EdgeSentry Switch Interface Guide
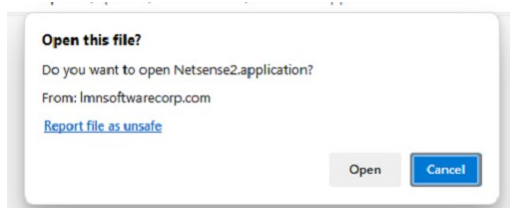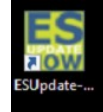
models: ES-102, ES-302, ES-304, ES-604

Before you start – Update the EdgeSentry

Switch integrations are updated regularly and are updated through the ES-Update utility.

If you have access to the EdgeSentry, make sure a keyboard, mouse and monitor are attached and update the EdgeSentry.

1/ On the main desktop, double click the ES-Update icon:

2/ Click on the OPEN button of the "Open this file?" dialog:

Open this file?
Do you want to open Netsense2.application?
From: lmnsoftwarecorp.com
Report file as unsafe
Open   Cancel

3/ If you get a windows message stating that the installation was blocked – Click on "More Information" and select "Update Anyway".

Switch Interface Configuration

Note – ensure that you have the **EdgeSentry Configuration Tool** installed and that you have completed the basic configuration steps outlined in the EdgeSentry **Configuration Guide**.

Step 1 – Add Switches to the Site

   a)   Launch the configuration tool and click on the red and yellow stop sign icon. The Switch Overview Menu will open:

   b)   There are three steps to adding a switch:
      1   Test communications to the switch by entering the switch IP address, manufacturer, username and password
      2   Click the "**Test Switch Communications**" button. If the information is correct, the information under "Assign a switch location" will populate with information about the switch.
      3   Assign the switch a name-location, then fill in the information under "**Fill out the security fields**" and click "**Save Switch**".

Note – A series of messages will appear confirming that the switch information has been added to EdgeSentry and the switch will appear in the list at the bottom half of the screen.

| Name/Location	Ip Address	Manufacturer	Model	Ports	Configure	Delete
Office Core Switch	192.168.0.2	Comnet	CWGE26FX2TX24MSPC	26	Configure Switch	Delete Switch
Power Rack Switch	192.168.0.5	Antaira	LMP-1002	11	Configure Switch	Delete Switch
Build Area Switch	192.168.0.8	Comnet-CNGE	CNGE11FX3TX8MSPOE	11	Configure Switch	Delete Switch
VoIP System Switch	192.168.0.6	Transition-Lantronix	SM8TAT2SA	10	Configure Switch	Delete Switch
Lab Area Switch	192.168.0.3	Cisco	CBS250-8PP-D	8	Configure Switch	Delete Switch
Parking Deck Switch	192.168.0.7	Netgear	M4100-D12G	12	Configure Switch	Delete Switch
Guardhouse Switch	192.168.0.4	Trendnet	TI-PG541i	6	Configure Switch	Delete Switch

Step 2 – Configure Switches

The EdgeSentry switch configuration allows you to harden the network by restricting access to the network in a number of ways. The Switch Status panel (below) shows the status of basic hardening steps and provides "one-click" configuration of each state:

Current Switch Status

Telnet Disabled:	New Credentials	Ports Locked:	Port Security Active:	SNMP V1 Disabled:	SNMP V3 Enabled:	Traps Set:	Changes Saved:	Archive / Restore
●	●	●	●	●	●	●	●	●
Disable Telnet	Edit Credentials	UnLock Ports	Port Security Off	Enable SNMP V1	Disable SNMP V3	Disable V3 Traps	Save Changes	Archive/Restore
		Lock ports	Port Security On	Disable SNMP V1	Enable SNMP V3	Enable V3 Traps		

The second panel shows the current loading of the switch and indicates each port status as one of:

Port is unused and unlocked

Port is unused and locked

Port is in use by a single device and unlocked

Port is in use by a single device and locked

Port is in an uplink port

Port Status		Port - PoE Control
Unused and Unlocked / In use and Unsecured		
Unused and Locked / In use and MAC locked		Last Saved: 2023-06-27 9:01:28
Uplink Port		

The "**Port-PoE Control**" button can be used to lock, unlock or cycle power of an individual port.

The third and bottom panels show the PoE usage per port (no PoE, standard PoE, PoE+ or High PoE) and the bottom panel displays the device name, IP address or mac address per port.

Step 3 – Configure Action Resets

ES200 Menus:

Go Back to Main ES200 menu or Back to EdgeSentry Menus

**View Network Topology** or search for devices by Name, Ip Address, or MAC

Generate Network Status, Network Layout, Network Security and Alert History Reports

Set ES200 Actions and Reset Conditions- to configure responses to security events

The **Action Resets** menu is the bottom menu in the panel shown above. *It is best to configure action resets after the learn process is completed and after the system has been running in a stable and consistent manner.*

An EdgeSentry action can be taken on most of the major event types. The action will either **turn off the port** of the device or **write a firewall rule** to the switch to prevent the activity.

To enable an action-reset, select the alert category (in this case **Unknown-Unauthorized Device**), enable the action-reset, and select the reset strategy (**5 Minutes**).

Unknown-Unauthorized Device Alerts　　On

Reset: ○ Manual　　● 5 Min　　○ 15 Min　　○ 1 Hour　　○ 8 Hour　　○ 1 Day
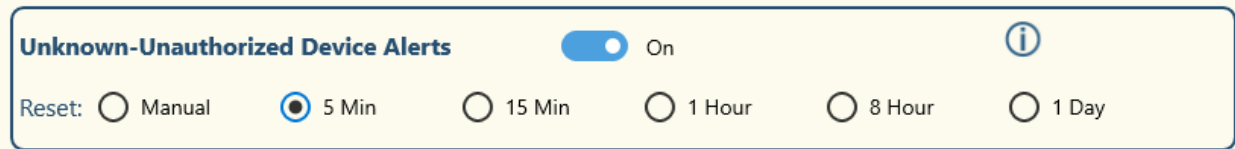
Enabling too many action-resets when new devices are being added to the network may cause confusing and unexpected network behaviour.

We suggest using the following procedure for enabling action-resets:

1/　　Review the alarm history for the event type

2/　　Ensure that there are few nuisance alerts for the event type

3/　　Enable one action-reset type at a time

4/　　Reset the event in a short period of time (5 minutes)