Sensor

Sensors to monitor your network performance and connectivity.

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

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 Sensor / Network Sensor / PING

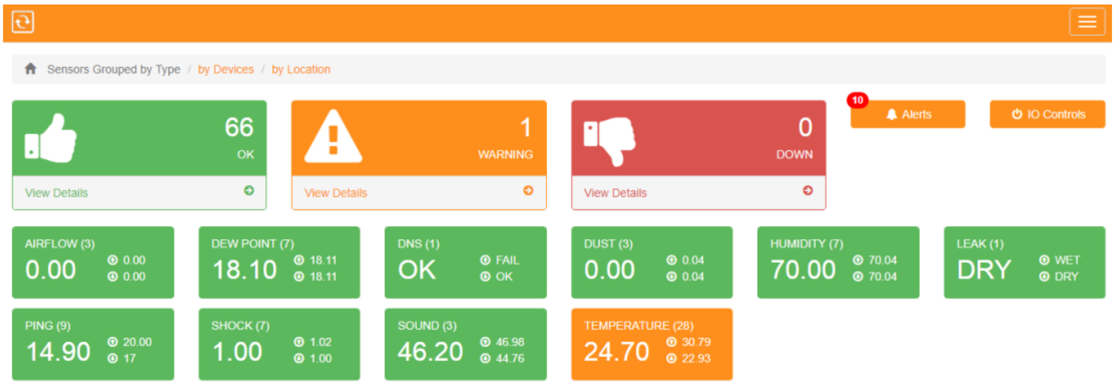
Add New PING Sensor

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: 192.168.9.14

Sensor Name: Ping Test

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



Sensors Grouped by Type / by Devices / by Location

66 OK — View Details

1 WARNING — View Details

0 DOWN — View Details

AIRFLOW (3) 0.00 — 0.00 / 0.00

DEW POINT (7) 18.10 — 18.11 / 18.11

DNS (1) OK — FAIL / OK

DUST (3) 0.00 — 0.04 / 0.04

HUMIDITY (7) 70.00 — 70.04 / 70.04

LEAK (1) DRY — WET / DRY

PING (9) 14.90 — 20.00 / 17

SHOCK (7) 1.00 — 1.02 / 1.00

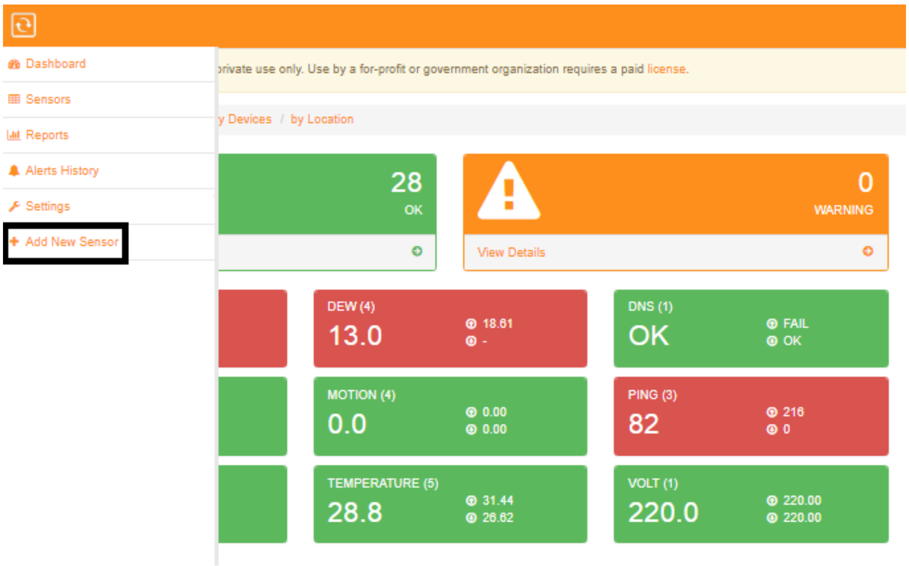
SOUND (3) 46.20 — 46.98 / 44.76

TEMPERATURE (28) 24.70 — 30.79 / 22.93

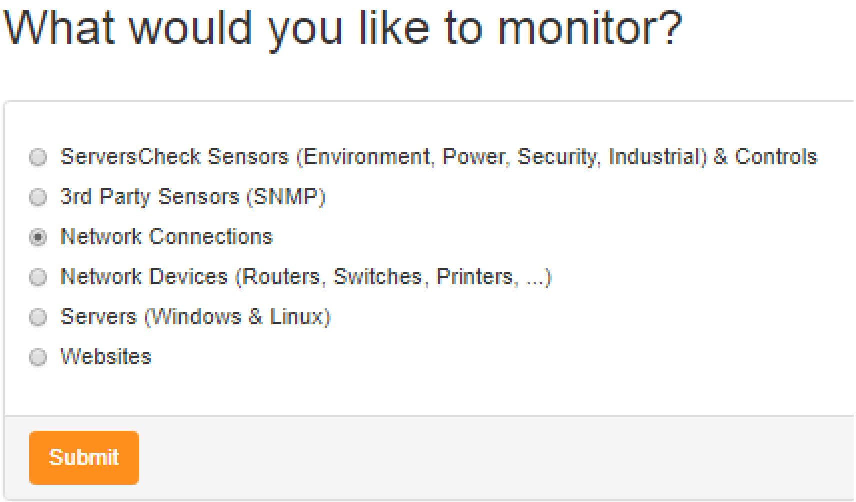
4.2.2. Adding Internet Speedtest Check

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**.



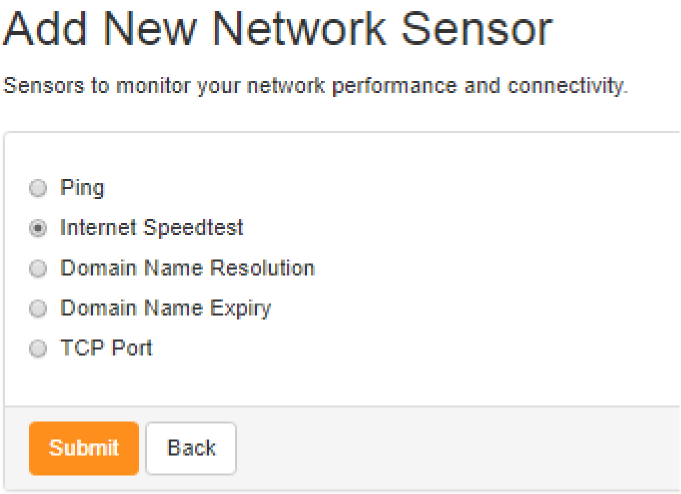
2. Select Network Connections.



What would you like to monitor?

○ ServersCheck Sensors (Environment, Power, Security, Industrial) & Controls
○ 3rd Party Sensors (SNMP)
● Network Connections
○ Network Devices (Routers, Switches, Printers, ...)
○ Servers (Windows & Linux)
○ Websites

3. Select Internet Speedtest.



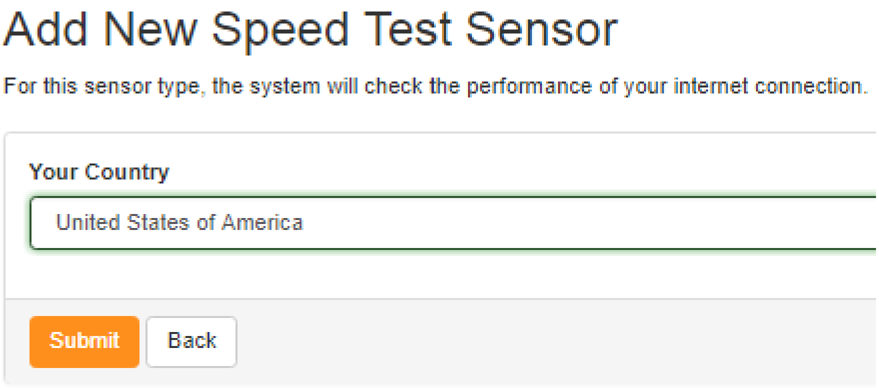
Add New Network Sensor

Sensors to monitor your network performance and connectivity.

○ Ping
● Internet Speedtest
○ Domain Name Resolution
○ Domain Name Expiry
○ TCP Port

Submit Back

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



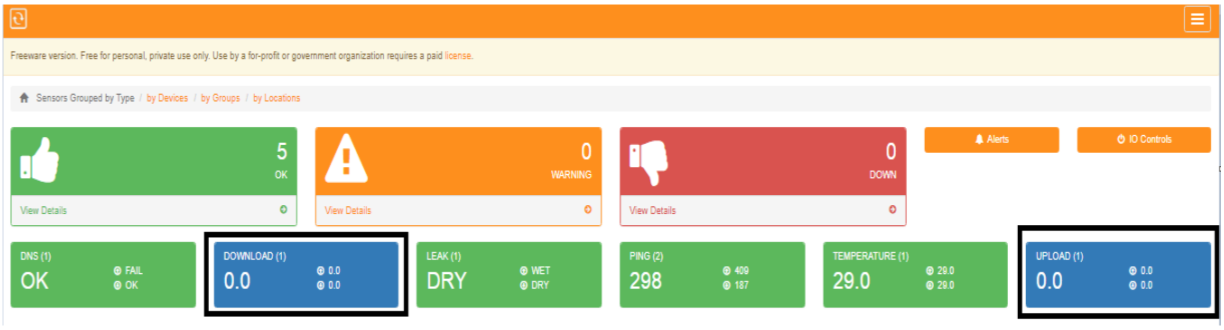
Add New Speed Test Sensor

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.



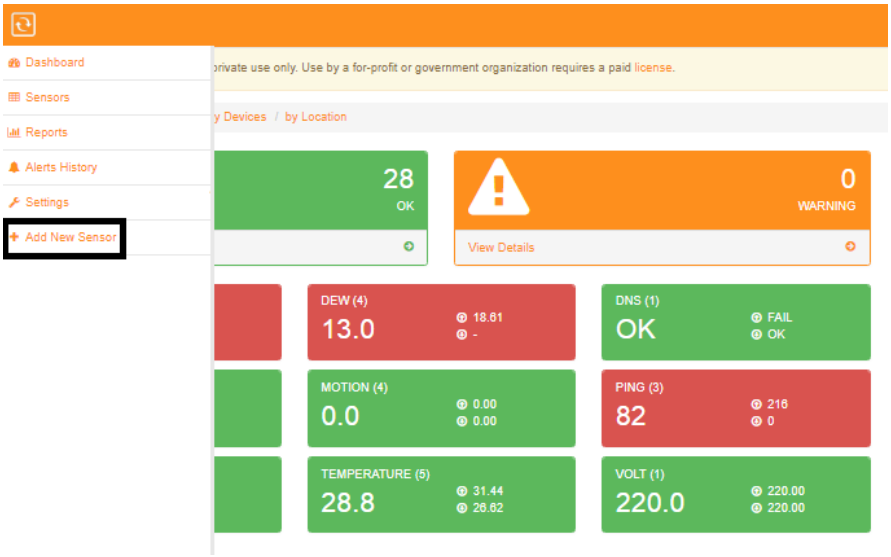
Freeware version. Free for personal, private use only. Use by a for-profit or government organization requires a paid license.

Sensors Grouped by Type / by Devices / by Groups / by Locations

4.2.3. Adding Domain Name Resolution Check

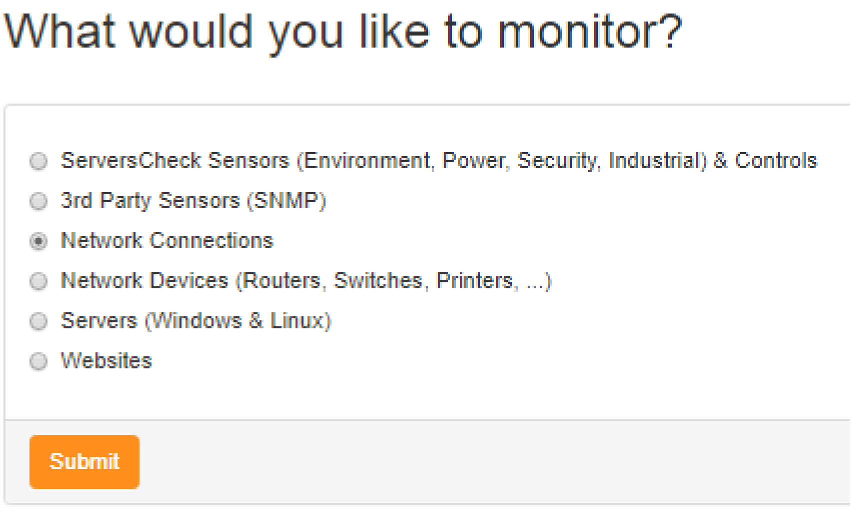
Each web server and any host connected to the internet has a unique IP address in textual form, translating it to an IP address. The system will perform a DNS resolution for the given domain name, record type and against the default or specified DNS server.

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



›rivate use only. Use by a for-profit or government organization requires a paid license.

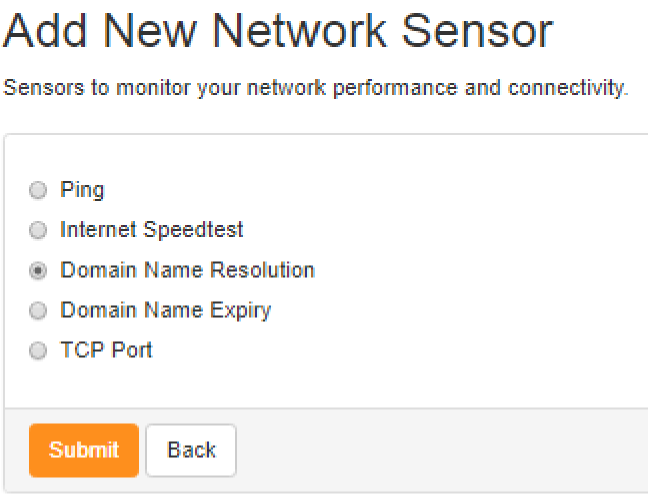
2. Select Network Connections.



What would you like to monitor?

○ ServersCheck Sensors (Environment, Power, Security, Industrial) & Controls
○ 3rd Party Sensors (SNMP)
● Network Connections
○ Network Devices (Routers, Switches, Printers, ...)
○ Servers (Windows & Linux)
○ Websites

3. Select Domain Name Resolution.



Add New Network Sensor

Sensors to monitor your network performance and connectivity.

○ Ping
○ Internet Speedtest
● Domain Name Resolution
○ Domain Name Expiry
○ TCP Port

4. Provide the Settings for the DNS Sensor.

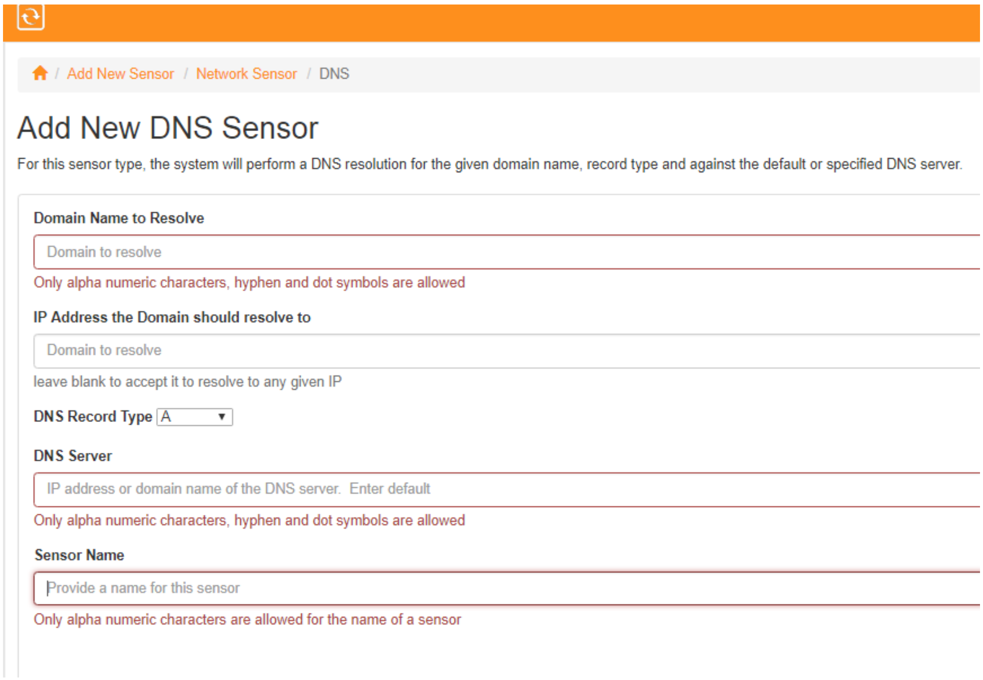
Domain Name to Resolve - Input the Domain name you intend to check. Only alphanumeric characters, hyphen and dot symbols are allowed.

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.



Add New DNS Sensor

For this sensor type, the system will perform a DNS resolution for the given domain name, record type and against the default or specified DNS server.

Domain Name to Resolve
Domain to resolve
Only alpha numeric characters, hyphen and dot symbols are allowed

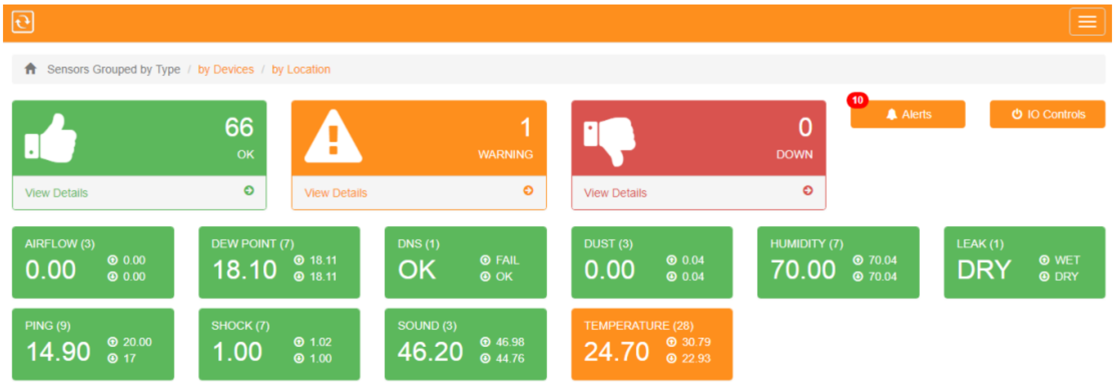
IP Address the Domain should resolve to
Domain to resolve
leave blank to accept it to resolve to any given IP

DNS Record Type A

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

Sensor Name
Provide a name for this sensor
Only alpha numeric characters are allowed for the name of a sensor

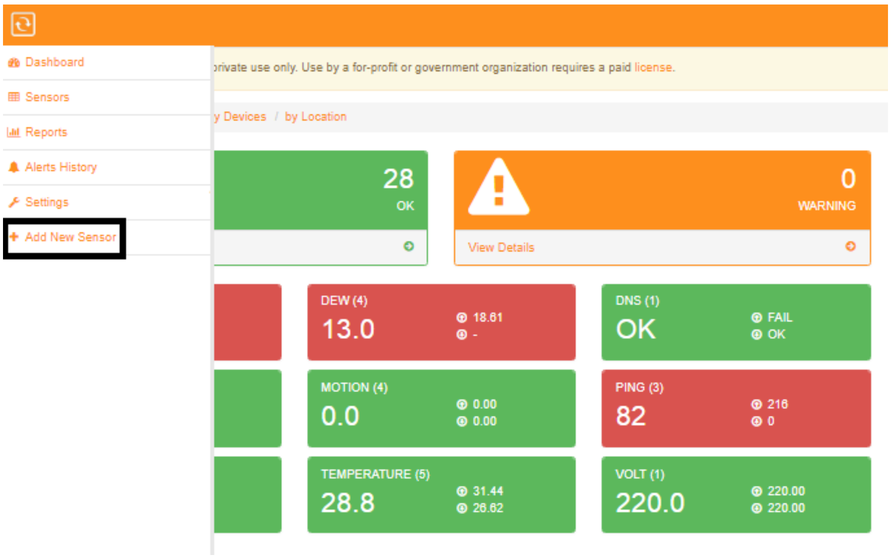
5. Once done, it should appear as one of the monitored checks on the Dashboard.


Sensors Grouped by Type / by Devices / by Location
66
OK
View Details
1
WARNING
View Details
0
DOWN
View Details
10
Alerts
IO Controls
AIRFLOW (3) 0.00 0.00 0.00
DEW POINT (7) 18.10 18.11 18.11
DNS (1) OK FAIL OK
DUST (3) 0.00 0.04 0.04
HUMIDITY (7) 70.00 70.04 70.04
LEAK (1) DRY WET DRY
PING (9) 14.90 20.00 17
SHOCK (7) 1.00 1.02 1.00
SOUND (3) 46.20 46.98 44.76
TEMPERATURE (28) 24.70 30.79 22.93

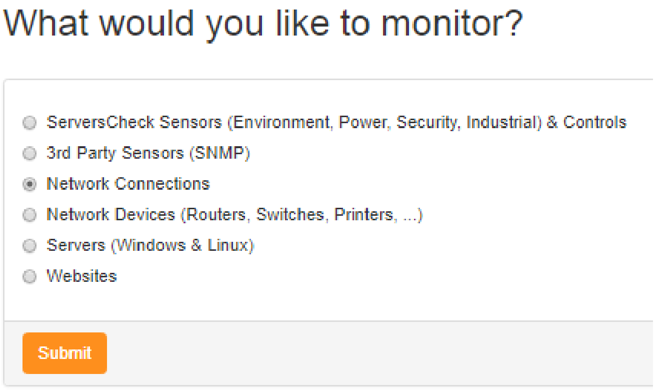
4.2.4. Adding Domain Name Expiry Check

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**.



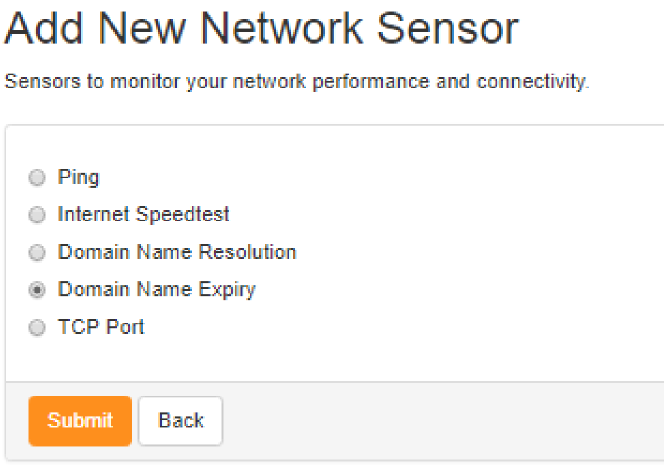
2. Select Network Connections.


What would you like to monitor?

○ ServersCheck Sensors (Environment, Power, Security, Industrial) & Controls
○ 3rd Party Sensors (SNMP)
● Network Connections
○ Network Devices (Routers, Switches, Printers, ...)
○ Servers (Windows & Linux)
○ Websites

Submit

3. Select Domain Name Expiry.



Add New Network Sensor

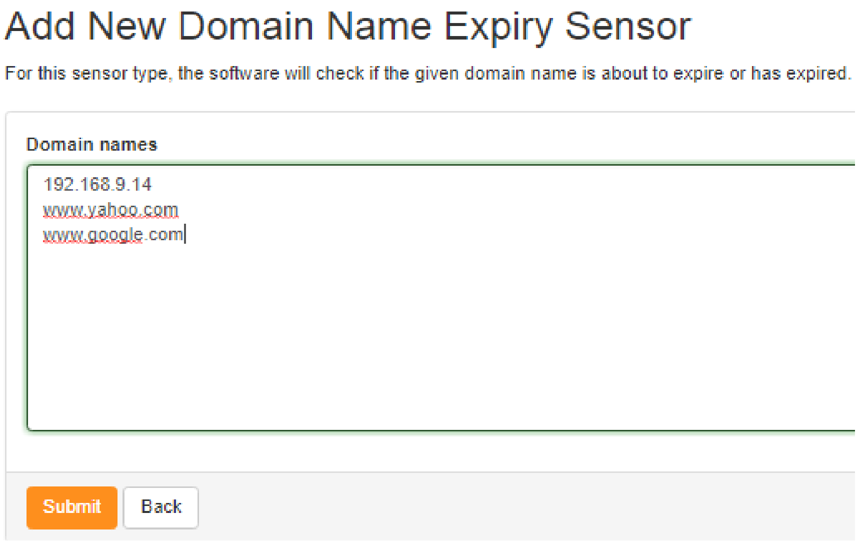
Sensors to monitor your network performance and connectivity.

○ Ping
○ Internet Speedtest
○ Domain Name Resolution
● Domain Name Expiry
○ TCP Port

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.



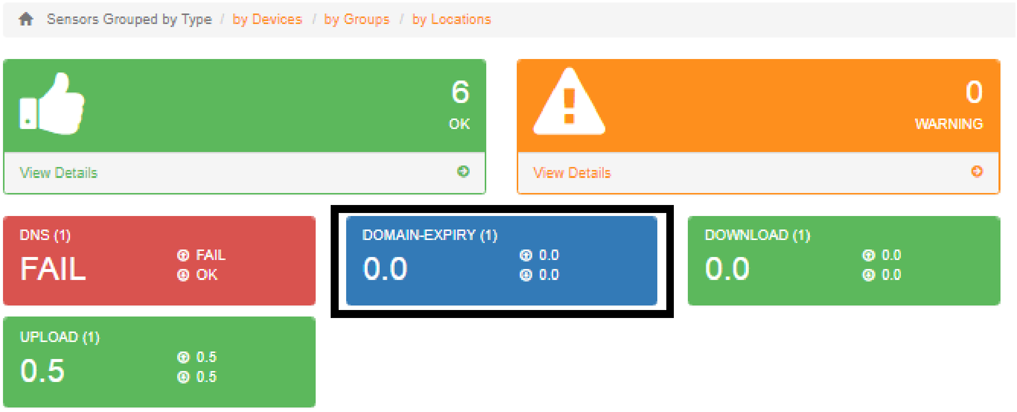
Add New Domain Name Expiry Sensor

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
```

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



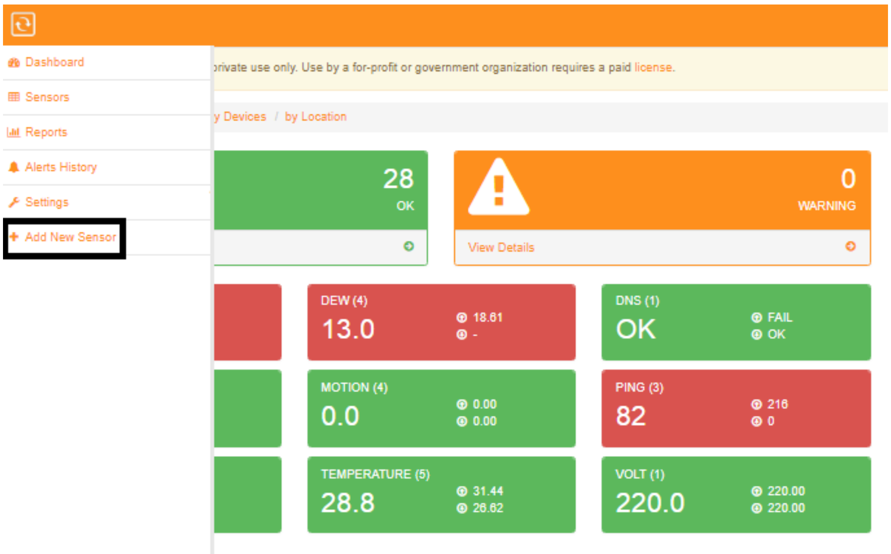
Sensors Grouped by Type / by Devices / by Groups / by Locations

6 OK	0 WARNING
DNS (1) FAIL — FAIL / OK	DOMAIN-EXPIRY (1) 0.0 — 0.0 / 0.0
DOWNLOAD (1) 0.0 — 0.0 / 0.0	UPLOAD (1) 0.5 — 0.5 / 0.5

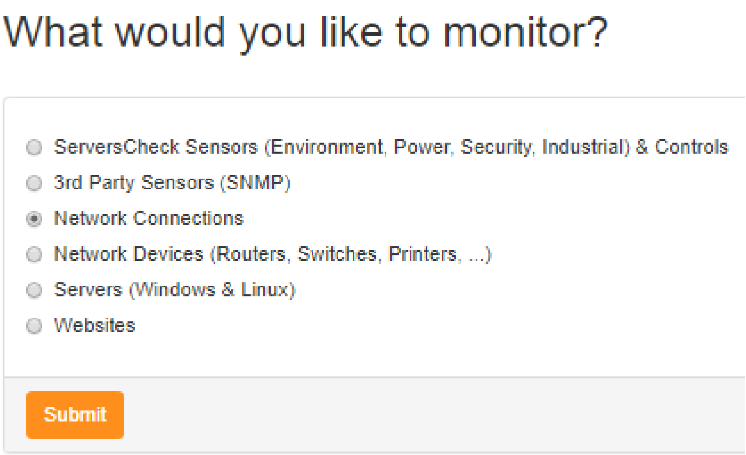
4.2.5. Adding TCP Port Check

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

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



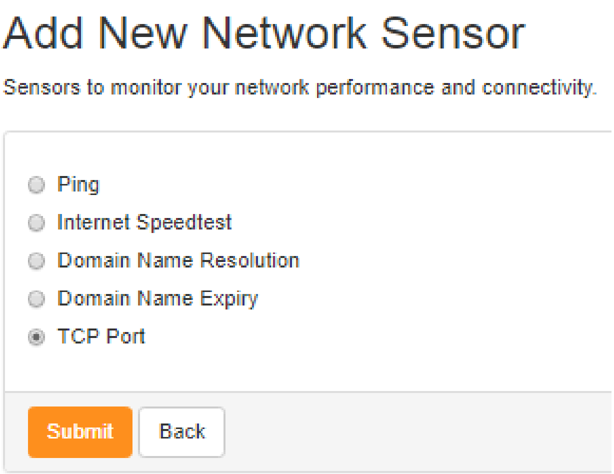
2. Select Network Connections.



What would you like to monitor?

○ ServersCheck Sensors (Environment, Power, Security, Industrial) & Controls
○ 3rd Party Sensors (SNMP)
● Network Connections
○ Network Devices (Routers, Switches, Printers, ...)
○ Servers (Windows & Linux)
○ Websites

3. Select TCP Port.



Add New Network Sensor

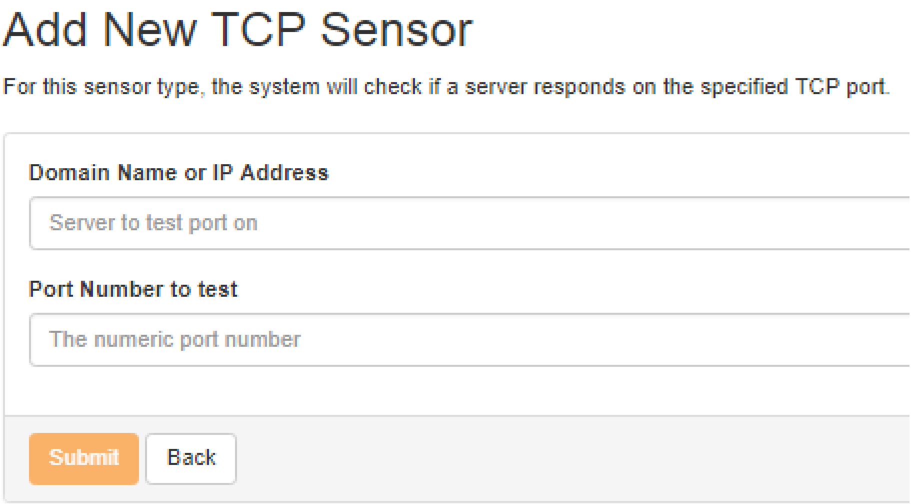
Sensors to monitor your network performance and connectivity.

○ Ping
○ Internet Speedtest
○ Domain Name Resolution
○ Domain Name Expiry
● 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.



Add New TCP Sensor

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

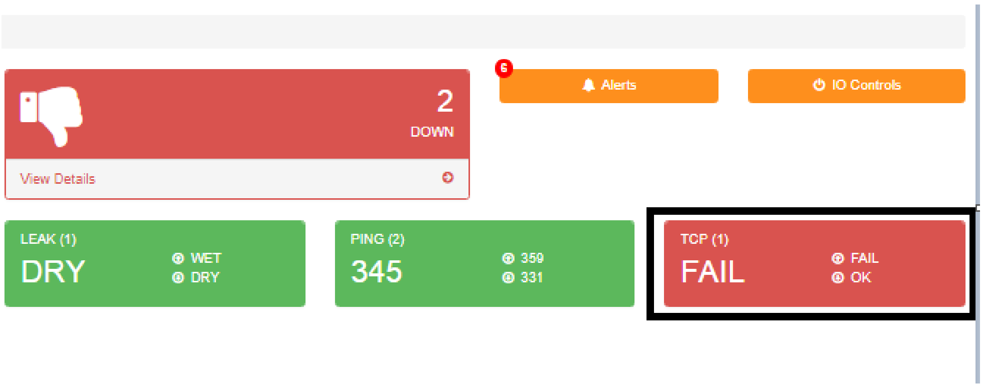
Domain Name or IP Address

Server to test port on

Port Number to test

The numeric port number

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



LEAK (1) DRY — WET, DRY

PING (2) 345 — 359, 331

TCP (1) FAIL — FAIL, OK

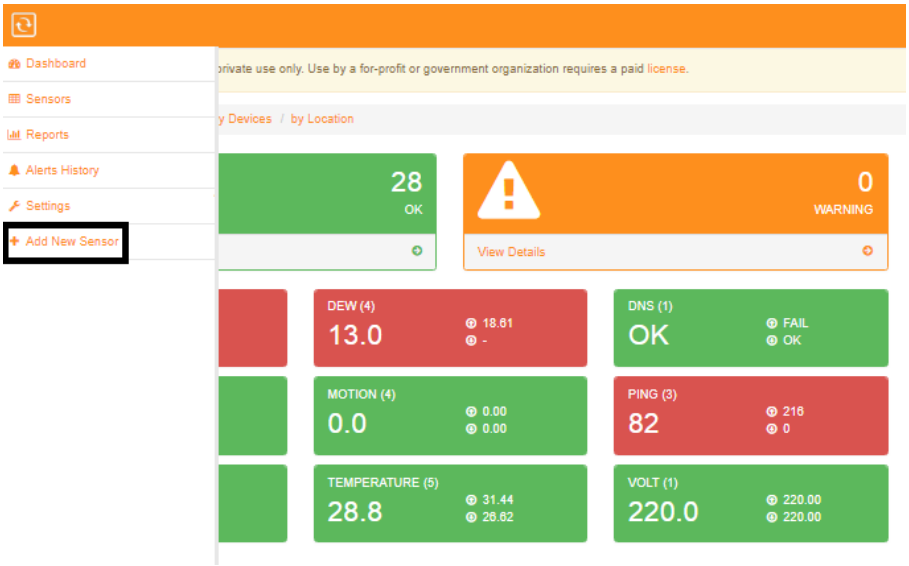
4.3. Adding Checks for Network Devices (Routers, Switches, Printers)

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

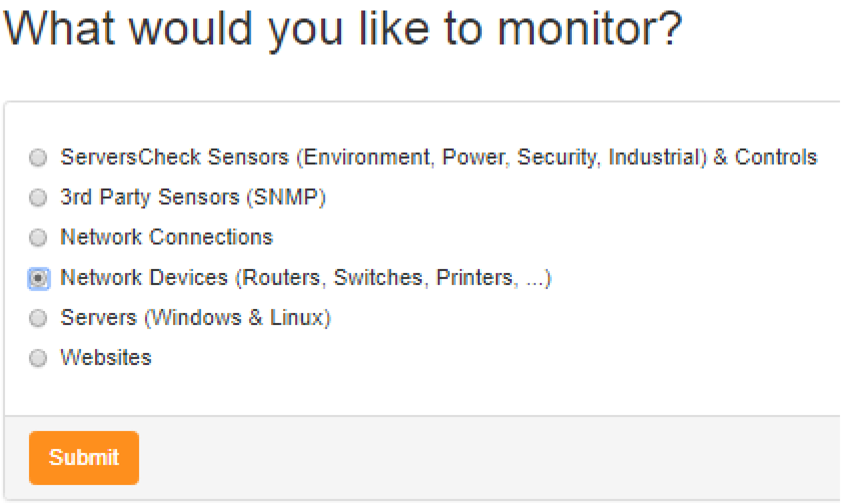
For this sensor type, the system will perform a PING check to the remote IP and measure its response time in ms (milliseconds).

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



rivate use only. Use by a for-profit or government organization requires a paid license.

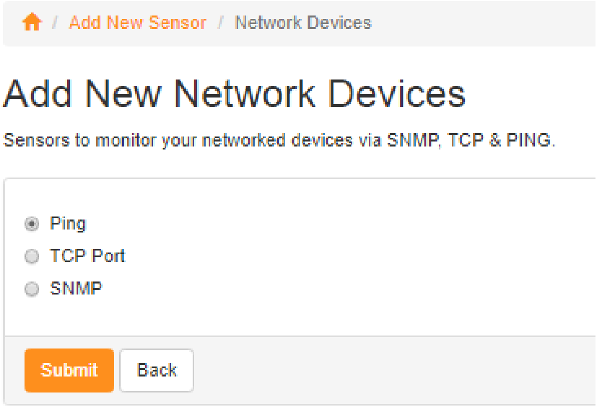
2. Select Network Devices.



What would you like to monitor?

○ ServersCheck Sensors (Environment, Power, Security, Industrial) & Controls
○ 3rd Party Sensors (SNMP)
○ Network Connections
● Network Devices (Routers, Switches, Printers, ...)
○ Servers (Windows & Linux)
○ Websites

3. Select PING.

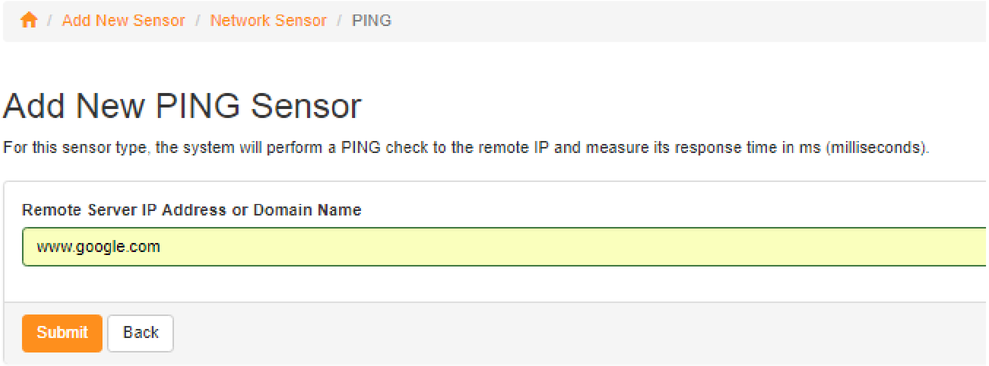


Add New Network Devices

Sensors to monitor your networked devices via SNMP, TCP & PING.

● Ping
○ TCP Port
○ SNMP

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



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).

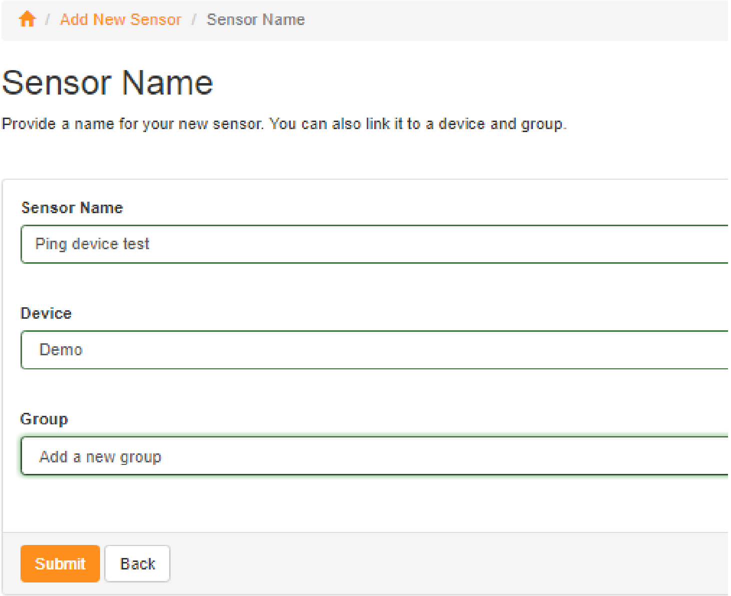
Remote Server IP Address or Domain Name: www.google.com

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: Ping device test

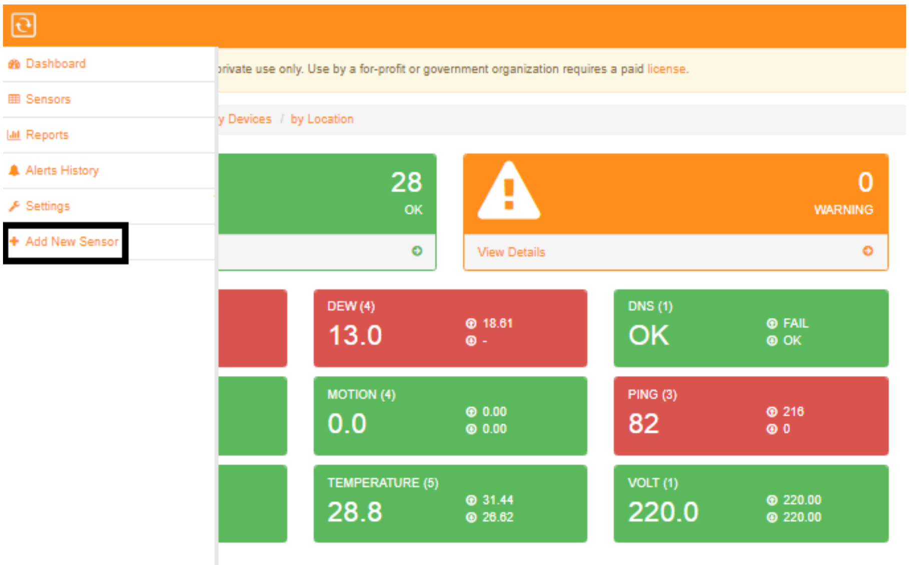
Device: Demo

Group: Add a new group

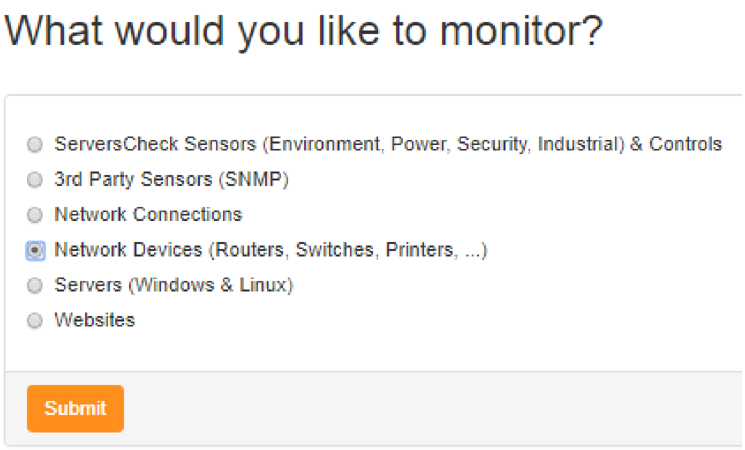
4.3.2. Adding Network Devices via TCP Port Check

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.

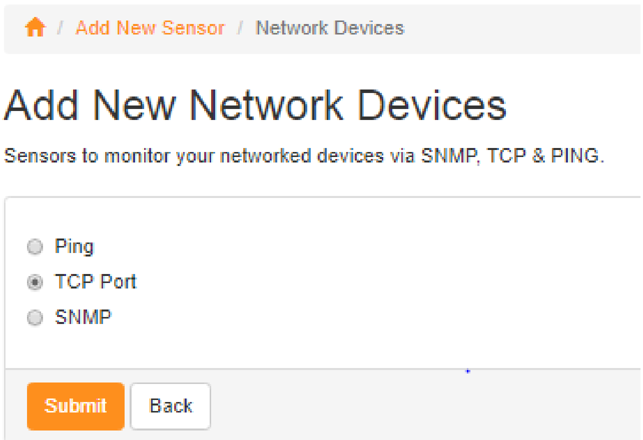


What would you like to monitor?

○ ServersCheck Sensors (Environment, Power, Security, Industrial) & Controls
○ 3rd Party Sensors (SNMP)
○ Network Connections
● Network Devices (Routers, Switches, Printers, ...)
○ Servers (Windows & Linux)
○ Websites

Submit

3. Select TCP Port.



/ Add New Sensor / Network Devices

Add New Network Devices

Sensors to monitor your networked devices via SNMP, TCP & PING.

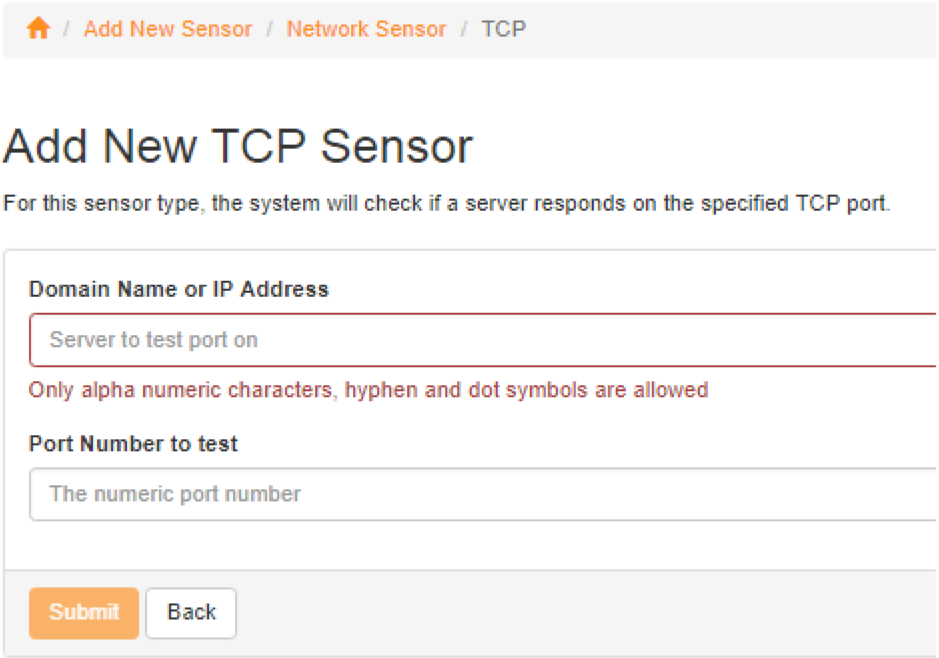
○ Ping
● TCP Port
○ SNMP

Submit Back

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.



🏠 / 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

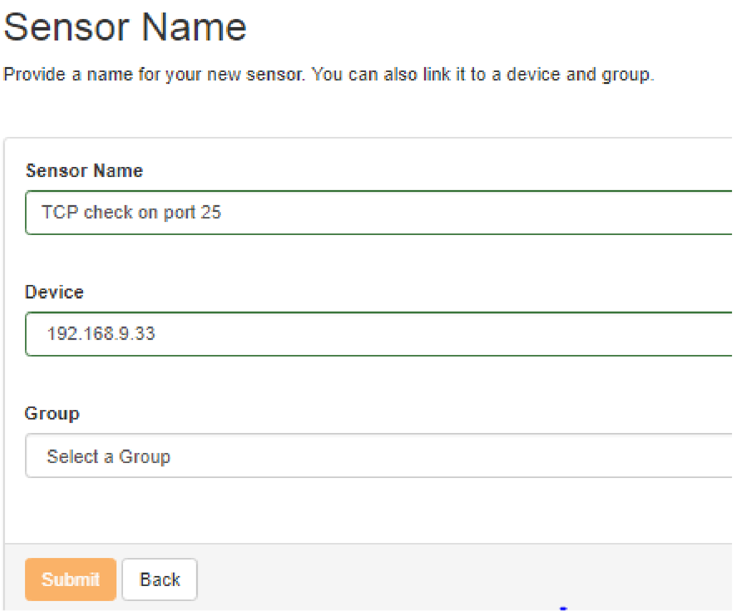
The numeric port number

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

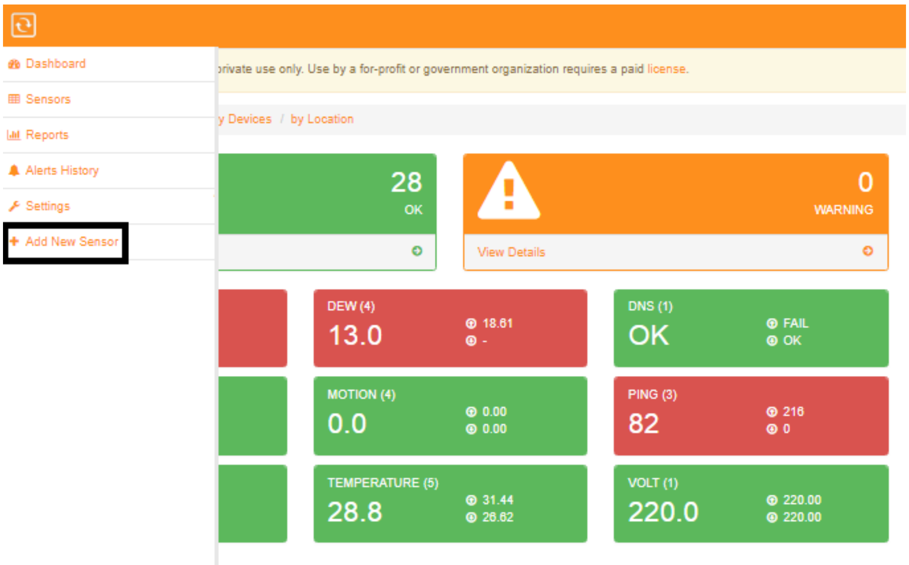
Group

Select a Group

4.3.3. Adding Network Devices via SNMP Check

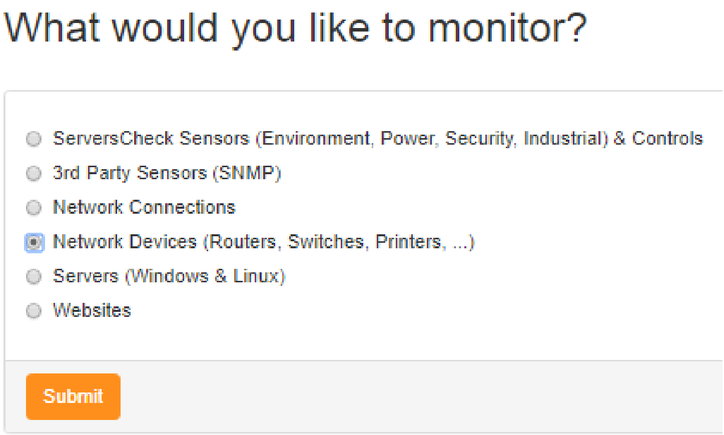
The system will scan your device using SNMP and detect any numeric values.

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



rivate use only. Use by a for-profit or government organization requires a paid license.

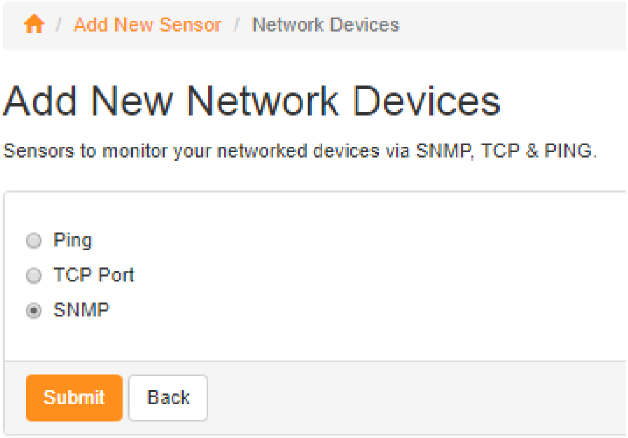
2. Select Network Devices.



What would you like to monitor?

○ ServersCheck Sensors (Environment, Power, Security, Industrial) & Controls
○ 3rd Party Sensors (SNMP)
○ Network Connections
● Network Devices (Routers, Switches, Printers, ...)
○ Servers (Windows & Linux)
○ Websites

3. Select SNMP.



Add New Sensor / Network Devices

Add New Network Devices

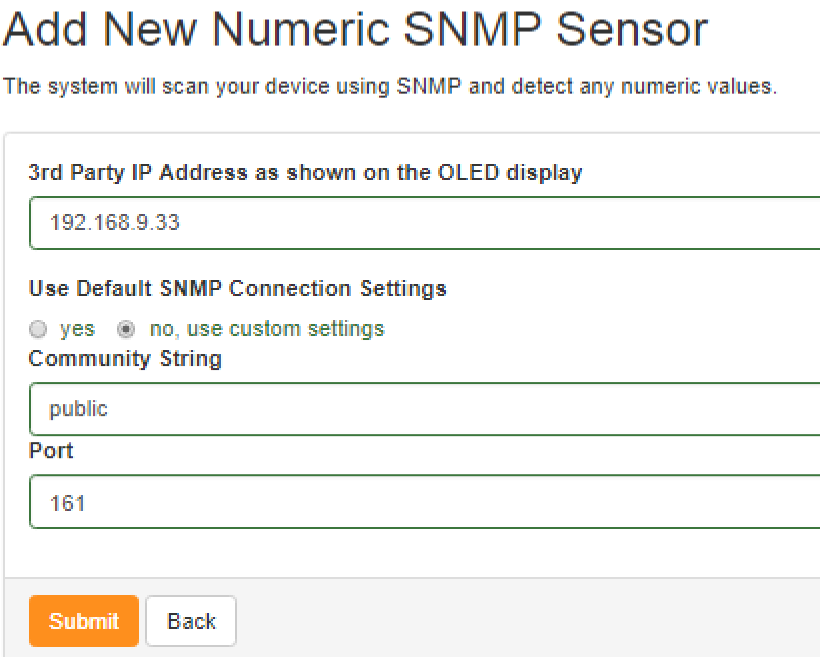
Sensors to monitor your networked devices via SNMP, TCP & PING.

○ Ping
○ TCP Port
● SNMP

4. 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

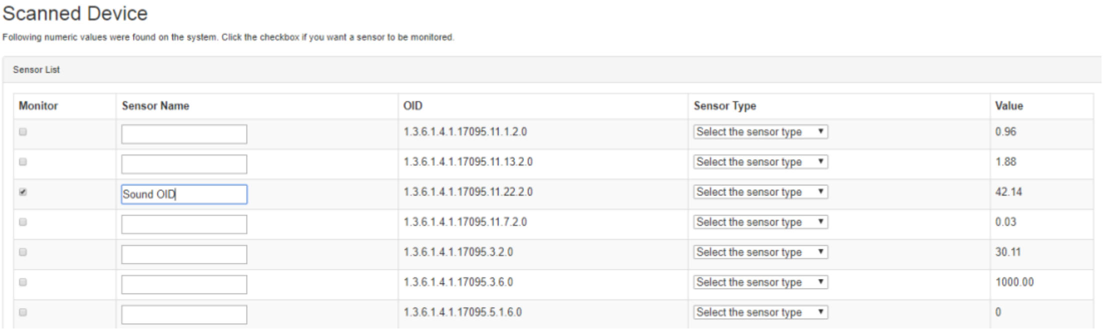
Community String

public

Port

161

5. 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
□		1.3.6.1.4.1.17095.11.1.2.0	Select the sensor type ▼	0.96
□		1.3.6.1.4.1.17095.11.13.2.0	Select the sensor type ▼	1.88
☑	Sound OID	1.3.6.1.4.1.17095.11.22.2.0	Select the sensor type ▼	42.14
□		1.3.6.1.4.1.17095.11.7.2.0	Select the sensor type ▼	0.03
□		1.3.6.1.4.1.17095.3.2.0	Select the sensor type ▼	30.11
□		1.3.6.1.4.1.17095.3.6.0	Select the sensor type ▼	1000.00
□		1.3.6.1.4.1.17095.5.1.6.0	Select the sensor type ▼	0

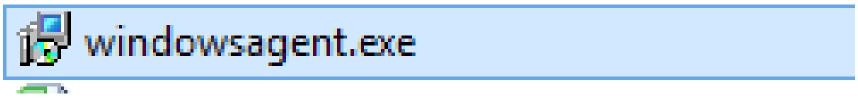
4.4. Adding Checks for Servers (Windows & Linux)

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

Installing the Windows Agent on a Windows Remote System

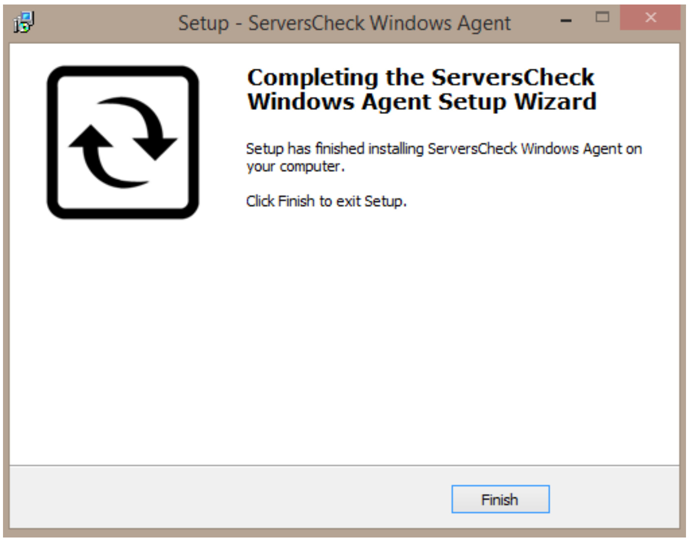
a. Download the Windows Agent from the link https://serverscheck.com/support/downloads.asp

b. Run the windowsagent.exe and Install. You need to have administrative privilege on the system you will install the agent.



windowsagent.exe

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

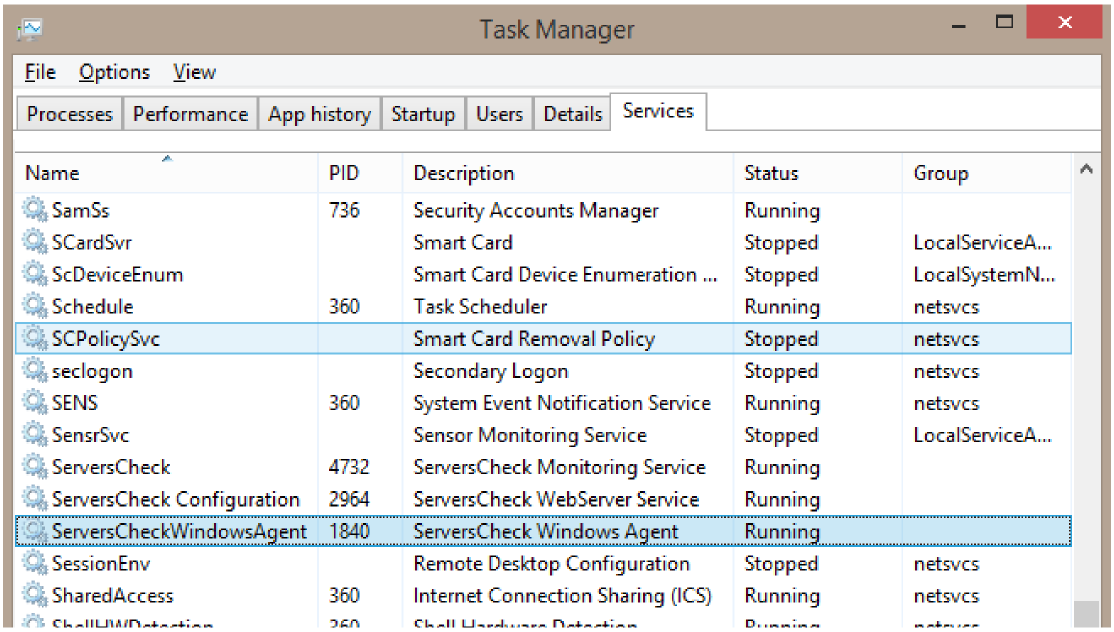


Completing the ServersCheck Windows Agent Setup Wizard

Setup has finished installing ServersCheck Windows Agent on your computer.

Click Finish to exit Setup.

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



Name	PID	Description	Status	Group
SamSs	736	Security Accounts Manager	Running	
SCardSvr		Smart Card	Stopped	LocalServiceA...
ScDeviceEnum		Smart Card Device Enumeration ...	Stopped	LocalSystemN...
Schedule	360	Task Scheduler	Running	netsvcs
SCPolicySvc		Smart Card Removal Policy	Stopped	netsvcs
seclogon		Secondary Logon	Stopped	netsvcs
SENS	360	System Event Notification Service	Running	netsvcs
SensrSvc		Sensor Monitoring Service	Stopped	LocalServiceA...
ServersCheck	4732	ServersCheck Monitoring Service	Running	
ServersCheck Configuration	2964	ServersCheck WebServer Service	Running	
ServersCheckWindowsAgent	1840	ServersCheck Windows Agent	Running	
SessionEnv		Remote Desktop Configuration	Stopped	netsvcs
SharedAccess	360	Internet Connection Sharing (ICS)	Running	netsvcs
ShellHWDetection	360	Shell Hardware Detection	Running	netsvcs

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.

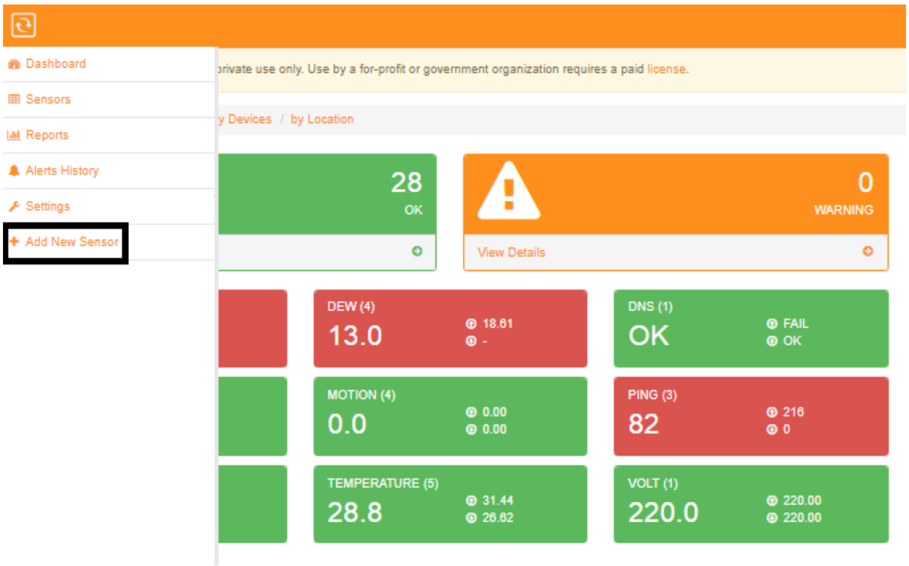
e. Linux Agent should run as a service on the background.

4.4.1. Adding Checks for Windows Servers

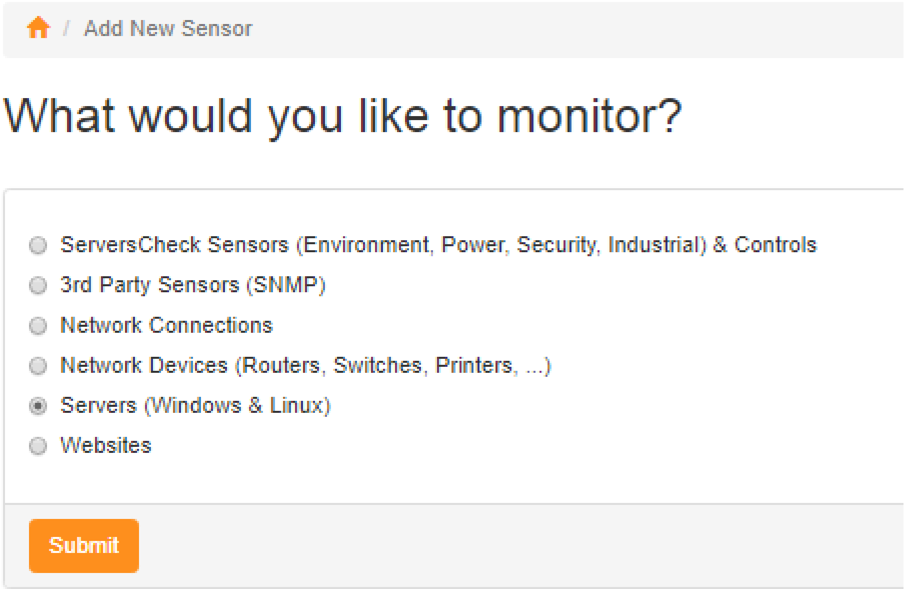
This check type requires the free Windows Agent to be installed on the remote system being monitored. The Windows Agent can be downloaded from this link - https://serverscheck.com/support/downloads.asp

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

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


rivate use only. Use by a for-profit or government organization requires a paid license.

2. Select Servers.

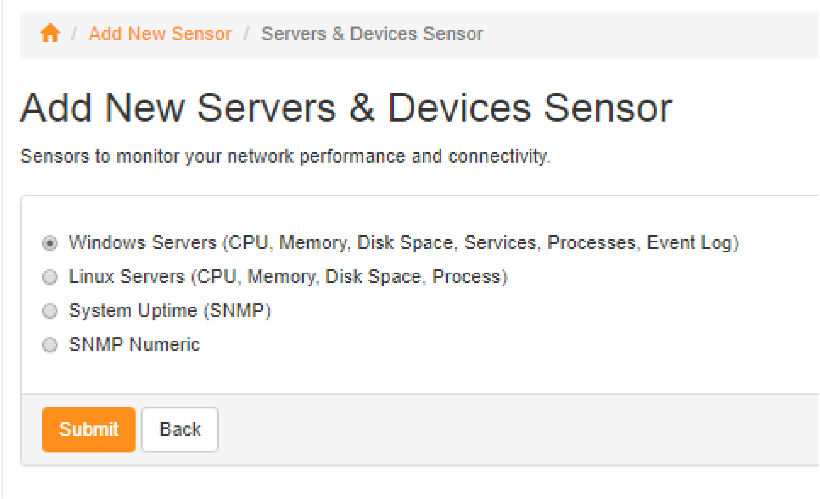


Add New Sensor

What would you like to monitor?

○ ServersCheck Sensors (Environment, Power, Security, Industrial) & Controls
○ 3rd Party Sensors (SNMP)
○ Network Connections
○ Network Devices (Routers, Switches, Printers, ...)
● Servers (Windows & Linux)
○ Websites

3. Select Windows Servers.



Add New Sensor / Servers & Devices Sensor

Add New Servers & Devices Sensor

Sensors to monitor your network performance and connectivity.

● Windows Servers (CPU, Memory, Disk Space, Services, Processes, Event Log)
○ Linux Servers (CPU, Memory, Disk Space, Process)
○ System Uptime (SNMP)
○ SNMP Numeric

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

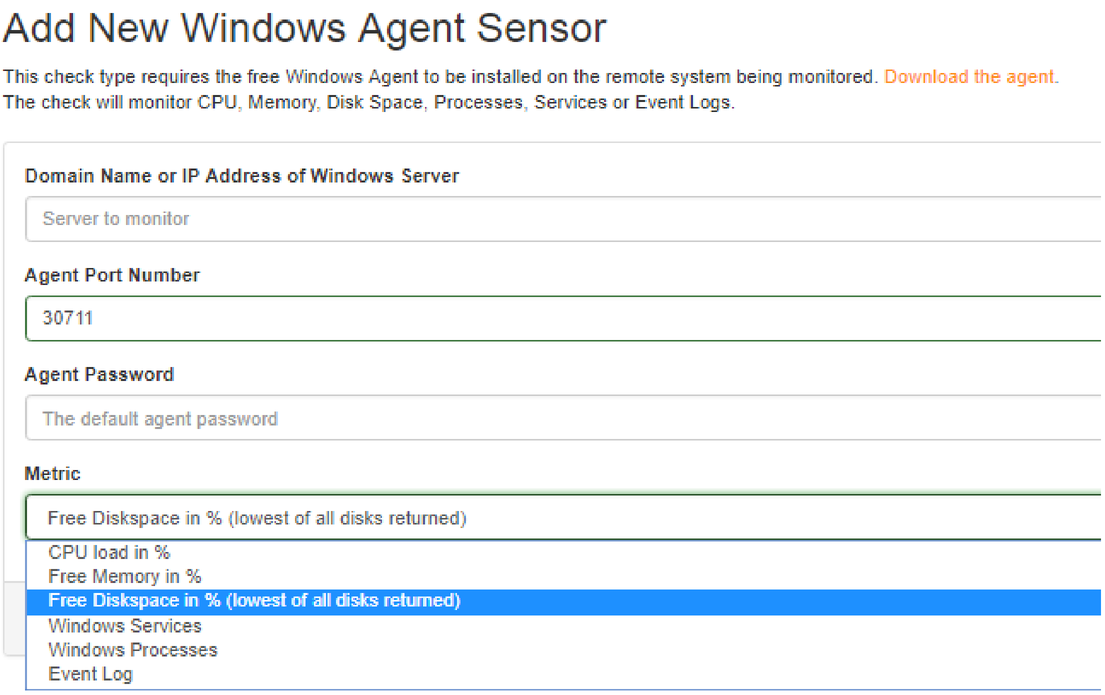
Domain Name or IP Address of Windows Server - Server to monitor.

Agent Port Number - Numeric Port number you want to monitor.
Default Port - 30711

Agent Password - default is passServerscheck

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)

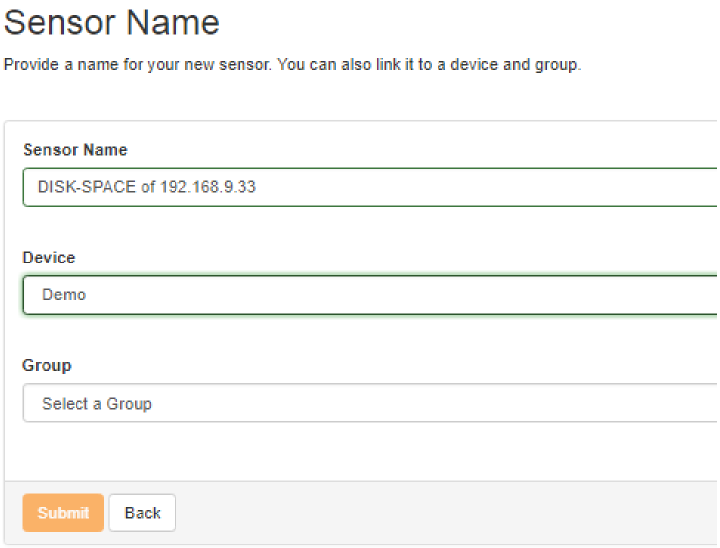
CPU load in %
Free Memory in %
Free Diskspace in % (lowest of all disks returned)
Windows Services
Windows Processes
Event Log

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

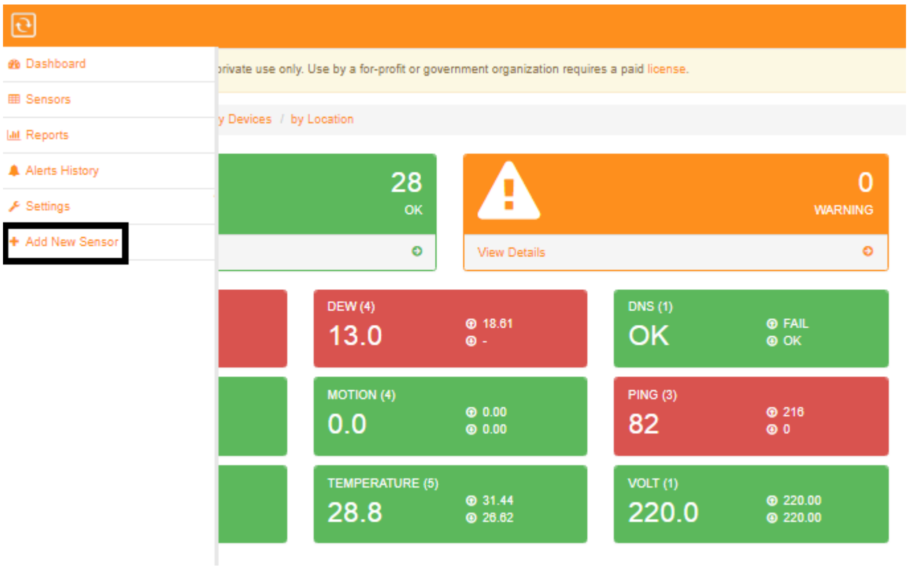
Select a Group

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

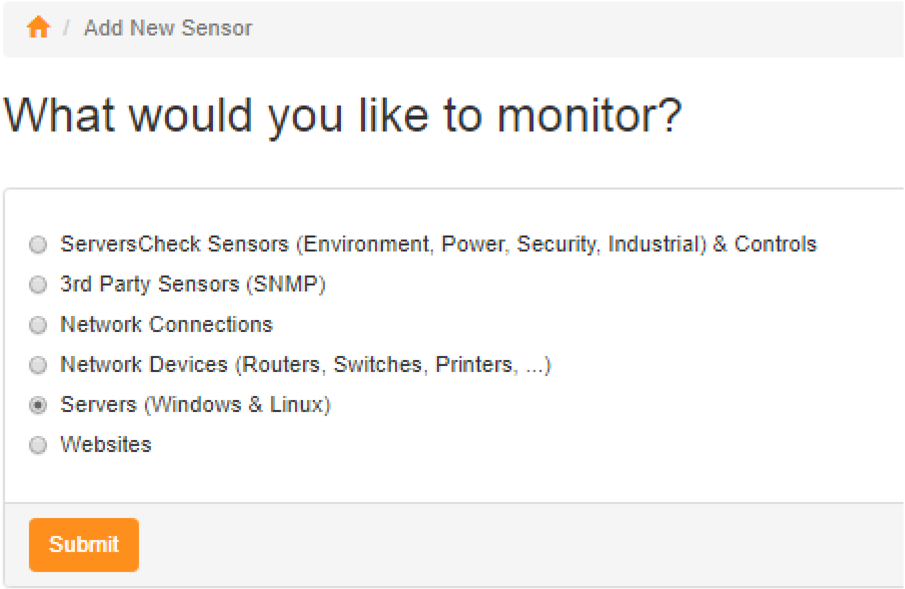
The check will monitor CPU, Memory, Disk Space or Processes state.

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



private use only. Use by a for-profit or government organization requires a paid license.

2. Select Servers.

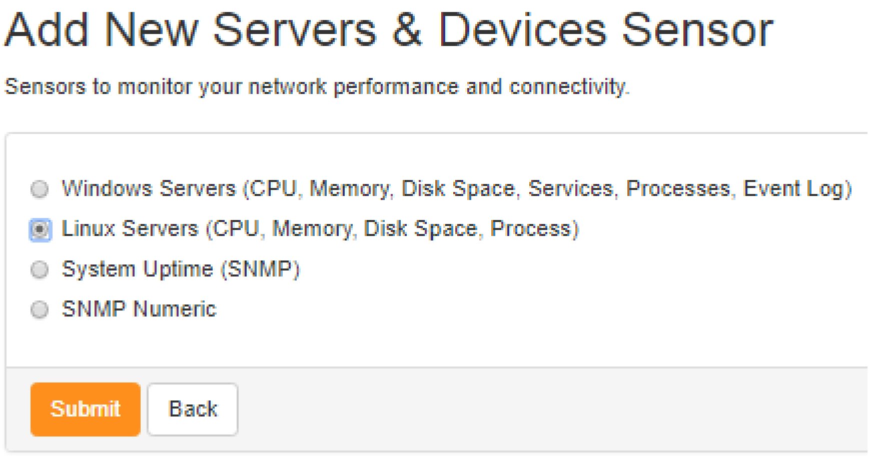


Add New Sensor

What would you like to monitor?

○ ServersCheck Sensors (Environment, Power, Security, Industrial) & Controls
○ 3rd Party Sensors (SNMP)
○ Network Connections
○ Network Devices (Routers, Switches, Printers, ...)
● Servers (Windows & Linux)
○ Websites

3. Select Linux Servers.



Add New Servers & Devices Sensor

Sensors to monitor your network performance and connectivity.

○ Windows Servers (CPU, Memory, Disk Space, Services, Processes, Event Log)
● Linux Servers (CPU, Memory, Disk Space, Process)
○ System Uptime (SNMP)
○ SNMP Numeric

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

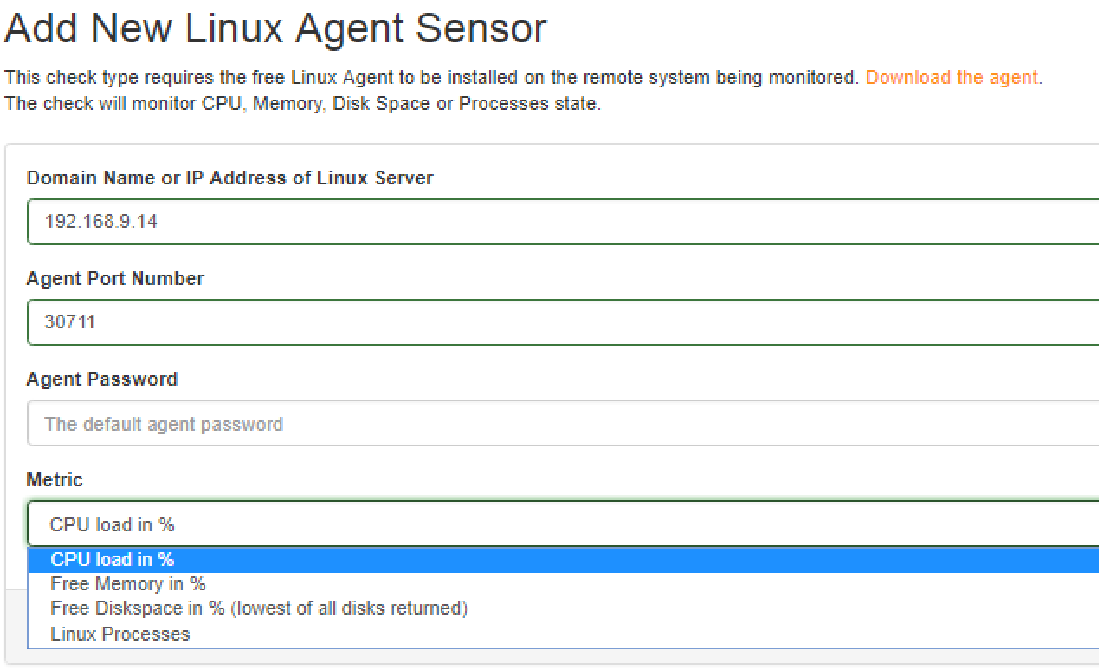
Domain Name or IP Address of Windows Server - Server to monitor.

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

Agent Password - default is passServerscheck

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

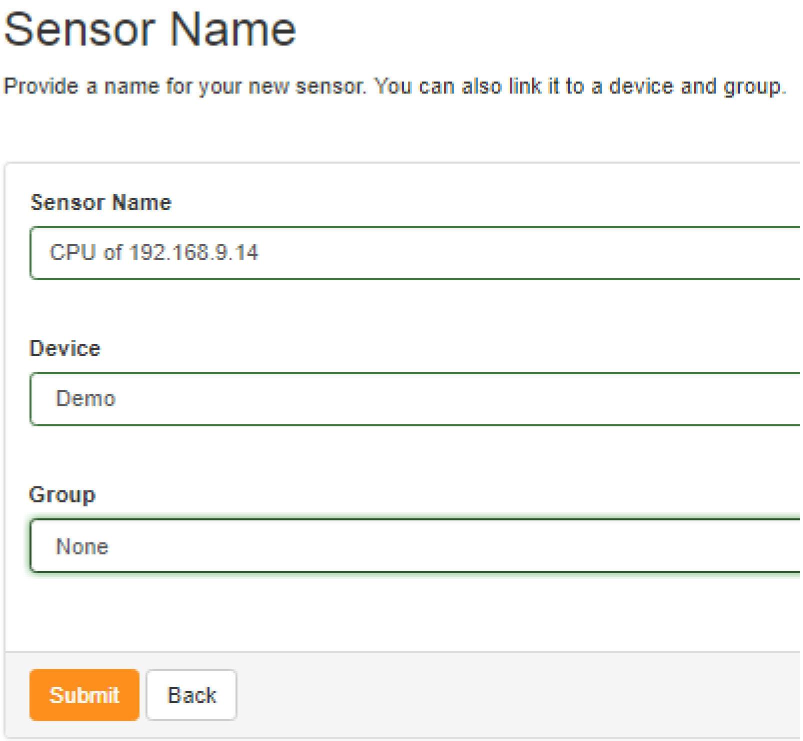
Metric
CPU load in %

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

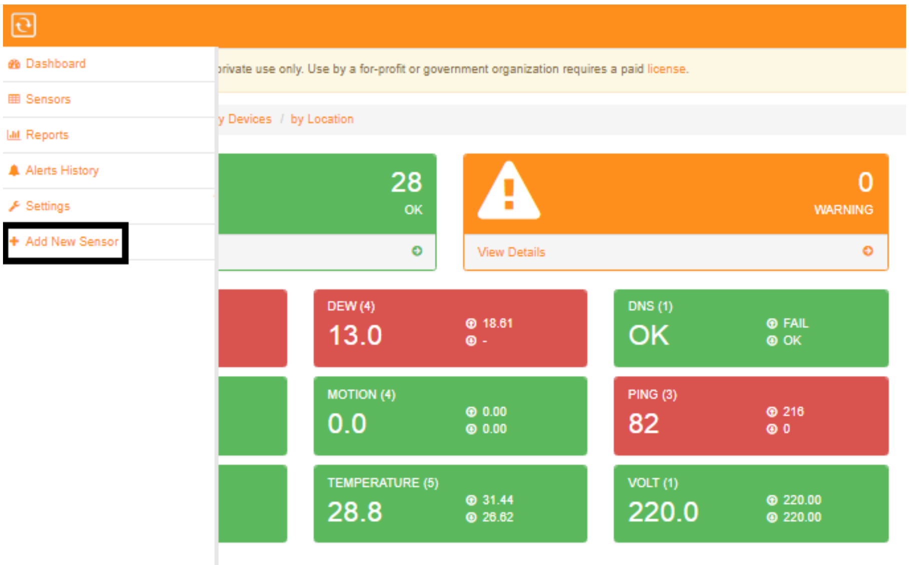
Device: Demo

Group: None

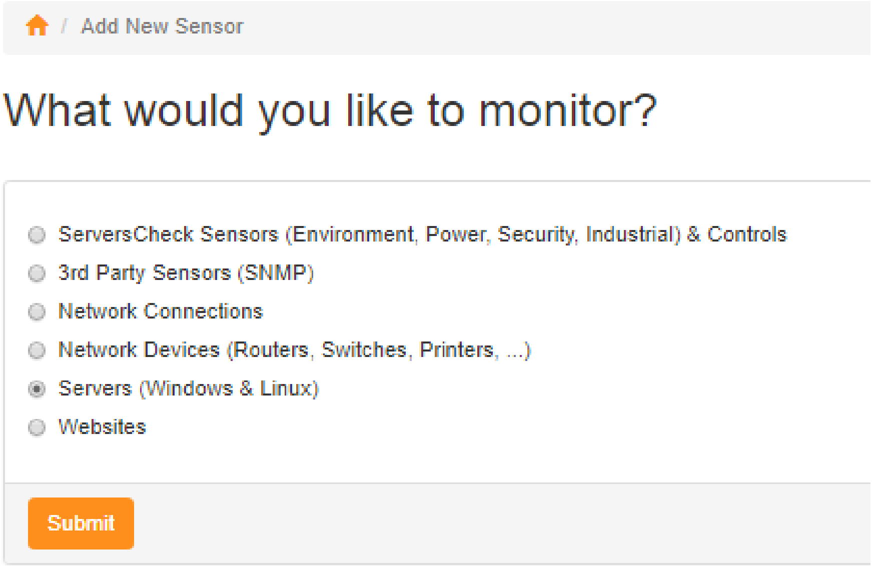
4.4.3. Adding Checks for System Uptime (SNMP)

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

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



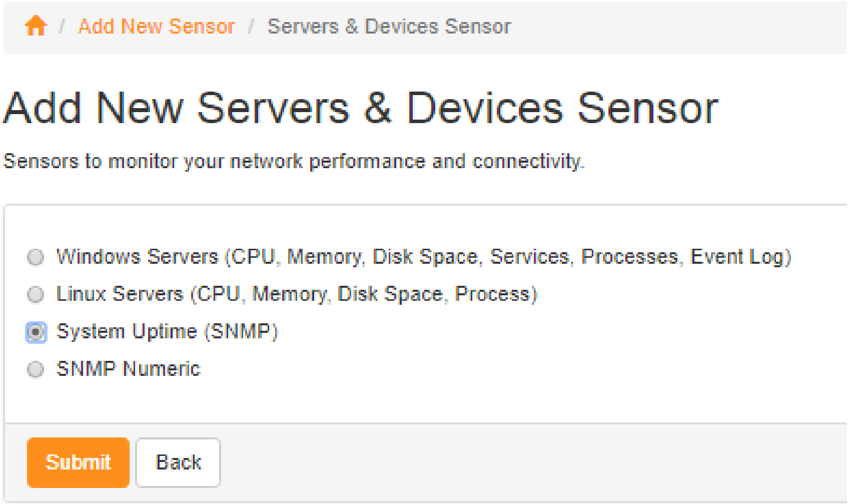
2. Select Servers.



What would you like to monitor?

○ ServersCheck Sensors (Environment, Power, Security, Industrial) & Controls
○ 3rd Party Sensors (SNMP)
○ Network Connections
○ Network Devices (Routers, Switches, Printers, ...)
● Servers (Windows & Linux)
○ Websites

3. Select System Uptime (SNMP).



Add New Servers & Devices Sensor

Sensors to monitor your network performance and connectivity.

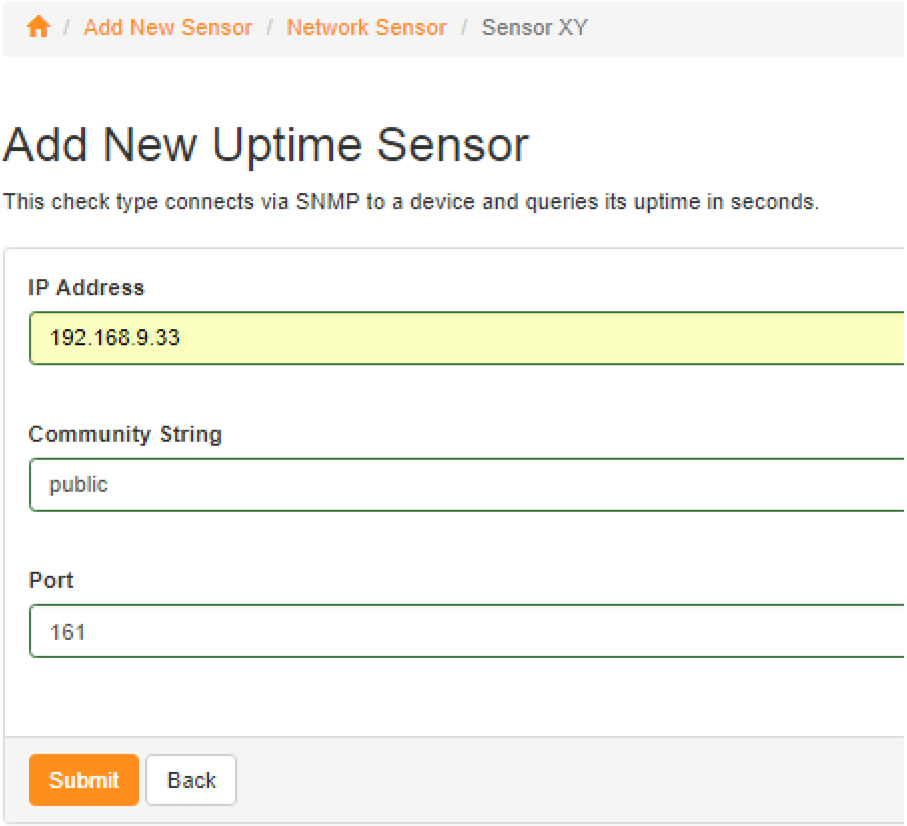
○ Windows Servers (CPU, Memory, Disk Space, Services, Processes, Event Log)
○ Linux Servers (CPU, Memory, Disk Space, Process)
● System Uptime (SNMP)
○ SNMP Numeric

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



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

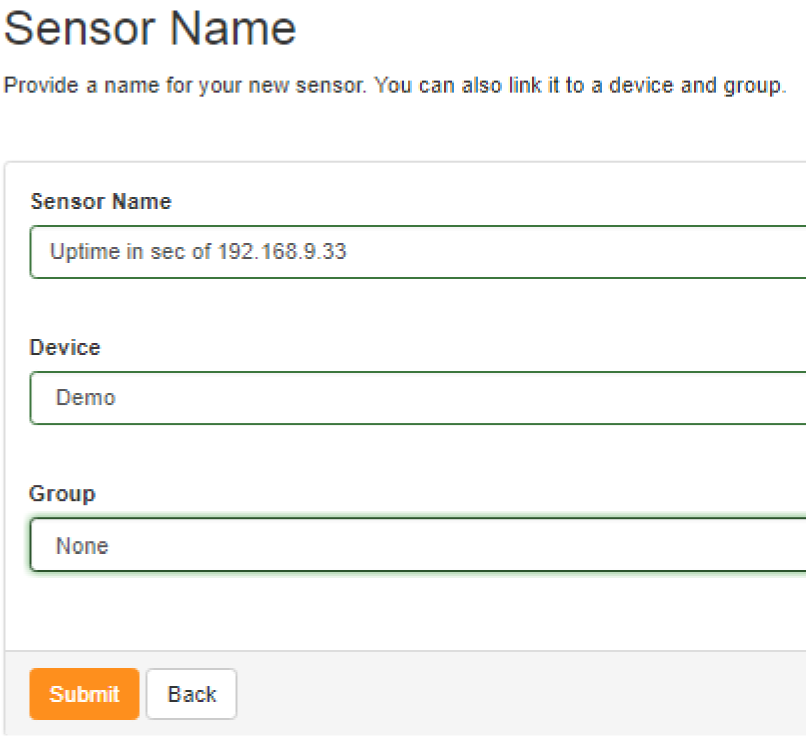
Port: 161

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

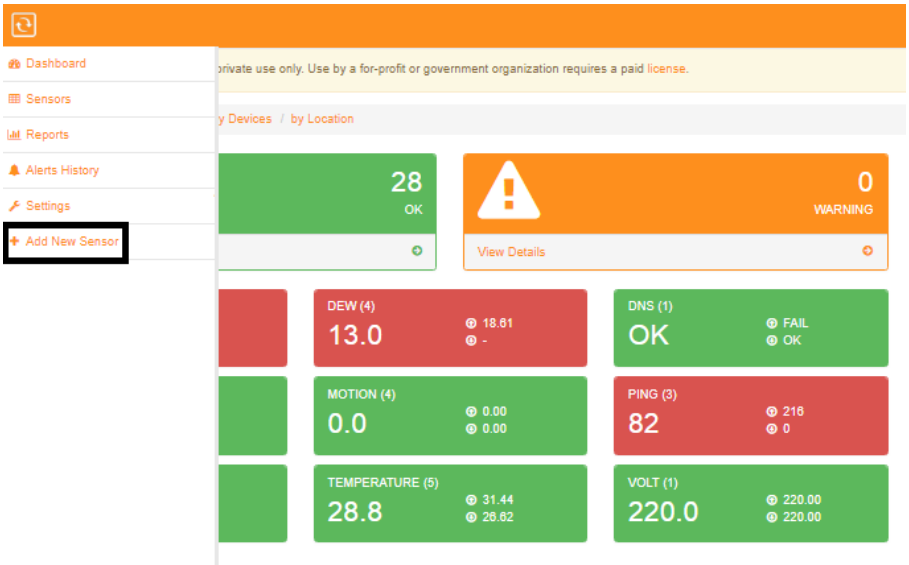
Device: Demo

Group: None

4.4.4. Adding Checks for SNMP Numeric

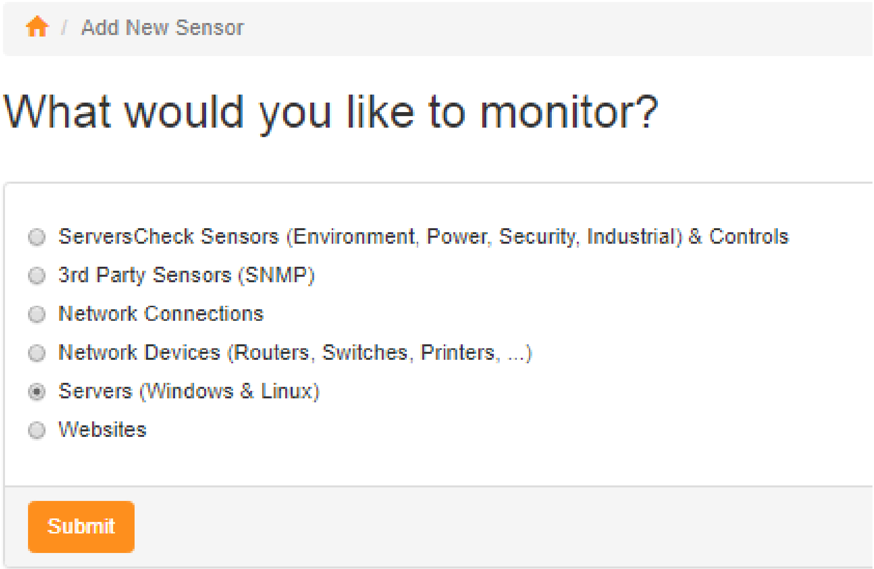
The system will scan your device using SNMP and detect any numeric values.

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



private use only. Use by a for-profit or government organization requires a paid license.

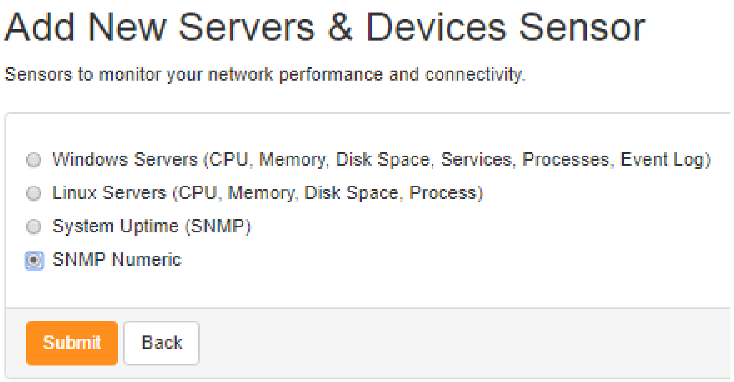
2. Select Servers.



What would you like to monitor?

○ ServersCheck Sensors (Environment, Power, Security, Industrial) & Controls
○ 3rd Party Sensors (SNMP)
○ Network Connections
○ Network Devices (Routers, Switches, Printers, ...)
● Servers (Windows & Linux)
○ Websites

3. Select SNMP Numeric.



Add New Servers & Devices Sensor

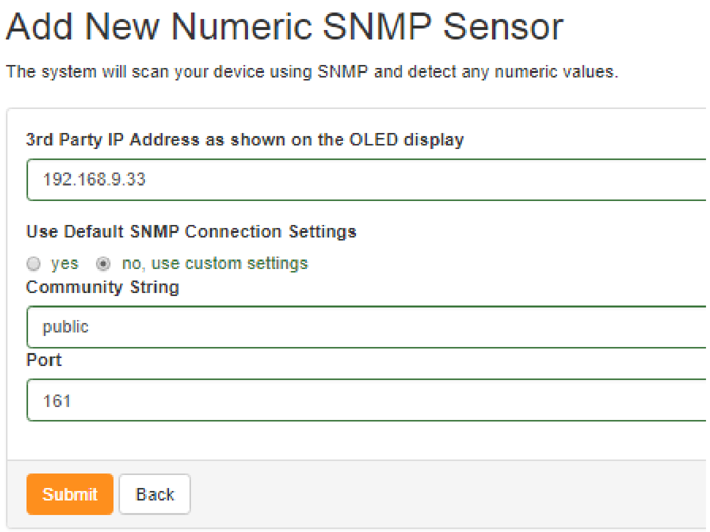
Sensors to monitor your network performance and connectivity.

○ Windows Servers (CPU, Memory, Disk Space, Services, Processes, Event Log)
○ Linux Servers (CPU, Memory, Disk Space, Process)
○ System Uptime (SNMP)
● SNMP Numeric

4. 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.

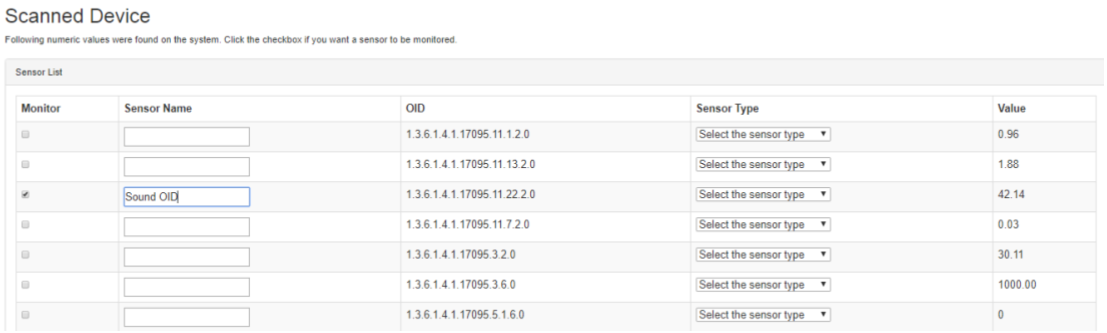
3rd Party IP Address as shown on the OLED display
192.168.9.33

Use Default SNMP Connection Settings
○ yes ● no, use custom settings

Community String
public

Port
161

5. 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
□		1.3.6.1.4.1.17095.11.1.2.0	Select the sensor type ▾	0.96
□		1.3.6.1.4.1.17095.11.13.2.0	Select the sensor type ▾	1.88
☑	Sound OID	1.3.6.1.4.1.17095.11.22.2.0	Select the sensor type ▾	42.14
□		1.3.6.1.4.1.17095.11.7.2.0	Select the sensor type ▾	0.03
□		1.3.6.1.4.1.17095.3.2.0	Select the sensor type ▾	30.11
□		1.3.6.1.4.1.17095.3.6.0	Select the sensor type ▾	1000.00
□		1.3.6.1.4.1.17095.5.1.6.0	Select the sensor type ▾	0

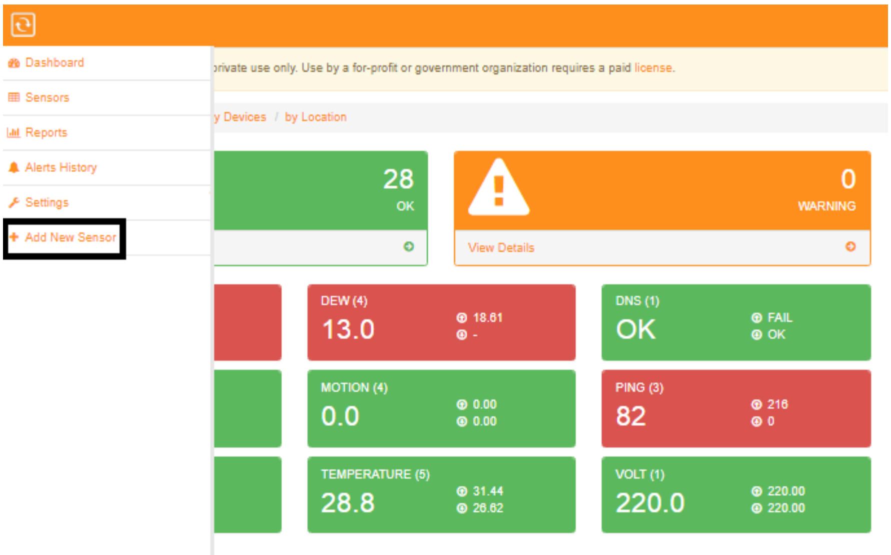
4.5. Adding Checks for Websites

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

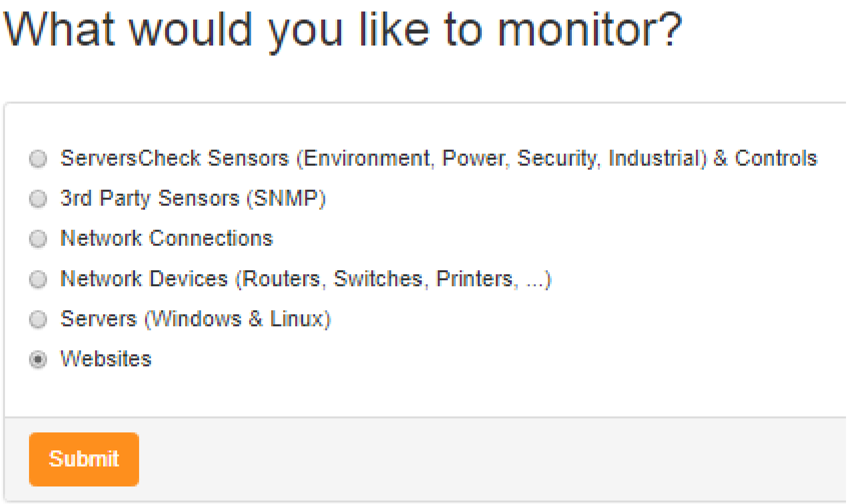
4.5.1. Adding SSL Certificate Validity Check

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**.



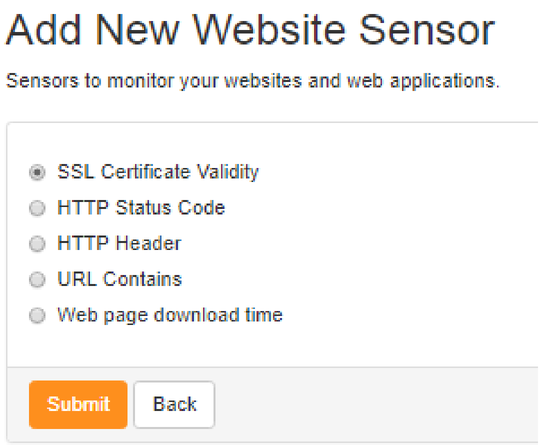
2. Select Websites.



What would you like to monitor?

○ ServersCheck Sensors (Environment, Power, Security, Industrial) & Controls
○ 3rd Party Sensors (SNMP)
○ Network Connections
○ Network Devices (Routers, Switches, Printers, ...)
○ Servers (Windows & Linux)
● Websites

3. Select SSL Certificate Validity.

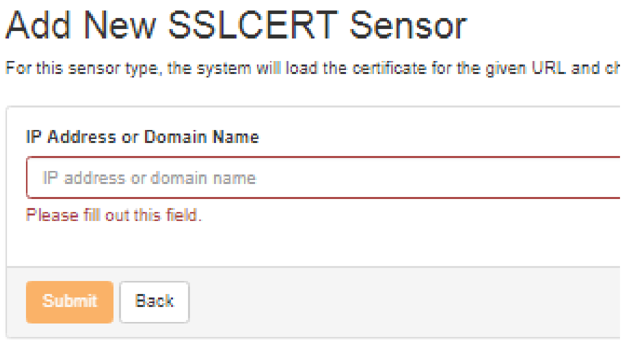


Add New Website Sensor

Sensors to monitor your websites and web applications.

● SSL Certificate Validity
○ HTTP Status Code
○ HTTP Header
○ URL Contains
○ Web page download time

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

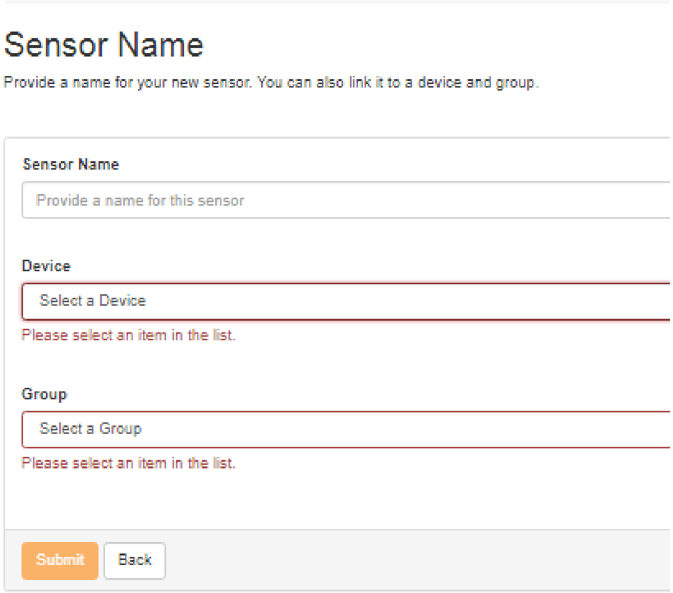
Please fill out this field.

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

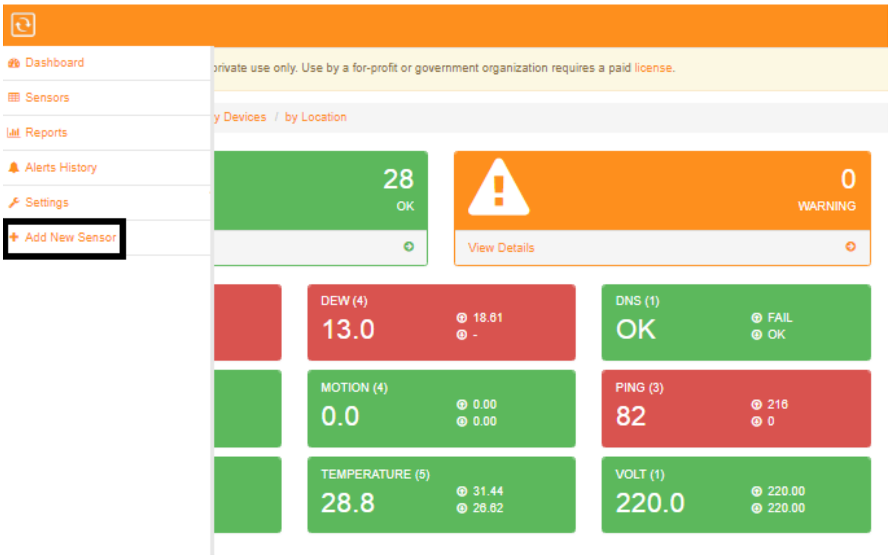
Select a Group

Please select an item in the list.

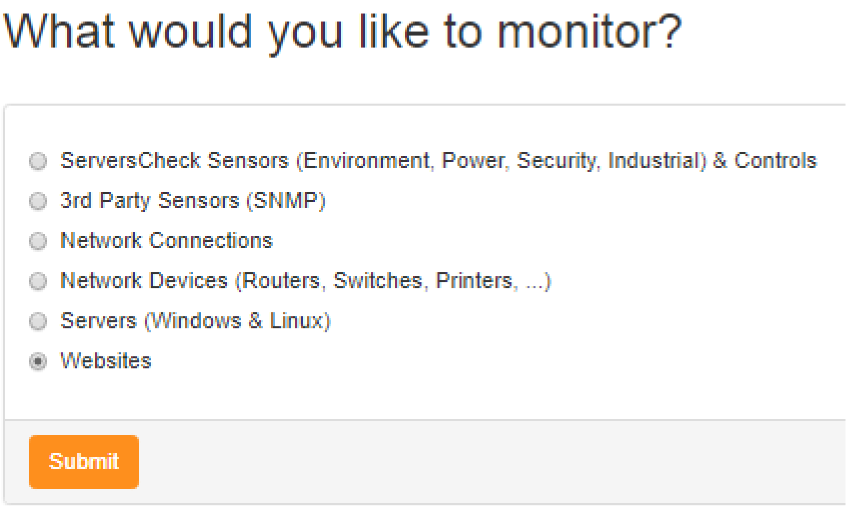
4.5.2. Adding HTTP Status Code Check

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**.



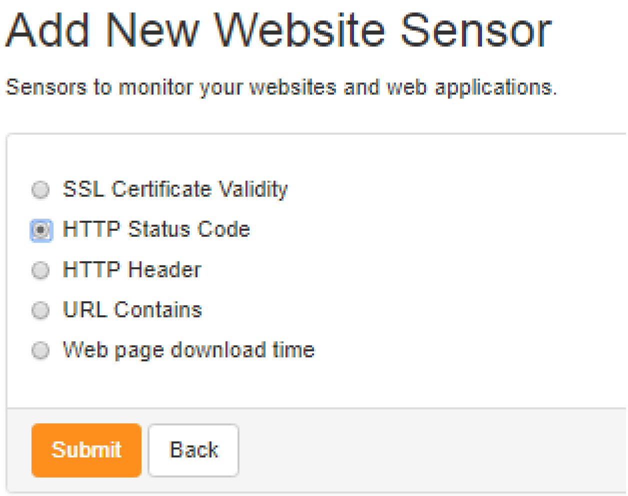
2. Select Websites.



What would you like to monitor?

○ ServersCheck Sensors (Environment, Power, Security, Industrial) & Controls
○ 3rd Party Sensors (SNMP)
○ Network Connections
○ Network Devices (Routers, Switches, Printers, ...)
○ Servers (Windows & Linux)
● Websites

3. Select HTTP Status Code.



Add New Website Sensor

Sensors to monitor your websites and web applications.

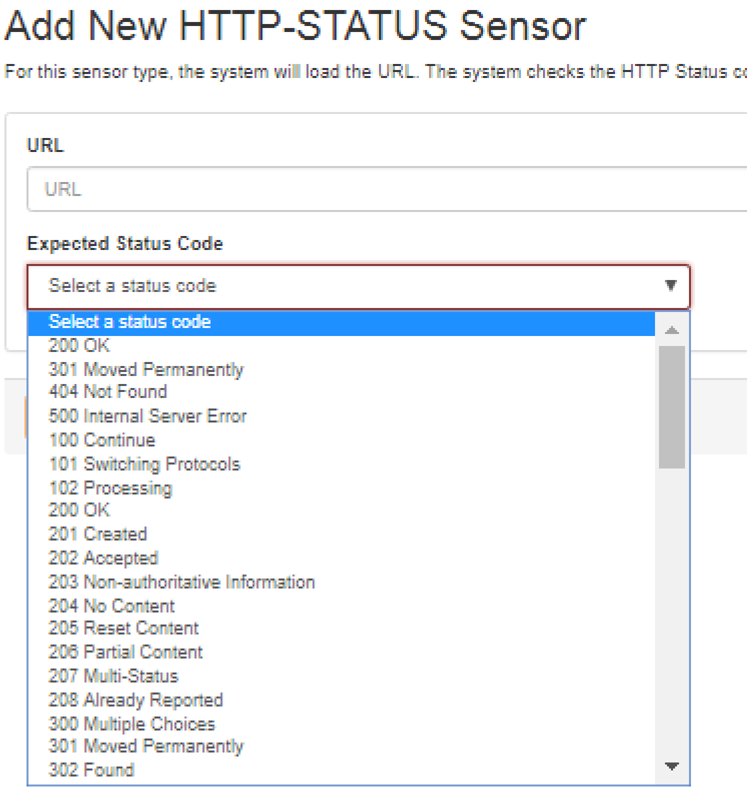
○ SSL Certificate Validity
● HTTP Status Code
○ HTTP Header
○ URL Contains
○ Web page download time

Submit Back

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 c

URL

URL

Expected Status Code

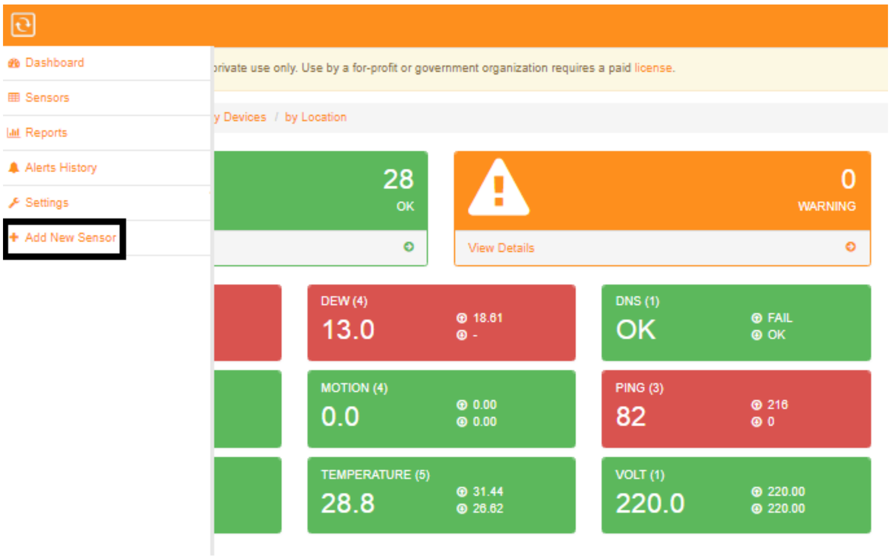
Select a status code ▼

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

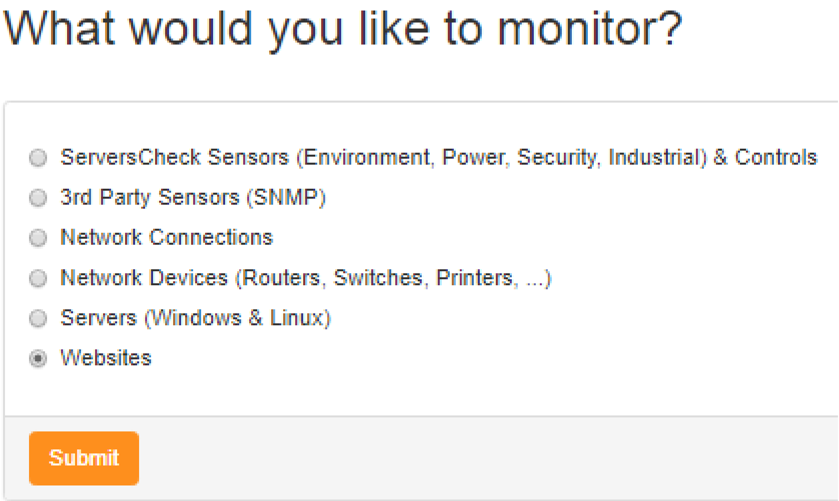
For this sensor type, the system will connect to the provided URL and load the HTTP Headers returned by the webserver. It will then see if the provided text can be found in the headers.

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



rivate use only. Use by a for-profit or government organization requires a paid license.

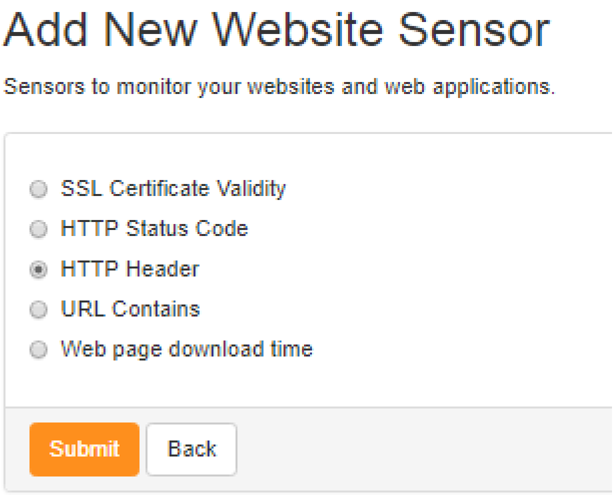
2. Select Websites.



What would you like to monitor?

○ ServersCheck Sensors (Environment, Power, Security, Industrial) & Controls
○ 3rd Party Sensors (SNMP)
○ Network Connections
○ Network Devices (Routers, Switches, Printers, ...)
○ Servers (Windows & Linux)
● Websites

3. Select HTTP Header.



Add New Website Sensor

Sensors to monitor your websites and web applications.

○ SSL Certificate Validity
○ HTTP Status Code
● HTTP Header
○ URL Contains
○ Web page download time

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

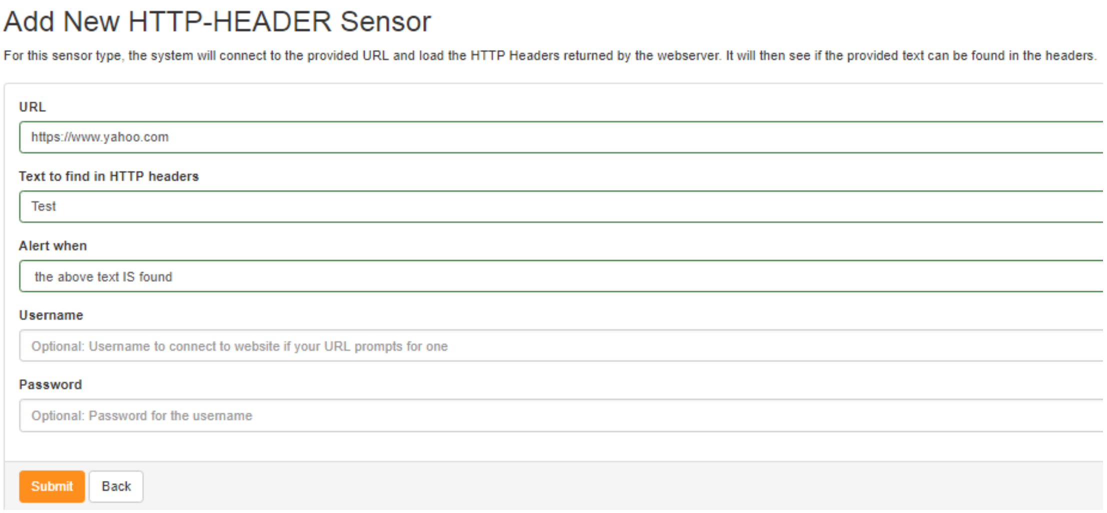
URL - Input the URL you want to check.

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

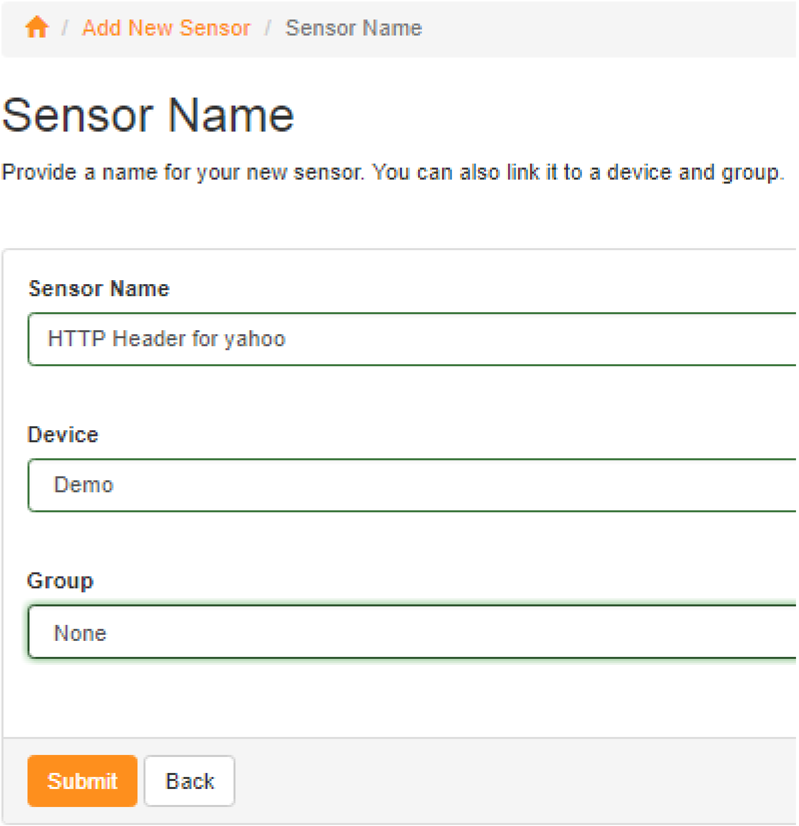
Password
Optional: Password for the username

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.



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

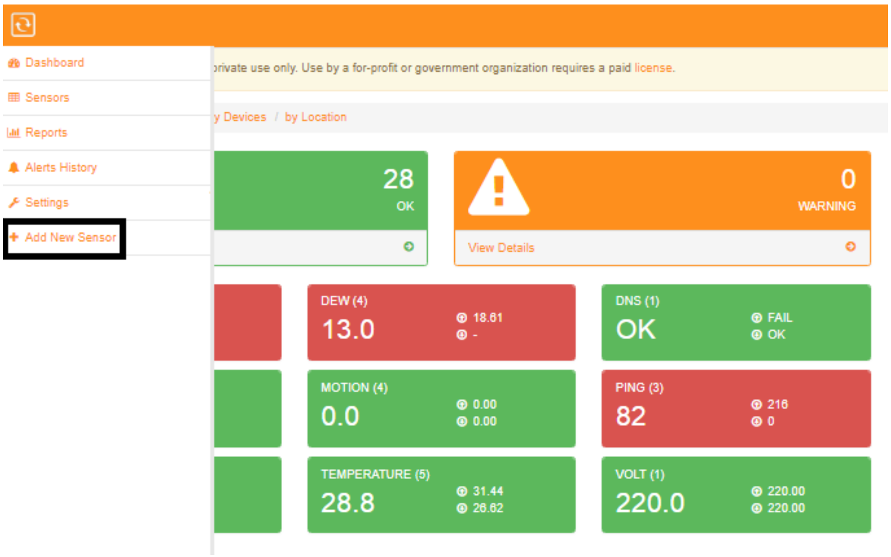
Device: Demo

Group: None

4.5.4. Adding URL Contains Check

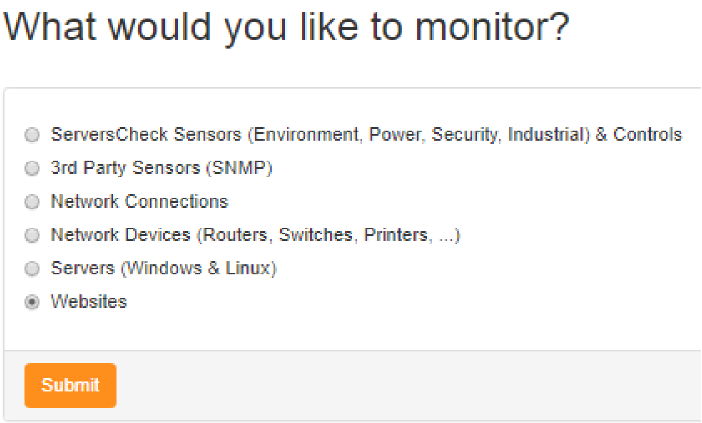
For this sensor type, the system will load the URL. It will scan the page to see if the given text can be found or not.

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



rivate use only. Use by a for-profit or government organization requires a paid license.

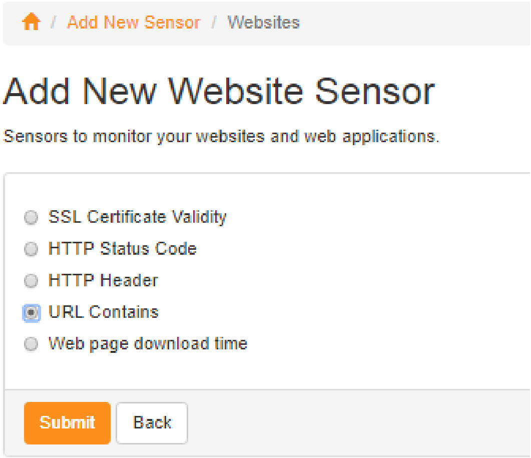
2. Select Websites.



What would you like to monitor?

○ ServersCheck Sensors (Environment, Power, Security, Industrial) & Controls
○ 3rd Party Sensors (SNMP)
○ Network Connections
○ Network Devices (Routers, Switches, Printers, ...)
○ Servers (Windows & Linux)
● Websites

3. Select URL Contains.



Add New Website Sensor

Sensors to monitor your websites and web applications.

○ SSL Certificate Validity
○ HTTP Status Code
○ HTTP Header
● URL Contains
○ Web page download time

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

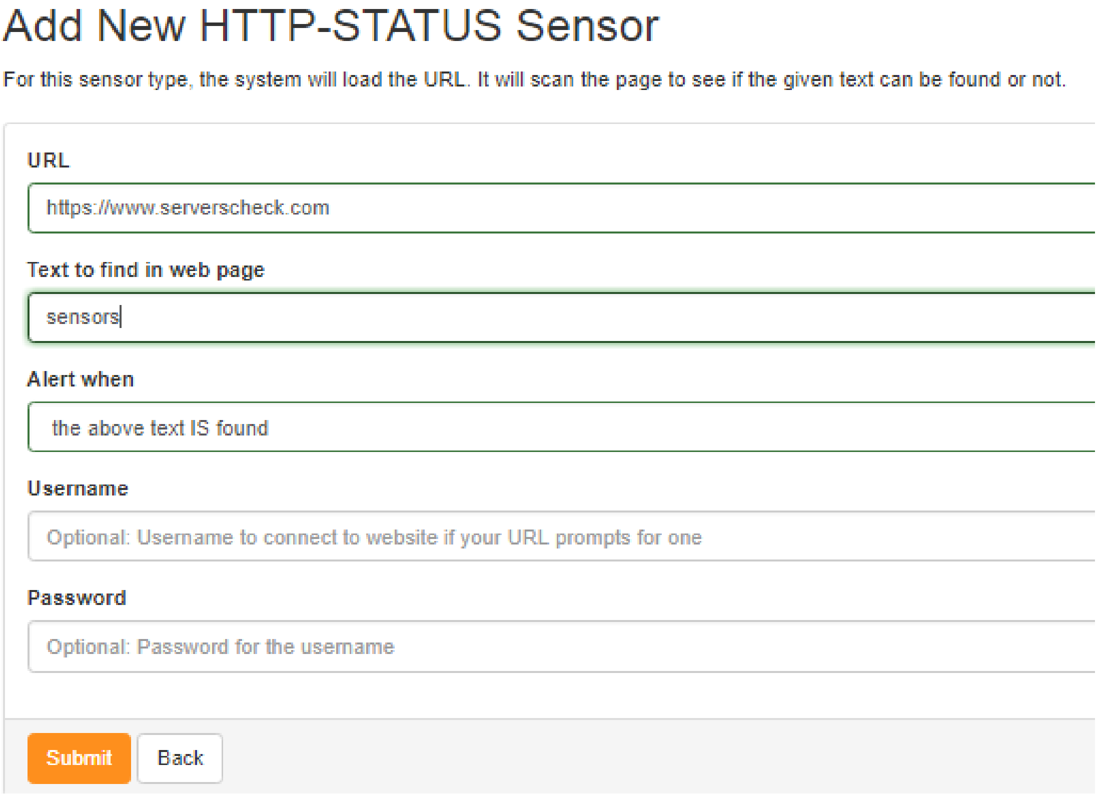
URL - Input the URL you want to check.

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.



Add New HTTP-STATUS Sensor

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.

URL: https://www.serverscheck.com

Text to find in web page: sensors

Alert when: the above text IS found

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

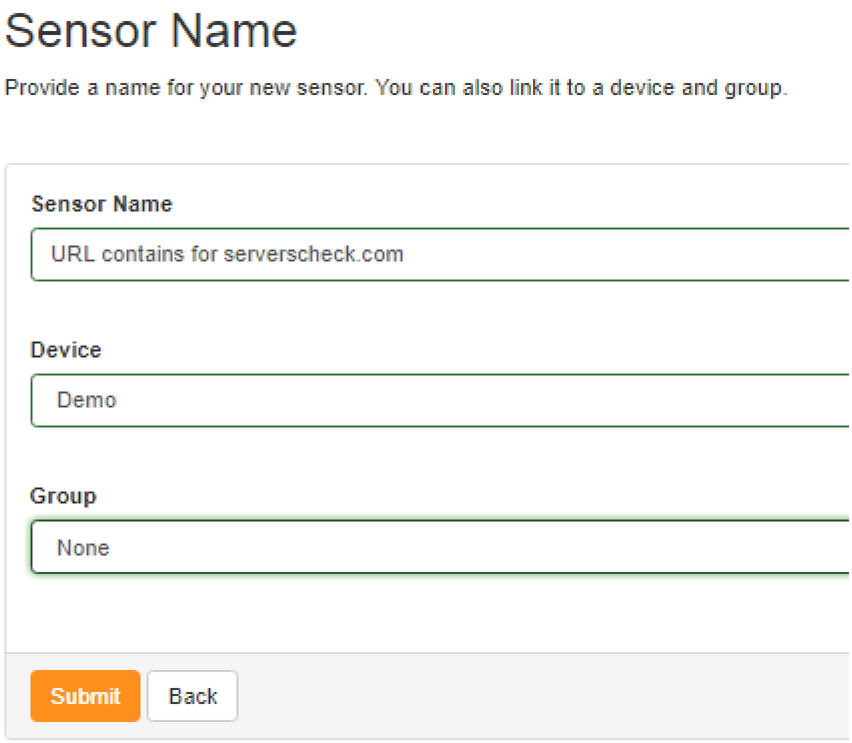
Password: Optional: Password for the username

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.



Sensor Name

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

Sensor Name: URL contains for serverscheck.com

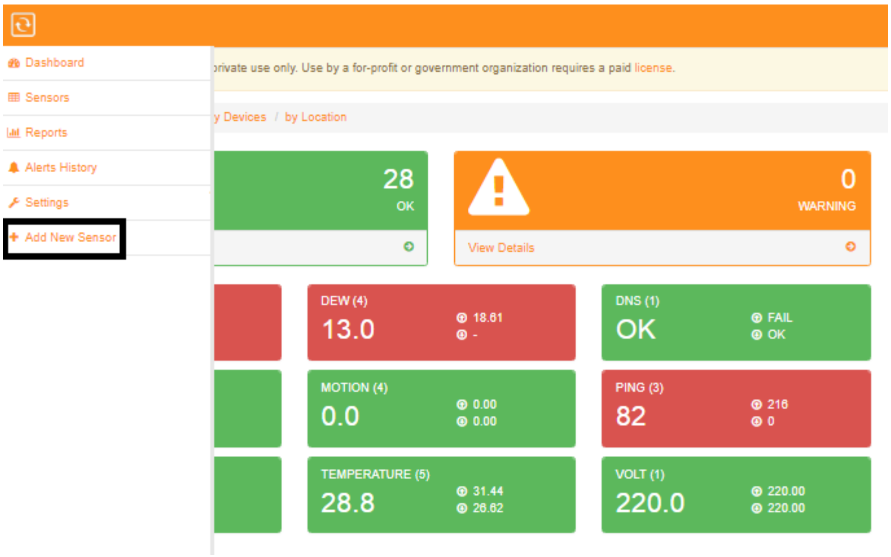
Device: Demo

Group: None

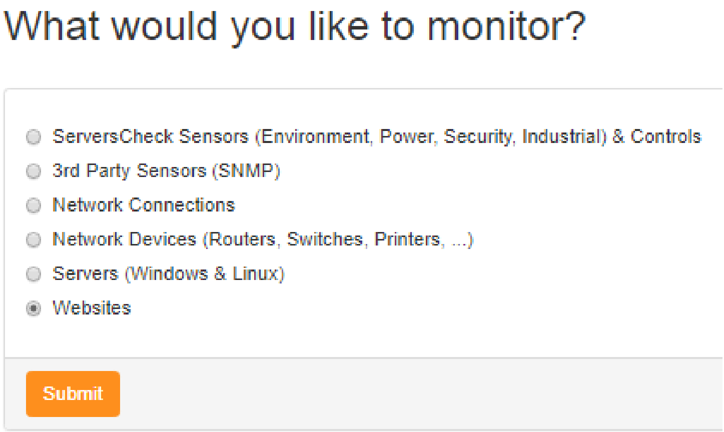
4.5.5. Adding URL Contains Check

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**.



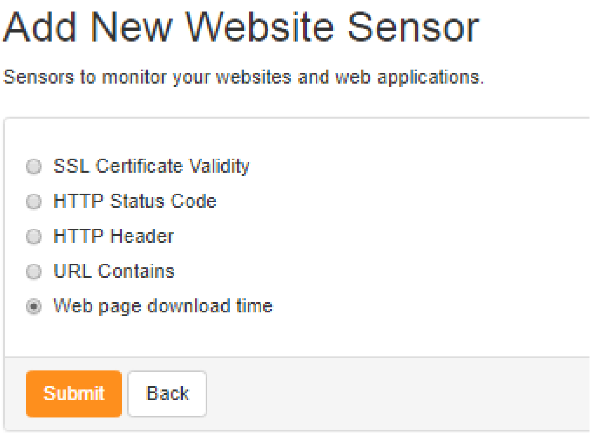
2. Select Websites.



What would you like to monitor?

○ ServersCheck Sensors (Environment, Power, Security, Industrial) & Controls
○ 3rd Party Sensors (SNMP)
○ Network Connections
○ Network Devices (Routers, Switches, Printers, ...)
○ Servers (Windows & Linux)
● Websites

3. Select Web page download time.



Add New Website Sensor

Sensors to monitor your websites and web applications.

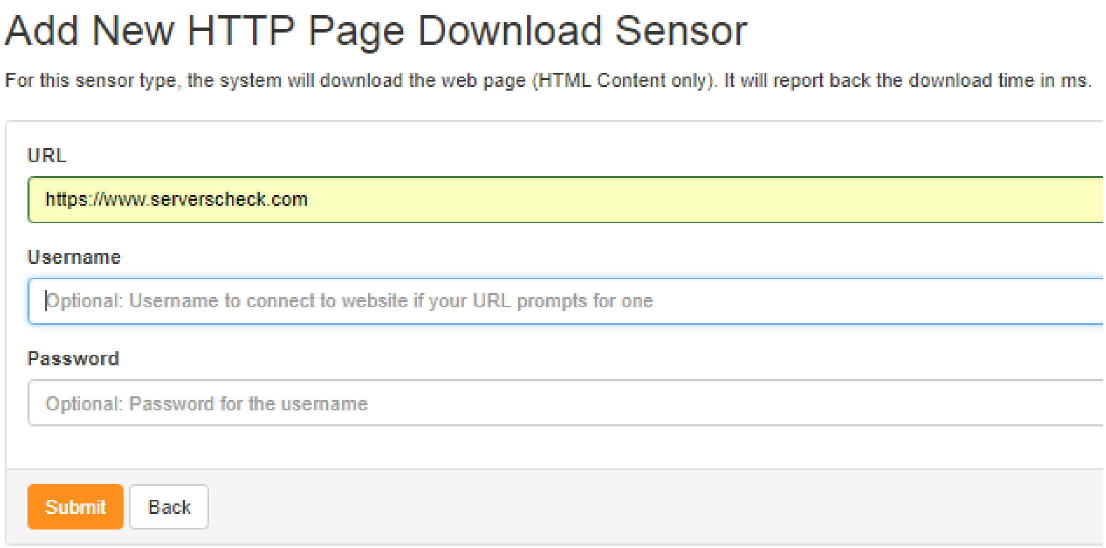
○ SSL Certificate Validity
○ HTTP Status Code
○ HTTP Header
○ URL Contains
● Web page download time

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

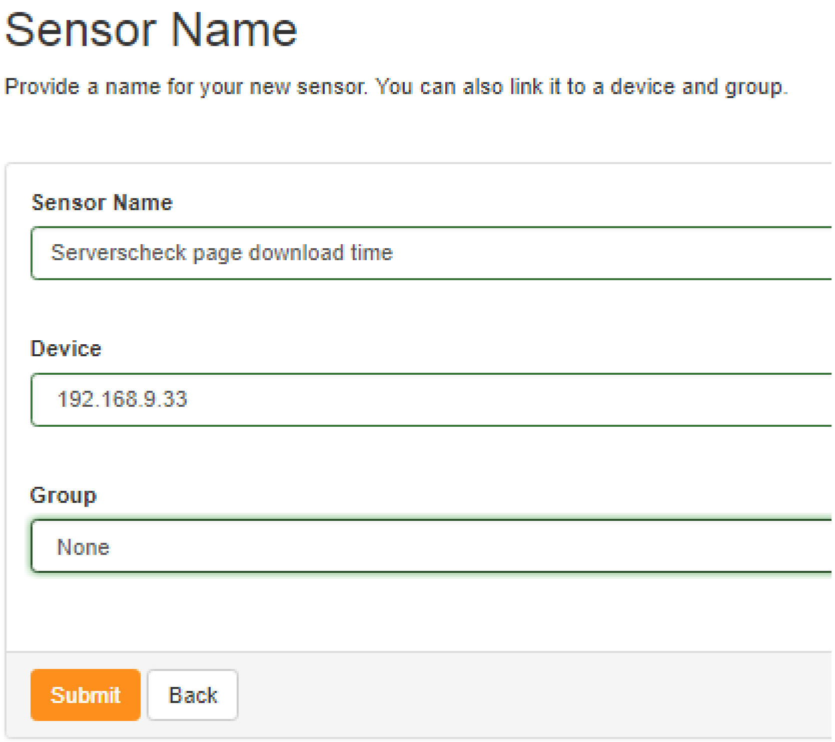
Password: Optional: Password for the username

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

5. Generating Reports

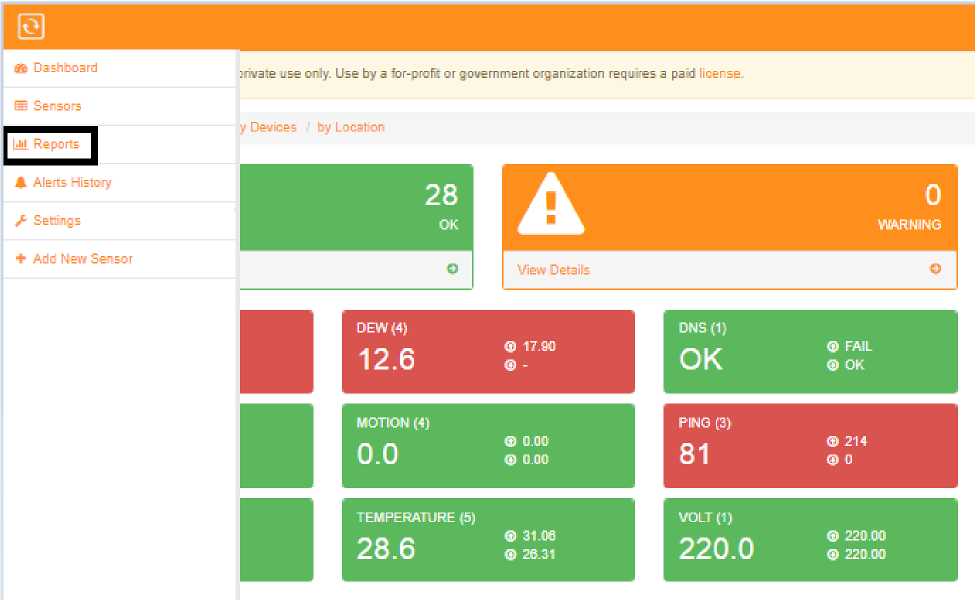
Serverscheck enables users to not only create custom graphs, but also schedule them to be refreshed at whatever rate needed.

Two ways to generate reports:

- by Sensor Names
- by Sensor Types

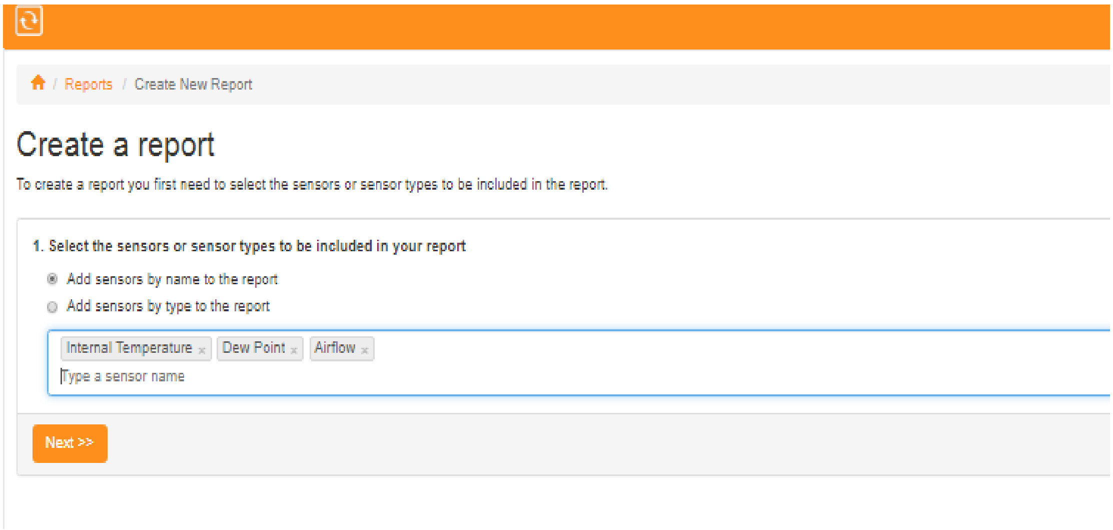
5.1. Generating By Sensor Names

1. Access **Menu** and go to **Reports**.



rivate use only. Use by a for-profit or government organization requires a paid license.

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.



Create a report

To create a report you first need to select the sensors or sensor types to be included in the report.

1. Select the sensors or sensor types to be included in your report

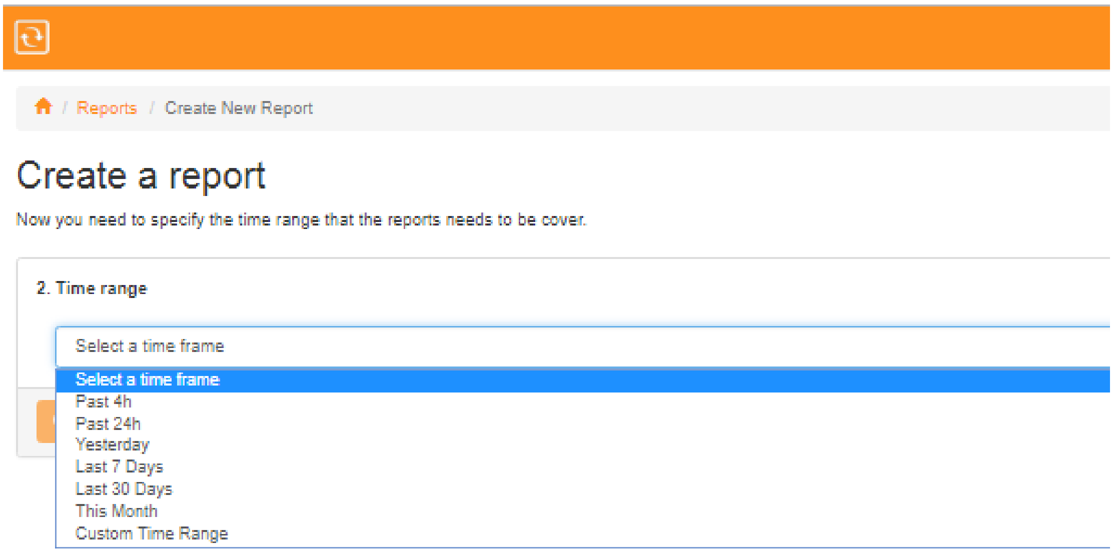
● Add sensors by name to the report
○ Add sensors by type to the report

Internal Temperature × Dew Point × Airflow ×
Type a sensor name

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



Reports / Create New Report

Create a report

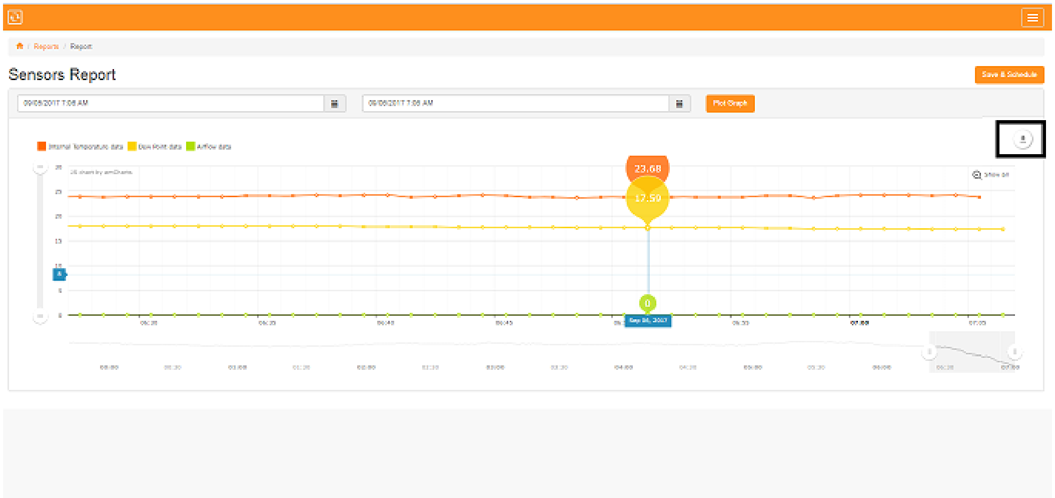
Now you need to specify the time range that the reports needs to be cover.

2. Time range

Select a time frame

- Select a time frame
- 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.



Reports / Report

Sensors Report

09/05/2017 7:08 AM

09/06/2017 7:08 AM

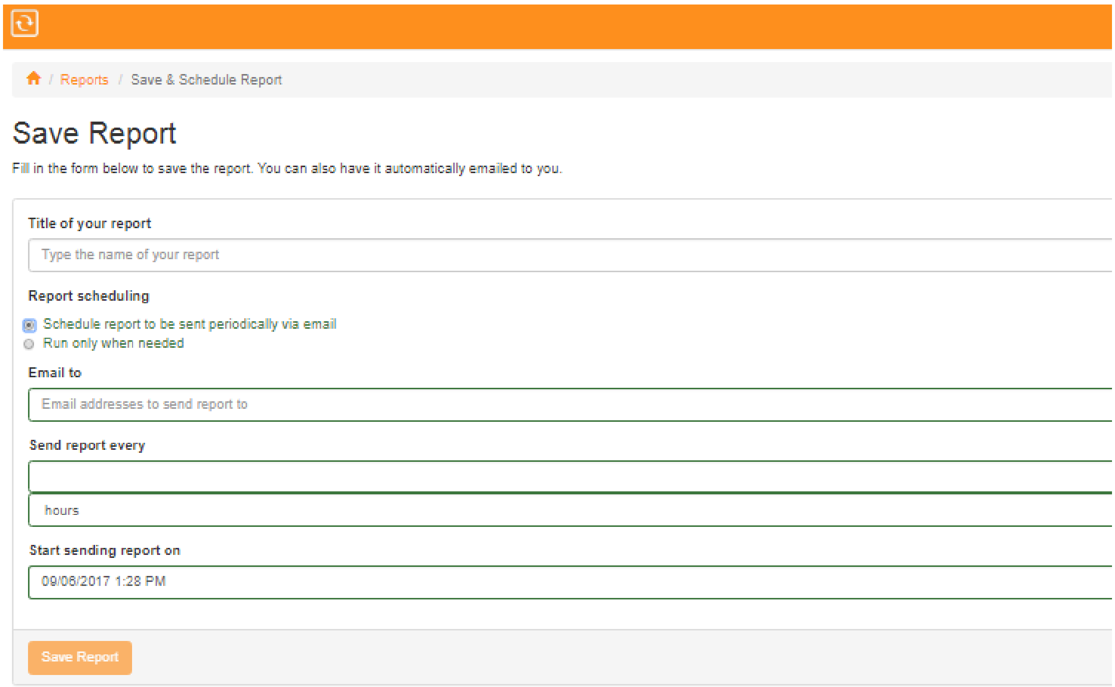
The image can be saved by clicking the arrow on the upper right hand side.

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.



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

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.

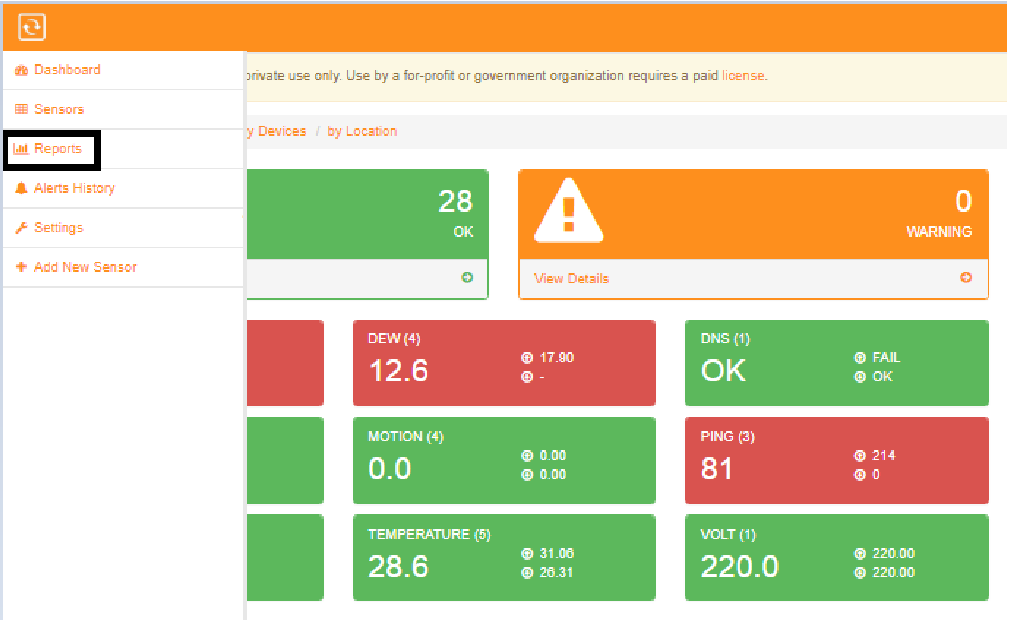
Send report every - Specify the number of hours or days for the report to be automatically be sent.

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

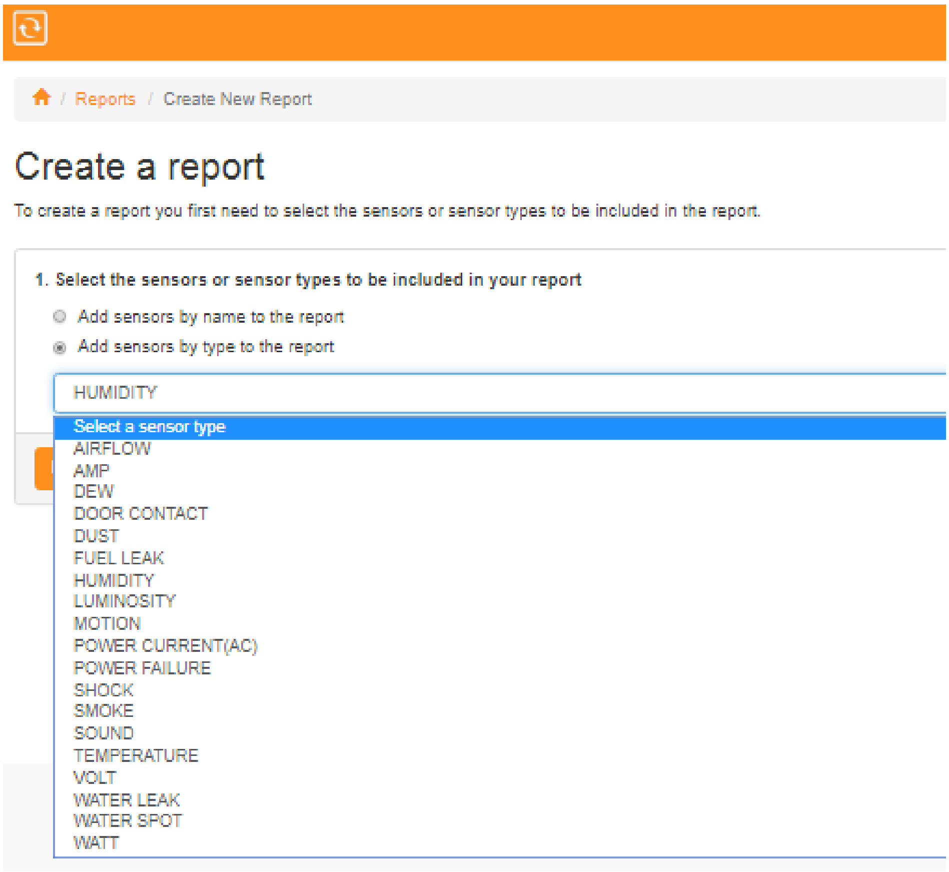
: Run only when needed - Will generate the report one time or only when you manually generate it.

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.



Create a report

To create a report you first need to select the sensors or sensor types to be included in the report.

1. Select the sensors or sensor types to be included in your report

○ Add sensors by name to the report

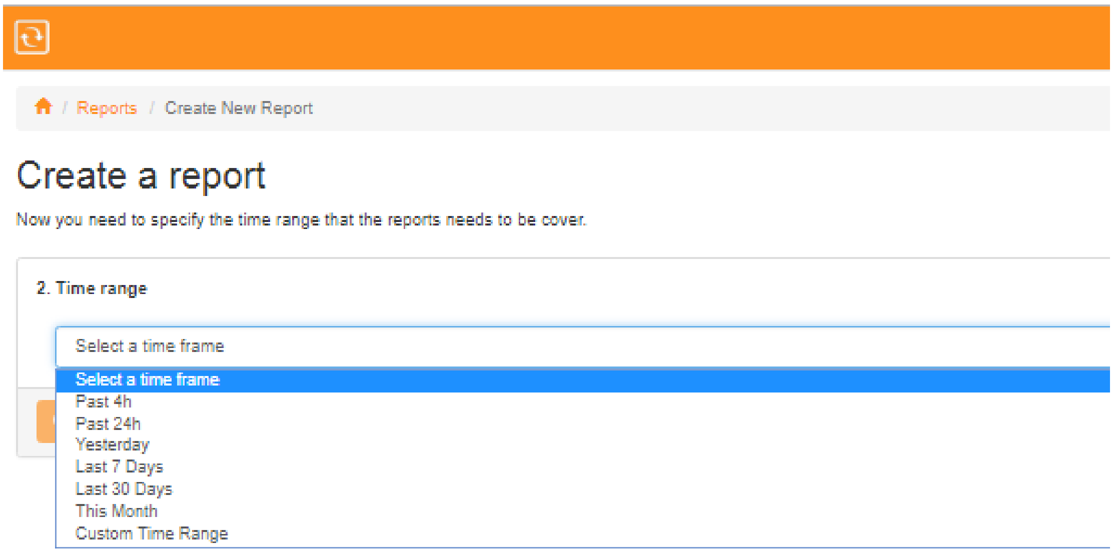
● Add sensors by type to the report

HUMIDITY

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

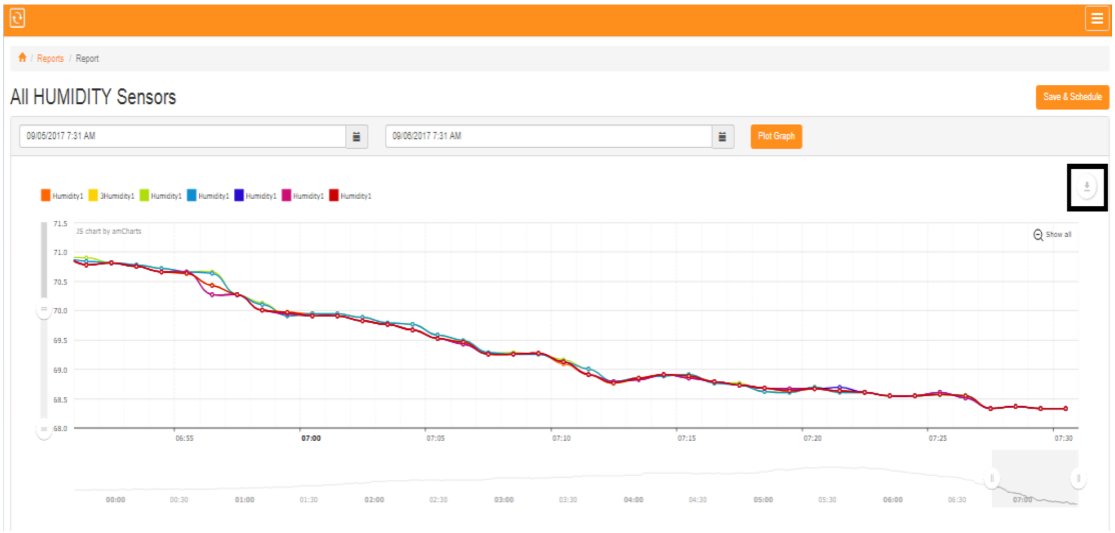


Create a report

Now you need to specify the time range that the reports needs to be cover.

2. 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.



All HUMIDITY Sensors

09/05/2017 7:31 AM

09/06/2017 7:31 AM

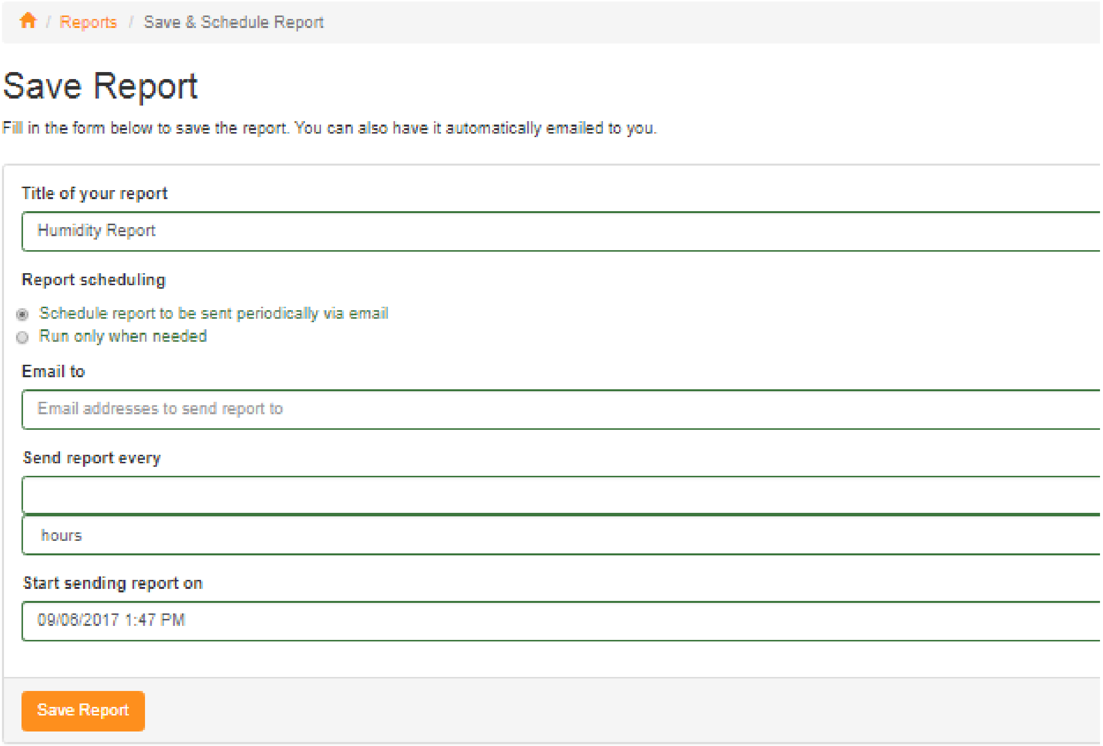
The image can be saved by clicking the arrow on the upper right hand side.

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

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

09/06/2017 1:47 PM

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

Report Scheduling:

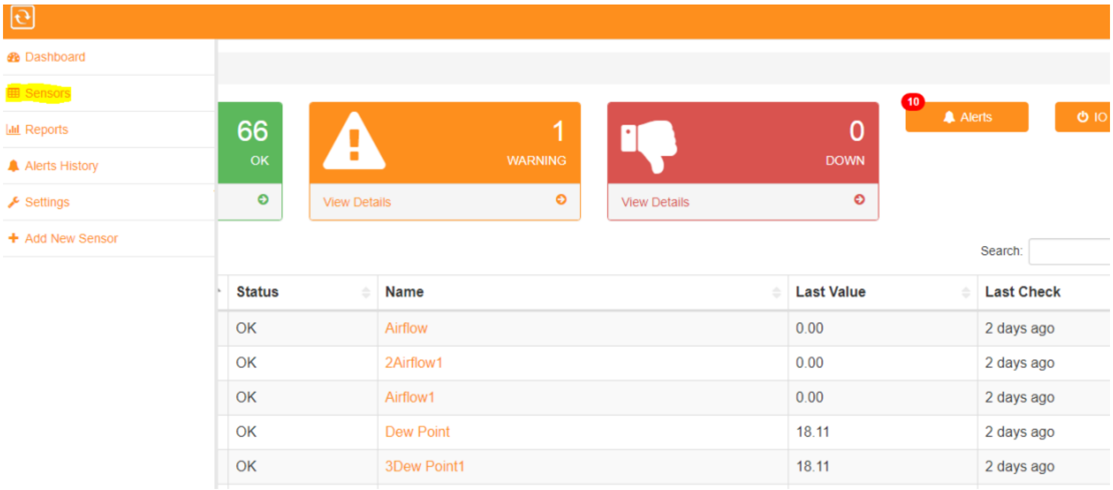
: schedule report to be sent periodically via email.

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.

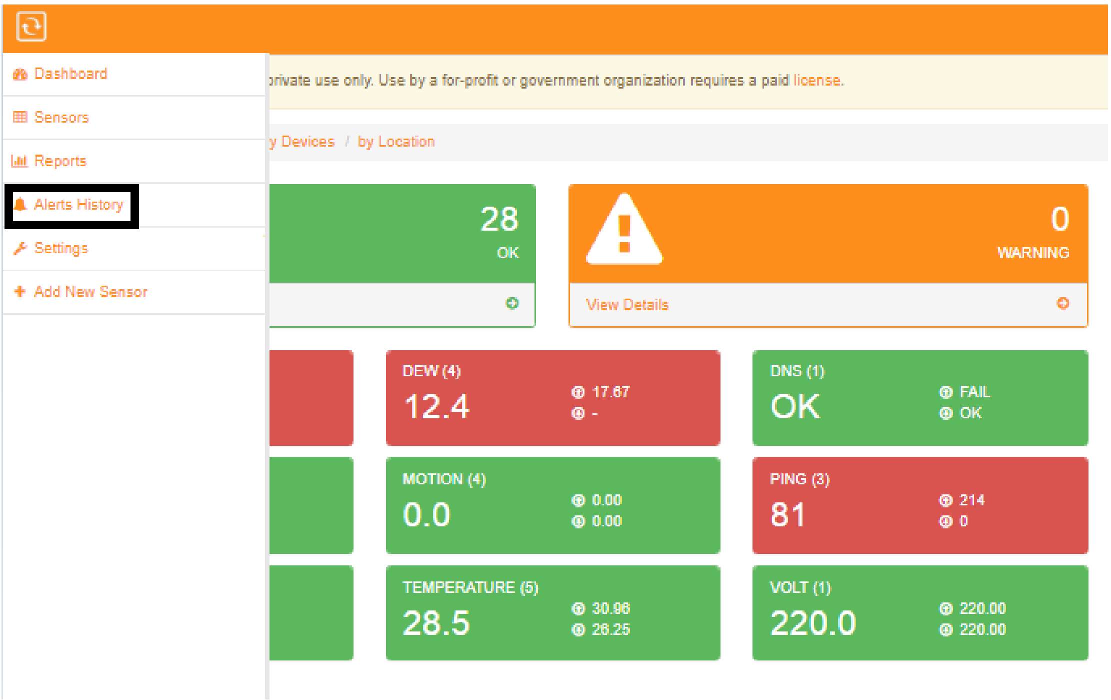


Status	Name	Last Value	Last Check
OK	Airflow	0.00	2 days ago
OK	2Airflow1	0.00	2 days ago
OK	Airflow1	0.00	2 days ago
OK	Dew Point	18.11	2 days ago
OK	3Dew Point1	18.11	2 days ago

5. Alerts History

Alerts would show on a first in first out basis.

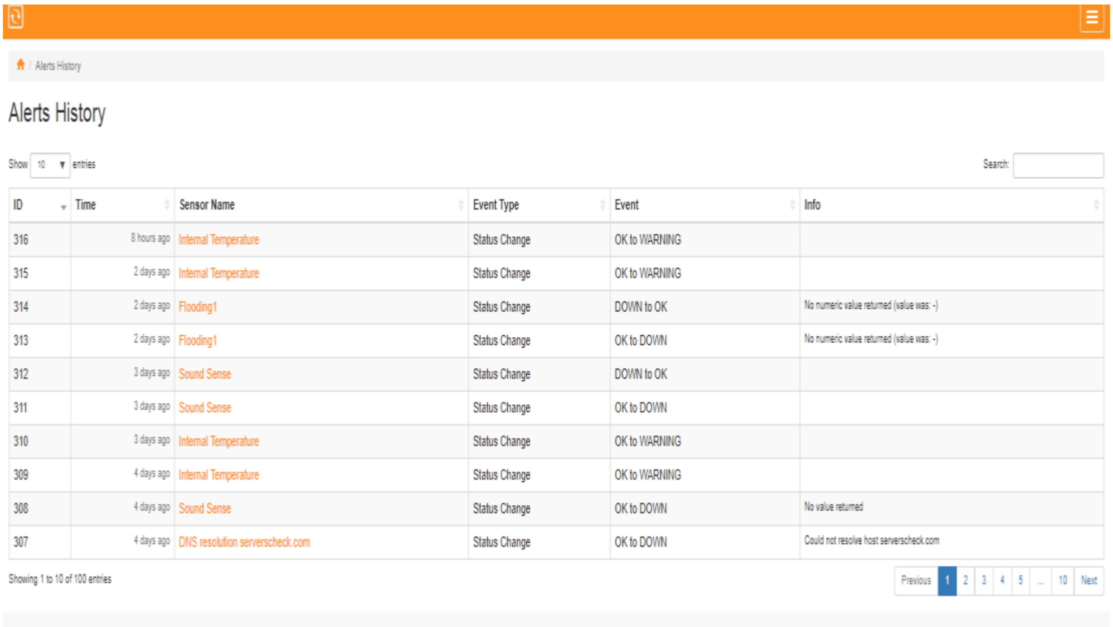
1. Click **Menu** and go to **Alerts History**.



ɔrivate use only. Use by a for-profit or government organization requires a paid license.

2. This would open up a windows 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.



Alerts History

Show 10 entries

Search:

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	Flooding1	Status Change	DOWN to OK	No numeric value returned (value was: -)
313	2 days ago	Flooding1	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

Showing 1 to 10 of 100 entries

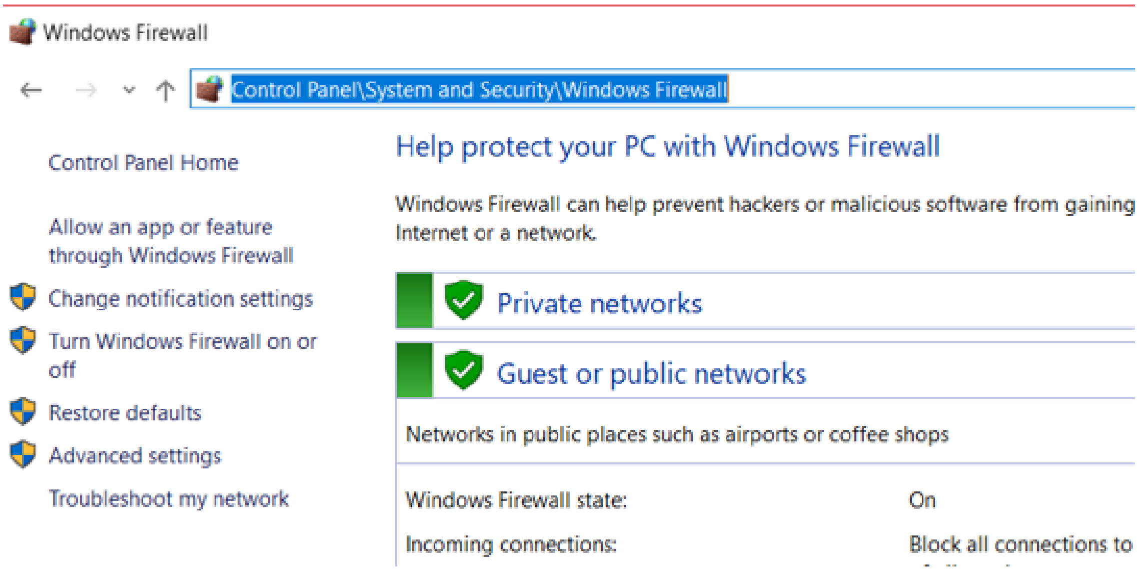
6. Adding Security to your Monitoring Software.

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.



Windows Firewall

Control Panel\System and Security\Windows Firewall

Help protect your PC with Windows Firewall

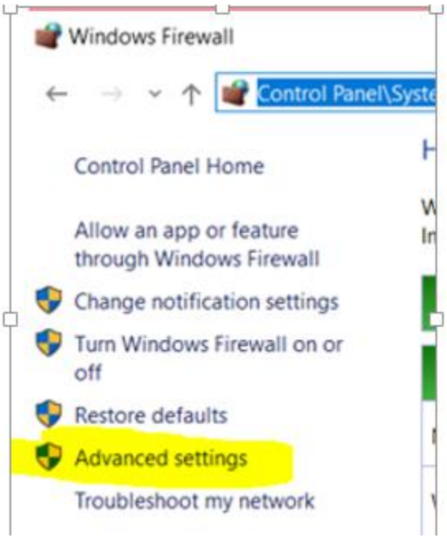
Windows Firewall can help prevent hackers or malicious software from gaining Internet or a network.

Networks in public places such as airports or coffee shops

Windows Firewall state: On

Incoming connections: Block all connections to

* Choose “Advance settings” on the left panel.

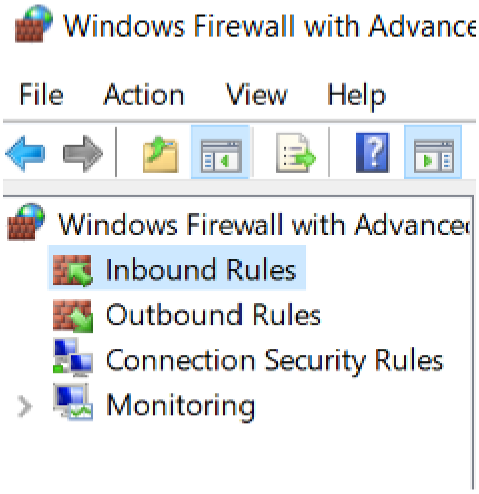


Windows Firewall

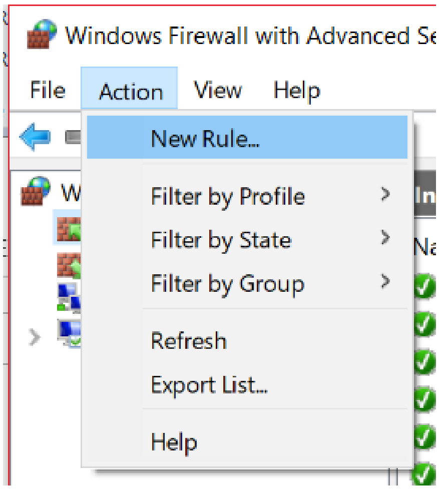
Control Panel\Syste

Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

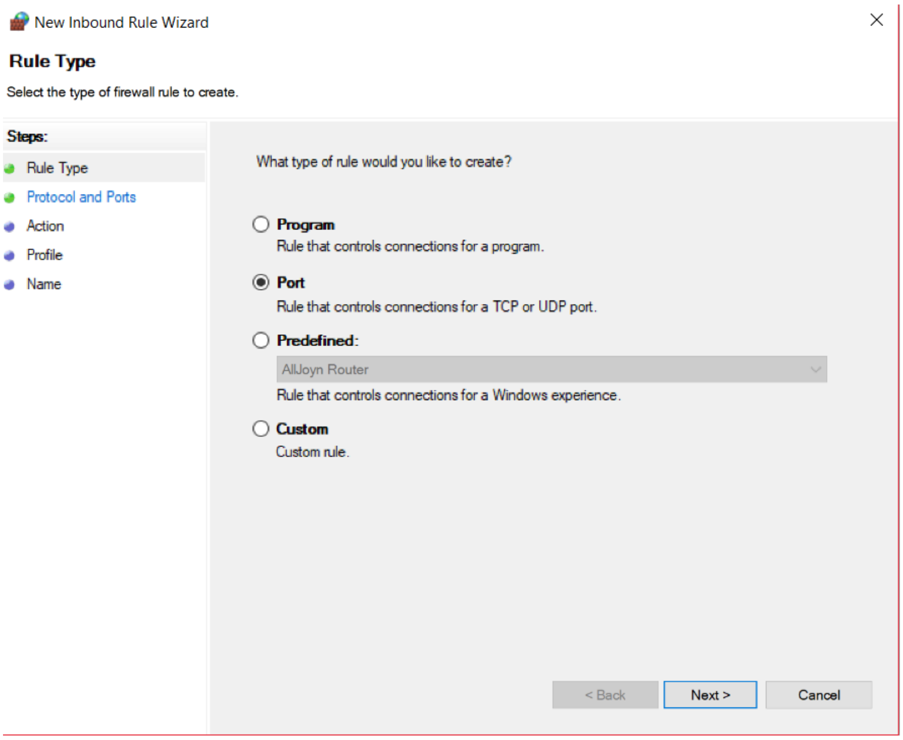
* Under firewall Advance Settings Highlight Inbound Rules.


Windows Firewall with Advance
File
Action
View
Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring

* Click on Action and then New Rule.



* On the next screen choose "PORT".



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What type of rule would you like to create?

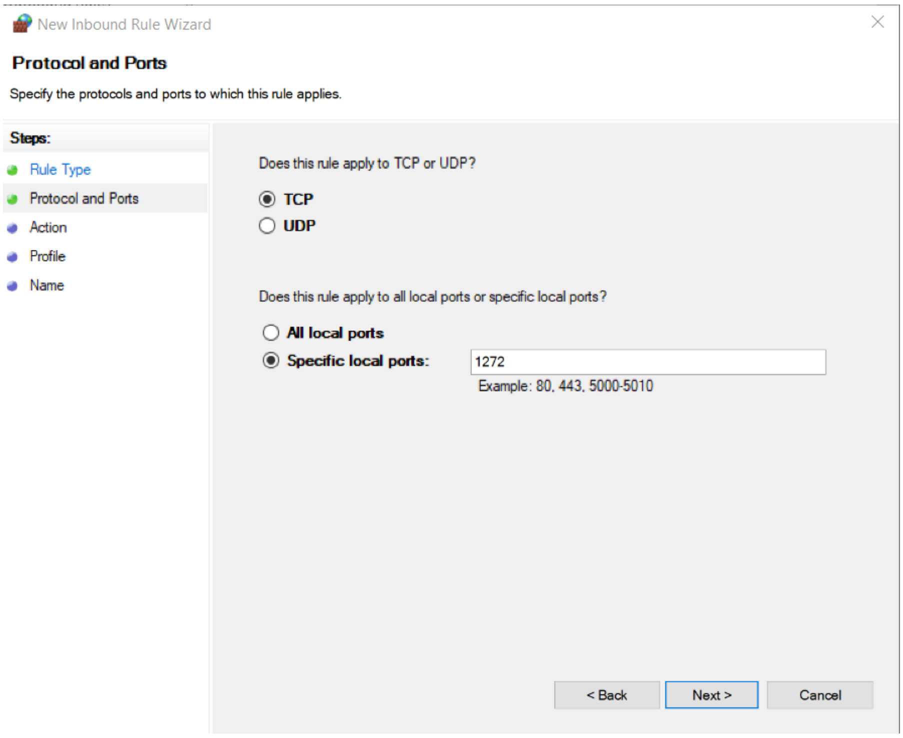
○ **Program**
Rule that controls connections for a program.

● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
AllJoyn Router
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

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



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

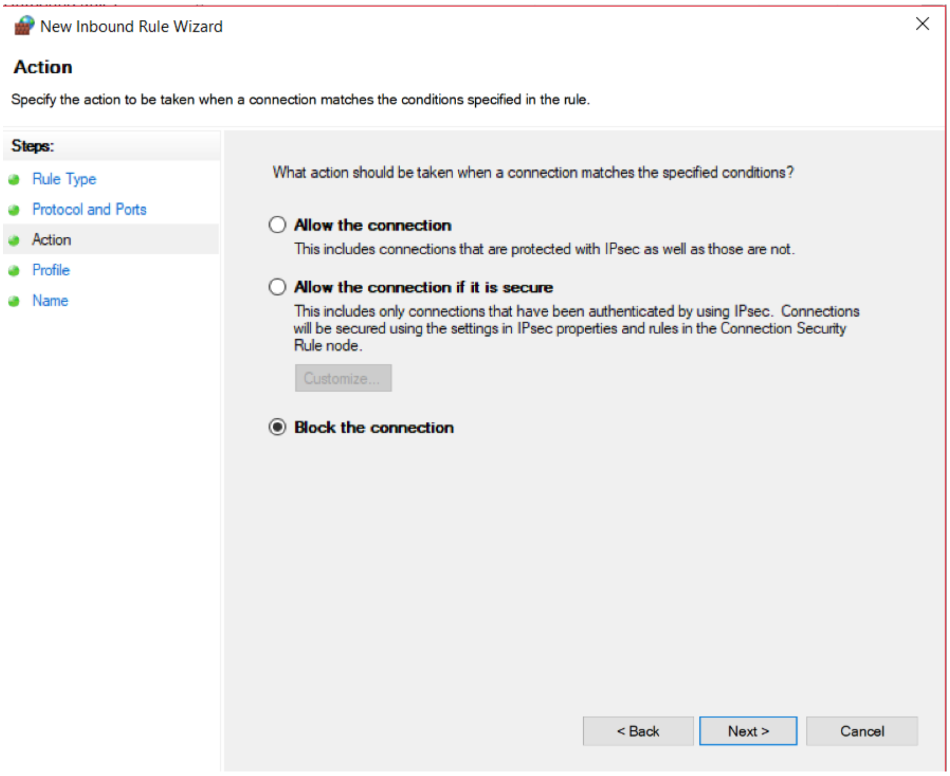
● TCP
○ UDP

Does this rule apply to all local ports or specific local ports?

○ All local ports
● Specific local ports: 1272

Example: 80, 443, 5000-5010

* Choose Block the Connection.



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

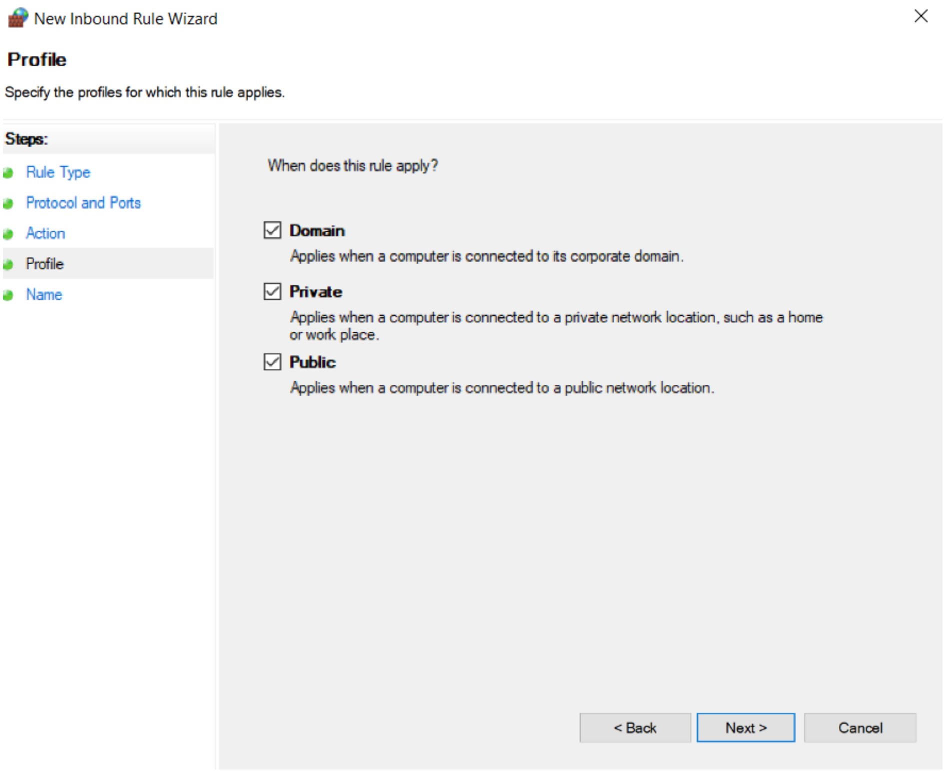
What action should be taken when a connection matches the specified conditions?

○ Allow the connection
This includes connections that are protected with IPsec as well as those are not.

○ Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

● Block the connection

* Put a check mark on all.



New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

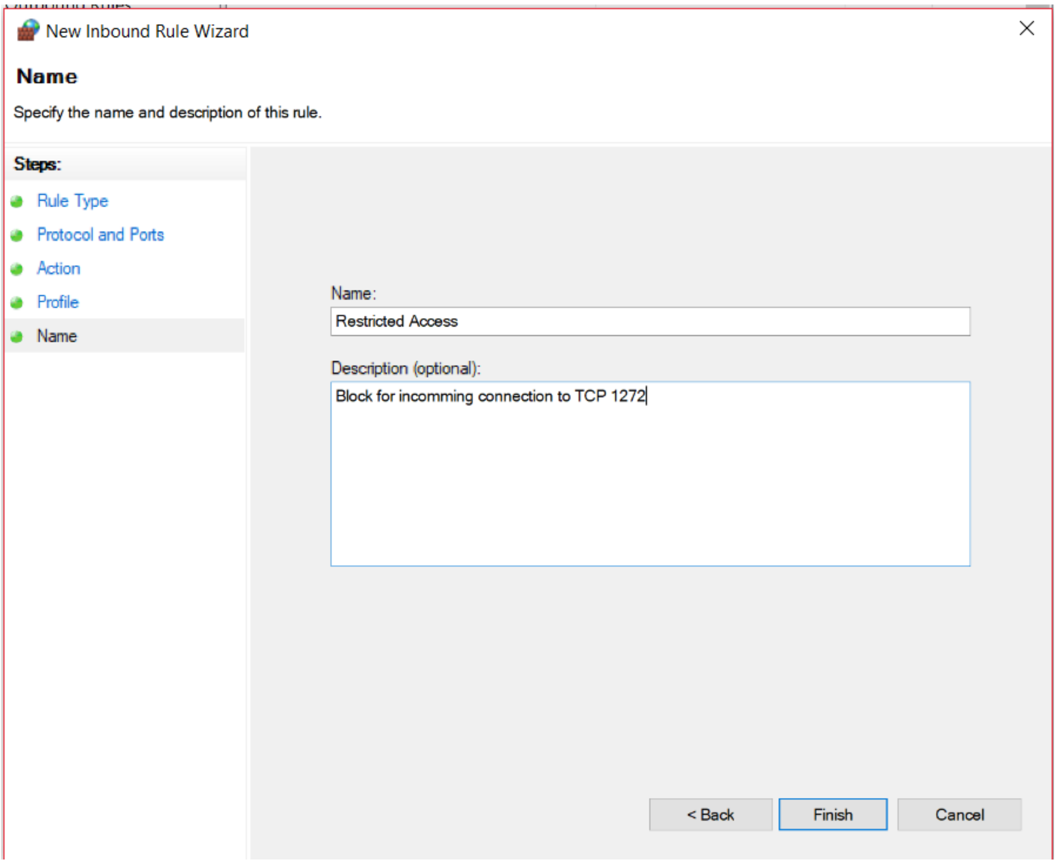
When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☑ **Public**
Applies when a computer is connected to a public network location.

* Create a label and finish set up.



New Inbound Rule Wizard

Name

Specify the name and description of this rule.

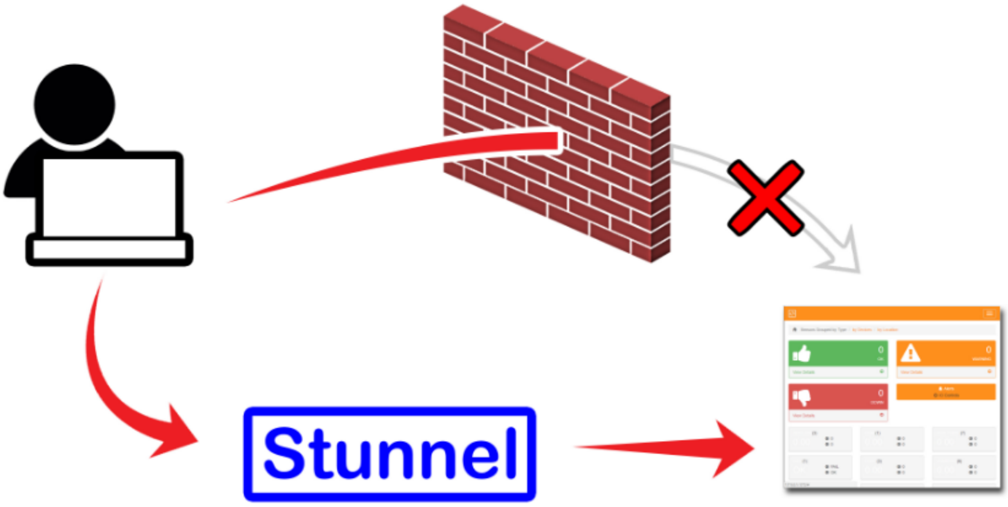
Name: Restricted Access

Description (optional): Block for incomming connection to TCP 1272

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. In the example below, we will be using Stunnel installed in the Monitoring Appliance to serve as a reverse proxy server.

6.1. Installing Stunnel

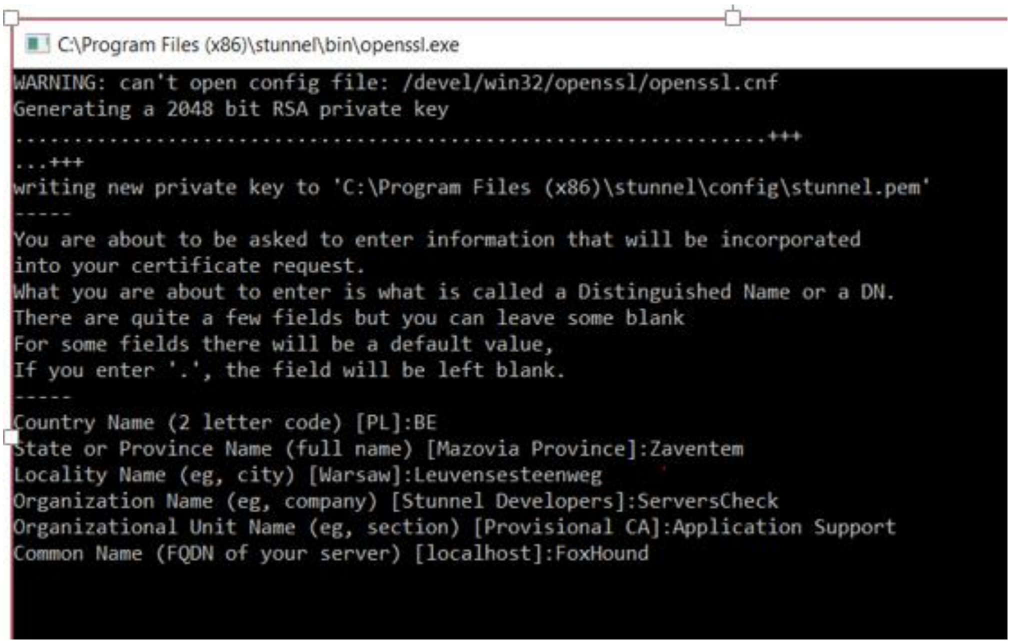
Here in our example, we used Stunnel which is an open source application used to provide TLS/SSL Tunneling service.



Below are the steps on how to install the Stunnel.

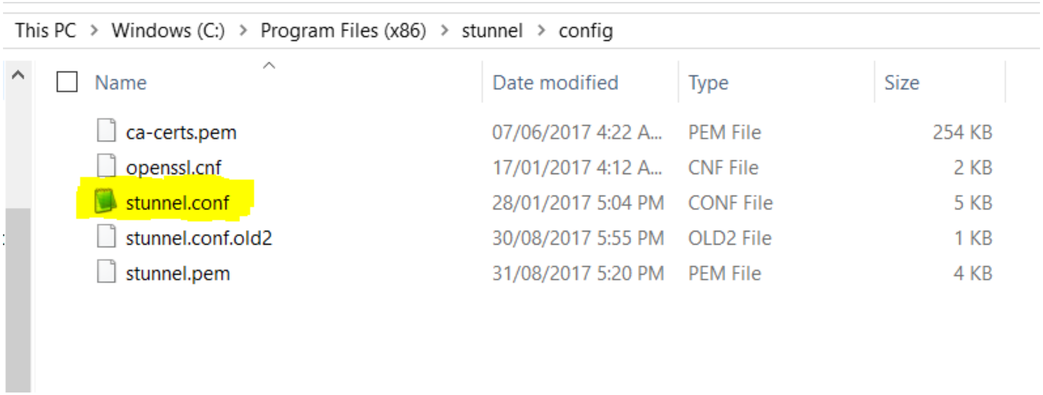
1. Download and Install the Stunnel Software (can be downloaded from: http://www.stunnel.org/

2. During the installation, you will be prompt to input details which will be needed to create certificates.



```
WARNING: can't open config file: /devel/win32/openssl/openssl.cnf
Generating a 2048 bit RSA private key
...............................................................+++
...+++
writing new private key to 'C:\Program Files (x86)\stunnel\config\stunnel.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [PL]:BE
State or Province Name (full name) [Mazovia Province]:Zaventem
Locality Name (eg, city) [Warsaw]:Leuvensesteenweg
Organization Name (eg, company) [Stunnel Developers]:ServersCheck
Organizational Unit Name (eg, section) [Provisional CA]:Application Support
Common Name (FQDN of your server) [localhost]:FoxHound
```

3. Access the config folder as shown in the image below and open stunnel.conf using a text editor.
Ex. Notepad, Notepad++



This PC > Windows (C:) > Program Files (x86) > stunnel > config

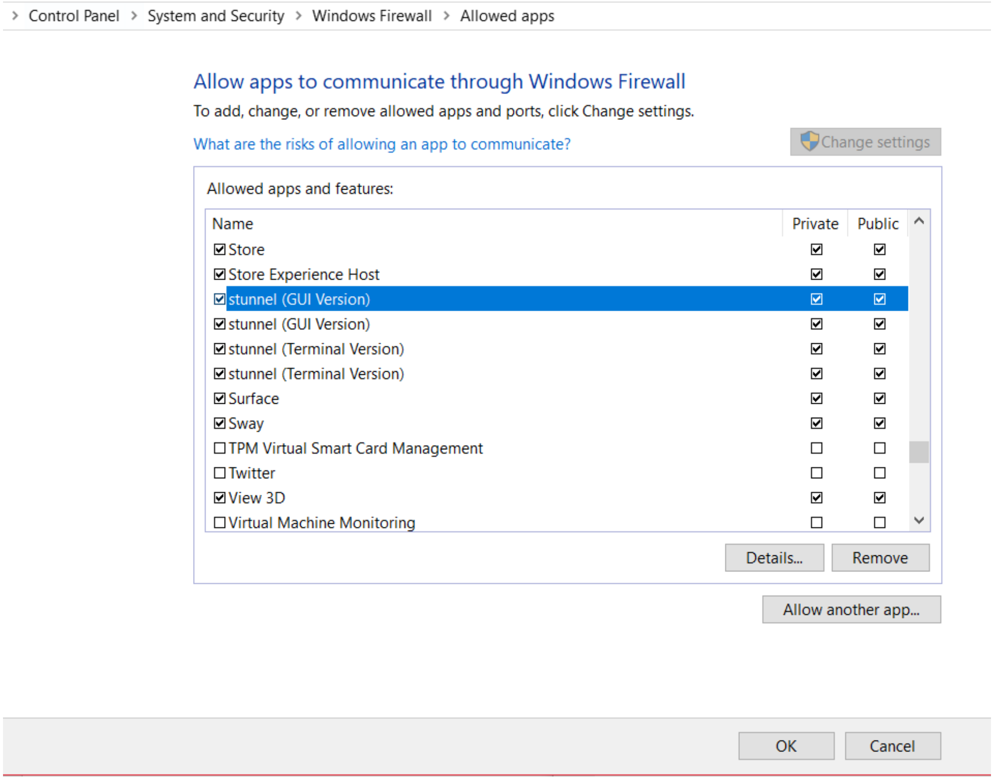
Name	Date modified	Type	Size
ca-certs.pem	07/06/2017 4:22 A...	PEM File	254 KB
openssl.cnf	17/01/2017 4:12 A...	CNF File	2 KB
stunnel.conf	28/01/2017 5:04 PM	CONF File	5 KB
stunnel.conf.old2	30/08/2017 5:55 PM	OLD2 File	1 KB
stunnel.pem	31/08/2017 5:20 PM	PEM File	4 KB

4. You should be able to see sample configuration commands. You can either edit the current or add the configuration below so that your connection can be forwarded to your monitoring software. This configuration will let you use your own certificates as it utilizes port 443.

Note: Hostname is the IP address of the computer where the software is installed.

```
[https]
accept  = 443
connect = hostname:1272
cert = stunnel.pem
TIMEOUTclose = 0
```

5. Make sure Stunnel is added on your allowed application in the firewall list



Control Panel > System and Security > Windows Firewall > Allowed apps

Allow apps to communicate through Windows Firewall

To add, change, or remove allowed apps and ports, click Change settings.

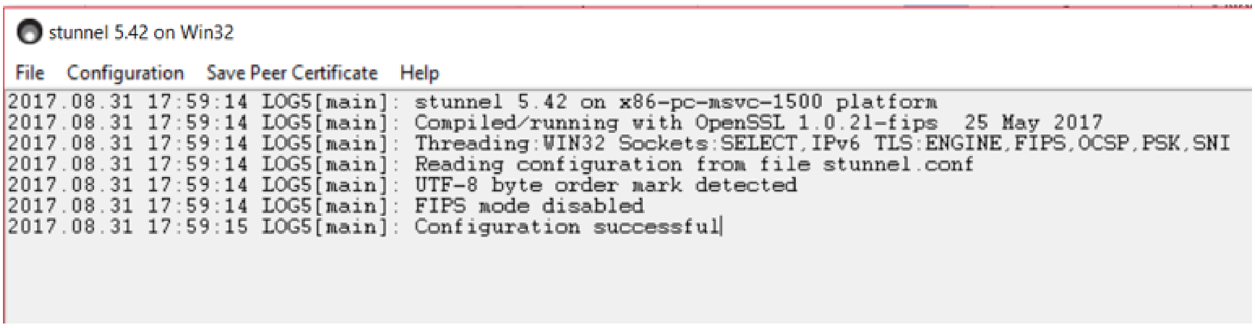
What are the risks of allowing an app to communicate?

Allowed apps and features:

Name	Private	Public
☑ Store	☑	☑
☑ Store Experience Host	☑	☑
☑ stunnel (GUI Version)	☑	☑
☑ stunnel (GUI Version)	☑	☑
☑ stunnel (Terminal Version)	☑	☑
☑ stunnel (Terminal Version)	☑	☑
☑ Surface	☑	☑
☑ Sway	☑	☑
☐ TPM Virtual Smart Card Management	☐	☐
☐ Twitter	☐	☐
☑ View 3D	☑	☑
☐ Virtual Machine Monitoring	☐	☐

6. Click on the desktop icon of the stunnel. You can also see and choose options on the Icon created on the system tray.

7. You should see a result like the image below once successful.



```
2017.08.31 17:59:14 LOG5[main]: stunnel 5.42 on x86-pc-msvc-1500 platform
2017.08.31 17:59:14 LOG5[main]: Compiled/running with OpenSSL 1.0.21-fips  25 May 2017
2017.08.31 17:59:14 LOG5[main]: Threading:WIN32 Sockets:SELECT,IPv6 TLS:ENGINE,FIPS,OCSP,PSK,SNI
2017.08.31 17:59:14 LOG5[main]: Reading configuration from file stunnel.conf
2017.08.31 17:59:14 LOG5[main]: UTF-8 byte order mark detected
2017.08.31 17:59:14 LOG5[main]: FIPS mode disabled
2017.08.31 17:59:15 LOG5[main]: Configuration successful
```

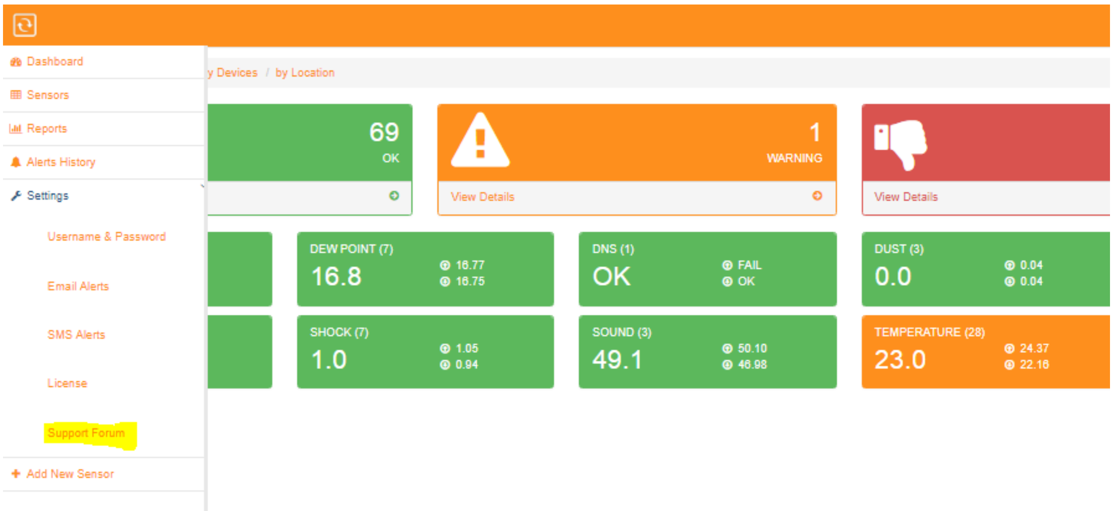
8. Access your monitoring software over your network via **https://**192.x.x.x. (http://192.x.x.x:1272 is now blocked for incoming connection)

9. For more advanced users you can configure and add your own certificates on the stunnel.pem file. For more info you can go to https://www.stunnel.org/howto.html

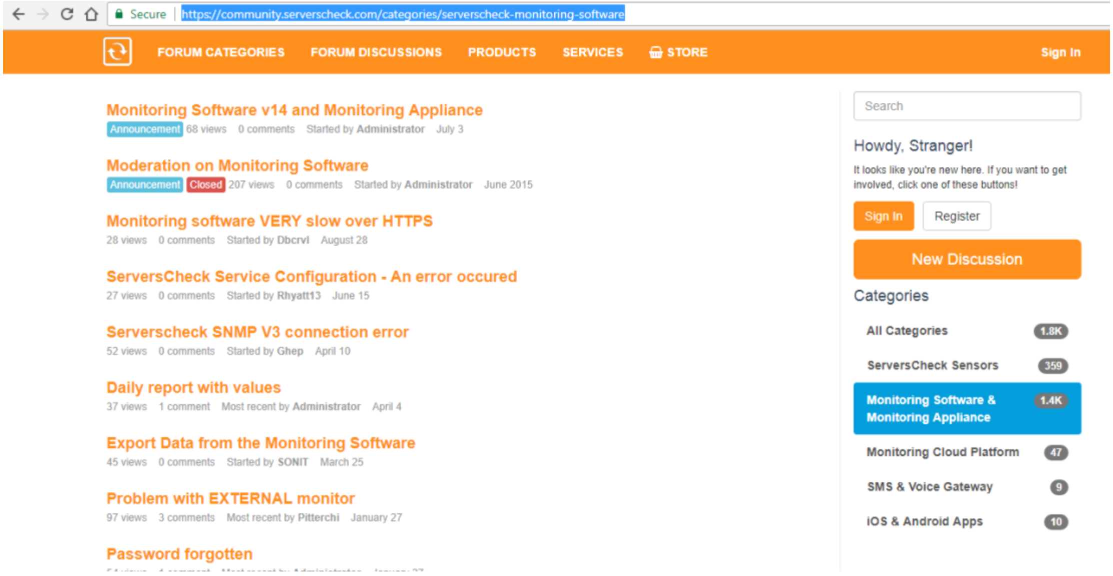
7. Support Forum

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 to **Menu** and click **Support Forum**.



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.



Monitoring Software v14 and Monitoring Appliance
Announcement 68 views 0 comments Started by Administrator July 3

Moderation on Monitoring Software
Announcement Closed 207 views 0 comments Started by Administrator June 2015

Monitoring software VERY slow over HTTPS
28 views 0 comments Started by Dbcrvl August 28

ServersCheck Service Configuration - An error occured
27 views 0 comments Started by Rhyatt13 June 15

Serverscheck SNMP V3 connection error
52 views 0 comments Started by Ghep April 10

Daily report with values
37 views 1 comment Most recent by Administrator April 4

Export Data from the Monitoring Software
45 views 0 comments Started by SONIT March 25

Problem with EXTERNAL monitor
97 views 3 comments Most recent by Pitterchi January 27

Password forgotten

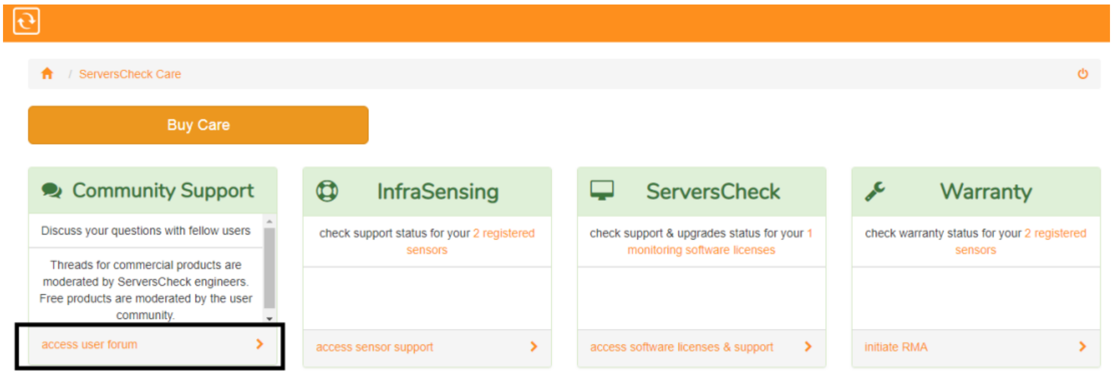
Howdy, Stranger!

It looks like you're new here. If you want to get involved, click one of these buttons!

Categories

All Categories	1.8K
ServersCheck Sensors	359
Monitoring Software & Monitoring Appliance	1.4K
Monitoring Cloud Platform	47
SMS & Voice Gateway	9
iOS & Android Apps	10

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.



Discuss your questions with fellow users

Threads for commercial products are moderated by ServersCheck engineers. Free products are moderated by the user community.

check support status for your 2 registered sensors

check support & upgrades status for your 1 monitoring software licenses

check warranty status for your 2 registered sensors