S2 Open-Sensor
Getting Started Guide

FEATURES

Front

Rear

KEY

1.	Kensington lock.
2.	USB 3.2 gen 2 Type-A.
3.	USB 2.0 Type-A.
4.	12 –24VDC rear jack.
5.	2x HDMI 2.0a.
6.	Intel® i219-LM 10/100/1000 Mbps RJ45 Ethernet (Outside Network).
7.	2x USB 3.2 gen 2 Type-A.
8.	2x USB 2.0 Type-A.
9.	Intel® i211-AT 10/100/1000 Mbps RJ45 Ethernet (Inside Network).

DEFAULT SETTINGS

Mode	Inline bridge – passive monitoring between Ethernet ports 6 and 9.
Bridge	Br0
Interface 1	Enp1s0 (port 9 – Inside Network)
Interface 2	Enp0s31f6 (port 6 – Outside Network)
Hostname	sniffa-s2
Management IP	192.168.1.140/24 on Br0
Default Gateway	192.168.1.254
DNS Server	8.8.8.8
Sniffa Manager IP	192.168.1.210
Syslog Server IP	192.168.1.210
Syslog Port	514
Admin User	*sniffaadmin*
Admin Password	**********
Operating System	Ubuntu Server – Version 24.04.2 LTS
Added Software	Snort™, Suricata™, Zeek™, Wireshark™ and NeoRouter™

sales@sniffa.uk

INCLUDED ACCESSORIES

1. UK Power Supply.

2. 2 x Ethernet Cables.

3. VESA Mounting Plate.

4. Getting Started Guide.

   Can also found online at:
   www.sniffa.uk/downloads/SniffaSensor-S2-GettingStartedGuide-WebVersion.pdf

   [This document]

sales@sniffa.uk

GETTING STARTED

1. Connect the UK Power Supply to the Open-Sensor Power inlet.

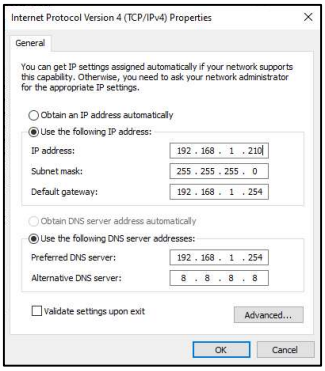
2. Connect one Ethernet Cable to the OUTSIDE Interface Socket of the Open-Sensor.
Connect the other end of the cable to the Outside Network Router or Switch Interface Socket.

3. Connect one Ethernet Cable to the INSIDE Interface Socket of the Open-Sensor.
Connect the other end of the cable to the Inside Network Router, Switch, Server or PC Interface Socket.

Note: This will be the device(s) or network you want to protect.

4. Configure a Management PC that is physically connected to the INSIDE network to be on the same subnet as the Open-Sensor.
Go to IPv4 settings of the connected network interface card to do this.

Note: Default Management PC IP address is set on the sensor to be 192.168.1.210/24.



5. Connect to the Open-Sensor on SSH port 22.
(e.g. Using Putty).
Run commands as necessary (from next page a to f).

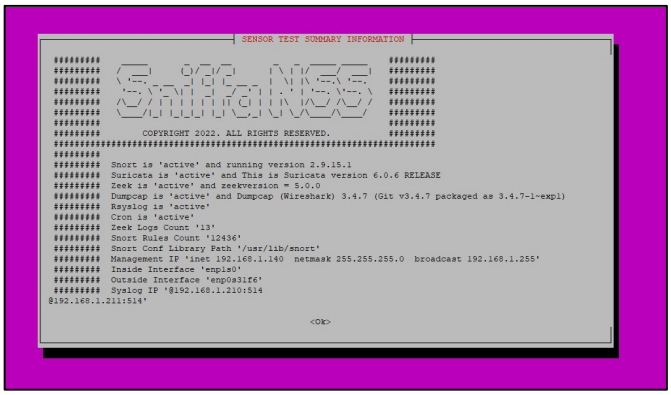
Note: Default Open-Sensor IP address is set to be 192.168.1.140/24.

sales@sniffa.uk

a. To View Running Software

To check if threat detection software is running and what versions, type the following commands at the terminal command line:

```
sniffaadmin@sniffa-s2:-$sudo sniffatest
```



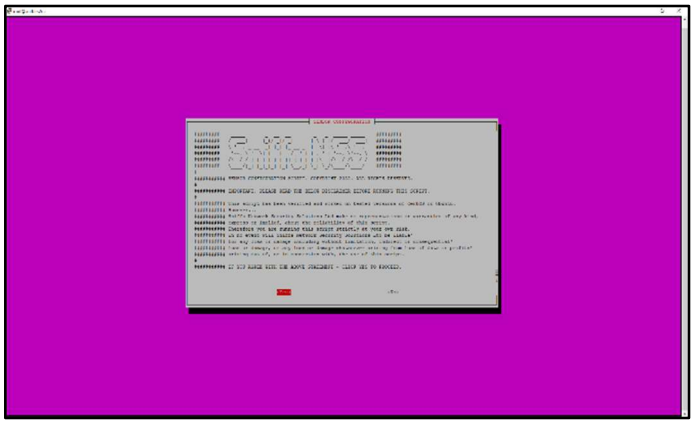
Press 'Ok' to save or 'Esc' to close dialogue.

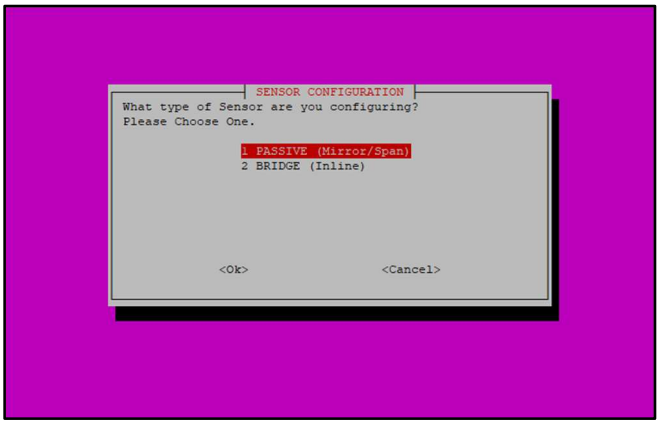
b. To Update Configuration

To update the configuration at any time, type the following command from the terminal command line:

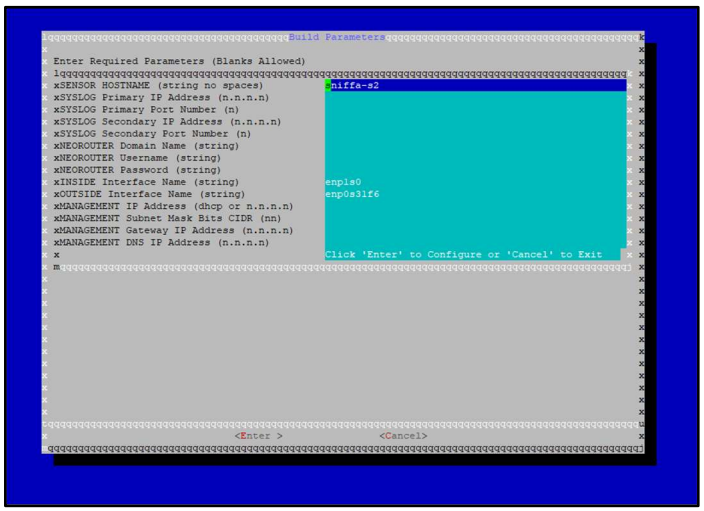
```
sniffaadmin@sniffa-s2:-$sudo sniffaconfig
```

Follow instructions to modify configuration settings as required.





sales@sniffa.uk



Will require a reboot for configuration settings to be made permanent (recommended).

c. To set the Timezone to UTC

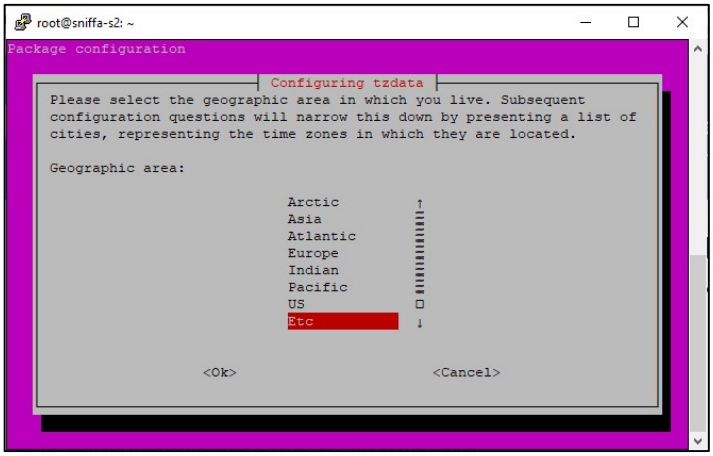
To see the current Timezone setting, type the following commands at the terminal command line:

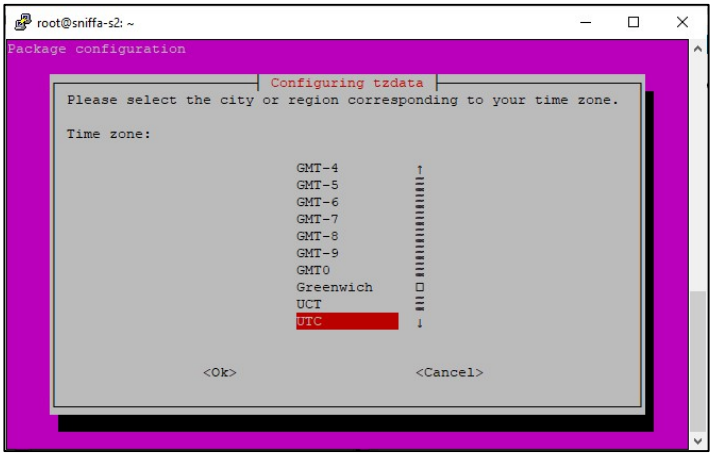
```
sniffaadmin@sniffa-s2:-$sudo date
```

Set the Timezone to UTC type the following commands at the terminal command line:

```
sniffaadmin@sniffa-s2:-$sudo dpkg-reconfigure tzdata
```

Select 'Etc' as the Geographic Area.





Select 'UTC' as the Timezone.

Press 'Ok' to save or 'Cancel/Esc' to close dialogue without saving.

sales@sniffa.uk

d. To View Logging

To check if the sensor is logging correctly, type the following commands at the terminal command line:

```
sniffaadmin@sniffa-s2:-$tail -f /var/log/syslog | grep 'zeek-'
```

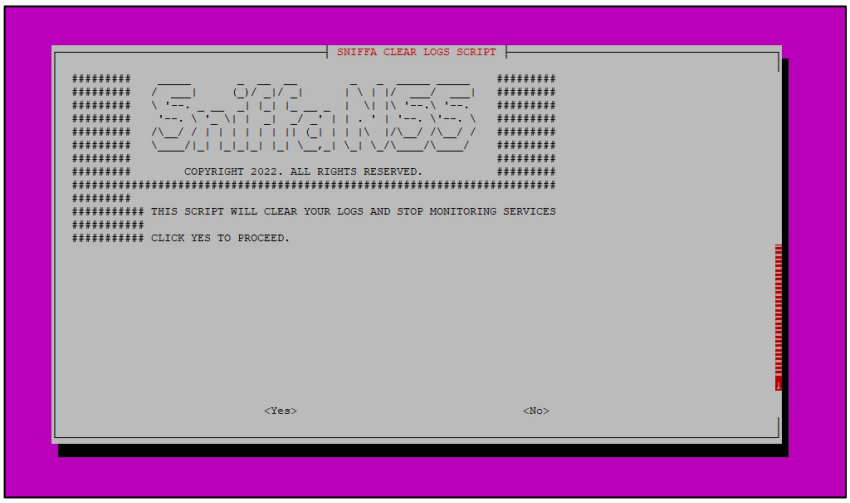
```
root@sniffa-s2-snort:/usr/local/sbin# tail -f /var/log/syslog | grep zeek-
Jul 22 16:11:24 sniffa-s2-snort zeek-dns 1658506269.609384      COoTDC38zqH9sv4NZ2      192.168.
F       F       F       0       -       -       F
Jul 22 16:11:24 sniffa-s2-snort zeek-conn 1658506254.590849     COoTDC38zqH9sv4NZ2      192.168.
0       -
Jul 22 16:11:24 sniffa-s2-snort zeek-conn 1658506224.652785     ChiFCh2OWYGoOXRns2      192.168.
0       -
Jul 22 16:11:24 sniffa-s2-snort zeek-conn 1658506224.669535     CCXLrq3k090JI4YZi6      192.168.
-
Jul 22 16:11:24 sniffa-s2-snort zeek-conn 1658506224.784982     CRDlshl7NuysgWYXn7      192.168.
0       -
Jul 22 16:11:24 sniffa-s2-snort zeek-conn 1658506224.790393     C2udLi2lTgFa7HOLNd      192.168.
-
Jul 22 16:11:25 sniffa-s2-snort zeek-conn 1658506225.350646     CTeAas2pExFa7lsd4       192.168.
0       -
Jul 22 16:11:25 sniffa-s2-snort zeek-conn 1658506225.391985     CWTYTlNfHU7LYlEIg       192.168.
-
Jul 22 16:11:25 sniffa-s2-snort zeek-conn 1658506225.452986     Cpuxx0xkEPLHyEr6        192.168.
0       -
Jul 22 16:11:25 sniffa-s2-snort zeek-conn 1658506225.463634     CyvmIj4aWLuW0nJoAa      192.168.
-
```

To stop the tail function, click Ctl+c

e. To Clear Logs

To clear the logs, type the following commands at the terminal command line:

```
sniffaadmin@sniffa-s2:-$sudo sniffaclearlogs
```



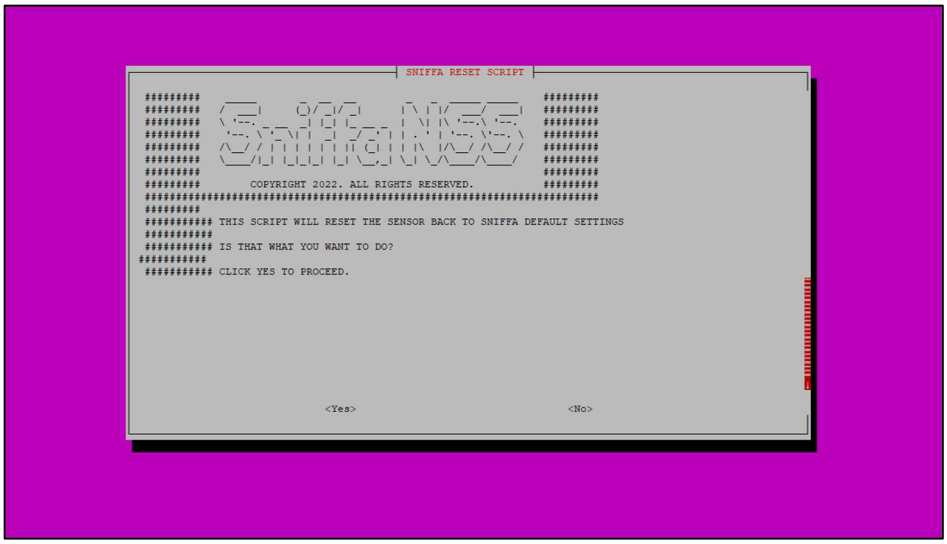
Press 'Yes to clear logs or 'No/Esc' to close dialogue without clearing any logs.

sales@sniffa.uk

f. To Reset to Default Settings

To reset the sensor to the default settings, type the following commands at the terminal command line:

```
sniffaadmin@sniffa-s2:-$sudo sniffareset
```



Will require a reboot for configuration settings to be made permanent (recommended)

FINISH OFF

6. Buy and Install the Sniffa Sensor Manager Application onto the Management PC that is connected to the INSIDE network.

   Sales@sniffa.uk
   www.sniffa-nss.com/products#shop

7. To finish off.

   - Add an MS SQL Database as required.
   - Add the Open-Sensor to the Sensor Manager Application.
   - Add an IIS Server and configure the Web Portal.
   - Add Users to the Web Portal.
   - Set Management PC Time zone to UTC.
   - Start Syslog on the Management PC.

   Note: Consult online runbook for instructions.
   www.sniffa-nss.com/knowledge