Datensaft inc.

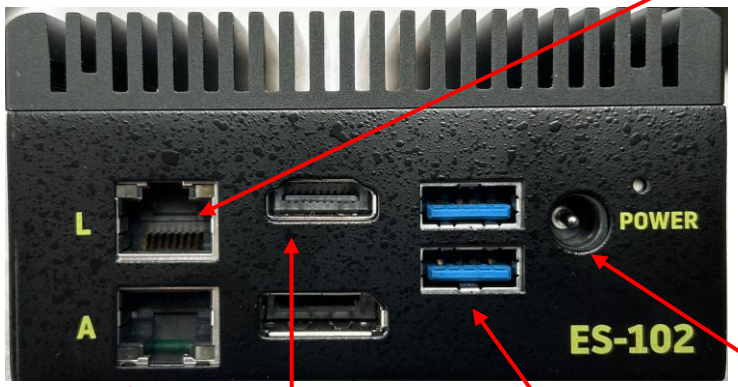
EdgeSentry configuration

With the **ES-Portal** app

This page intentionally left blank

Basic Wiring – network connections

ES-102



L (Listening) Port
Used for capturing network communications
Unmanaged switch network:
- connects to any port on the switch where the servers are located

Managed switch network:
- Connects at a switch where the servers are located. That switch port should be configured as a Mirror or SPAN port (see slide #11)

Monitor
HDMI port

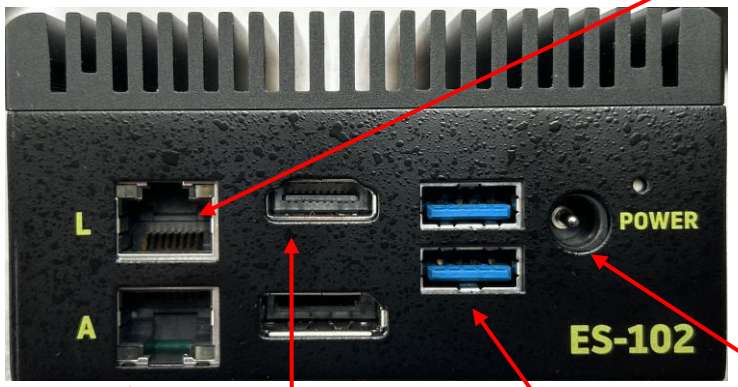
Power connection

USB ports for keyboard/mouse

A (Administration) Port
This port is used for administration, monitoring and outbound internet communications.

Basic Wiring – network connections

ES-102



L (Listening) Port
Used for capturing network communications
Unmanaged switch network:
- connects to any port on the switch where the servers are located

Managed switch network:
- Connects at a switch where the servers are located. That switch port should be configured as a Mirror or SPAN port (see slide #11)

Monitor
HDMI port

Power connection

USB ports for keyboard/mouse

A (Administration) Port
This port is used for administration, monitoring and outbound internet communications.

Basic Wiring – IP Addresses

ES-102

2 ethernet ports:
If one logical network
L (Listening) – assign an APIPA address (169.254.1.x)
A (Administration) – Use DHCP or assign an address in the range of the logical network

If two logical networks
L (Listening) – Use DHCP or assign an address in the range of the monitored network
A (Administration) – Use DHCP or assign an address in the range of the logical network used for Administration or internet access

Basic Wiring – network connections

ES-304 / ES-604

Monitor HDMI port

USB ports for keyboard/mouse

Power connection

L (Listening) Port
Used for capturing network communications
Unmanaged switch network:
- connects to any port on the switch where the servers are located

Managed switch network:
- Connects at a switch where the servers are located. That switch port should be configured as a Mirror or SPAN port (see slide #11)

A (Administration) Port
This port is used for administration, monitoring and outbound internet communications.

(2) Ports
These port are used for connections to ancillary networks for the switch interface (control plane) or UPS networks.

Basic Wiring – IP Addresses

ES-304 / ES-604

4 ethernet ports:

If one logical network

L (Listening) – assign an APIPA address (169.254.1.x)

A (Administration) – Use DHCP or assign an address in the range of the logical network

If two logical networks

L (Listening) – Use DHCP or assign an address in the range of the monitored network

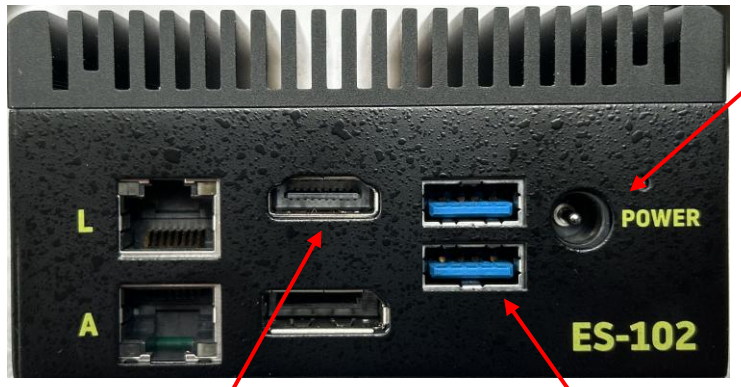
A (Administration) – Use DHCP or assign an address in the range of the logical network used for Administration or internet access

Spare Ports

Used for connections to the control plane network for the switch interface or to the UPS network for UPS monitoring.

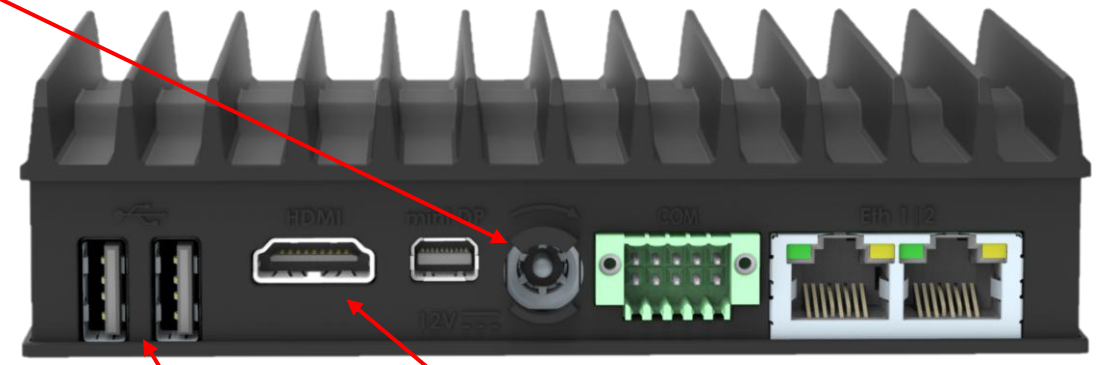
First power-up

- Connect a keyboard and mouse to the USB ports
- Connect a monitor to the HDMI port
- Apply power to the EdgeSentry



HDMI (Monitor) port and USB ports

Power



USB Ports and HDMI (Monitor) port

First login

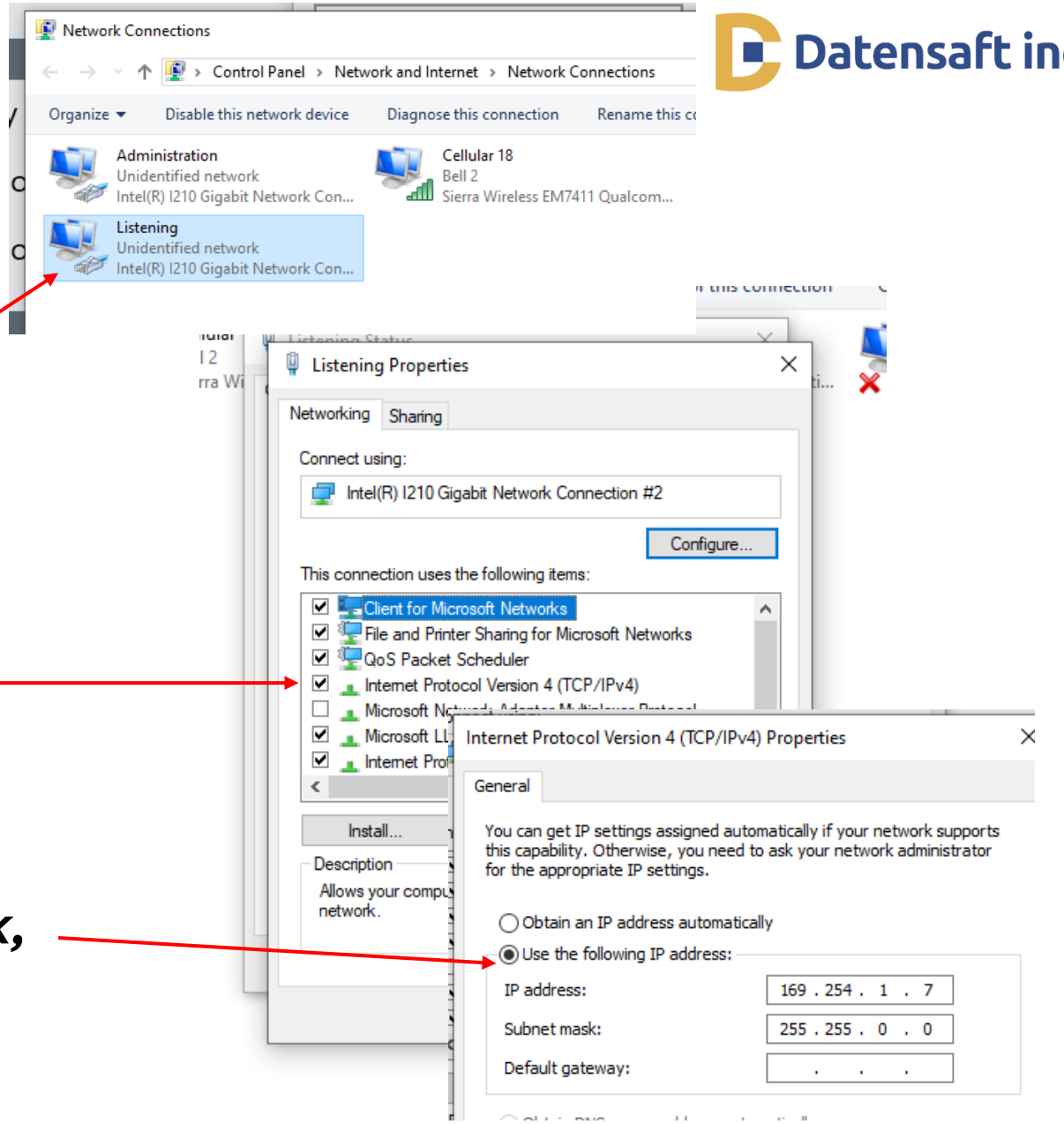
- The Windows EdgeSentry login is on a sticker on the bottom of the unit and also on a sheet of paper in the box
- Login and change the password

Set IP Addresses

- Go to the Windows ***Network & Internet settings***, Select Change adapter options and select the interface you want to alter.

- Select ***Properties***, then double click the ***Internet Protocol Version (TCP/IPv4)*** option.

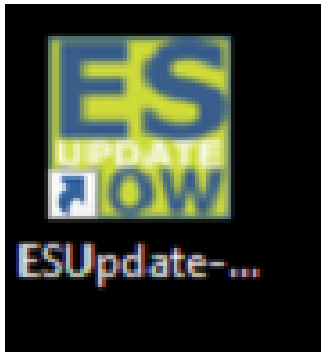
- ***Set the IP Address and subnet mask, or set DHCP***



Update EdgeSentry Core

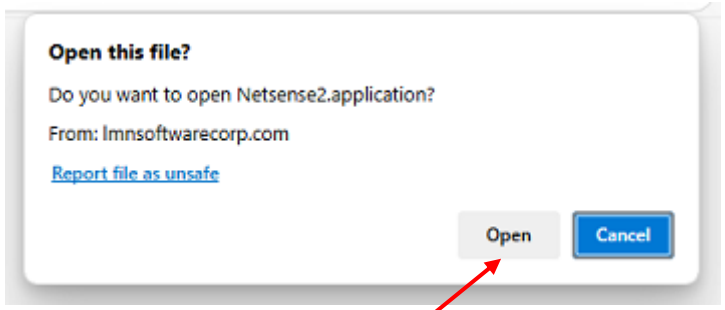
- Make sure your EdgeSentry is connected to the internet
- Double click the “Update Now” icon

1



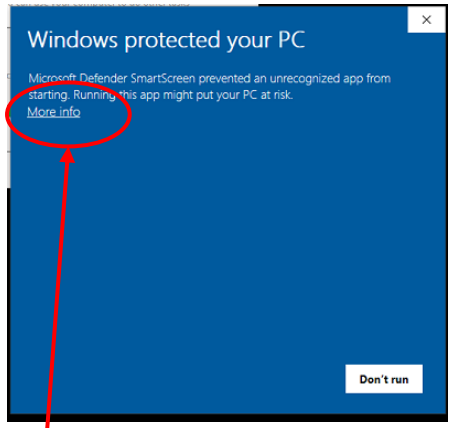
Double click

2



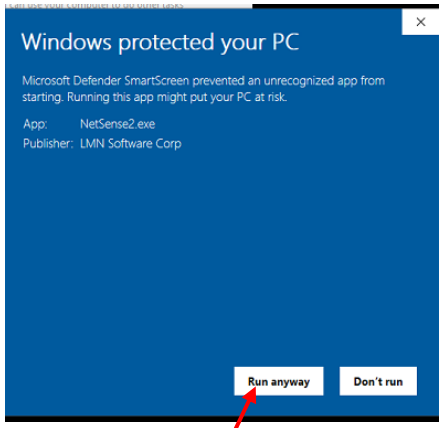
Click

3



Click

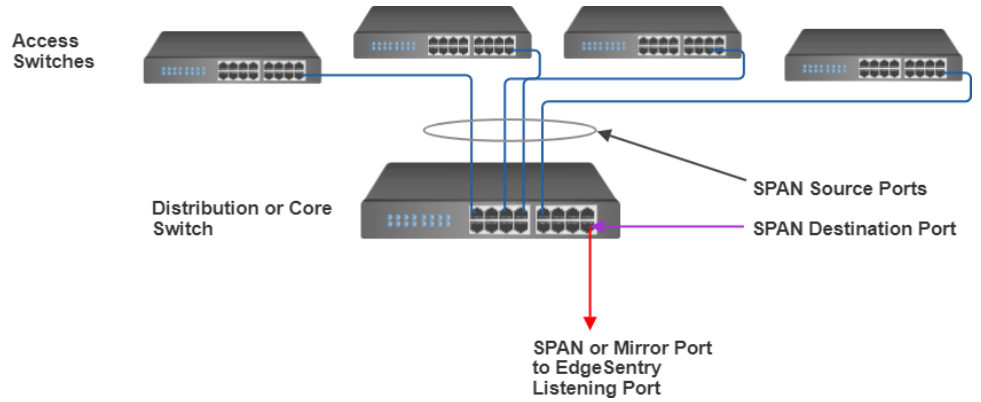
4



Click

Managed switch Mirror or SPAN Port

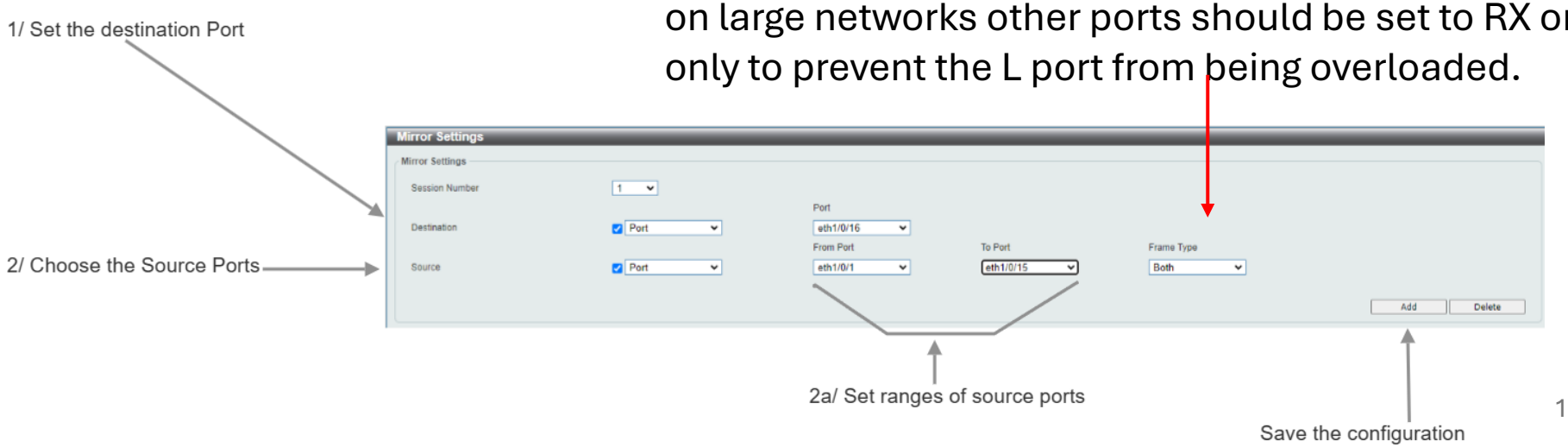
This step is necessary ONLY if you are connecting EdgeSentry to a managed switch, otherwise proceed to the next slide.



Choose the source ports that need to be monitored by EdgeSentry

Configure the Mirror (or SPAN) in the switch, specifying the source and destination (L) port

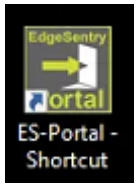
Router ports can be configured for traffic in BOTH directions, on large networks other ports should be set to RX only or TX only to prevent the L port from being overloaded.

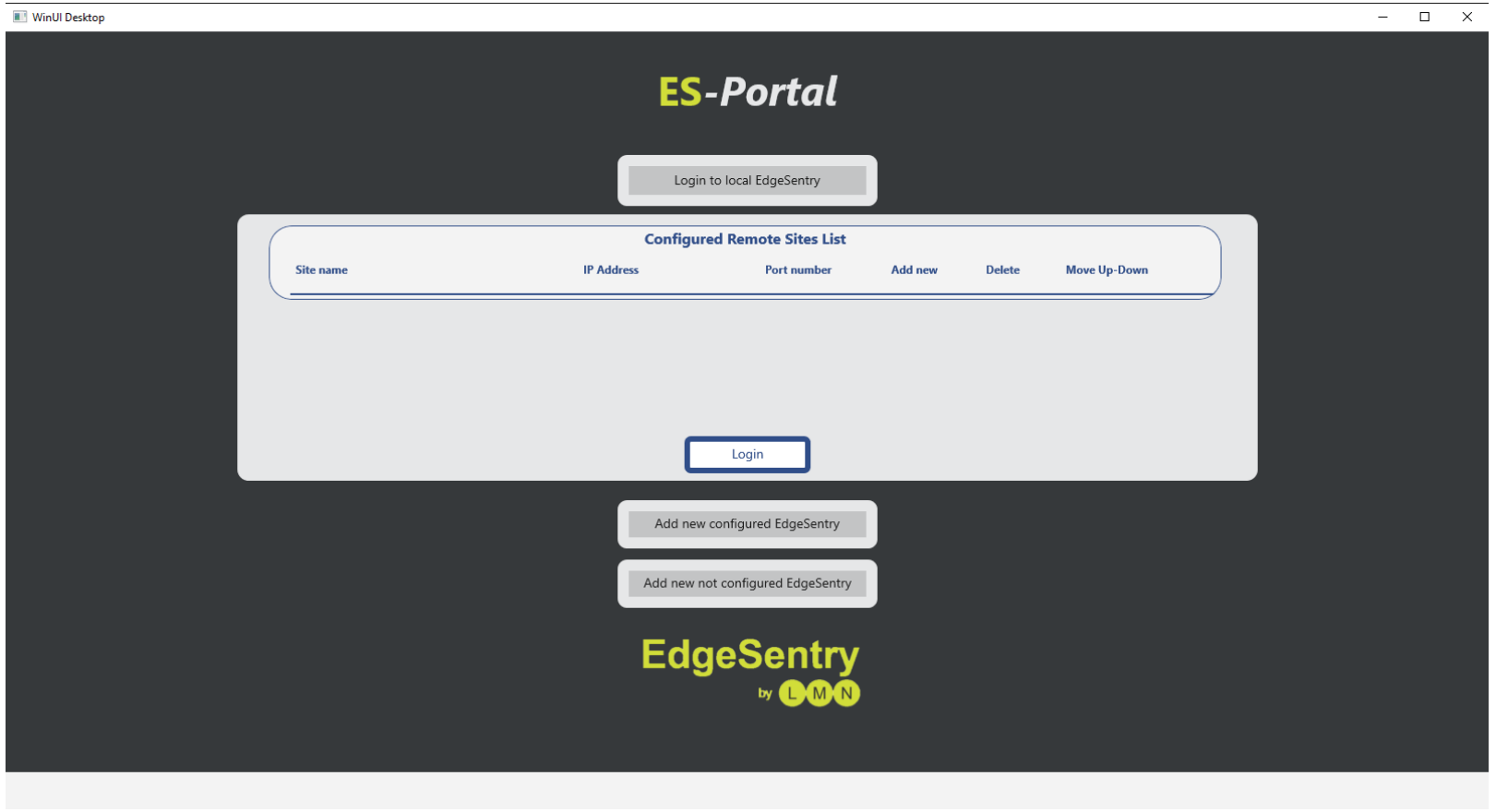


Launch ES-Portal

Is the ES-Portal software open on the desktop?

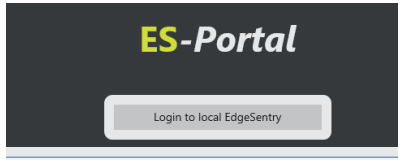
If not, locate the ES-Portal shortcut on the desktop and double click it.





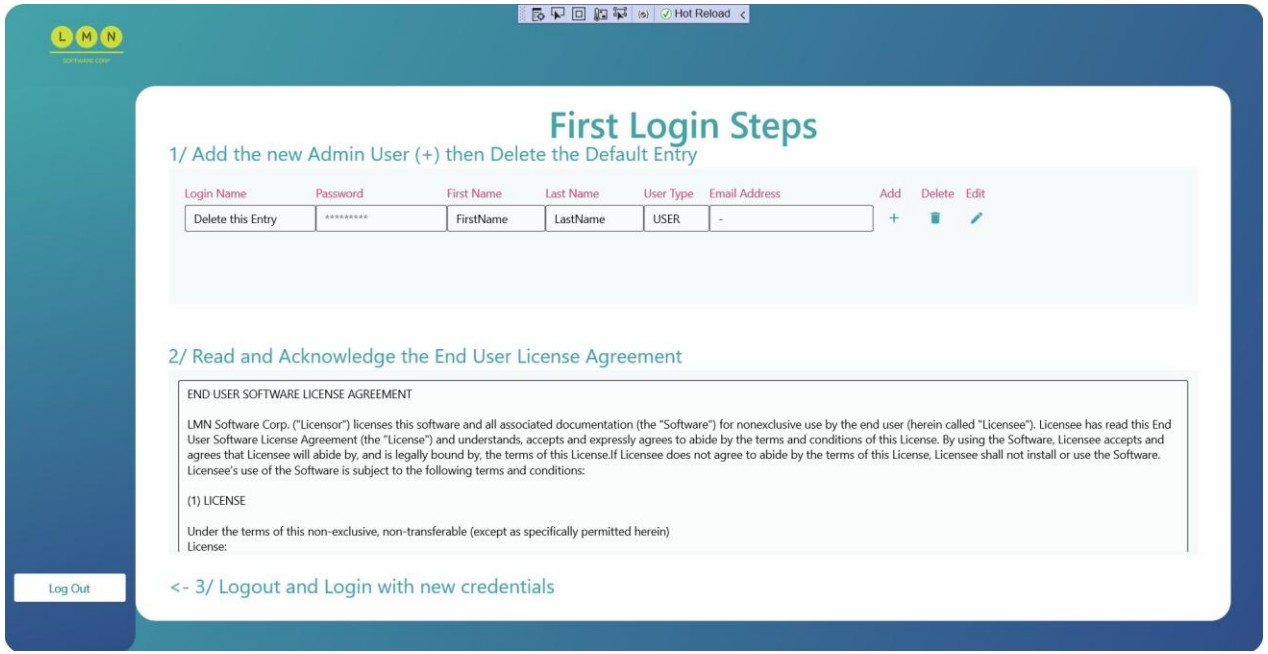
First login steps

Click “Login to Local EdgeSentry”



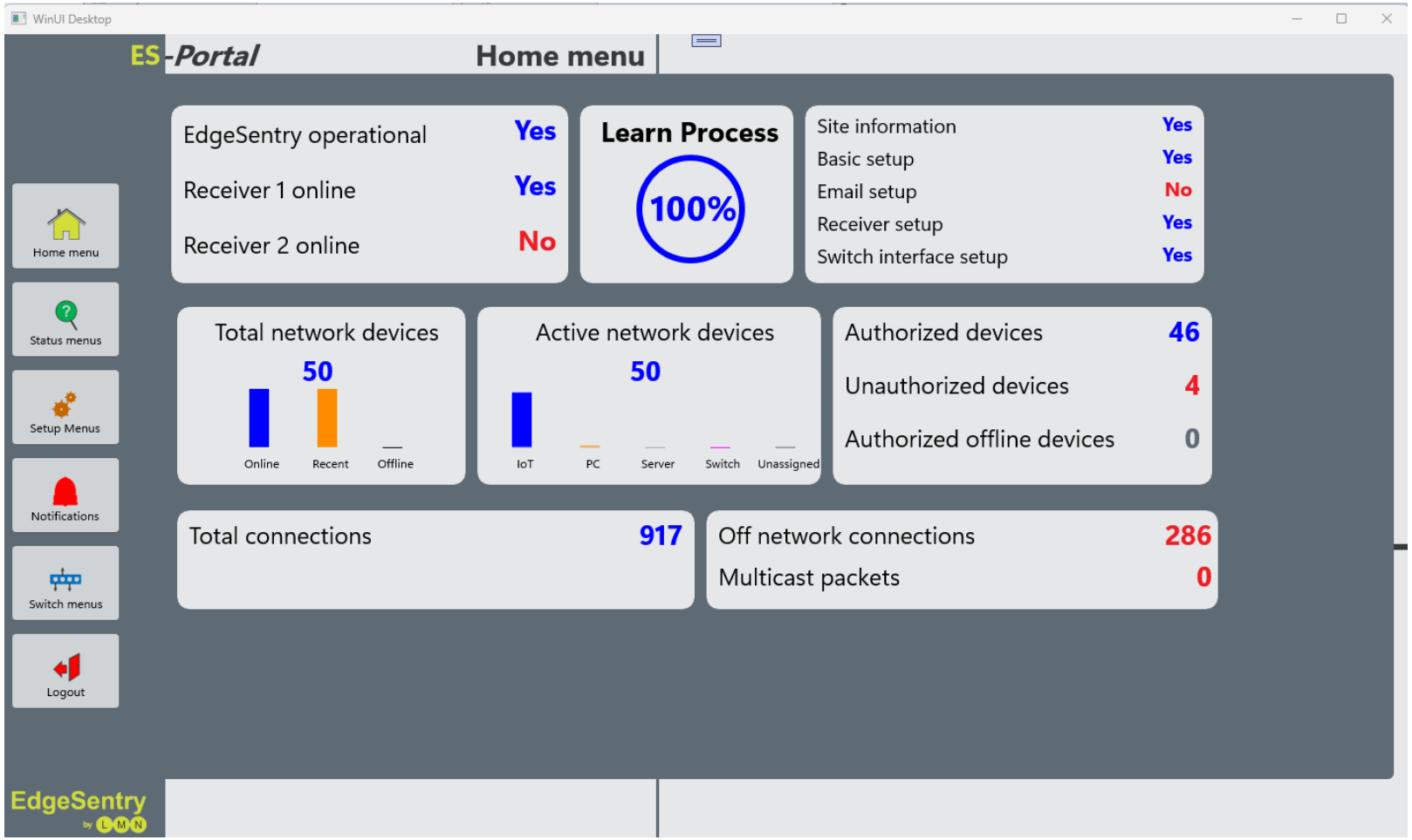
If the system has not been configured, you will be taken to a page for adding new users and acknowledging the End User License Agreement (EULA).

- Add new ADMIN users (for remote access)
- Delete the default user
- Read and acknowledge the EULA
- Log out and log in again using the “Login to Local EdgeSentry” button



The ES-Portal menu system

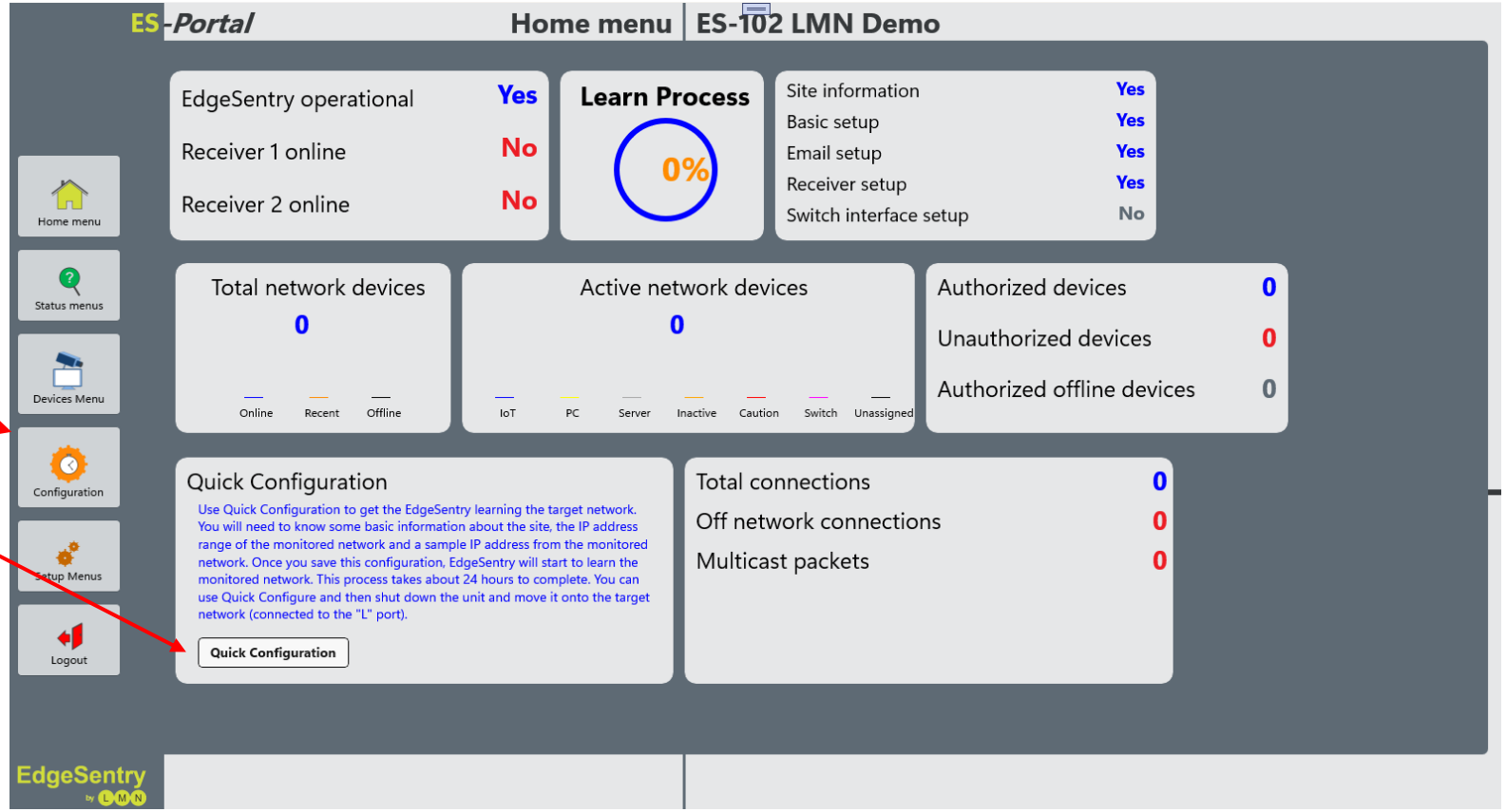
The “Home” menu provides a summary of the EdgeSentry configuration status and a menu bar for configuring and monitoring the EdgeSentry



The ES-Portal menu system

The “Home” menu before the EdgeSentry has “learned” the network

Select either “Quick Configuration” button

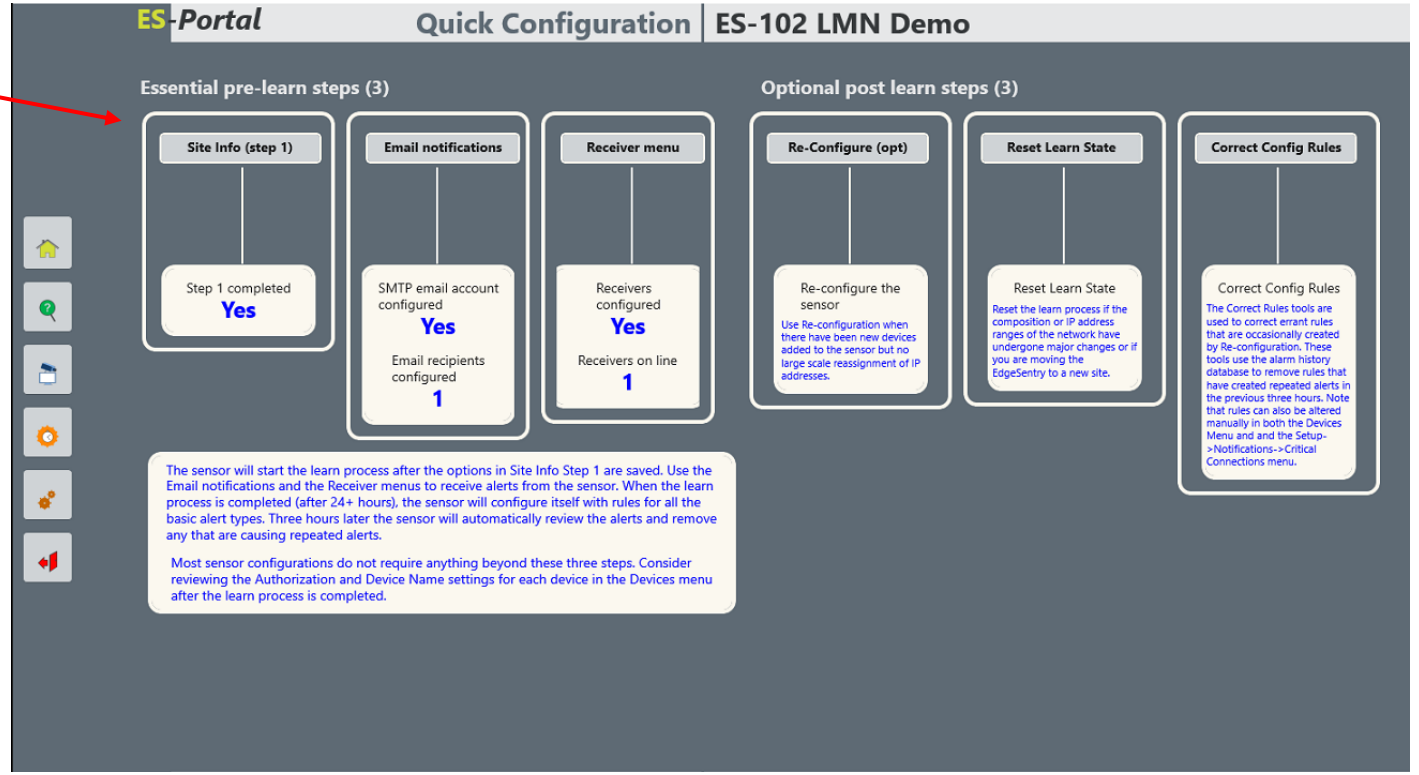


Quick Configuration

First steps:

- Site information
- Email notifications
- Receiver setup

Site info is the essential to get the sensor into learn mode. The other steps can be done at a later date.



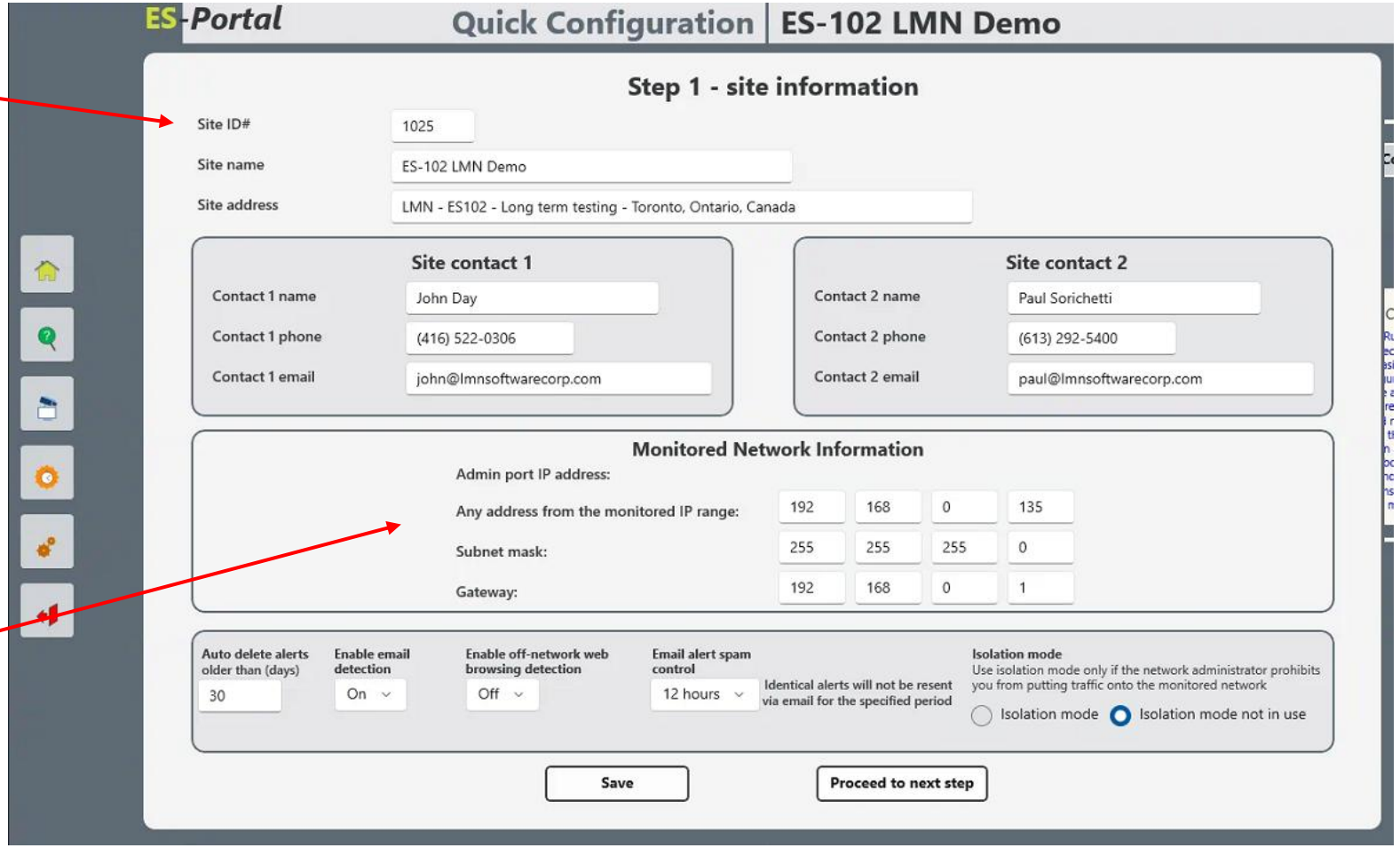
Quick Configuration

Fill in information about the site

Site ID# - a unique number for each EdgeSentry that is going to be monitored with a receiver.

Site information and site contacts is important as this information is used whenever the EdgeSentry communicates via email or the receiver.

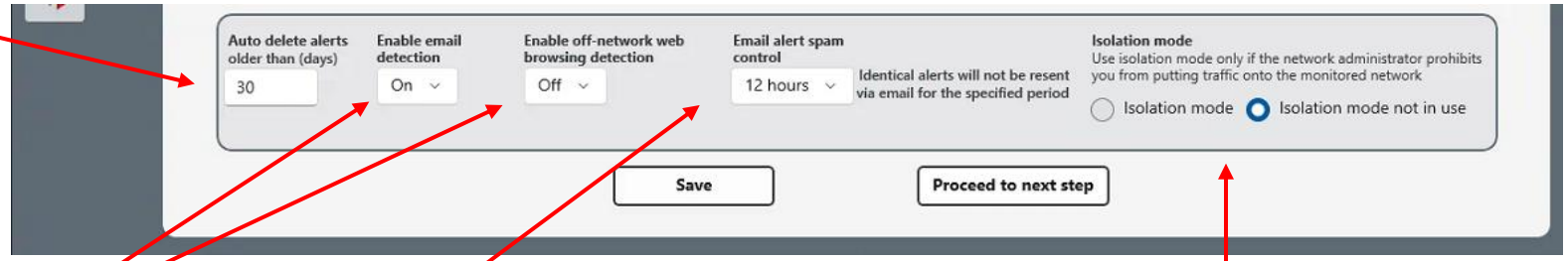
Monitored network information must be filled out for the EdgeSentry to go into learn mode.



Quick Configuration

5 configuration settings

Auto delete – The minimum number of days the EdgeSentry will hold alert information in it's database.



Email and Browsing detection – enable these if the users are not permitted to use the network for business activities (recommended)

Isolation mode – Default to "not in use" Select Isolation mode only if the client has specified that the sensor not put any traffic onto the monitored network.

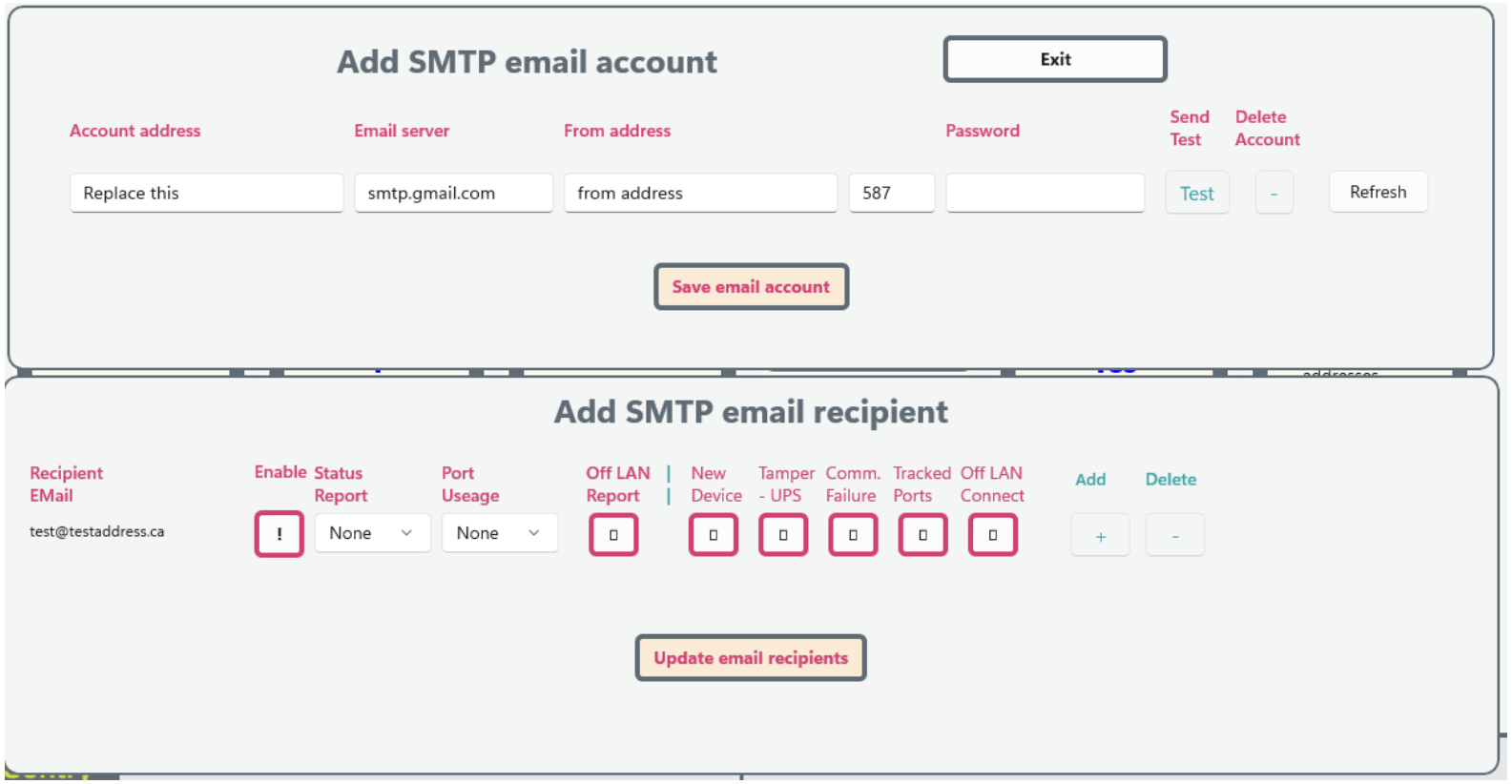
Email alert spam control – limits the number of times a day a specific alert will be sent –12 or 24 hours recommended

Click Save– this will put the sensor into learn mode. Click "Proceed to next step"

Quick Configuration

Input the SMTP **account email address**, **server,** a "**from Address**" (this is used as a destination address during testing), the **Port number** and the **account password.**

Save your settings, then click the "**Test**" button – after 20 seconds a message will confirm that the message has been sent or that there was an error.



Add email recipients

Click the "+" button to add a new user. Provide the email address and select daily/weekly/monthly reports for the user to receive and a selection of alerts.

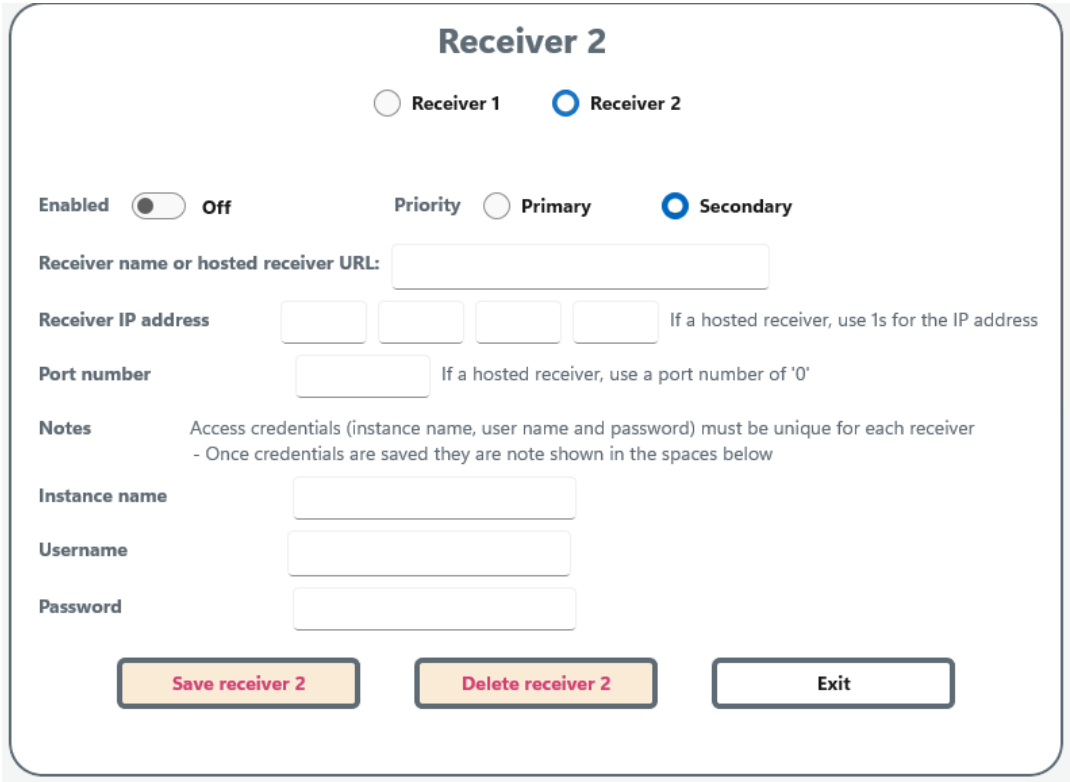
Quick Configuration

Select the receiver you want to configure, click the enable button and set it as primary (if using 2 receivers, one should be set as secondary).

Provide a **name for the receiver**, the **IP address** and **port number**.

Fill in the instance name and the credentials to write data to the EdgeSentry receiver.

Save the receiver.



Note that the Home menu will display the receiver online status, but that ***it can take up to 15 minutes for the receiver to connect*** when first set up or after a reboot of the EdgeSentry.

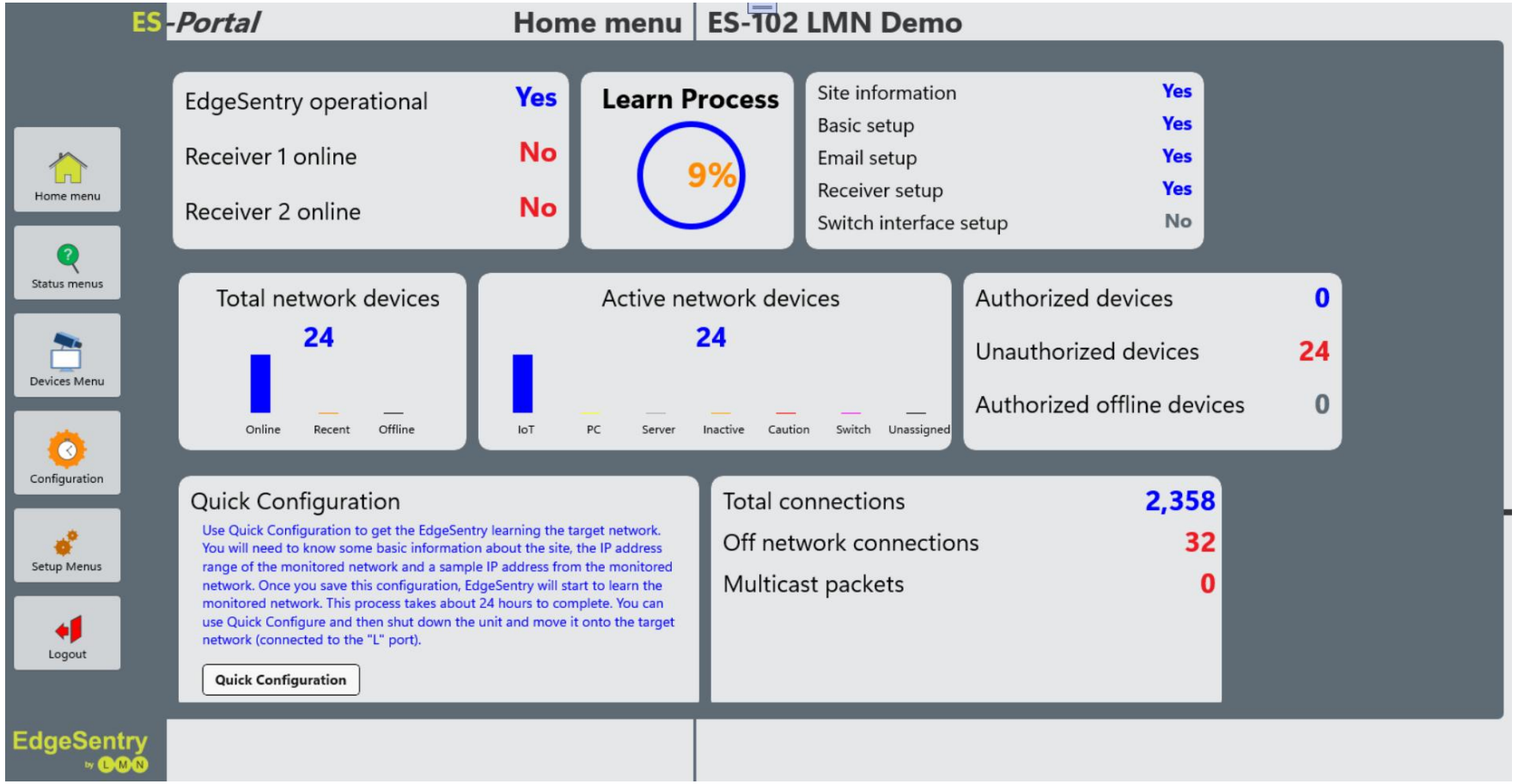
Quick Configuration

The learn process

The Sensor is in the “Learn” process which can take between 24 and 48 hours to complete

The sensor will compile device and connection information over this time.

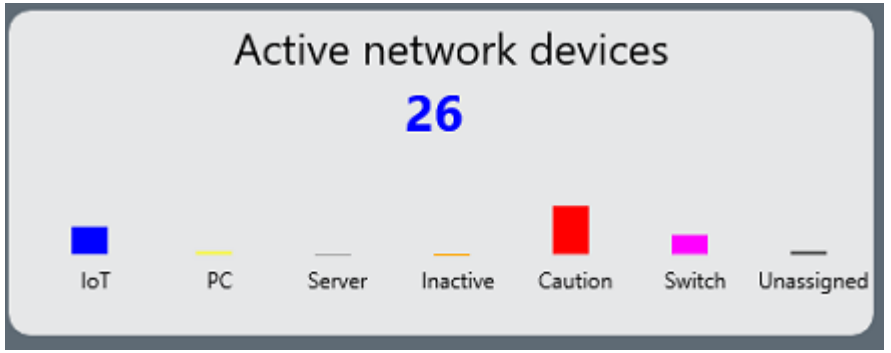
The learn process is complete when the Learn Process = 100% and the devices have been sorted into categories.



Quick Configuration

Learn process completed

The learn process is complete
when the Learn Process = 100%
and
the devices have been sorted into
categories.



The learn process also creates a set of log files when it completes that you will find in the **My Documents->Reports** directory. Successful completion of the Auto-config process creates the following files:

Auto-Configuration Report
or
1-AssignPCs.txt
2-AssignServers.txt
3-AssignInactive.txt
4-AssignServerSideCCM.txt
5-AssignEdgeCCM.txt
6-MonitorAllNonPCs.txt

Notes

- If there are not enough connections being monitored, the system will not complete this process but will retry on each system reboot. ***The Auto-Config process can also be run from ES-Portal.***
- Not all the files will be created during auto-configuration, presence of a few of the files indicates that the process has completed

Quick Configuration

Auto-configuration corrections

Three hours after the learn process is completed, the system will check for faults in the configuration and remove any alerts that faulty rules. If you are not sure if this part of the process has been completed, check the reports directory (**My Documents -> Reports**) for the following log files:

1-CCM_Rules_Removed.txt
2-OffNetwork_Rules_Removed.txt
3-IdleTime_Rules_Adjusted.txt
4-Ping_Rules_Adjusted.txt

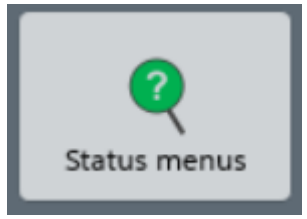
Note – the system only creates these files if the process is required, so the presence of just one of these four files indicates that the correction process has completed successfully.

The Auto-Configuration correction can also be run from ES-Portal from the **Quick Configuration->Re-Configure** menu.

Quick Configuration

Normal Operation

Once EdgeSentry has completed the Learn, Auto-Configuration and Correction processes your system should be operational and creating alerts. To view current alerts, click on the Status button.



Note that the status menu can take 5-10 seconds to open if there are a high number of system alerts.

The status menu shows a time line with alerts displayed on it grouped as “Security”, “Connectivity” and “Network”.

You can view detail of the alerts by clicking on the colored dots.

The ES-Portal menu system

The “Home” menu provides a summary of the EdgeSentry configuration

The “Status” menu provides a summary of the system status

The “Devices” menu shows all devices that have been detected on the network

The “Quick Configuration” menus determine the basic configuration of the sensor

The “Setup” menus (Setup, Notifications, Switches) are for configuration of advanced settings – hovering over the Setup Menus icon will display the sub menu

The “Logout” button returns you to the Login screen

The ES-Portal menu system

The “Setup” menu sub menus: (Setup, Notifications, Switches)

The “Setup” menu – basic system settings

The “Notification” menu – Email, Receivers and Critical Connection menus

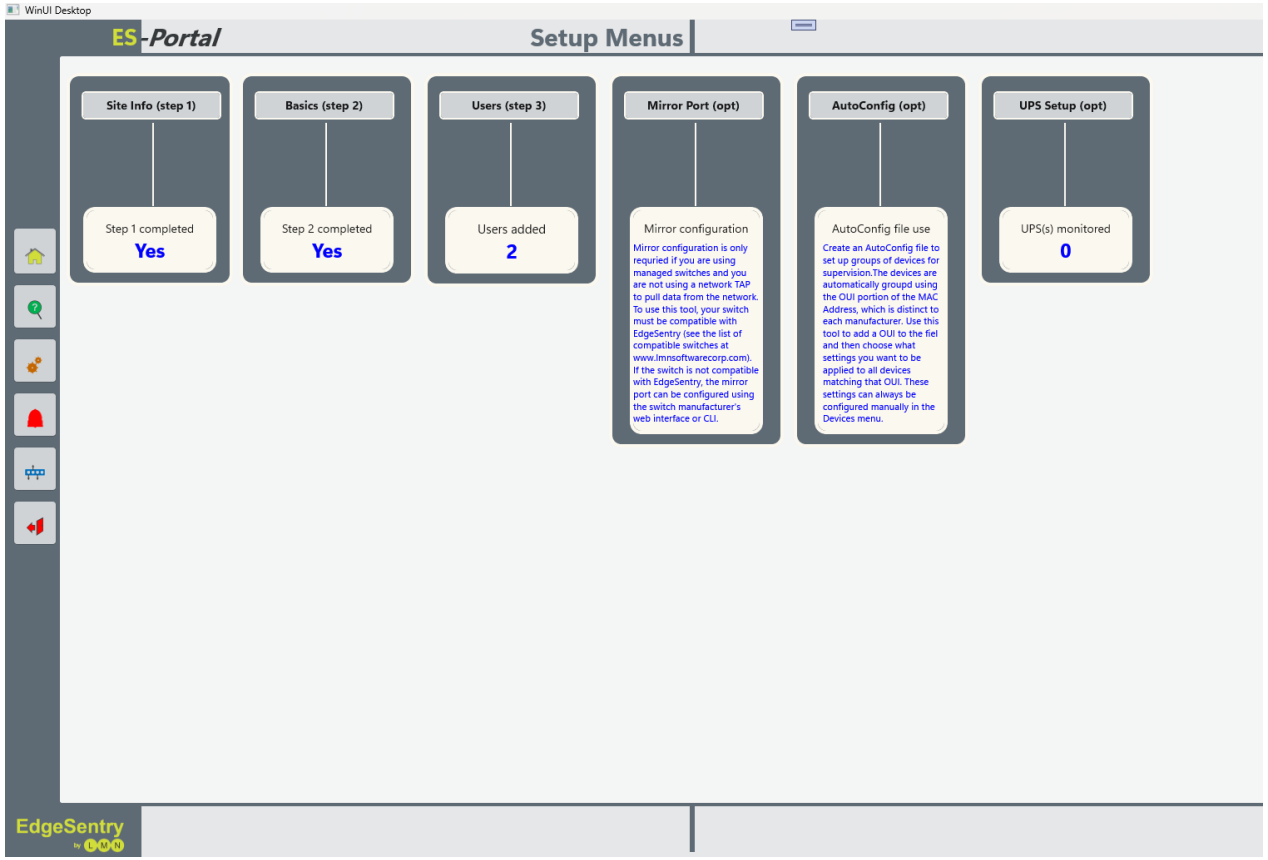
The “Switch” menu – used to add compatible switches to the EdgeSentry

Full configuration – Setup Menus

Click the “Setup” button

Initial setup requires entering **Site Info**, **Basics** and adding **Users** who will have remote access to the EdgeSentry.

At this point you can also (optionally) set up a **Mirror Port** on an EdgeSentry compatible switch, build an **AutoConfig File or add UPSs** for monitoring.



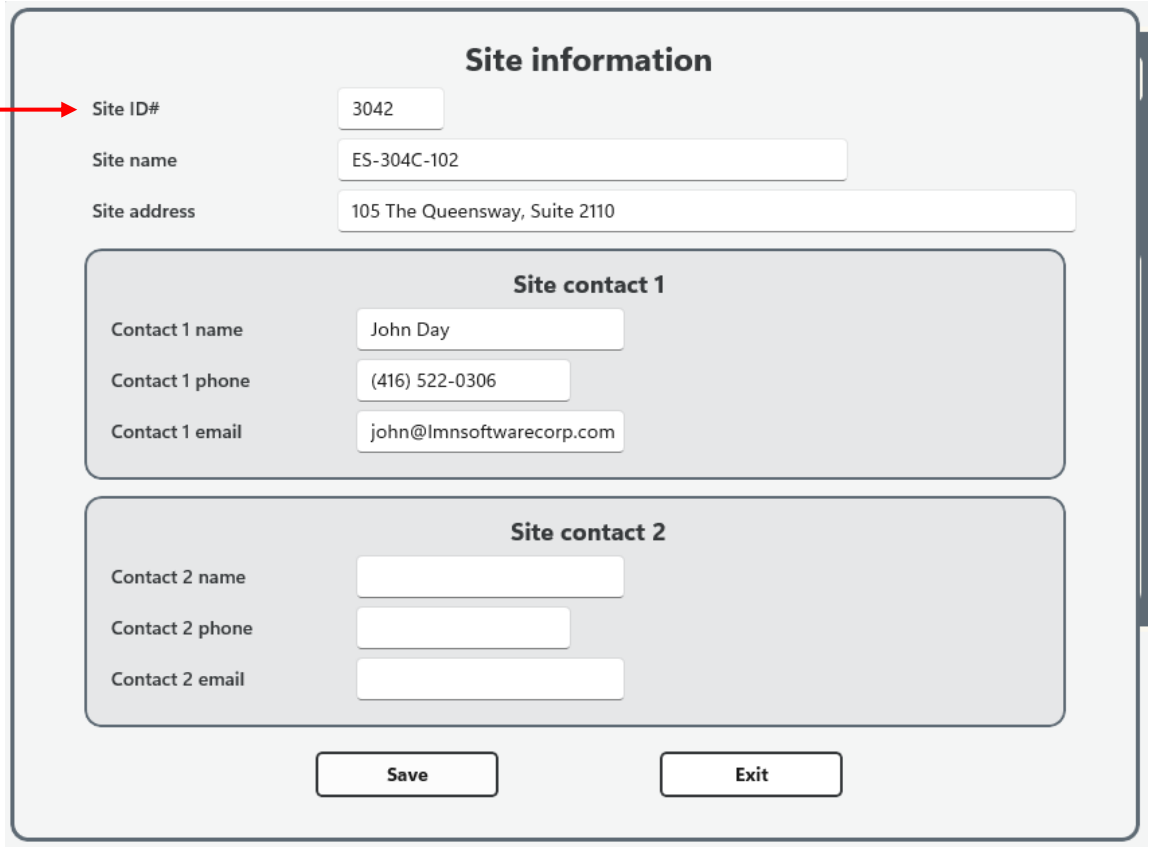
Full configuration – Setup– Site Info

Click the “Site Info” button

Provide a unique number as a Site ID
This ID is used when multiple sites are being monitored with a single EdgeSentry receiver.

Fill out the Site name/address and contacts. These are used in alert emails and notifications about the site.

When you save these settings, **EdgeSentry will start the Learn process**. In the Home menu you will see the Learn status increment about every 20 minutes and you will see the device numbers start to populate.



Full configuration – Setup Basics

Click the “Setup” button

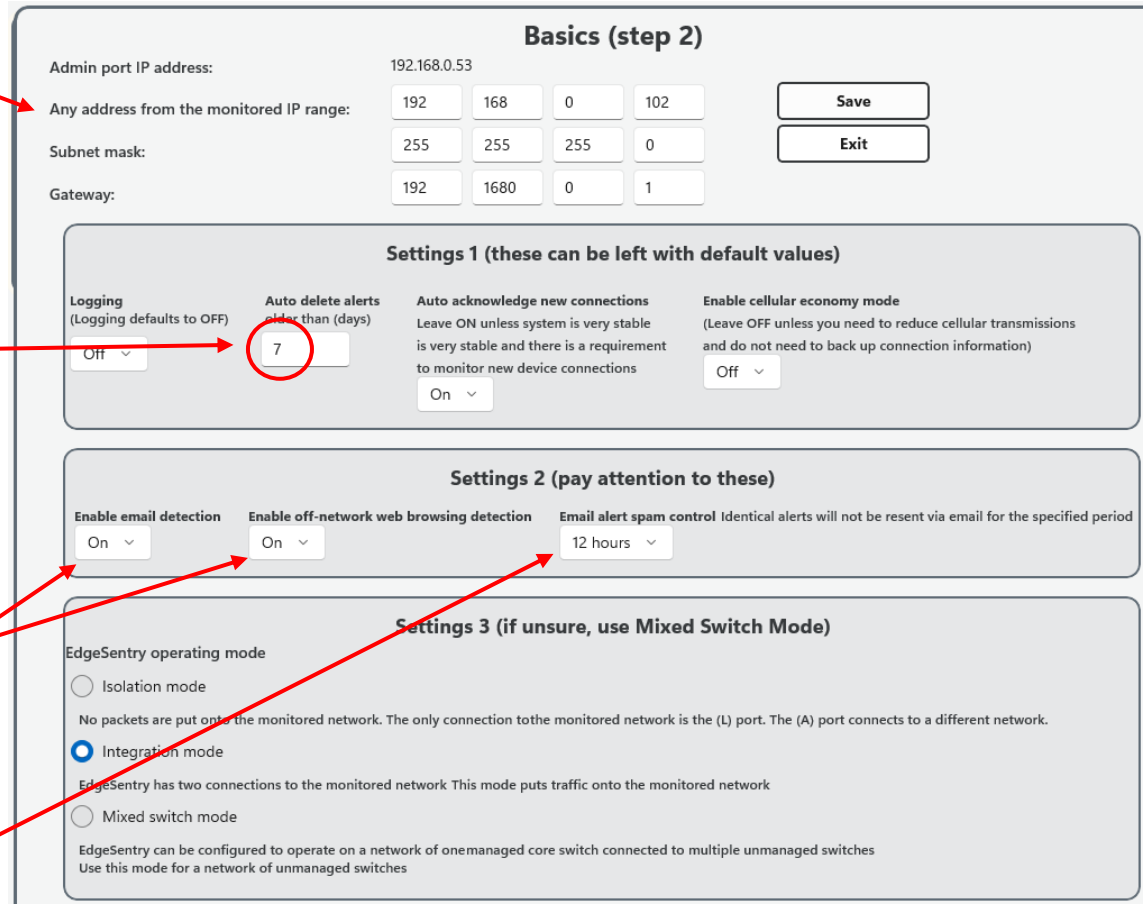
1/ **Enter an IP address from the monitored network’s IP address range.** This is used to determine whether sensed devices are part of the local network or not.

2/ **Enter the subnet mask and gateway.** Note that the system will not enter Learn Mode without this information.

3/ **Set the number of days before alerts are auto deleted.** These systems usually hold 365 or more days of information. Reducing the number of days can make the database more responsive for searches.

4/ **Enable email detection and off-network browser detection** Networks get malware infections from email and web browsing. If there is not reason for someone to use this network for email/web browsing, then enable detection for each of these. Specific IP addresses can be authorized for email/browsing in the “Notifications->Trusts” menu

5/ **Set the time before an email alert will be repeated.** Setting this parameter prevents a user from being “spammed” with email alerts. It is recommended to set this to 12 hours, even if you are not currently using email alerts.

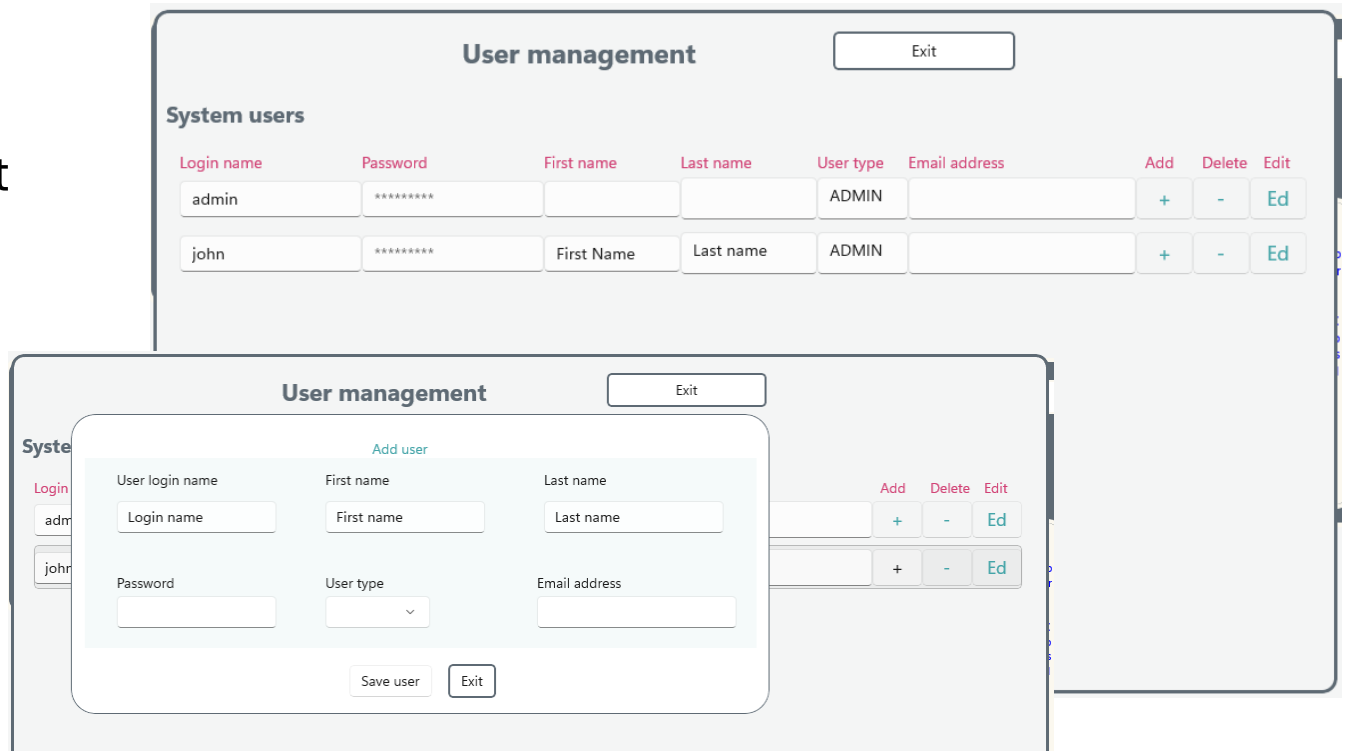


Full configuration – Setup Menus

Click the “Users” button

Users added here are given access to EdgeSentry using ES-Portal through a local network. Users must be set up as ADMIN to access using ES-Portal.

Clicking the “+” button will display the “Add User” popup.



Full configuration – Notifications

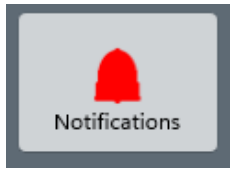
Notifications are critical function of network monitoring. There are four basic ways that EdgeSentry can be monitored and these can be used in any combination:

1/ **Email** – requires the use of a SMTP email account

2/ **ES-Portal (desktop) monitoring** – this is usually done using a remote desktop application

3/ **Receiver Monitoring** – Set up an EdgeSentry Receiver on the local site or out on the internet and send a site's data to that location. ES-Monitor software is used for monitoring the EdgeSentry receiver.

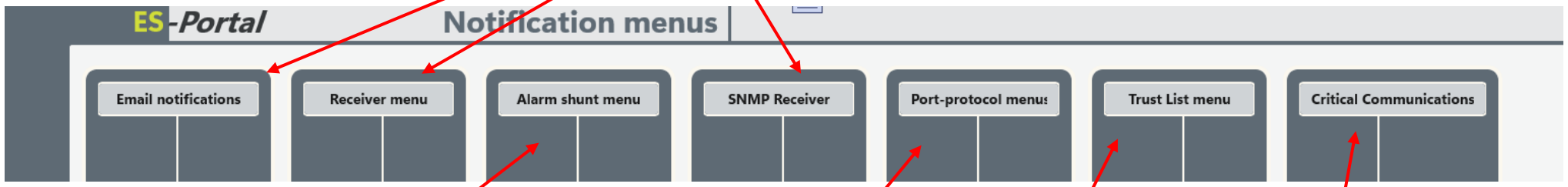
4/ **SNMP monitoring** - using the Genetec IoT plugin or a SNMP receiver.



Click the "Notifications" button

Full configuration - Notifications

Monitoring is set up using the **Email**, **Receiver** and **SNMP** menus.



The **Alarm Shunt** menu is used to mute alerts that are occurring frequently but are not relevant to the site.

The **Port Protocol** menu is used to set up alerts when specific port/protocols are used. You can select from a list of commonly monitored ports (FTP, Telnet) or add your own port/Protocols.

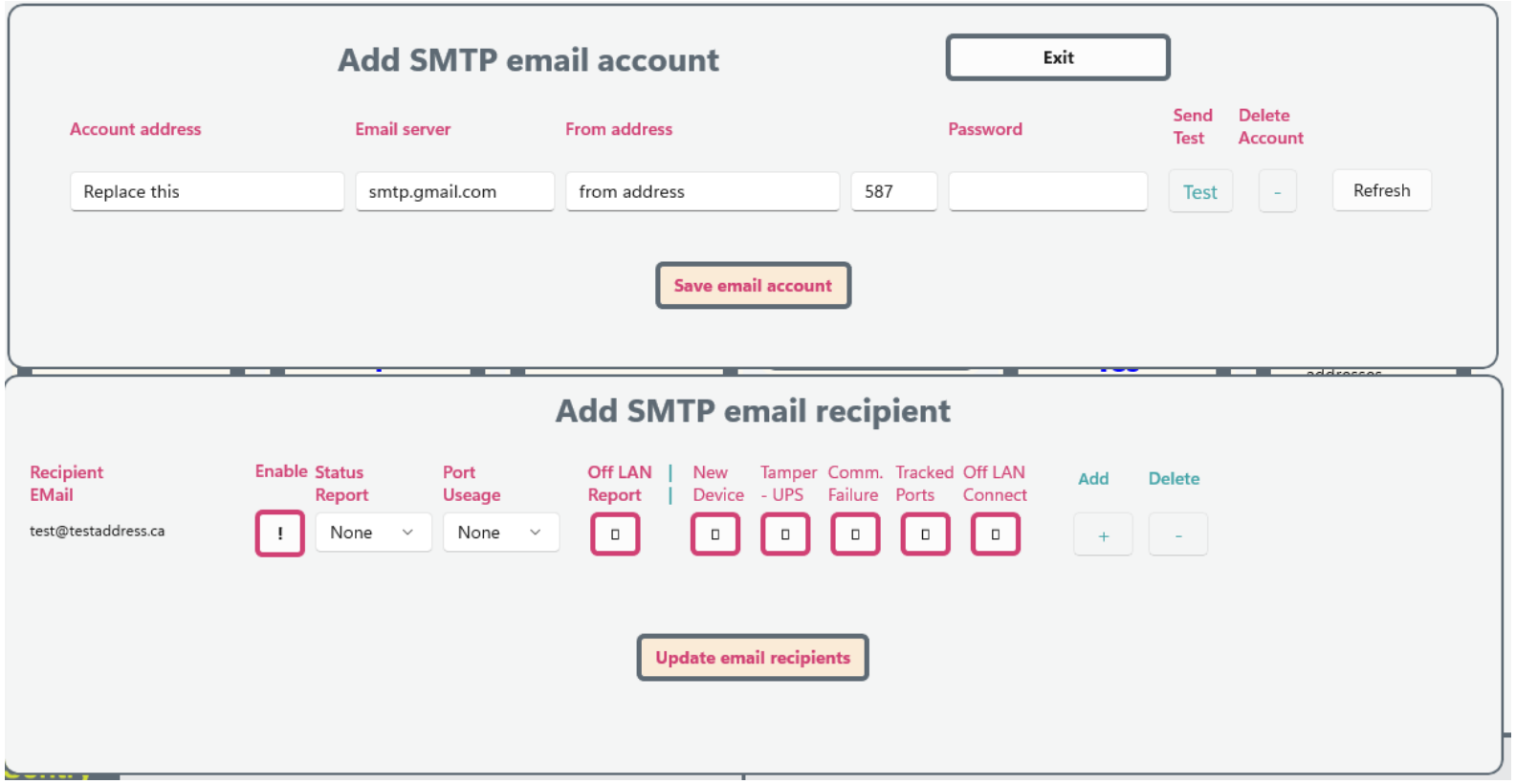
The **Critical Communications** menu is used to detect if a regular critical IPv4 connection is lost between two devices.

The **Trust List** menu is used to prevent off network, email or browsing alerts for trusted local or remote (off network) addresses.

Full configuration – Email Notifications

Input the SMTP **account email address**, **server,** a "**from Address**" (this is used as a destination address during testing), the **Port number** and the **account password.**

Save your settings, then click the "**Test**" button – after 20 seconds a message will confirm that the message has been sent or that there was an error.



Add email recipients

Click the "+" button to add a new user. Provide the email address and select daily/weekly/monthly reports for the user to receive and a selection of alerts.

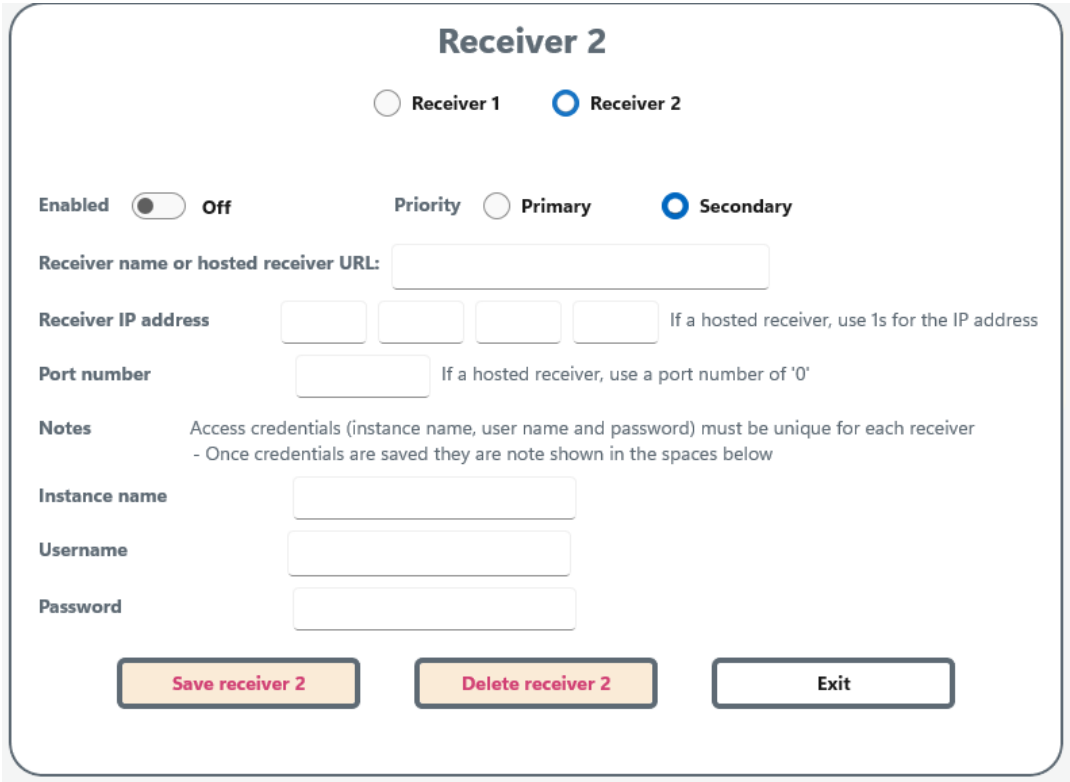
Full configuration – Receiver Notifications

Select the receiver you want to configure, click the enable button and set it as primary (if using 2 receivers, one should be set as secondary).

Provide a **name for the receiver**, the **IP address** and **port number**.

Fill in the instance name and the credentials to write data to the EdgeSentry receiver.

Save the receiver.

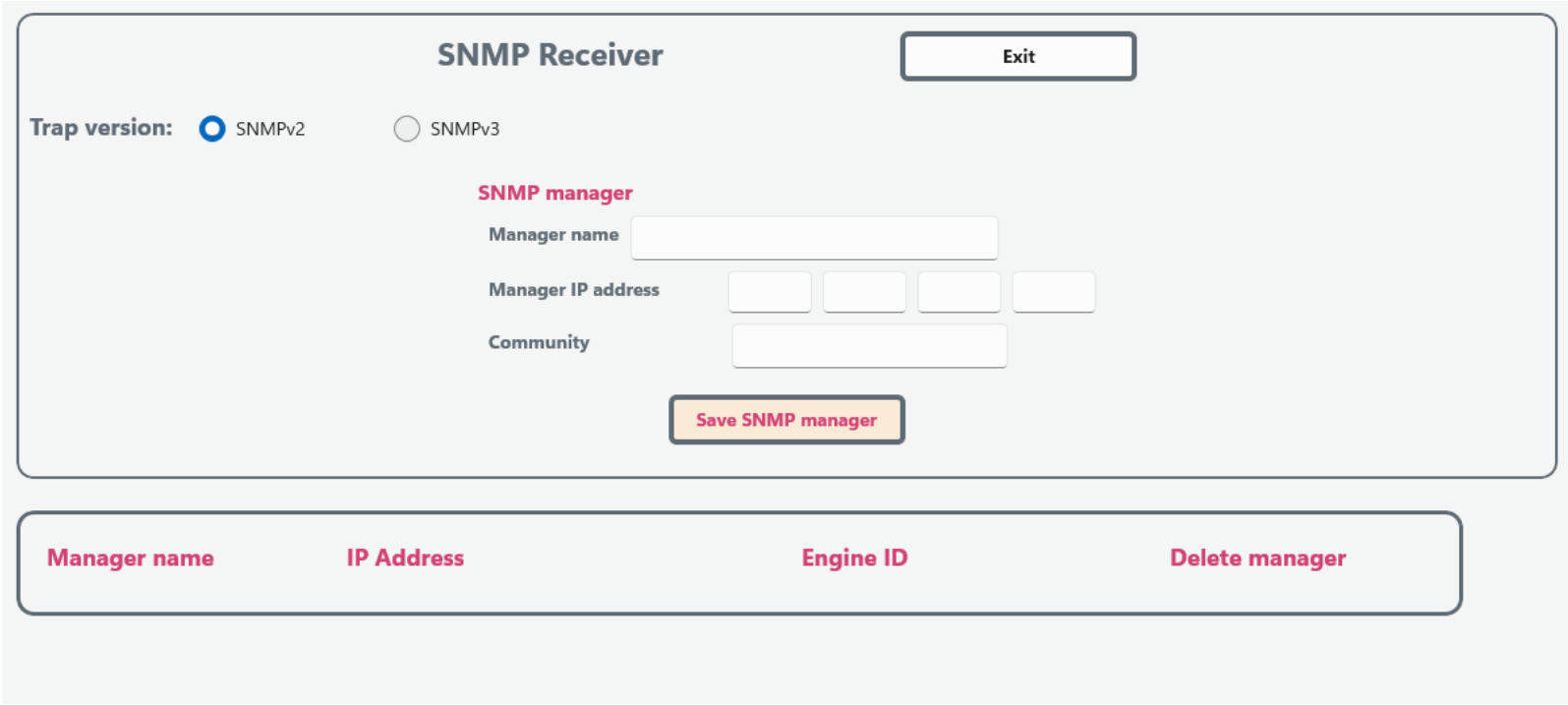


Note that the Home menu will display the receiver online status, but that ***it can take up to 15 minutes for the receiver to connect*** when first set up or after a reboot of the EdgeSentry.

Initial configuration – SNMP Notifications

Note: At the time this manual was created, the SNMPv3 communications are not available. **Use the SNMPv2** settings until further notice.

There is currently a restriction of **two SNMP managers**.



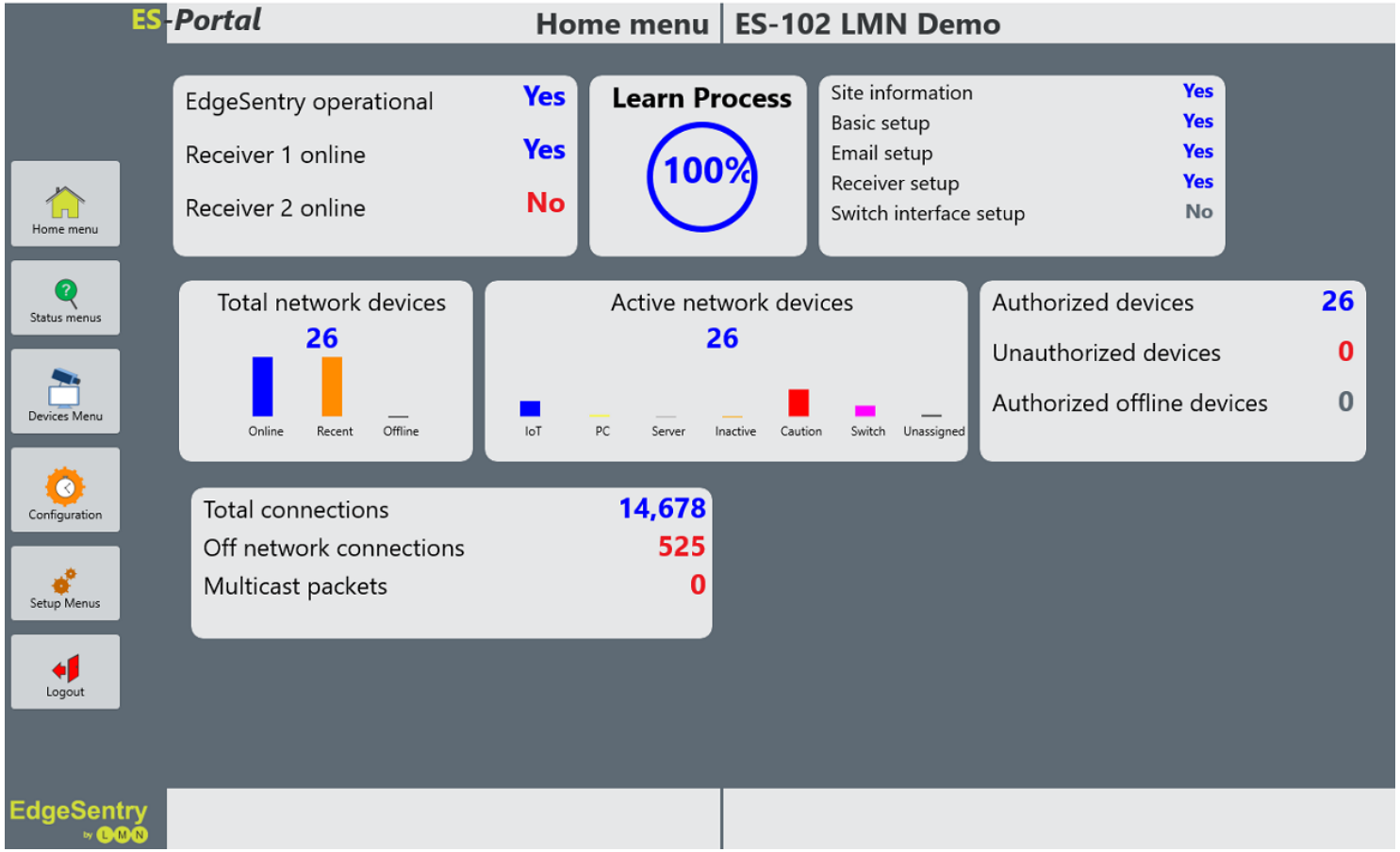
Verify the Community name you are using and enter the **Manager name**, **IP address** and **Community name**. **Save** the SNMP manager.

Post learn configuration

The learn process is completed when the indicator shows 100%. Sometimes this will take longer than 24 hours if the unit performed a Windows update during the learn process.

You should see the approximate number of devices from the network and if the site has internet access, you will normally see some number of off-network connections.

There is an auto-configuration process that runs after the learn process is complete and on system startup.

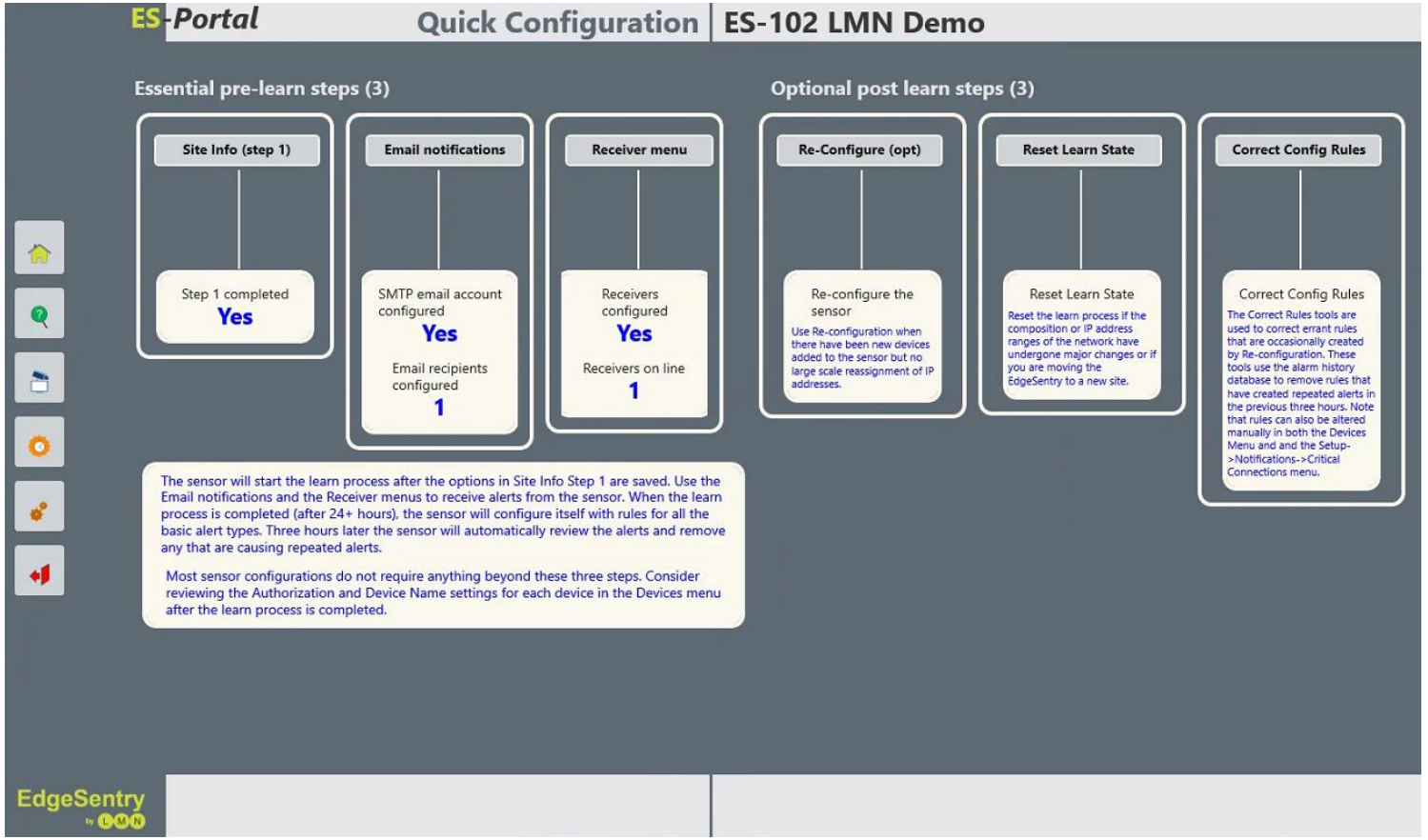


The Auto-Configuration process is completed when devices are automatically categorized as IoT, PC, Server Router, Inactive or Caution.

Post learn configuration

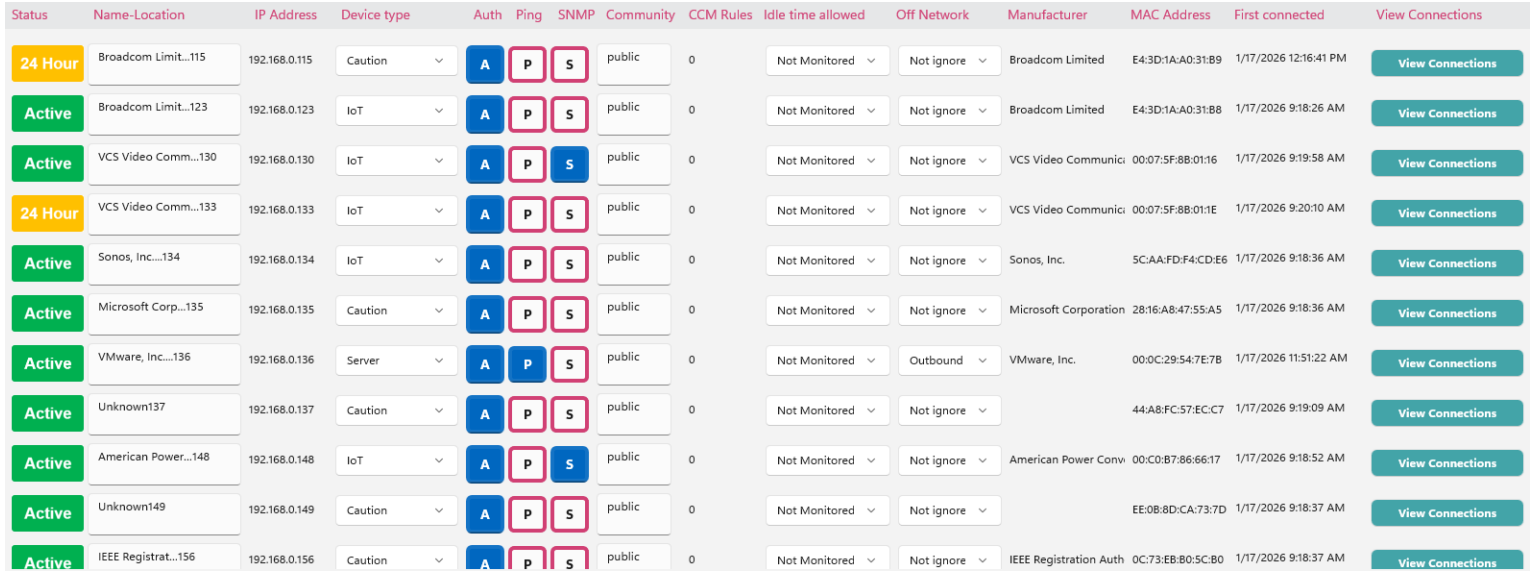
After Auto-Configuration has completed the system will operate for 3 hours, then check for and correct faulty auto-configuration rules.

Both the Auto-Configuration and Rule Correction processes can be run manually from ES-Portal via the Quick Configuration menus.



Post learn configuration – Network devices

The Network devices table shows all the devices that have been sensed by EdgeSentry since EdgeSentry was installed. The list can be sorted by Name, IP Address, Manufacturer and the first connected date.



Status	Name-Location	IP Address	Device type	Auth	Ping	SNMP	Community	CCM Rules	Idle time allowed	Off Network	Manufacturer	MAC Address	First connected	View Connections
24 Hour	Broadcom Limit...115	192.168.0.115	Caution	A	P	S	public	0	Not Monitored	Not ignore	Broadcom Limited	E4:3D:1A:A0:31:B9	1/17/2026 12:16:41 PM	View Connections
Active	Broadcom Limit...123	192.168.0.123	IoT	A	P	S	public	0	Not Monitored	Not ignore	Broadcom Limited	E4:3D:1A:A0:31:B8	1/17/2026 9:18:26 AM	View Connections
Active	VCS Video Comm...130	192.168.0.130	IoT	A	P	S	public	0	Not Monitored	Not ignore	VCS Video Communica	00:07:5F:8B:01:16	1/17/2026 9:19:58 AM	View Connections
24 Hour	VCS Video Comm...133	192.168.0.133	IoT	A	P	S	public	0	Not Monitored	Not ignore	VCS Video Communica	00:07:5F:8B:01:1E	1/17/2026 9:20:10 AM	View Connections
Active	Sonos, Inc....134	192.168.0.134	IoT	A	P	S	public	0	Not Monitored	Not ignore	Sonos, Inc.	5C:AA:FD:F4:CD:E6	1/17/2026 9:18:36 AM	View Connections
Active	Microsoft Corp...135	192.168.0.135	Caution	A	P	S	public	0	Not Monitored	Not ignore	Microsoft Corporation	28:16:A8:47:55:A5	1/17/2026 9:18:36 AM	View Connections
Active	VMware, Inc....136	192.168.0.136	Server	A	P	S	public	0	Not Monitored	Outbound	VMware, Inc.	00:0C:29:54:7E:7B	1/17/2026 11:51:22 AM	View Connections
Active	Unknown137	192.168.0.137	Caution	A	P	S	public	0	Not Monitored	Not ignore		44:A8:FC:57:EC:C7	1/17/2026 9:19:09 AM	View Connections
Active	American Power...148	192.168.0.148	IoT	A	P	S	public	0	Not Monitored	Not ignore	American Power Conv	00:C0:B7:86:66:17	1/17/2026 9:18:52 AM	View Connections
Active	Unknown149	192.168.0.149	Caution	A	P	S	public	0	Not Monitored	Not ignore		EE:0B:8D:CA:73:7D	1/17/2026 9:18:37 AM	View Connections
Active	IEEE Registrat...156	192.168.0.156	Caution	A	P	S	public	0	Not Monitored	Not ignore	IEEE Registration Auth	0C:73:EB:B0:5C:B0	1/17/2026 9:18:37 AM	View Connections

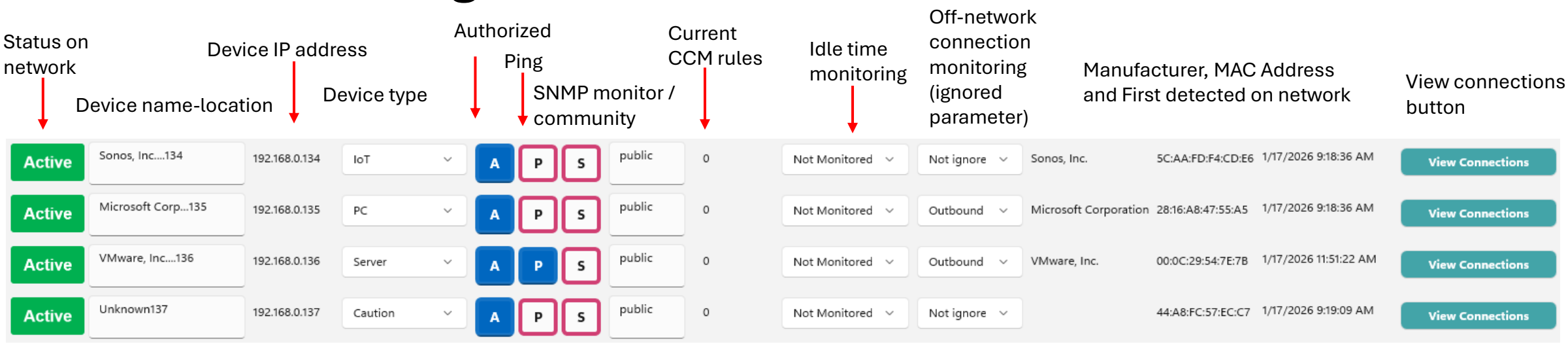
There are a number of steps you can take to fine-tune your configuration

1/ Provide name/locations for the devices

2/ Confirm the device type for each entry in the list, particularly any devices that are shown as “Caution”

3/ Verify that every non-PC device is being monitored by at least one of CCM, SNMP, Ping or Idle-time

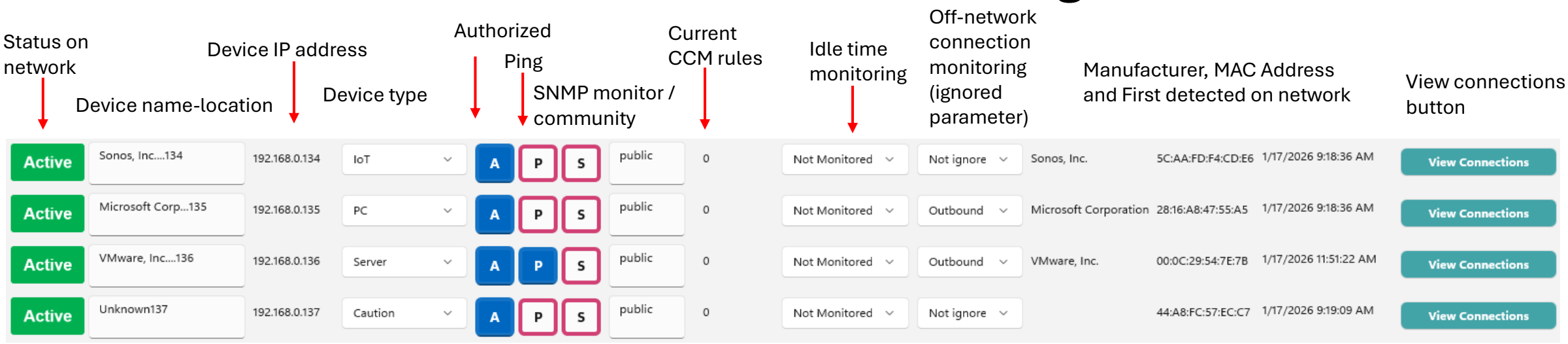
Post learn configuration – Network devices



4/ Device supervision: There are five ways that EdgeSentry can supervise devices.

- By **default**, if a device is marked as "IoT" it will be ping checked several times daily.
- Selecting **"P" (Ping)** means that the device will be Ping test several times each hour
- Selecting **"S"** enables **SNMPv1 monitoring** and requires that the device have SNMPv1 enabled with the correct community
- **CCM monitoring** rules are Auto-configured by the sensor and can also be manually configured in the Notifications menu (under Critical Communications)
- **Idle Time monitoring** allows you to set the maximum time a device can be silent on the network before an alert is created.

Network devices - recommended settings

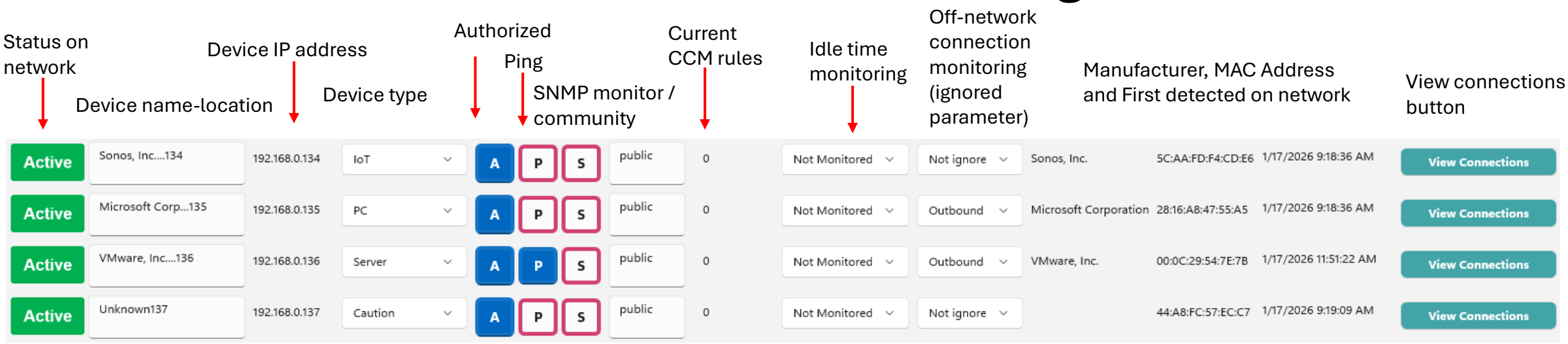


IoT Device – use CCM for supervision (this should be configured automatically at the end of the learn process). IoT devices should be configured to detect off network connections – Off Network set to “Not ignore”

Server– use CCM and Ping for supervision (Servers should be detected and configured automatically at the end of the learn process). Server devices should be configured to ignore outbound off network connections – Off Network set to “Outbound”

PC – Only supervise if they are supposed to be on the network all the time. Use Ping or Idle Time for supervision. PCs should be detected and configured automatically at the end of the learn process. PCs should be configured to ignore outbound off network connections – Off Network set to “Outbound”

Network devices - recommended settings



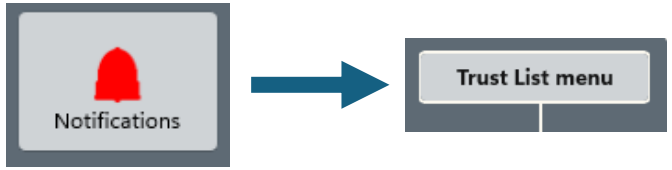
Router– Usually not supervised. Router make lots of off-network connections so Off Network set to “Outbound”

Network switch – Usually not supervised. Network switches should not make off-network connections so set Off Network set to “Not ignore”

Caution – Verify that this device has a purpose on the network and configure it as IoT, PC or Server. If it should not be on the network toggle the Authorized button off (to red).

Inactive – This device has not been active on the network for a period of time and should be de-authorized - toggle the Authorized button off (to red).

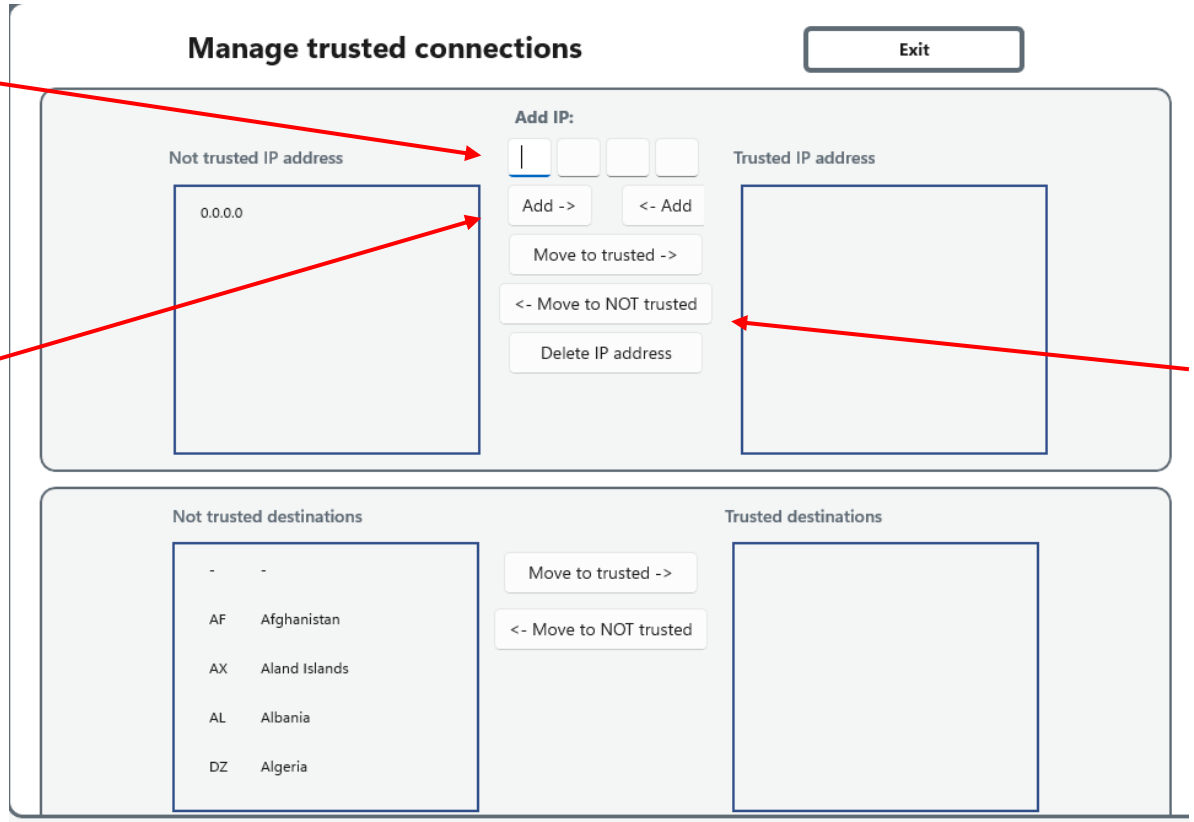
Post learn configuration – Trust Lists



Trust Lists are used to authorize **off LAN connections**, **use of email** for a specific IP and **use of off-network browsing** for a specific IP.

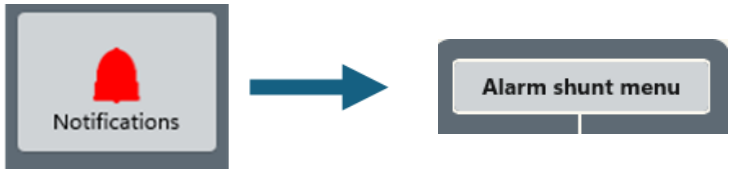
1/ Fill in the IP Address in the “Add an IP Address” space

2/ Select the list you want to place the address in.



3/ Highlight and move addresses between the lists.

Post learn configuration – Shunting alerts

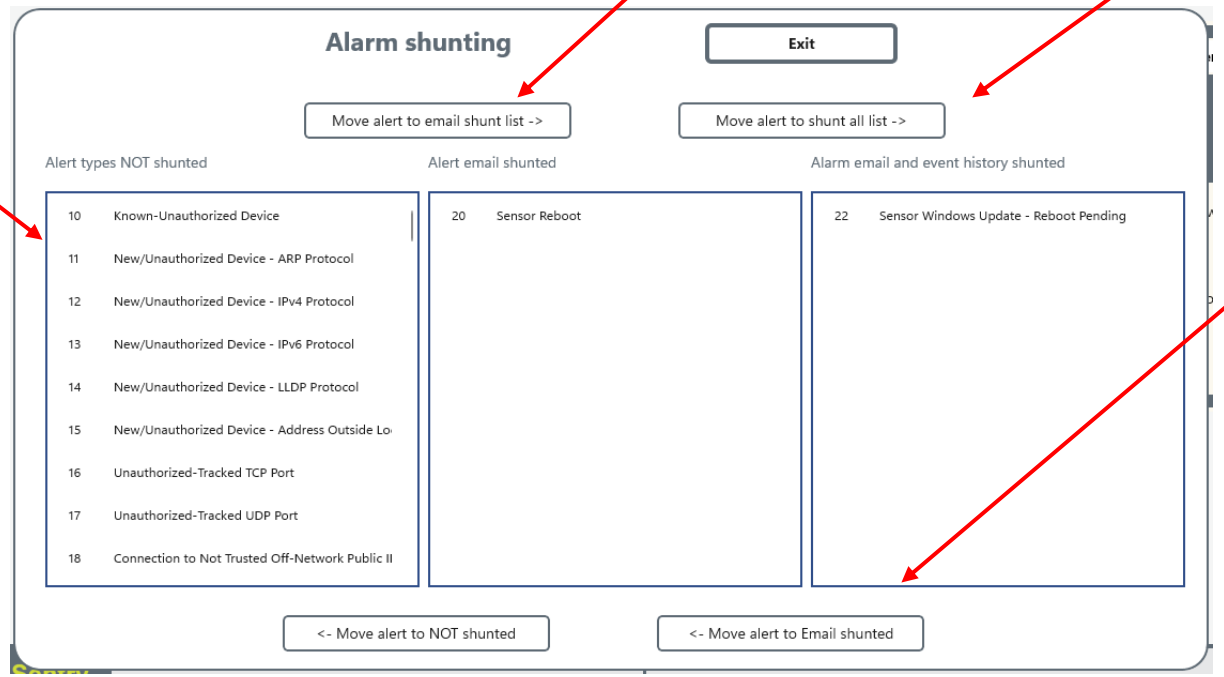


Alarm Shunts are used to **“turn off” specific alerts**. If you shunt from email, the alert won’t be sent via email but will still be recorded in the alarm database. If you choose to “”Shunt All” the alert won’t be sent by email or recorded in the alarm database.

1/ Select the alert from the “Not shunted” list

2/ Click “Move alert to email shunt list”

3/ If required, Click “Move alert to shunt all list”



4/ Alerts can be moved off the shunt lists using the buttons at the bottom

Post learn configuration – Critical Communications

EdgeSentry can monitor for **regular critical IPv4 communications**. EdgeSentry will monitor for that connection and warn you if it is not present within the specified time interval.

Monitoring parameters

- IPv4 packet monitoring only
- Source IP address
- Destination IP address
- Destination port number
- Minimum packet size
- Maximum packet size
- Time Frame (in intervals from 1-60 minutes)

Usually the manufacturer of the devices you are monitoring will be able to tell you **the port, packet size** and **time frame** information.

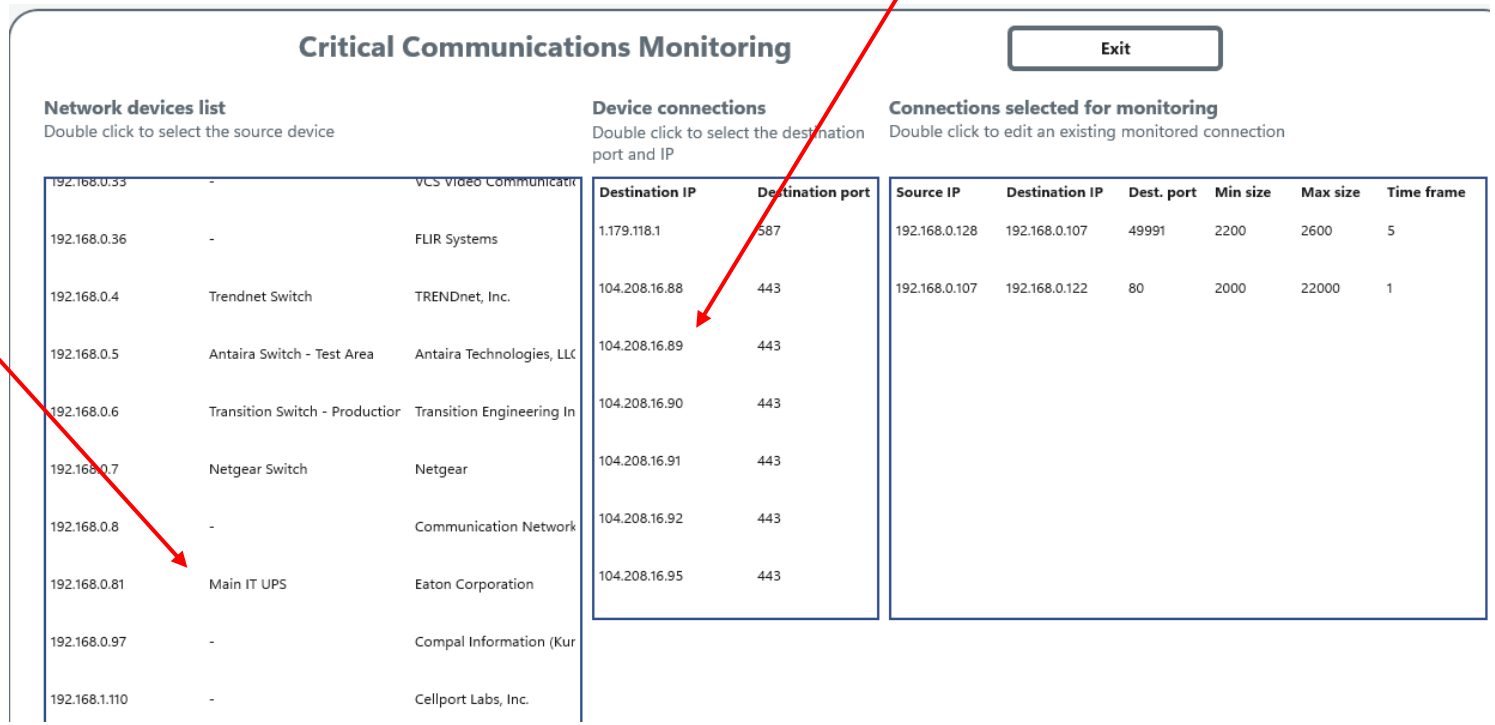
If that information is unavailable or incomplete, you can use WireShark to get the information from the network. Note that you should always clear use of WireShark with the IT department before using it.

There is no actual limit on the number of devices you can select for critical communications monitoring nor for the number of connections per device that you monitor.

Post learn configuration – Critical Communications

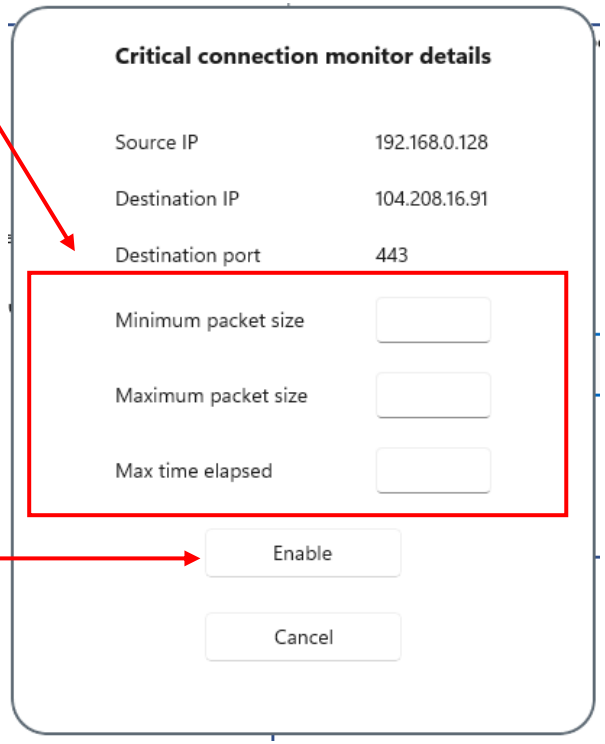
1/ Select your source device from the master list of devices.

2/ Select the destination IP and port from the list of detected connections.



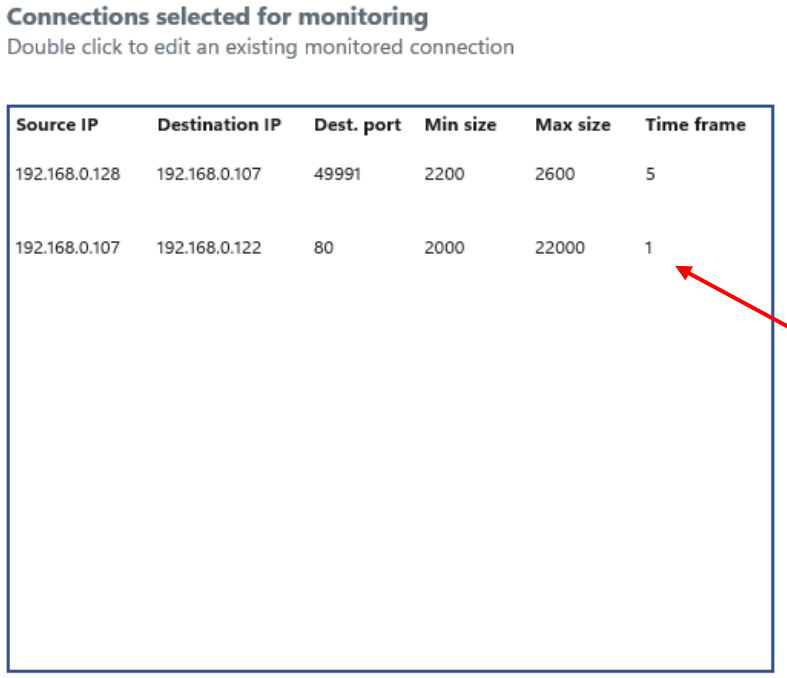
Post learn configuration – Critical Communications

3/ Choose minimum and maximum allowed packet sizes, and the time frame which you expect the packet to be sensed.



4/ Click "Enable" to **save** the connection for monitoring.

5/ The connection will appear in the monitored connections list below.



6/ Double click on any monitored connection to **edit** the monitoring parameters or to **delete** monitoring of that connection.

Questions-need assistance with setup?

- Phone Support, virtual training sessions and remote access support are available on request.
- Virtual training can be booked in advance via email
- Remote access support can be booked in advance via email and involves installation of a ConnectWise client (provided by LMN) on the EdgeSentry.

John Day
(416) 522-0306
jday@datensaft.com