EdgeSentry Configuration Guide

models: ES-102, ES-302, ES-304, ES-604

Overview

EdgeSentry is a network appliance for monitoring, hardening, documenting and securing IoT centric networks. EdgeSentry appliances provide real time alerts via email, client software or to an on-line network receiver. LMN Software Corp also manufactures the **ES-*Monitor*** network monitoring software for companies that intend to monitor potentially large numbers of EdgeSentry appliances.

EdgeSentry is designed to be simple to install and simple to understand. A novice installer should be able to complete an EdgeSentry installation on a network within an hour. A basic installation includes the following steps:

Connecting the EdgeSentry and putting it in "Learn Mode":

See the EdgeSentry ***Wiring Guide***

- Choosing a basic monitoring configuration (Isolation Mode vs Integration Mode)
- Connecting the appliance to a network switch's SPAN or MIRROR port
- Setting the EdgeSentry network addresses
- Initial configuration of EdgeSentry using LMN's Configuration Tool software (available at: **https://www.lmnsoftwarecorp.com/easy-install.html)**

Configuring EdgeSentry:

Covered in this guide:

- Setting up Notifications and Receivers
- Naming devices
- Authorizing devices
- Device supervision
- Setting up UPSs for monitoring
- Port and protocol monitoring

Once an EdgeSentry has learned the network, an advanced installation could include setting up interfaces to the site's layer 2-3 network switches. There are also a number of special topics that you may want to address at this point, such as managing nuisance alarms ("Spam"), hardening the network and setting up active security.

Setting up Network Switch Hardening, Active Security and Site documentation:

See ***Switch Interface Guide***

- Adding managed network switches to EdgeSentry
- Hardening the network switches
- Mapping the network
- Setting up active security
- Generating site documentation

Fine Tuning an EdgeSentry installation:

See the ***Full EdgeSentry Configuration Manual***

- Managing alerts and “spam”
- Adding Users to EdgeSentry
- Setting up outbound email alerts
- Setting up EdgeSentry backups and reporting to a local/remote receiver
- Restarting Learn Mode
- Changing the EdgeSentry device password
- UPS Monitoring

Contents

Downloading EdgeSentry Configuration Tool

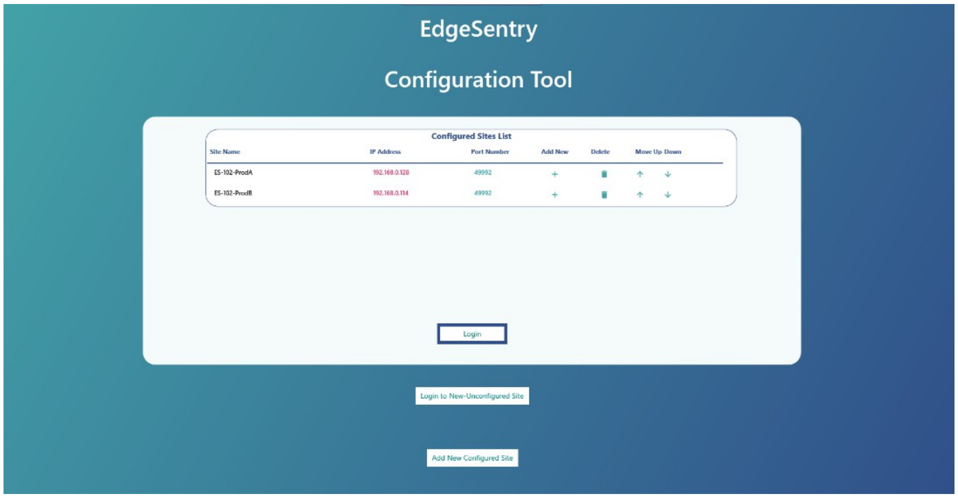
All of the sections in this manual require use of the EdgeSentry Configuration Tool software. Note that this software is client software for a technician laptop or PC and cannot be run on the EdgeSentry device.

Download the software from:

https://www.lmnsoftwarecorp.com/easy-install.html

First Connection

When you launch the EdgeSentry for the first time you will have to add your EdgeSentry sites to the login screen. The EdgeSentry devices are added as either "**Add New Configured Site** or a "**Login to New-Unconfigured Site**



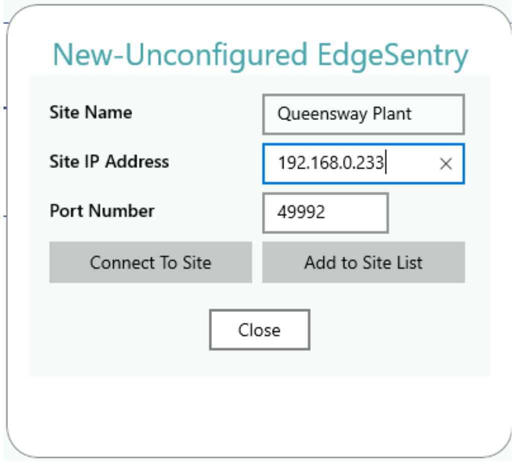
EdgeSentry

Configuration Tool

Configured Sites List

Site Name	IP Address	Port Number	Add New	Delete	Move Up Down
ES-102-ProdA	192.168.0.128	49992	+	🗑	↑ ↓
ES-102-ProdB	192.168.0.114	49992	+	🗑	↑ ↓

If this is a new, unconfigured EdgeSentry click on "**Login to New-Unconfigured Site**" otherwise select "**Add New Configured Site**".



New-Unconfigured EdgeSentry

Site Name: Queensway Plant

Site IP Address: 192.168.0.233

Port Number: 49992

New-Unconfigured Site / Configured Site dialogue

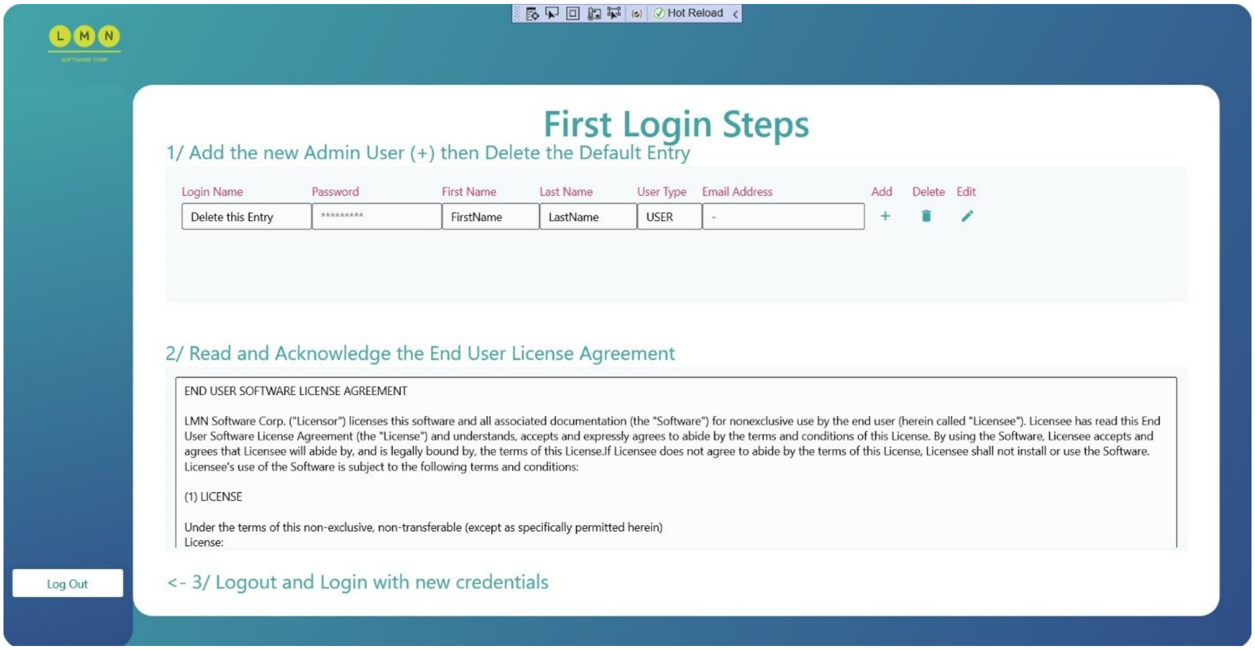
Fill in a site name, the site IP address and the site port number (49992 is the default site port number).

Click "**Add to Site List**"

Click "**Connect to Site**".

The next time you connect to the site it should be listed in the Configured Sites List.

If this is the first time the site is being configured, you will be forced to set a new Administrator connection password and to read and confirm the End User License Agreement.



First Login Steps

1/ Add the new Admin User (+) then Delete the Default Entry

Login Name	Password	First Name	Last Name	User Type	Email Address	Add	Delete	Edit
Delete this Entry	*********	FirstName	LastName	USER	-	+	🗑	✎

2/ Read and Acknowledge the End User License Agreement

END USER SOFTWARE LICENSE AGREEMENT

LMN Software Corp. ("Licensor") licenses this software and all associated documentation (the "Software") for nonexclusive use by the end user (herein called "Licensee"). Licensee has read this End User Software License Agreement (the "License") and understands, accepts and expressly agrees to abide by the terms and conditions of this License. By using the Software, Licensee accepts and agrees that Licensee will abide by, and is legally bound by, the terms of this License.If Licensee does not agree to abide by the terms of this License, Licensee shall not install or use the Software. Licensee's use of the Software is subject to the following terms and conditions:

(1) LICENSE

Under the terms of this non-exclusive, non-transferable (except as specifically permitted herein)
License:

<- 3/ Logout and Login with new credentials

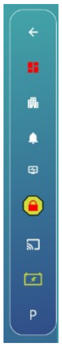
1/ Click the "**+**" sign and add a new Administrative User with a username and password

2/ Delete the existing "Delete this Entry" user by clicking on the Delete icon next to it.

3/ Read the ***End User License Agreement*** and click the **Acknowledge** box at the bottom.

4/ **Log Out** of the site and log back in using your new credentials.

Putting the EdgeSentry in Learn Mode

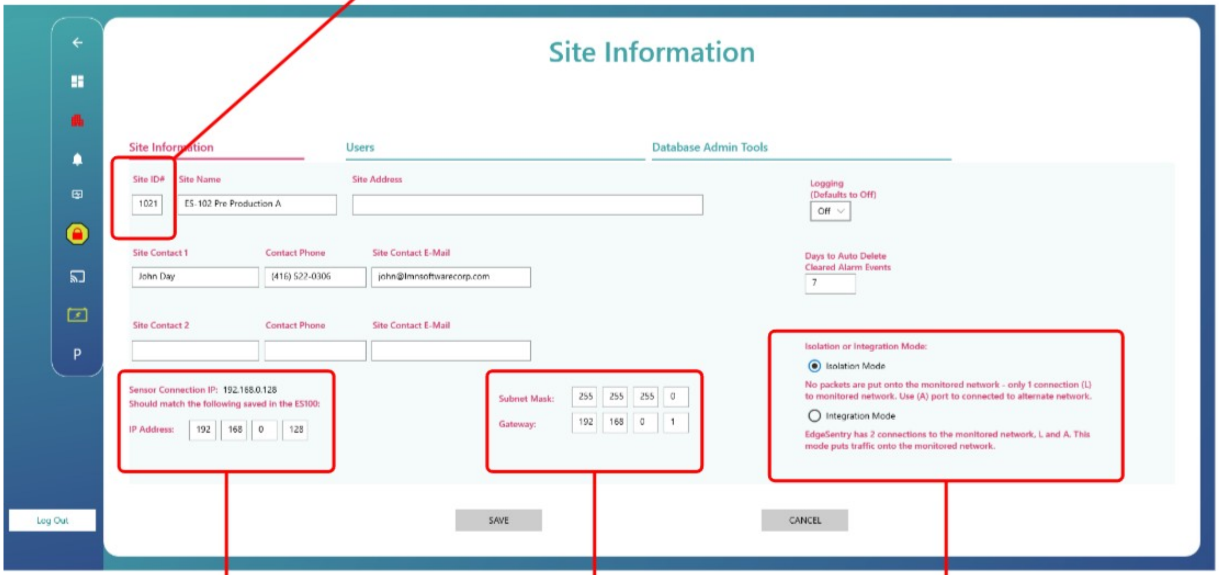


<- Click on the Building Icon (second from the top) to go to the Site Information screen

Site Information

Fill out the information in the Site Information screen, paying particular attention to the four settings highlighted below. Once this is done, press “SAVE” and the EdgeSentry will go into Learn Mode for the next 24-36 hours.

Site ID# - must be a unique number if you are monitoring multiple sites with an EdgeSentry receiver



Site Information

Site Information | Users | Database Admin Tools

Site ID#: 1021
Site Name: ES-102 Pre Production A
Site Address:
Logging (Defaults to Off): Off

Site Contact 1: John Day
Contact Phone: (416) 522-0306
Site Contact E-Mail: john@lmnsoftwarecorp.com

Days to Auto Delete Cleared Alarm Events: 7

Site Contact 2:
Contact Phone:
Site Contact E-Mail:

Sensor Connection IP: 192.168.0.128
Should match the following saved in the ES100:
IP Address: 192 168 0 128

Subnet Mask: 255 255 255 0
Gateway: 192 168 0 1

Isolation or Integration Mode:

● Isolation Mode

No packets are put onto the monitored network - only 1 connection (L) to monitored network. Use (A) port to connected to alternate network.

○ Integration Mode

EdgeSentry has 2 connections to the monitored network, L and A. This mode puts traffic onto the monitored network.

SAVE | CANCEL

IP Address - Fill in the IP Address of the EdgeSentry here - when you hit "**SAVE**", this will cause EdgeSentry to go into Learn Mode.

Subnet Mask and Gateway - the EdgeSentry uses this information to categorize whether devices are part of the local network or are "off network" connections.

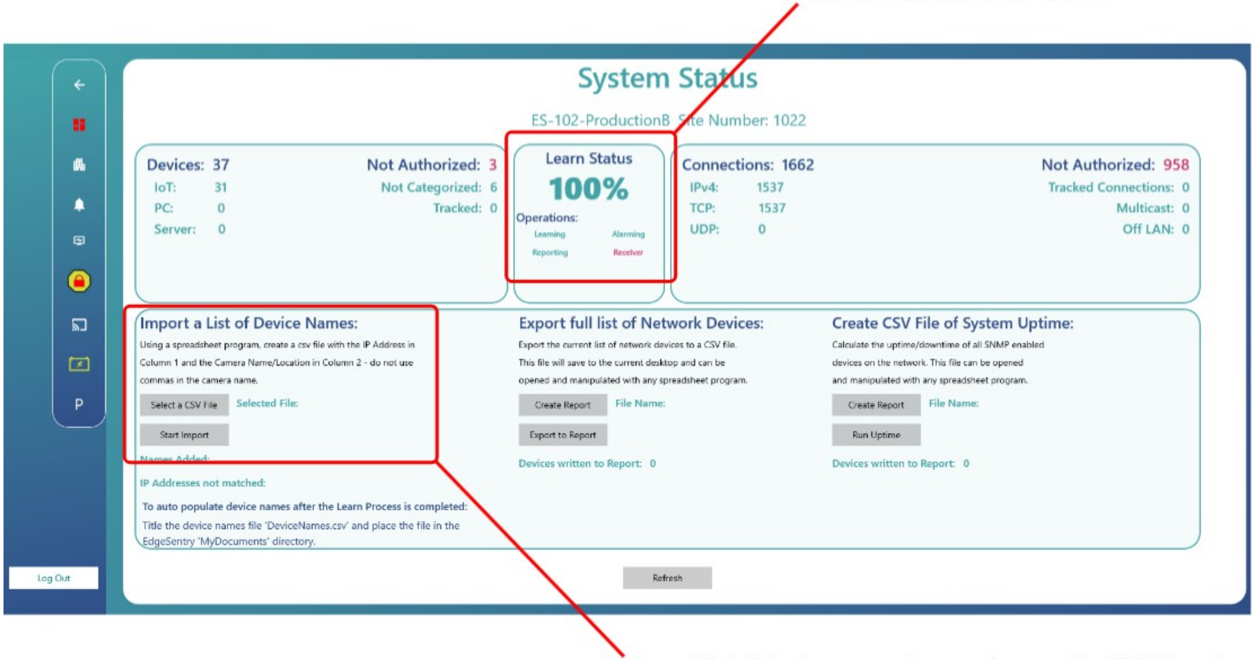
EdgeSentry Operation Mode - See the **Wiring Guide** for a description of Isolation Mode and integration mode.

Getting Started

Wiring, powering up and putting the EdgeSentry in learn mode is covered in the **Wiring Guide**. Once the EdgeSentry has been configured with an IP address and the IP Address has been set in the EdgeSentry using the Configuration Tool, the EdgeSentry will switch into “learn mode”. Learn mode takes between 24 and 36 hours to complete and requires that the EdgeSentry be running continuously for 24 hours.

The System Status Page

The learn process is completed



System Status

ES-102-ProductionB Site Number: 1022

Devices: 37
IoT: 31
PC: 0
Server: 0

Not Authorized: 3
Not Categorized: 6
Tracked: 0

Learn Status
100%
Operations:

Connections: 1662
IPv4: 1537
TCP: 1537
UDP: 0

Not Authorized: 958
Tracked Connections: 0
Multicast: 0
Off LAN: 0

Import a List of Device Names:

Using a spreadsheet program, create a csv file with the IP Address in Column 1 and the Camera Name/Location in Column 2 - do not use commas in the camera name.

Selected File:

Names Added:

IP Addresses not matched:

To auto populate device names after the Learn Process is completed:

Title the device names file 'DeviceNames.csv' and place the file in the EdgeSentry 'MyDocuments' directory.

Export full list of Network Devices:

Export the current list of network devices to a CSV file. This file will save to the current desktop and can be opened and manipulated with any spreadsheet program.

File Name:

Devices written to Report: 0

Create CSV File of System Uptime:

Calculate the uptime/downtime of all SNMP enabled devices on the network. This file can be opened and manipulated with any spreadsheet program.

File Name:

Devices written to Report: 0

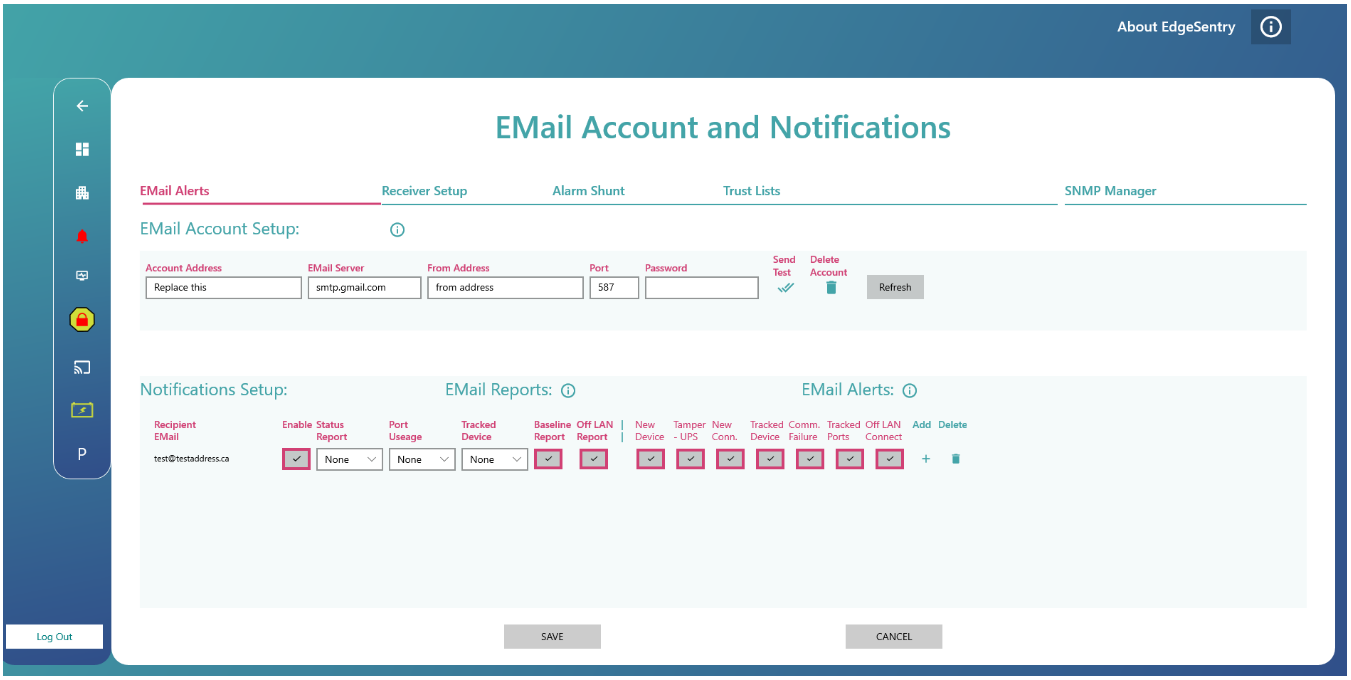
Import list of device names (cross referenced by IP Address)

A/ Upload a list of device names into EdgeSentry:

1/ Create a spreadsheet with the IP address of each device in column 1 and the device name in column 2. Ensure that there are no commas in the device names.
2/ Save the file as a csv file.
3/ From the Configuration Tool **System Status** page, go to ***Import a List of Device Names*** and click on “**Select a CSV File**”. Navigate to the file with your device names
4/ Click on “**Start Import**” – the system will notify you of the number of devices names that were matched.

Notifications Page

The primary use of the Notifications Page is to set up how EdgeSentry reports its status to either the client or a security integrator. This menu is used to set up email notifications or backup and reporting to an EdgeSentry Receiver. If the client is monitoring the site themselves using the **EdgeSentry Dashboard**, then there is no need to configure these settings.



EMail Account and Notifications

EMail Account Setup:

Account Address	EMail Server	From Address	Port	Password
Replace this	smtp.gmail.com	from address	587	

Notifications Setup: EMail Reports: EMail Alerts:

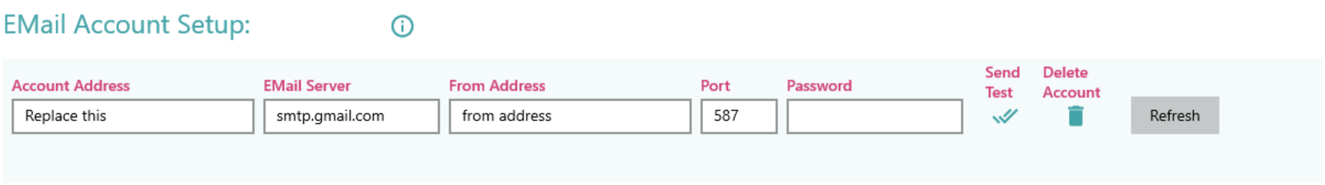
Recipient EMail	Enable	Status Report	Port Useage	Tracked Device	Baseline Report	Off LAN Report	New Device	Tamper - UPS	New Conn.	Tracked Device	Comm. Failure	Tracked Ports	Off LAN Connect
test@testaddress.ca	☑	None	None	None	☑	☑	☑	☑	☑	☑	☑	☑	☑

The Notifications menu is for managing outbound communications from the EdgeSentry. Most basic configurations will include alert notifications being sent by email and/or alerts being communicated to an EdgeSentry Receiver. The Alarm Shunt and Trust Lists pages are covered in the manual sections on Alarm Management.

Basics of setting up an email account

EdgeSentry currently uses SMTP for outbound emails and this requires that you have a simple SMTP account. There are a number of services that provide free or low cost outbound SMTP Email services. Brevo is one such service, though there are many others out there. Please note that Gmail has enhanced their security such that you cannot use a Gmail account as the outbound SMTP account.

Shown below is the default view of the outbound SMTP account configuration in the Notifications menu.



EMail Account Setup:

Account Address	EMail Server	From Address	Port	Password	Send Test	Delete Account
Replace this	smtp.gmail.com	from address	587		✓	

Fill in the following information:

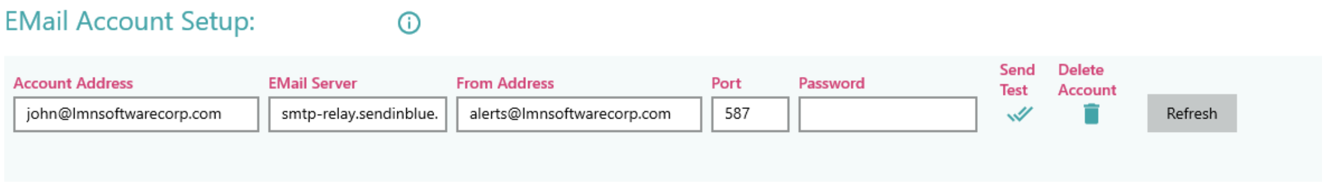
1/ The outbound account name – this is usually an email address under which the SMTP service was configured.

2/ The SMTP service will provide you with a Email Server address

3/ You need to provide a "from" email address – this can be anything as long as it is in a recognizable email form.

4/ The SMTP Service will also provide you with a default port to use – often this will be 587

5/ Enter your SMTP service password.

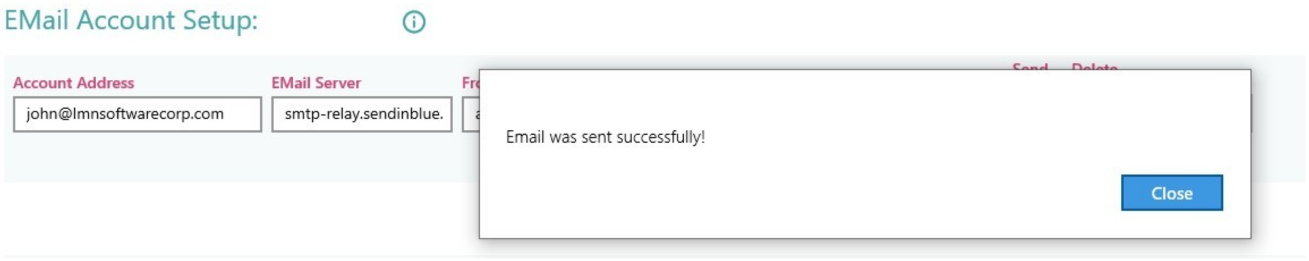


EMail Account Setup:

Account Address	EMail Server	From Address	Port	Password	Send Test	Delete Account
john@lmnsoftwarecorp.com	smtp-relay.sendinblue.	alerts@lmnsoftwarecorp.com	587		✓	

6/ Press the **SAVE** button. Note that the password will disappear after it has been entered correctly and saved.

Click on the double check mark ("Send Test") to test the email. Note that the email will send to the "from" address you have entered. After about a minute, a message will appear showing that the email sent correctly or showing an error in the communications. Note that this message checks communications from the EdgeSentry to the mail service but not beyond. If the "from" address is non-existent, that will not cause the test email to fail!



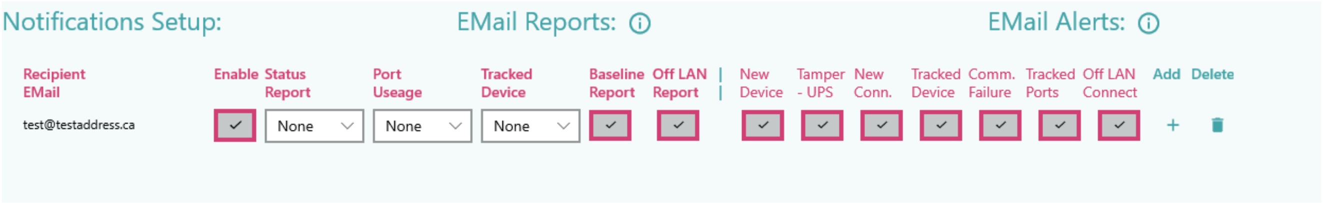
EMail Account Setup:

Account Address	EMail Server
john@lmnsoftwarecorp.com	smtp-relay.sendinblue.

Email was sent successfully!

Adding Email Recipients – Alerts and Reports

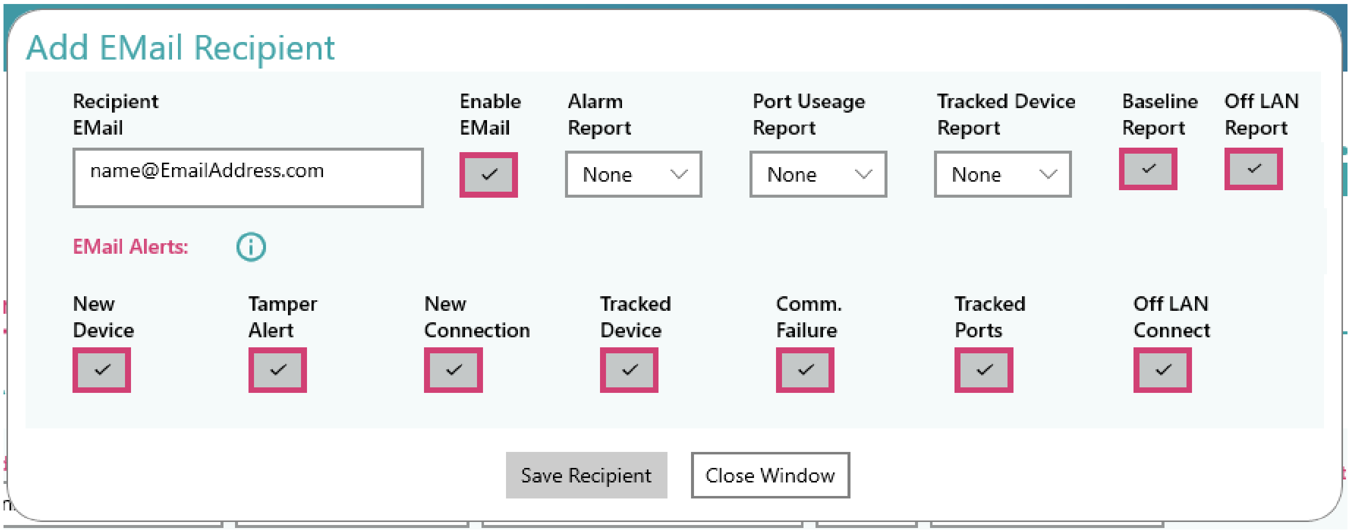
Once the email account is testing correctly, add an email recipient by clicking the green "+".



Notifications Setup: EMail Reports: ⓘ EMail Alerts: ⓘ

Recipient EMail	Enable	Status Report	Port Useage	Tracked Device	Baseline Report	Off LAN Report	New Device	Tamper - UPS	New Conn.	Tracked Device	Comm. Failure	Tracked Ports	Off LAN Connect	Add	Delete
test@testaddress.ca	☑	None	None	None	☑	☑	☑	☑	☑	☑	☑	☑	☑	+	🗑

The “Add Email Recipient” popup will appear on screen.



Add EMail Recipient

Recipient EMail	Enable EMail	Alarm Report	Port Usage Report	Tracked Device Report	Baseline Report	Off LAN Report
name@EmailAddress.com	☑	None	None	None	☑	☑

EMail Alerts: ⓘ

New Device	Tamper Alert	New Connection	Tracked Device	Comm. Failure	Tracked Ports	Off LAN Connect
☑	☑	☑	☑	☑	☑	☑

Fill in the following fields:

1/ Recipient Email

2/ If you want to start sending email notifications right away, click the Enable Email box (it will turn blue when enabled)

3/ Select reports that you want to have sent to the recipient and the required frequency.

4/ Click on the alerts you want the recipient to receive. DO NOT select all email alerts – this will likely cause “spamming” which may be enough to busy out your SMTP service!

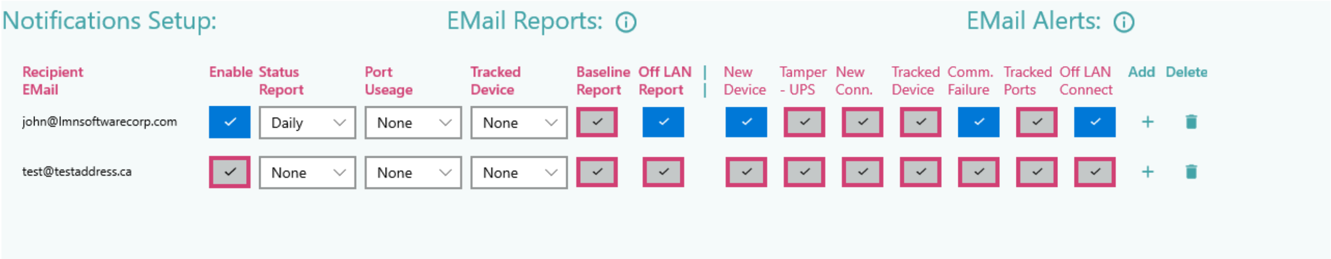
If this is a new installation and you are unsure of what to add, use the following guidelines:

Reports:

- Use the Alarm or Status Report as the basic daily summary of activity on the system

Alerts:

For **security alerts** check the “New Device” box. Do not select “Off LAN Connections” until you have verified that all PC connections have been set to “ignore outbound” in the Devices page. See the **Full EdgeSentry Configuration Manual** section on “**Preventing SPAM**” for more details.



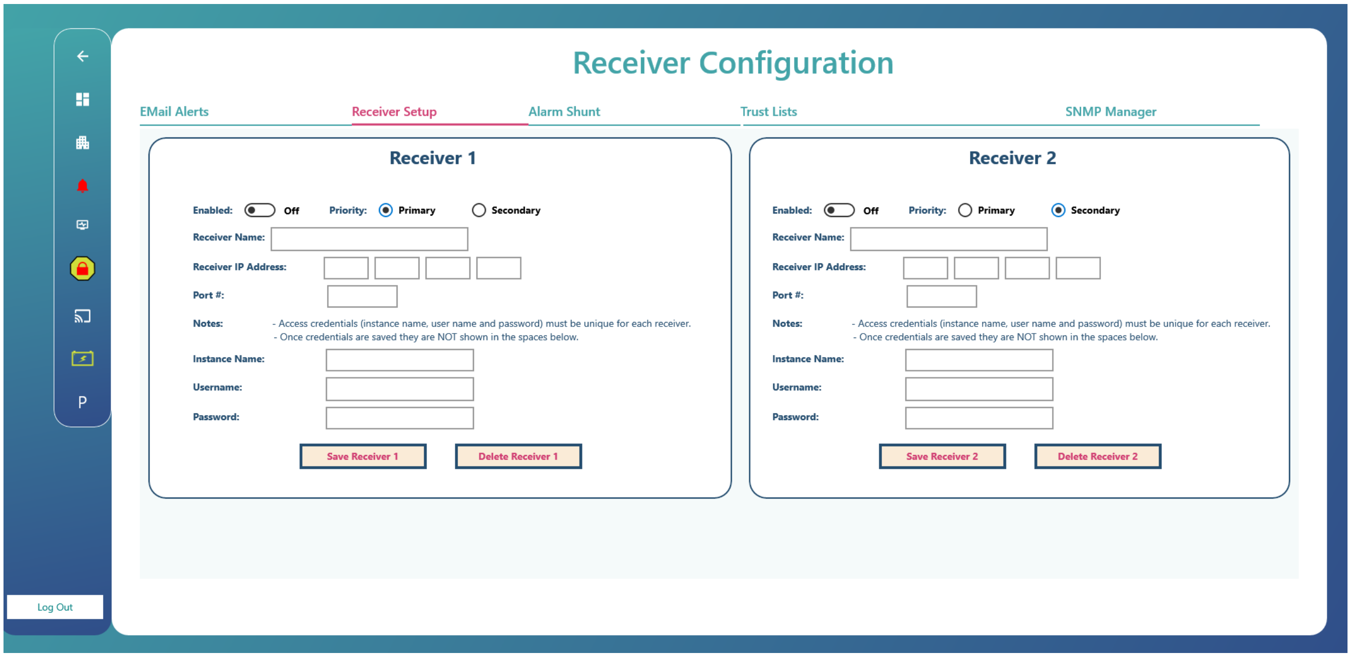
Notifications Setup: EMail Reports: ⓘ EMail Alerts: ⓘ

Recipient EMail	Enable	Status Report	Port Useage	Tracked Device	Baseline Report	Off LAN Report	New Device	Tamper - UPS	New Conn.	Tracked Device	Comm. Failure	Tracked Ports	Off LAN Connect	Add	Delete
john@lmnsoftwarecorp.com	☑	Daily	None	None	☐	☑	☑	☐	☐	☐	☑	☐	☑	+	🗑
test@testaddress.ca	☐	None	None	None	☐	☐	☐	☐	☐	☐	☐	☐	☐	+	🗑

For **communications alerts** select “Comm Failure” and (optionally) “Tamper and UPS” alerts. “Tracked Ports” should only be selected if you have selected some ports and protocols to be alarmed on in the Ports menu AND you have verified that there are not devices currently using those ports on your system. If you alarm a port that is currently being used on your network, this could generate hundreds of alerts very quickly (SPAM).

Setting up a Receiver

Click on “Receiver Setup” on the top menu bar.



Receiver Configuration

Receiver 1

Enabled: Off   Priority: ● Primary ○ Secondary

Receiver Name:

Receiver IP Address:

Port #:

Notes: - Access credentials (instance name, user name and password) must be unique for each receiver.
- Once credentials are saved they are NOT shown in the spaces below.

Instance Name:

Username:

Password:

Save Receiver 1   Delete Receiver 1

Receiver 2

Enabled: Off   Priority: ○ Primary ● Secondary

Receiver Name:

Receiver IP Address:

Port #:

Notes: - Access credentials (instance name, user name and password) must be unique for each receiver.
- Once credentials are saved they are NOT shown in the spaces below.

Instance Name:

Username:

Password:

Save Receiver 2   Delete Receiver 2

To set up a receiver, you should have the following information:

1/ EdgeSentry Site Number (set in the Site information menu) – note that this must be a unique number

2/ Receiver IP Address

3/ Receiver Port Number

4/ Receiver Instance Name (this is set at the receiver at the time it was configured)

5/ Receiver Credentials –***identical usernames and passwords cannot be used for both receivers***. Note that the username and password will disappear after they have been entered successfully. You can update other receiver parameters without having to re-enter the receiver credentials.

Fill out each of the required fields:

Enabled (click to toggle)

Receiver Name A common name for the receiver, alphanumeric only (no special characters)

Receiver IP Numeric only

Port Number Numeric only

Instance Name AlphaNumeric, must match the name used in the receiver setup

User Name Alphanumeric, no special characters

Password Minimum 9 characters, minimum one uppercase, one lowercase, one number

After the receiver has been saved in the EdgeSentry there will be a pause of up to 5 minutes before the EdgeSentry starts communicating with the Receiver. You can check the communication status of the EdgeSentry by logging into the receiver and checking the following:

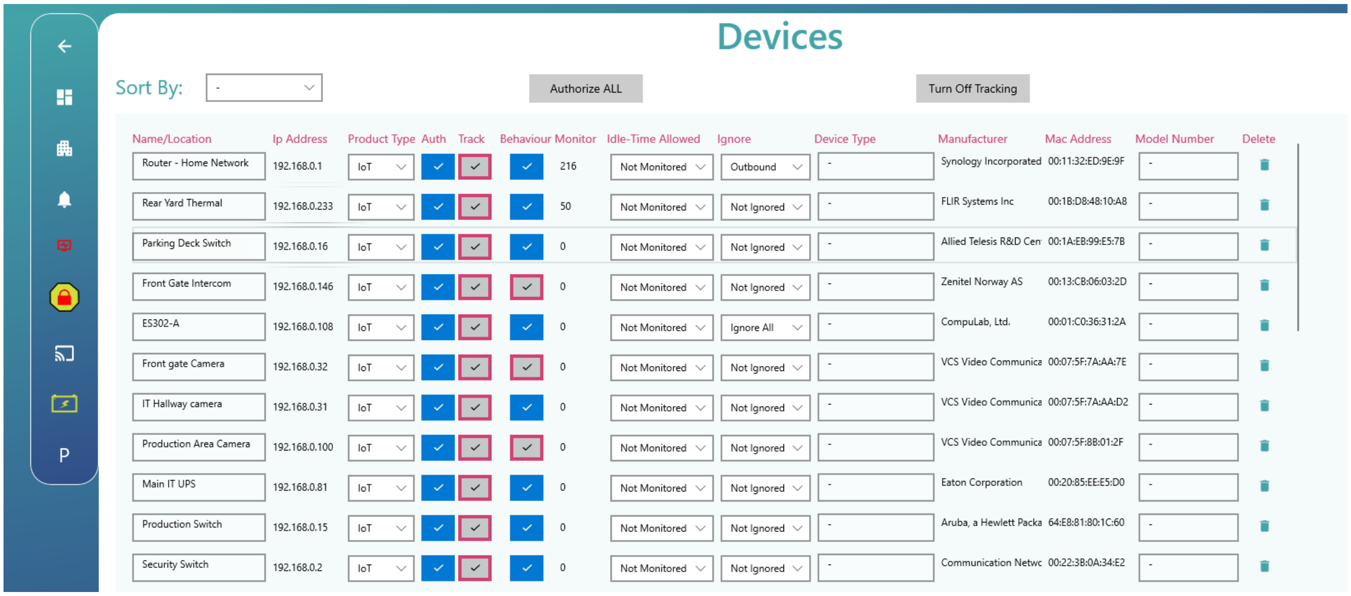
- The EdgeSentry site number is showing as a monitored site
- During the first 10 minutes of communication the site number will show in the “Communication Error” window. It will stay listed here until it has completed 10 consecutive minutes of communications.

Working with Devices – the Devices Page

There are two critical fields in the Devices Page – the device name/location and the “Product Type” setting. Ensure that these are configured as a minimum, though choosing and configuring a device supervision strategy is also highly recommended.

Note that the makeup of Devices page will vary depending on whether the EdgeSentry has been placed in Isolation Mode or Integration Mode. Do not change the mode of the EdgeSentry without being sure that you understand the implications of the change. If you need more information on changing between modes, see the EdgeSentry **Wiring Guide**.

Devices Page – in Isolation Mode



Devices

Sort By: -

Name/Location	Ip Address	Product Type	Auth	Track	Behaviour Monitor	Idle-Time Allowed	Ignore	Device Type	Manufacturer	Mac Address	Model Number	Delete
Router - Home Network	192.168.0.1	IoT	☑	☑	☑ 216	Not Monitored	Outbound	-	Synology Incorporated	00:11:32:ED:9E:9F	-	🗑
Rear Yard Thermal	192.168.0.233	IoT	☑	☑	☑ 50	Not Monitored	Not Ignored	-	FLIR Systems Inc	00:1B:D8:48:10:A8	-	🗑
Parking Deck Switch	192.168.0.16	IoT	☑	☑	☑ 0	Not Monitored	Not Ignored	-	Allied Telesis R&D Cen	00:1A:EB:99:E5:7B	-	🗑
Front Gate Intercom	192.168.0.146	IoT	☑	☑	☑ 0	Not Monitored	Not Ignored	-	Zenitel Norway AS	00:13:CB:06:03:2D	-	🗑
ES302-A	192.168.0.108	IoT	☑	☑	☑ 0	Not Monitored	Ignore All	-	CompuLab, Ltd.	00:01:C0:36:31:2A	-	🗑
Front gate Camera	192.168.0.32	IoT	☑	☑	☑ 0	Not Monitored	Not Ignored	-	VCS Video Communica	00:07:5F:7A:AA:7E	-	🗑
IT Hallway camera	192.168.0.31	IoT	☑	☑	☑ 0	Not Monitored	Not Ignored	-	VCS Video Communica	00:07:5F:7A:AA:D2	-	🗑
Production Area Camera	192.168.0.100	IoT	☑	☑	☑ 0	Not Monitored	Not Ignored	-	VCS Video Communica	00:07:5F:8B:01:2F	-	🗑
Main IT UPS	192.168.0.81	IoT	☑	☑	☑ 0	Not Monitored	Not Ignored	-	Eaton Corporation	00:20:85:EE:E5:D0	-	🗑
Production Switch	192.168.0.15	IoT	☑	☑	☑ 0	Not Monitored	Not Ignored	-	Aruba, a Hewlett Packa	64:E8:81:80:1C:60	-	🗑
Security Switch	192.168.0.2	IoT	☑	☑	☑ 0	Not Monitored	Not Ignored	-	Communication Netwc	00:22:3B:0A:34:E2	-	🗑

Devices Menu Isolation Mode fields:

Device Name/Location The name/location of the device - Alphanumeric characters only

Product Type Choose one of: IoT, PC or Server

Auth Check the box if this device is Authorized to be on the network

Track If the device is NOT authorized to be on the network, check the **Track** option to track the device’s connections on the network.

Behaviour Monitor Behaviour monitoring builds a profile of device connections and packet sizes to determine what is normal or abnormal device behaviour.

Idle Time Allowed Idle time monitoring allows the device to be silent on the network for a limited period of time before creating an alert. This would normally only be used for devices that don’t create enough traffic to be monitored with behaviour monitoring.

Ignore The ignore function allow you to turn off alerts for off network connections for a specific device. Typically this is used only for **PC** devices and is set for "**Ignore Outbound**" connections.

Device Type (Optional field) This is a field you can use for your own purposes

Model Number (Optional field) This is a field you can use to track device model numbers

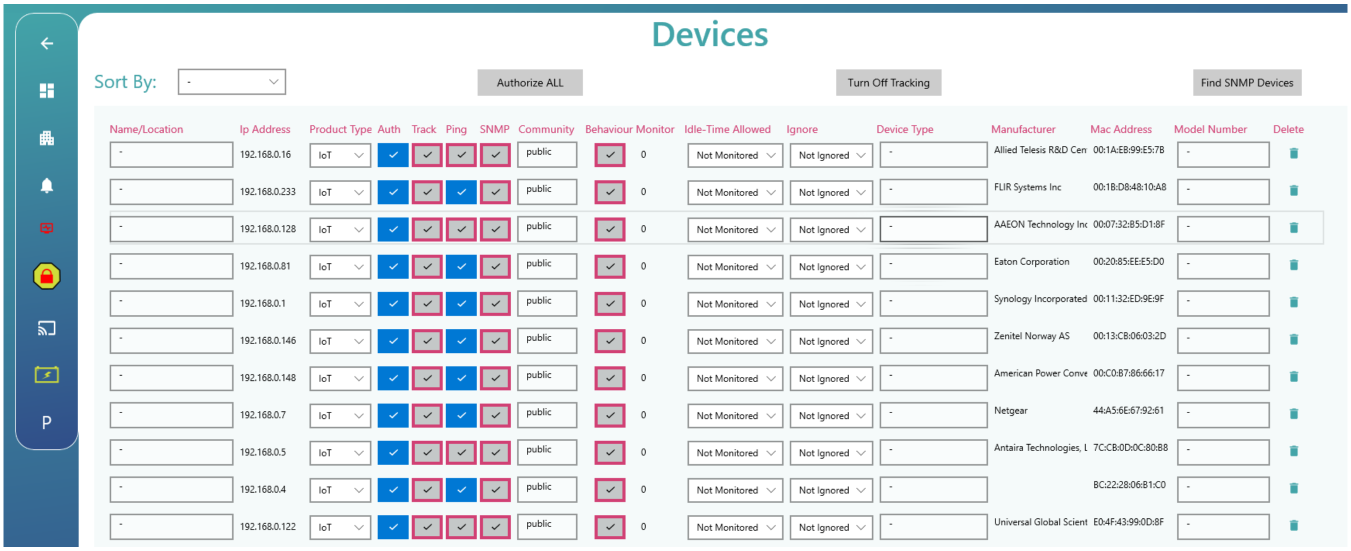
Typical Device Settings:

IoT Product Type Auth checked, Behaviour Checked, Idle Time Not Monitored, Ignore Not Ignored

PC Product Type Auth checked, Behaviour NOT Checked, Idle Time set to 24 hours, Ignore Outbound

Server Product Type Auth checked, Behaviour Checked, Idle Time Not Monitored, Ignore Outbound

Devices Page – in Integration Mode



Name/Location	Ip Address	Product Type	Auth	Track	Ping	SNMP	Community	Behaviour	Monitor	Idle-Time Allowed	Ignore	Device Type	Manufacturer	Mac Address	Model Number	Delete
-	192.168.0.16	IoT	☑	☑	☑	☑	public	☑	0	Not Monitored	Not Ignored	-	Allied Telesis R&D Cen	00:1A:EB:99:E5:7B	-	🗑
-	192.168.0.233	IoT	☑	☑	☑	☑	public	☑	0	Not Monitored	Not Ignored	-	FLIR Systems Inc	00:1B:D8:48:10:A8	-	🗑
-	192.168.0.128	IoT	☑	☑	☑	☑	public	☑	0	Not Monitored	Not Ignored	-	AAEON Technology Inc	00:07:32:B5:D1:8F	-	🗑
-	192.168.0.81	IoT	☑	☑	☑	☑	public	☑	0	Not Monitored	Not Ignored	-	Eaton Corporation	00:20:85:EE:E5:D0	-	🗑
-	192.168.0.1	IoT	☑	☑	☑	☑	public	☑	0	Not Monitored	Not Ignored	-	Synology Incorporated	00:11:32:ED:9E:9F	-	🗑
-	192.168.0.146	IoT	☑	☑	☑	☑	public	☑	0	Not Monitored	Not Ignored	-	Zenitel Norway AS	00:13:CB:06:03:2D	-	🗑
-	192.168.0.148	IoT	☑	☑	☑	☑	public	☑	0	Not Monitored	Not Ignored	-	American Power Conve	00:C0:B7:86:66:17	-	🗑
-	192.168.0.7	IoT	☑	☑	☑	☑	public	☑	0	Not Monitored	Not Ignored	-	Netgear	44:A5:6E:67:92:61	-	🗑
-	192.168.0.5	IoT	☑	☑	☑	☑	public	☑	0	Not Monitored	Not Ignored	-	Antaira Technologies, L	7C:CB:0D:0C:80:B8	-	🗑
-	192.168.0.4	IoT	☑	☑	☑	☑	public	☑	0	Not Monitored	Not Ignored	-		BC:22:28:06:B1:C0	-	🗑
-	192.168.0.122	IoT	☑	☑	☑	☑	public	☑	0	Not Monitored	Not Ignored	-	Universal Global Scient	E0:4F:43:99:0D:8F	-	🗑

Devices Menu Integration Mode fields:

Device Name/Location The name/location of the device - Alphanumeric characters only

Product Type Choose one of: IoT, PC or Server

Auth Check the box if this device is Authorized to be on the network

Track If the device is NOT authorized to be on the network, check the **Track** option to track the device's connections on the network.

Ping EdgeSentry will periodically ping the selected device to ensure that it is present on the network.

SNMP EdgeSentry will use **SNMP ver 1 Read-Only** to verify the device is functional and to verify the device's MAC Address. Note that the device has to have SNMP ver 1 enabled with the same community name.

Community If using SNMP to monitor a device, set the community field to the same community used in the device.

Behaviour Monitor Behaviour monitoring builds a profile of device connections and packet sizes to determine what is normal or abnormal device behaviour.

Idle Time Allowed Idle time monitoring allows the device to be silent on the network for a limited period of time before creating an alert. This would normally only be used for devices that don't create enough traffic to be monitored with behaviour monitoring.

Ignore The ignore function allow you to turn off alerts for off network connections for a specific device. Typically this is used only for **PC** devices and is set for "**Ignore Outbound**" connections.

Device Type (Optional field) This is a field you can use for your own purposes

Model Number (Optional field) This is a field you can use to track device model numbers

Typical Device Settings:

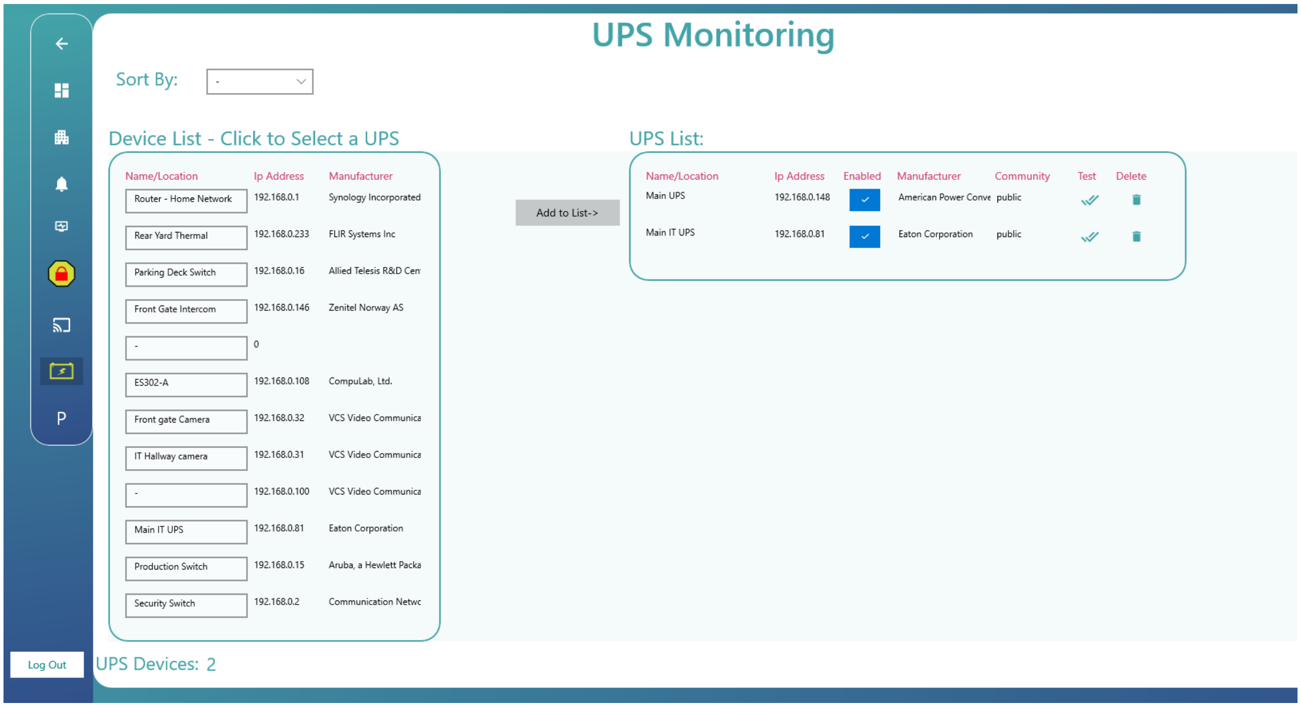
IoT Product Type Auth checked, Either PING or Behaviour Checked, Idle Time Not Monitored, Ignore Not Ignored

PC Product Type Auth checked, PING and Behaviour NOT Checked, Idle Time set to 24 hours, Ignore Outbound

Server Product Type Auth checked, Behaviour Checked, Idle Time Not Monitored, Ignore Outbound

Adding UPS Monitoring - The UPS Monitoring Page

In order for EdgeSentry to monitor a UPS it must meet the conditions outlined below. If you are using the EdgeSentry in Isolation mode, then you may also be required to move the UPSs onto a dedicated network so that you can use SNMP version 1 read only without putting traffic onto the monitored network.



UPS Monitoring

Device List - Click to Select a UPS

Name/Location	Ip Address	Manufacturer
Router - Home Network	192.168.0.1	Synology Incorporated
Rear Yard Thermal	192.168.0.233	FLIR Systems Inc
Parking Deck Switch	192.168.0.16	Allied Telesis R&D Cen
Front Gate Intercom	192.168.0.146	Zenitel Norway AS
-	0	
ES302-A	192.168.0.108	CompuLab, Ltd.
Front gate Camera	192.168.0.32	VCS Video Communica
IT Hallway camera	192.168.0.31	VCS Video Communica
-	192.168.0.100	VCS Video Communica
Main IT UPS	192.168.0.81	Eaton Corporation
Production Switch	192.168.0.15	Aruba, a Hewlett Packa
Security Switch	192.168.0.2	Communication Netwo

UPS List:

Name/Location	Ip Address	Enabled	Manufacturer	Community	Test	Delete
Main UPS	192.168.0.148	☑	American Power Conve	public	✓✓	🗑
Main IT UPS	192.168.0.81	☑	Eaton Corporation	public	✓✓	🗑

UPS Devices: 2

EdgeSentry is able to monitor any UPS that meets all of the following conditions:

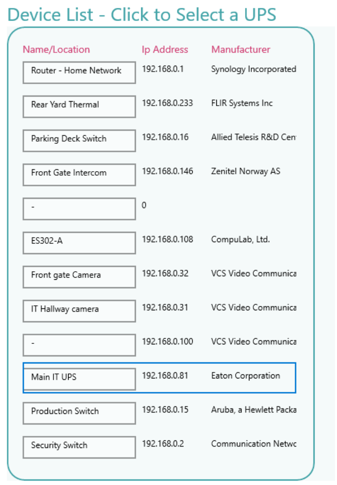
1/ Supports the SNMP UPS MIB - RFC 1628

2/ Has a network interface card for SNMP communications and is networked

3/ Has SNMP version 1 Read-Only enabled

Note that if you are using Isolation mode on your EdgeSentry, you may have to discuss the use of SNMP ver 1 with the site IT department and get their agreement to place the UPSs on a separate network dedicated to UPS monitoring.

To add a UPS for monitoring:



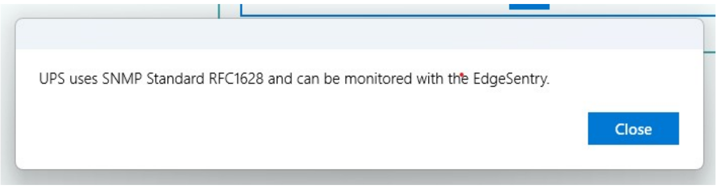
Device List - Click to Select a UPS

Name/Location	Ip Address	Manufacturer
Router - Home Network	192.168.0.1	Synology Incorporated
Rear Yard Thermal	192.168.0.233	FLIR Systems Inc
Parking Deck Switch	192.168.0.16	Allied Telesis R&D Cen
Front Gate Intercom	192.168.0.146	Zenitel Norway AS
-	0	
ES302-A	192.168.0.108	CompuLab, Ltd.
Front gate Camera	192.168.0.32	VCS Video Communica
IT Hallway camera	192.168.0.31	VCS Video Communica
-	192.168.0.100	VCS Video Communica
Main IT UPS	192.168.0.81	Eaton Corporation
Production Switch	192.168.0.15	Aruba, a Hewlett Packa
Security Switch	192.168.0.2	Communication Netwo

1/ Scroll through the device list at the left until you find a UPS to monitor. Click on the device to select it (it will outline in a blue rectangle)

2/ click on the “Add to List ->” button. The UPS will appear in the UPS List.

3/ Click the “Test” button.

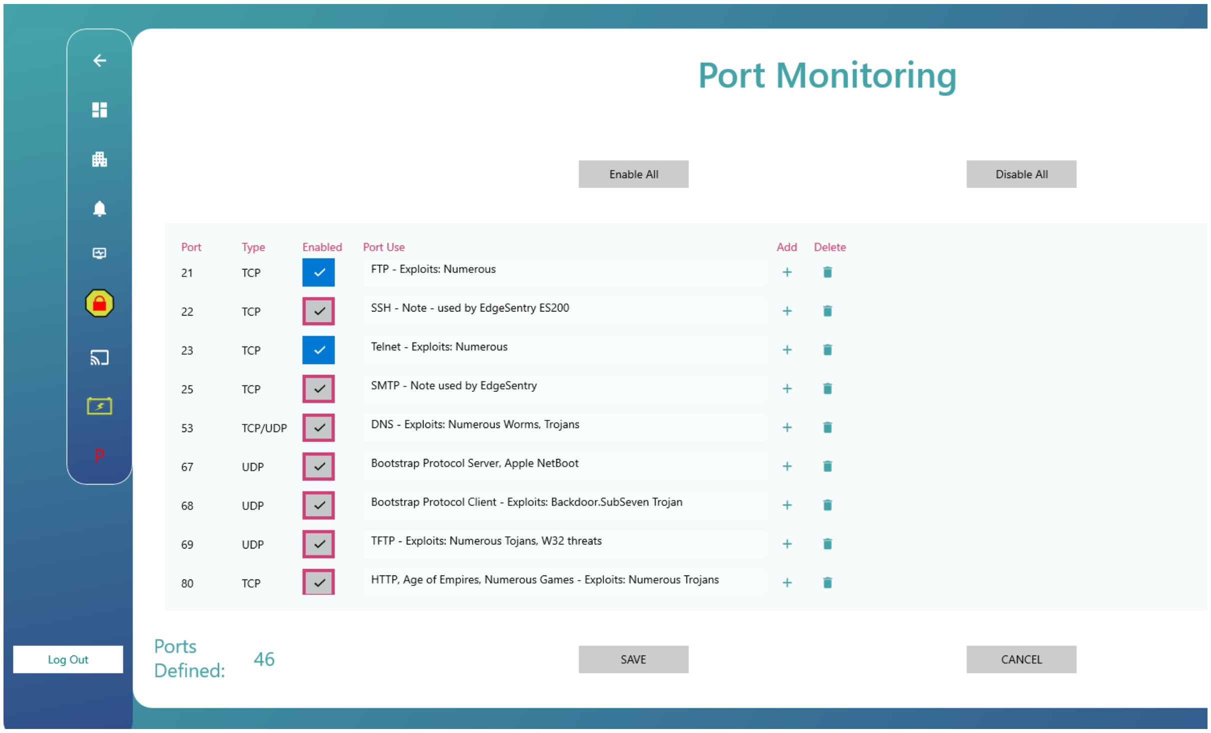


UPS uses SNMP Standard RFC1628 and can be monitored with the EdgeSentry.

4/ A confirmation will appear confirming that the UPS can be monitored with EdgeSentry.

The Port Monitoring Page

By default, EdgeSentry will monitor the network for use of FTP and Telnet. If EdgeSentry is in Isolation mode it is advisable that you also add SNMP to the port monitoring list – enable this by clicking on the box next to port 25 in the **Port Monitoring List** and clicking on “**SAVE”** at the bottom of the screen.



Port	Type	Enabled	Port Use	Add	Delete
21	TCP	☑	FTP - Exploits: Numerous	+	🗑
22	TCP	☑	SSH - Note - used by EdgeSentry ES200	+	🗑
23	TCP	☑	Telnet - Exploits: Numerous	+	🗑
25	TCP	☑	SMTP - Note used by EdgeSentry	+	🗑
53	TCP/UDP	☑	DNS - Exploits: Numerous Worms, Trojans	+	🗑
67	UDP	☑	Bootstrap Protocol Server, Apple NetBoot	+	🗑
68	UDP	☑	Bootstrap Protocol Client - Exploits: Backdoor.SubSeven Trojan	+	🗑
69	UDP	☑	TFTP - Exploits: Numerous Tojans, W32 threats	+	🗑
80	TCP	☑	HTTP, Age of Empires, Numerous Games - Exploits: Numerous Trojans	+	🗑

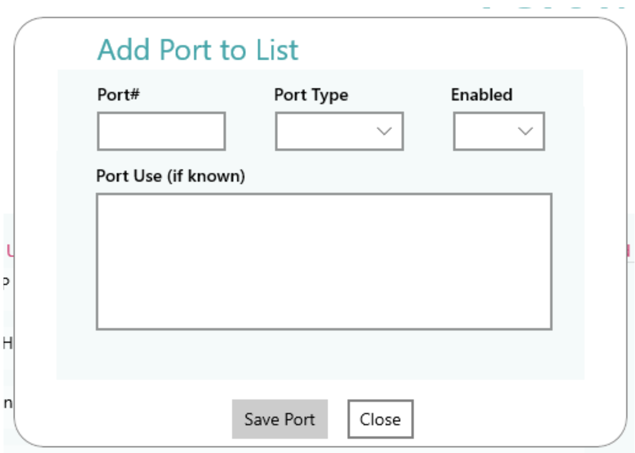
Ports Defined: 46

EdgeSentry will create priority alerts for any monitored/forbidden network port/protocols that are used on the network. Furthermore, the EdgeSentry switch interface functionality can allow you to block use of monitored or forbidden ports.

To enable a port for monitoring:

- Scroll through the list and find the port if it is pre-configured. Check the “Enabled” box for that port.

If the port is not pre-configured, check the “+” icon.



1/ Input the port number (numeric only)

2/ Select TCP, UPD or TCP/UDP

3/ Enable the port monitoring for this port

4/ Provide a description of why you are monitoring for this behaviour or a reference to the device it pertains to.

5/ Click “Save Port” and the port will be added to the list.

Completion of the Basic EdgeSentry Configuration

Once you have completed these steps, the EdgeSentry is configured for monitoring. There are steps that may need to be taken at a later date to manage nuisance alerts or authorize additional devices that have been added to the network. These steps are covered in the **Full EdgeSentry Configuration Manual**.

Additionally you may want to add the site's Layer 2/3 network switches to the EdgeSentry configuration. The EdgeSentry network switch integration provides the following benefits:

- Easily find the switch and port number where any device is connected to the network
- Harden the network switches against intrusion
- Add network switch alerts to EdgeSentry
- View switch loading and PoE usage in simple to understand diagrams
- View the topology of your network and detect any unknown uplinks
- Enable active security for EdgeSentry Alerts

In order to add switches to the EdgeSentry, they must be managed switches that are on the EdgeSentry supported switches list on the website. See the EdgeSentry **Switch Interface Guide** for the configuration steps.