X3-SERIES

X3-440G-ID

X3-880G-ID

IN-LINE SSL/TLS DECRYPTION

USER MANUAL

If you have any questions, you can contact us through our website:

www.profitap.com

or by email:

support@profitap.com

For the latest documentation and software, visit our Resource Center:

https://resources.profitap.com/
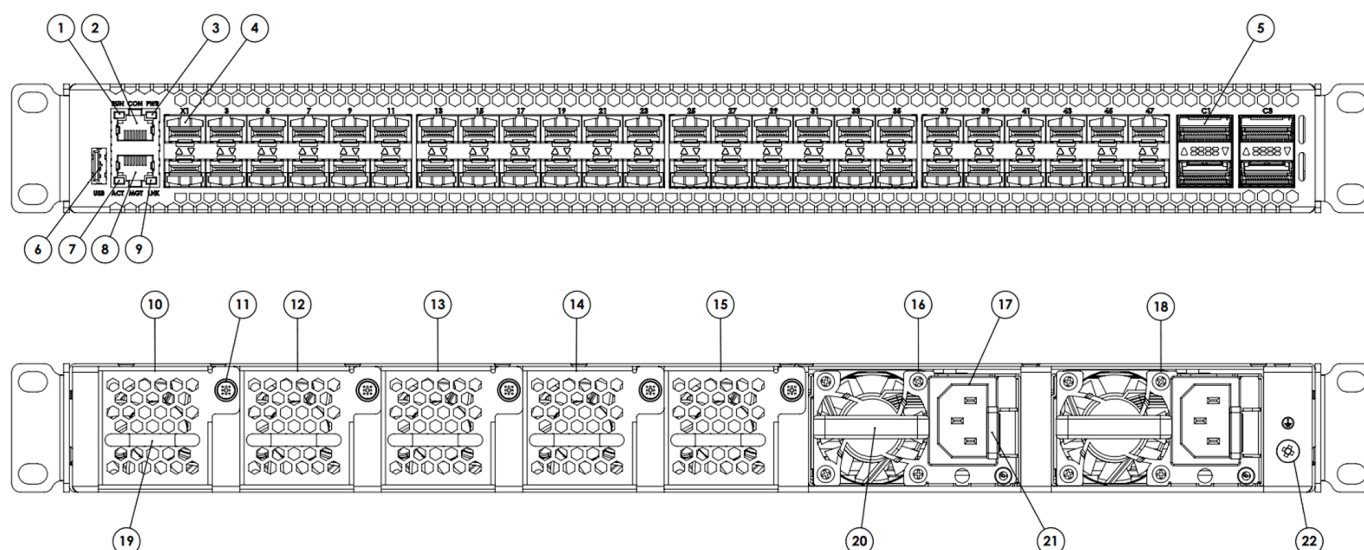
TABLE OF CONTENTS

1. Overview

This document provides information about the configuration and operation of X3-Series In-Line SSL/TLS Decryption Tools.

2. Hardware Guide

2.1 Included Accessories

- DB9 to RJ45 serial cable
- (2) Front-mounting ears with (8) screws
- (2) Rear-mounting ears
- (2) AC power cords

2.2 Physical Description

Front View		Rear View	
1	Status LED	10/12/13/14/15	(5) FAN modules
2	Console port	11	FAN module locking screw
3	Power LED	16/18	(2) modular Power Supply Units
4	(48) 1G/10G SFP+	17	PSU input connector
5	(4) 40G/100G QSFP28	19	FAN module handle
6	USB port	20	PSU handle
7	Management port Activity LED	21	PSU lock
8	Management port	22	Grounding lug
9	Management port Link LED		

2.3 Ports Description

2.3.1 Console Port

This serial port is intended to be used for local configuration and administration of the X3 device with Command Line Interface (CLI).

Port parameters: RJ45, RS232, 115200, N, 8, 1

Default username and password for serial connection:

- Username: **root**
- Password: **passok**

2.3.2 Management Port

This port is intended to be used for local and remote configuration and administration of the X3 device with SSH.

Port parameters: RJ45, 10BASE-T/100BASE-TX, Auto negotiation, Auto MDI/MDIX

Default username and password for SSH connection:

- Username: **root**
- Password: **passok**

2.3.3 USB Port

Port parameters: USB 2.0

2.4 Unpacking and Installing the Device

1. Unbox the X3 unit;
2. Refer to the list of included accessories and check the contents of the box;
3. Attach the (2) mounting ears to the main unit using the (8) screws;
4. Install the X3 unit in the rack;
5. Connect the ground wire to the grounding lug (#22);
6. Power up the X3 unit.

2.5 Troubleshooting and Maintenance

2.5.1 Replacing FAN Module

X3 fan tray contains five fan modules. If a fan module fails, you should replace it, however X3 will function with one failed fan module. You can remove individual fan modules using the following procedure:

1. Unscrew the FAN module locking screw (#11);
2. Remove the FAN module using the Fan module handle (#19);
3. Place the new FAN module in the empty slot;
4. Tighten the locking screw (#11).

2.5.2 Replacing PSU

X3 power tray contains two PSU modules. If a PSU module fails, you should replace it, however X3 will function with one failed PSU module. You can remove individual PSU module using the following procedure:

1. Disconnect the power cord from the PSU (#17) to be replaced;
2. Push the PSU lock (#21) on the left;
3. Pull the PSU using the handle (#20);
4. Insert the new PSU until the lock (#21) is in its locked position;
5. Connect the power cord to the new PSU (#17).

3. Configuration

3.1 Initial IP Settings

- IP: 192.168.10.51
- Subnet mask: 255.255.255.0
- Default gateway: 192.168.10.1

3.2 Initial Setup

Initial setup can be done via the management port or the serial console port.

Using any terminal software, connect to the device through SSH or serial connection.

Login, using the following credentials:

- Username: **root**
- Password: **passok**

After logging in, the user can access the system shell and administrate the device using the canonical GNU/Linux OS facilities.

The IP and subnet mask of the device can be changed using the following command:

```
ip addr add [ip_addr/mask] dev eth1
```

With `ip_addr` being the IP address and `mask` being the CIDR prefix. For example:

```
ip addr add 10.10.10.180/16 dev eth1
```

The user password can be changed using the following command:

```
passwd
```
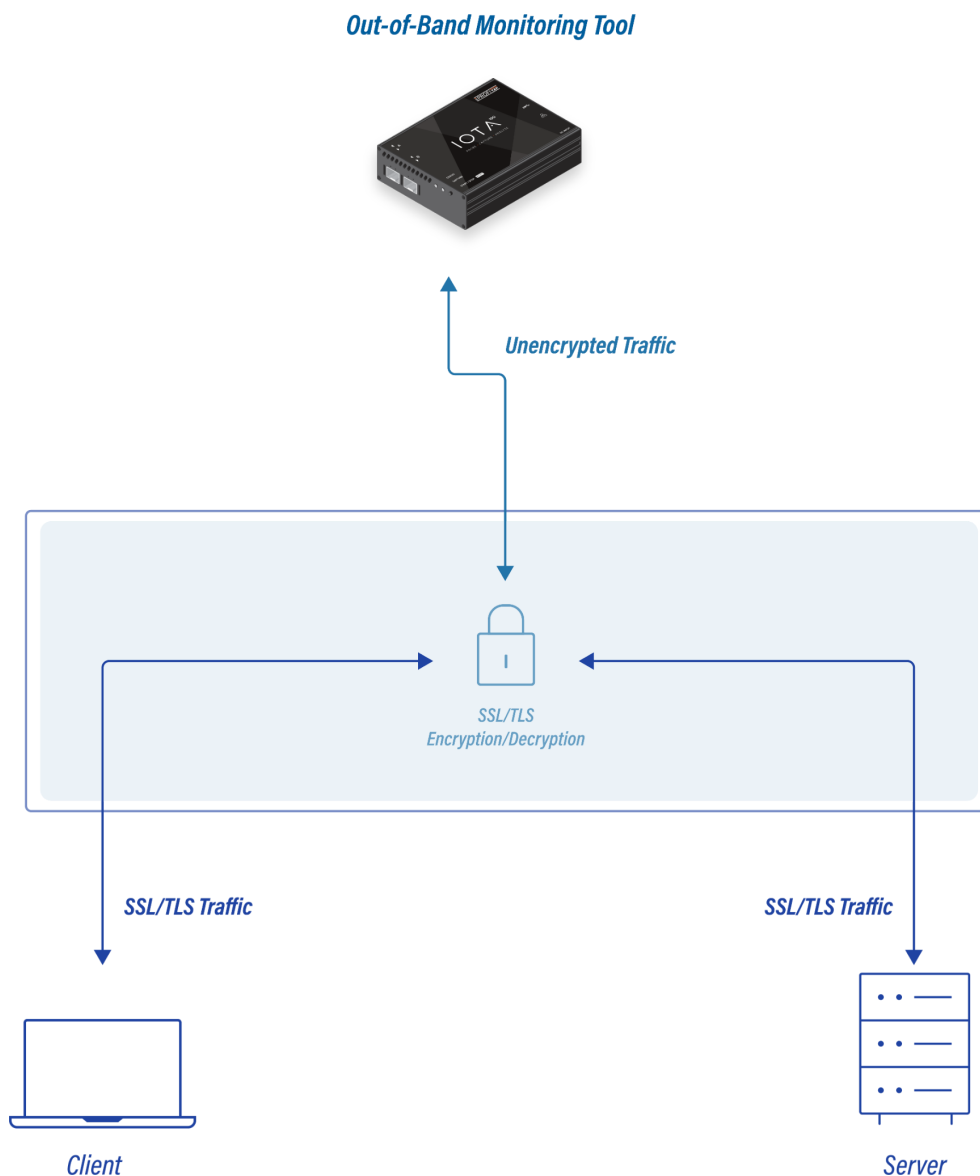
3.3 In-Line SSL/TLS Decryption

3.3.1 Theory of Operation

In-line decryption in X3 is done by negotiating an encrypted connection between the client and the X3 device, and another encrypted connection between the X3 device and the server. The X3 device decrypts then re-encrypts the data passing through, and sends the unencrypted data to the analysis tools. The advantage of this approach is the ability to handle TLS v1.3, which enforces Ephemeral Diffie-Hellman key exchange protocols.

Profitap X3-Series In-Line SSL/TLS decryption device is capable of performing passive in-line decryption.

Passive In-Line Decryption

Passive in-line decryption creates a simple chain between the decryption and encryption engine, mirroring out the duplicated packets to one monitoring device. This approach can be followed when we need to perform traffic capture and monitoring on links which are using TLS v1.3. In this scenario, the X3 device will break the EDH-protected connection and allow the monitoring appliance to receive unencrypted traffic.

Out-of-Band Monitoring Tool

Unencrypted Traffic

SSL/TLS
Encryption/Decryption

SSL/TLS Traffic

SSL/TLS Traffic

Client

Server

Passive in-line configuration

Client	X3 Device	Server
#1 SYN →		#2 SYN →
		← #3 SYN-ACK
		#4 ACK →
← #5 SYN-ACK		
#6 ACK →		
#7 Client Hello →		#8 Client Hello →
← #10 Server Hello		← #9 Server Hello
#11 Client Key Exchange →		#12 Client Key Exchange →

Data Exchange

Client	X3 Device	Server
#13 Client Finish →		#14 Client Finish →
← #16 Server Finish		← #15 Server Finish
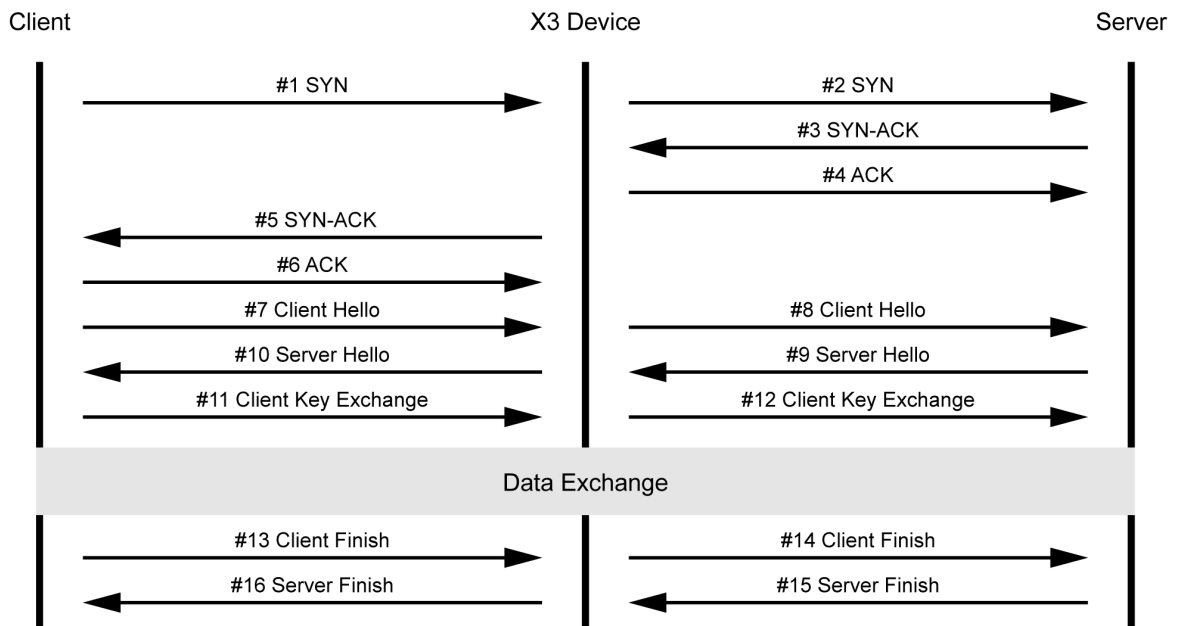
Overview of the communication between the client, X3 device, and server.

3.3.2 Configuration

The client-server configuration is done via the following command:

```
/profitap/x3-ssl -f do_configure [options]
```

The configuration options can be provided as CLI arguments, or as environment variables. Environment variables can be set with e.g.:

```
export X3_INTERFACE_CLIENT="1"
```

The available options and the relative environment variables are the following:

Option	Environment variable	Value description	Value example
--interface-client	X3_INTERFACE_CLIENT	Physical interface used to connect the client device to the X3 in-line appliance (any port number between 1–52).	1
--interface-client-speed	X3_INTERFACE_CLIENT_SPEED	Speed configured for the Client physical interfaces. Options are `1000` (1GE) and `10000` (10GE)	1000
--interface-client-ip	X3_INTERFACE_CLIENT_IP	IP address used by the X3 interface connected to the client (must be on the same subnet as the client).	10.10.10.30
--client-ip	X3_CLIENT_IP	Client device IP address.	10.10.10.20
--client-ip-mask	X3_CLIENT_IP_MASK	CIDR mask used in the IP address for the server.	24
--interface-server	X3_INTERFACE_SERVER	Physical interface used to connect the server to the X3 in-line appliance (any port number between 1–52).	2
--interface-server-speed	X3_INTERFACE_SERVER_SPEED	Physical interface used to connect the server to the X3 in-line appliance (any port number between 1–52).	1000
--interface-server-ip	X3_INTERFACE_SERVER_IP	IP address used on the X3 interface to connect to the server (must be on the same subnet as the server).	20.20.20.30
--server-ip	X3_SERVER_IP	IP address of the server.	20.20.20.40
--server-ip-mask	X3_SERVER_IP_MASK	CIDR mask used in the address for the server.	24

--server-port	X3_SERVER_PORT	TCP port used by the SSL/TLS server.	443
--interface-tool-1	X3_INTERFACE_TOOL_1	Physical interface used to output the decrypted HTTP traffic to a tool (any port number between 1–52). This is used in both "active" and "passive" mode	25
--interface-tool-1-speed	X3_INTERFACE_TOOL_1_SPEED	Speed configured on the interface going to the active or passive inline appliance	1000
--interface-tool-2	X3_INTERFACE_TOOL_2	Physical interface used to send and receive the decrypted HTTP traffic to a tool (any port number between 1–52). This is used only in "active" mode	26
--interface-tool-2-speed	X3_INTERFACE_TOOL_2_SPEED	Speed configured on the interface going to the active inline appliance	1000
--tls-versions	X3_TLS_VERSIONS	TLS string versions used by the X3 SSL/TLS interface to the client.	TLSv1.3

Example:

```
/profitap/x3-ssl.sh -f do_configure --interface-client 1 --interface-client-speed
1000 --interface-client-ip 10.10.10.30 --client-ip 10.10.10.20-interface-server 2
-interface-server-speed 1000 --interface-server-ip 20.20.20.30 --server-ip
20.20.20.40 --server-ip-mask 20.20.20.40/24 --https-server-port 443
--interface-tool-1 25 --interface-tool-1-speed 1000 --tls-versions TLSv1.3
```

When the configuration is submitted to the device, it is applied immediately, and is saved to automatically be reapplied on device reboot.

It is possible to completely reset the device configuration and reboot the device with the following command:

```
/profitap/x3-ssl -f do_reset_config_reboot
```

3.3.3 Monitoring

Using the X3-Series CLI, it is possible to monitor the state of the device interfaces and traffic counters.

The ports status is available via the following command:

```
/profitap/x3-ssl -f do_get_ports_status
```

This will output, for instance:

```
Port      Link      Speed     Mode
1         DOWN      10000     RX
2         DOWN      10000     TX
3         DOWN      10000     TX
4         DOWN      10000     TX
5         DOWN      10000     TX
6         DOWN      10000     TX
7         DOWN      10000     TX
8         DOWN      10000     TX
9         DOWN      10000     TX
10        DOWN      10000     TX
11        DOWN      10000     TX
12        DOWN      10000     TX
13        DOWN      10000     TX
14        DOWN      10000     TX
15        DOWN      10000     TX
16        DOWN      10000     TX
17        DOWN      10000     TX
18        DOWN      10000     TX
19        DOWN      10000     TX
20        DOWN      10000     TX
21        DOWN      10000     TX
22        DOWN      10000     TX
23        DOWN      10000     TX
24        DOWN      10000     TX
25        DOWN      10000     TX
```

Ports statistics are available via the following command:

```
/profitap/x3-ssl -f do_get_ports_statistics
```

This will output, for instance:

Port	RX-Pkts	RX-Bytes	RX-Mpbs	RX-Usage	RX-Bad-CRC	RX-Errors	RX-Dropped	TX-Pkts	TX-Bytes	TX-Mbps	TX-Usage	TX-Errors
1	0	0.00	0.00	0.0000	0	0	0	0	0.00	0.00	0.0000	0
2	0	0.00	0.00	0.0000	0	0	0	0	0.00	0.00	0.0000	0
3	0	0.00	0.00	0.0000	0	0	0	0	0.00	0.00	0.0000	0
4	0	0.00	0.00	0.0000	0	0	0	0	0.00	0.00	0.0000	0
5	0	0.00	0.00	0.0000	0	0	0	0	0.00	0.00	0.0000	0
6	0	0.00	0.00	0.0000	0	0	0	0	0.00	0.00	0.0000	0
7	0	0.00	0.00	0.0000	0	0	0	0	0.00	0.00	0.0000	0
8	0	0.00	0.00	0.0000	0	0	0	0	0.00	0.00	0.0000	0
9	0	0.00	0.00	0.0000	0	0	0	0	0.00	0.00	0.0000	0
10	0	0.00	0.00	0.0000	0	0	0	0	0.00	0.00	0.0000	0
11	0	0.00	0.00	0.0000	0	0	0	0	0.00	0.00	0.0000	0
12	0	0.00	0.00	0.0000	0	0	0	0	0.00	0.00	0.0000	0
13	0	0.00	0.00	0.0000	0	0	0	0	0.00	0.00	0.0000	0
14	0	0.00	0.00	0.0000	0	0	0	0	0.00	0.00	0.0000	0
15	0	0.00	0.00	0.0000	0	0	0	0	0.00	0.00	0.0000	0
16	0	0.00	0.00	0.0000	0	0	0	0	0.00	0.00	0.0000	0
17	0	0.00	0.00	0.0000	0	0	0	0	0.00	0.00	0.0000	0
18	0	0.00	0.00	0.0000	0	0	0	0	0.00	0.00	0.0000	0
19	0	0.00	0.00	0.0000	0	0	0	0	0.00	0.00	0.0000	0
20	0	0.00	0.00	0.0000	0	0	0	0	0.00	0.00	0.0000	0
21	0	0.00	0.00	0.0000	0	0	0	0	0.00	0.00	0.0000	0

Legal

Disclaimer

The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranty of merchantability or fitness for any particular purpose. The manufacturer reserves the right to revise this publication and to make changes in the content thereof without obligation of the manufacturer to notify any person of such revision or changes.

Copyright

This publication, including all photographs and illustrations, is protected under international copyright laws, with all rights reserved. Neither this manual, nor any of the material contained herein, may be reproduced without written consent of the author.

Trademarks

The trademarks mentioned in this manual are the sole property of their owners.