

FEATURES



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



S2 Open-Sensor Getting Started Guide

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 Sniffa Network Security Solutions Limited is a company registered in England and Wales No. 11834354, VAT No. 317589765

2. Senif



GETTING STARTED

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

- 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.
- 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.

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.







General	
You can get IP settings assign this capability. Otherwise, you for the appropriate IP settings	ed automatically if your network supports need to ask your network administrator
Obtain an IP address aut	omatically
Use the following IP addr	ess:
IP address:	192 . 168 . 1 . 210
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 1 . 254
Obtain DNS server addre	ss automatically rver addresses:
Preferred DNS server:	192 . 168 . 1 . 254
Alternative DNS server:	8.8.8.8
Validate settings upon e	xit Advanced



3. 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.



4.



xSYSLOG Primary TP Address (n.n.n.n)	sniffa-s2
xSYSLOG Primary Port Number (n)	
xSISLOG Secondary IF Address (n.n.n.n) xSYSLOG Secondary Port Number (n)	
xNEOROUTER Domain Name (string) xNEOROUTER Username (string)	× ×
xNEOROUTER Password (string)	A STATE OF
xINSIDE Interface Name (string) xOUTSIDE Interface Name (string)	enpiso x x enp0s31f6 x x
xMANAGEMENT IP Address (dhop or n.n.n.n)	2 × 2
xMANAGEMENT Gateway IP Address (n.n.n.n)	
xMANAGEMENT DNS IP Address (n.n.n.n) x	Click 'Enter' to Configure or 'Cancel' to Exit x x
	qaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
	X
	x
	×
	x x x x
	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
	2 2 3 4 4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5 5
	2 2 3 3 4 5 4 5 6 6 7 8 6 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8
	2 2 2 3 3 4 5 4 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5

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.

Proot@sniffa-s2: ~	- [⊐ × [d	🗗 root@sniffa-s2: ~		- (×
Package configuration	rdat a	∧ Pa	ckage configuration	ing tzdata		^
Please select the geographic area in whi configuration questions will narrow this cities, representing the time zones in w	tch you live. Subsequent a down by presenting a list of which they are located.	£	Please select the city or region Time zone:	corresponding to your time	zone.	
Geographic area: Arctic Asia Atlantic Europe Indian Pacific US <mark>Etc</mark>			GMT-4 GMT-5 GMT-6 GMT-7 GMT-8 GMT-9 GMT0 Green UCT UCT	wich		
<0k>	<cancel></cancel>			<cancel></cancel>		~

Select 'UTC' as the Timezone.

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



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-'

roo	t@si	niffa-s2-:	snort:/usr/local	/sbin# tai:	l -f /var/log/syslog	grep zeek-	
Jul		16:11:24	sniffa-s2-snort	zeek-dns	1658506269.609384	C0oTDC38zqH9sv4NZ2	192.168.
F							
Jul		16:11:24	sniffa-s2-snort	zeek-conn	1658506254.590849	C0oTDC38zqH9sv4NZ2	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	CRD1sh17NuysgWYXn7	192.168.
0							
Jul	22	16:11:24	sniffa-s2-snort	zeek-conn	1658506224.790393	C2udLi21TgFa7HOLNd	192.168.
-							
Jul	22	16:11:25	sniffa-s2-snort	zeek-conn	1658506225.350646	CTeAas2pExFa71sd4	192.168.
0							
Jul	22	16:11:25	sniffa-s2-snort	zeek-conn	1658506225.391985	CWITIINTHU/LIIEIG	192.168.
-	22	16.11.05			1650506005 450006	C	100 100
our	22	10:11:25	shirra-S2-short	zeek-conn	1050500225.452986	CDUXXOXKEPLHYER6	192:168.
U T-1		16.11.25	aniffo al anort	goolt-comp	1659506225 462624	Cummin do Mi u Mon To Ao	102 169
our		10.11:25	SHILLA-S2-SHOLL	2cex-conn	1030300223.403034	Cyvilli J HawLuwonooAa	152:100.

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

SNIFFA CLEAR LOGS SCR.	IPT	
**************************************	************	
<yes></yes>	<no></no>	

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

6. sales@sniffa.uk

Sniffa Network Security Solutions Limited is a company registered in England and Wales No. 11834354, VAT No. 317589765



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.
- 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.

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

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