

v1.20_WIDS



WIPS/WIDS - () .

, , , , .

(1.18.0) :

- 1. DDoS ;
- 2. ;
- 3. ;
- 4. , SSID;
- 5. , MAC;
- 6. ;
- 7. .

eltex-wids-service - , / "" WIPS/WIDS.

WIPS/WIDS .

- EMS (-) 2- .

GUI EMS :

Лицензия					
		SFP, WOP-2ac-SFP			
21	WIRELESS devices by external vendors	GenericAp	9000	1	
22	Wireless WIPSWIDS		10	9	
Всего		63	153810	86	

✖ Закрыть

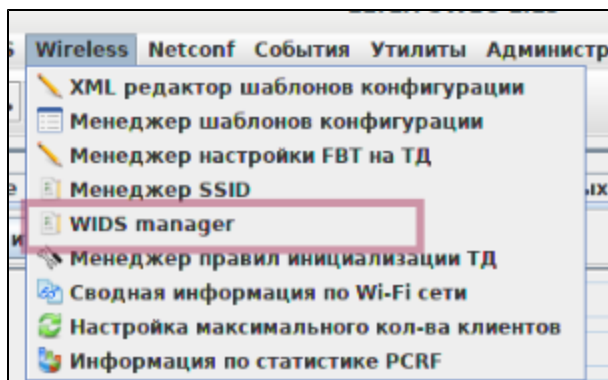
/licence.xml:

/usr/lib/eltex-
ems/conf/licence

/usr/lib/eltex-ems/conf/licence/licence-dist.xml

```
<group>
  <title>Wireless WIPSWIDS</title>
  <count>10</count>
  <typeList>
    <type>WiFi</type>
  </typeList>
</group>
```

WIPS/WIDS , GUI EMS "Wireless" "WIDS manager":



" "

GUI EMS . :

- " WIDS/WIPS " - , . , , WIDS/WIPS, 1. - - WIPS/WIDS .
- " WIDS/WIPS" - , . , , " WIDS/WIPS " , , , .

Мониторинг		Конфигурация		Статистика RRD		Доступ	
Описание		Пользователи Wi-Fi		Мониторинг конкурентных ТД			
Обновить		Редактировать					
Web password							
BRAS сервис	<input type="checkbox"/>						
MAC адрес	E0:D9:E3:4B:FB:20						
Tunnel IP							
Имя ESR							
OTT (Over-the-top)	None						
Дата инициализации устройства	27.06.2019 08:08:54						
Вкл WIPS/WIDS сервис	<input checked="" type="checkbox"/>						
Реальное применение WIPS/WIDS	<input checked="" type="checkbox"/>						
----- Параметры инициализации -----							
ФИО							

- "" :
 1. " WIDS/WIPS ";
 2. " WIDS/WIPS".
- "" - " WIDS/WIPS"

Описание	Пользователи Wi-
Сеть	
Беспроводной доступ	
Доступ	
Радио интерфейсы	
WIDS/WIPS	
Виртуальные точки доступа	
Key holder data	
Global RADIUS	
QoS. Main	
QoS. EDCA parameters	
Client QoS. Global	
Client QoS. Class Map	
Client QoS. Policy Map	
WDS	
Captive Portal. Global	
Captive Portal. Instance	
Cluster. Main	
AirTune сервис	
Системное время	
Системные события	
SNMP	
SNMP trap	
CLI/telnet	
CLI/ssh	

:

1. " " -, , ;
2. "" -, ;
3. "" -, - , MAC- SSID .

" " , Beacon , WIDS, .

, *Shared key* .

, , , , " " ""

" " MAC- SSID, , "", , .

```
      : 2019-05-13 15:31:04
      : WEP-12ac_13
      :      : E0:D9:E3:4F:9D:F0, ssid Eltex-Local, 1!
      : CRITICAL
OID      : 1.3.6.1.4.1.35265.1.60.1.8.3.0.2
```

, , "" . *eltex-wids-service*.

" *WIDS/WIPS*" " " .

Описание

Пользователи Wi-Fi

Мониторинг конкурентных ТД

Мониторинг

Конфигурация

Доступ

Сеть

Беспроводной доступ

Доступ

Радио интерфейсы

WIDS/WIPS

Виртуальные точки доступа

Key holder data

Global RADIUS

QoS. Main

QoS. EDCA parameters

Client QoS. Global

Client QoS. Class Map

Client QoS. Policy Map

WDS

Captive Portal. Global

Captive Portal. Instance

Cluster. Main

AirTune сервис

Системное время

Системные события

SNMP

SNMP trap

CLI/telnet

CLI/ssh

Обновить

Редактировать

В XML

WIDS Parameters

Status

Full

Shared key

1234567890

WIDS list URL

ws://100.111.50.1:9095/MacLists

WIDS MAC list

WhiteList

Scan mode

Passive

Passive scan interval, sec

20

Passive scan duration, ms

100

Prevention mode

None

Misconfigure detection

Off

DoS Detection Parameters

Mode

Up

Interval, sec

1

DoS-trigger

250

Assoc threshold

500

Reassoc threshold

500

Disassoc threshold

500

Auth threshold

500

Deauth threshold

500

Rts threshold

500

Cts threshold

500

Prob threshold

500

Beacon threshold

500

Blockack threshold

500

Blockackreq threshold

500

Pspoll threshold

500

Bruteforce Detection Parameters

Interval, sec

5

Threshold


25

Enable MAC Blacklist

On

Timeout, sec

1800



WIDS Parameters		
Status	Full/Down/Key-only	Full - . Down - . . Key-only - , . Key-only Beacon , "" , . <i>Shared key.</i>
Shared key	ASCII 10 32	, . - , .

WIDS list URL	ws://<ip>:<port>/MacLists	eltex-wids-service. .
WIDS MAC list		MAC-, <i>"Wireless - WIDS Manager"</i> .
Scan mode	Passive/Sentry /Home-only	. Passive - (Passive scan interval) (Passive scan duration) () , . , . . Sentry - . Home-only - , . Passive , .
Passive scan interval, sec	5..3600	. -: 20.
Passive scan duration, ms	10..2000	. -: 100.
Home-only scan interval, sec	5..3600	Home-only. -: 20.
Home-only scan duration, ms	10..2000	Home-only. -: 100.
Prevention mode	None/Rogue/All	. None - . . Rogue - MAC-, "", DeAuth "" "" . All - DeAuth , "", , "" .
Misconfigure detection	Off/On	, . -: off - v1.17_ <div> : 01.07.2019 02:13:09 : wep12 : . system: ; wids-service: ; : CRITICAL OID : 1.3.6.1.4.1.35265.1.60.1.8.3.0.6 </div>
DoS Detection Parameters		
Mode	Up/Down	DoS-. -: down. DoS . , destination mac mac- . (Beacon)
Interval, sec	1..86400	, . , SNMP- . <div> : 08.07.2019 17:30:20 : WEP-12ac_13 : " " wlan1(5GHz): Beacon (159 99). 40 : CRITICAL OID : 1.3.6.1.4.1.35265.1.60.1.8.3.0.1 </div> -: 1.
DoS-trigger	1..1000000000	, . , DoS-. -: 250.
... treshlold	1..10000	(Assoc, ReAssoc, DiAssoc, Auth, DeAuth, RTS, CTS, Prob, Beacon, BlockAck, BlockAckReq, Pspoll) -: 500.
Bruteforce Detection Parameters		

Interval, sec	0..86400	<p>. SSID (Personal Enterprise) . Threshold , "".</p> <pre> : 12.07.2019 14:37:02 : WEP-12ac_13 : " " wlan0vap2(2.4GHz)(_ES_24_test_timers_enter), -: 0c:9d:92:6e:d9:20 : CRITICAL OID : 1.3.6.1.4.1.35265.1.60.1.1.1.14 </pre> <p>:- 5. Interval = 0, "" .</p>
Threshold	1..10000	<p>. :- 25.</p>
Enable MAC Blacklist	On/Off	<p>MAC- , "", Timeout. "MAC Blacklist" Timeout, , . :- off</p>
Timeout, sec	1..86400	<p>MAC- . :- 1800</p>

1.18.0 . (ap-security) - :

180 3 (login/password) telnet/ssh/web/consol, ip-, , 5, .

```

: 19.09.2019 13:26:02
: WEP-12ac_13
: tel c 100.111.50.151.
: MAJOR
OID : 1.3.6.1.4.1.35265.1.60.1.7.1.1

```

logon-snmp-retries	0..127	<p>, logon-snmp-interval, ip- "".</p> <p>: 3</p>
logon-snmp-interva, sec	1..86400	<p>, .</p> <p>: 180</p>
logon-snmp-freeze-interval, sec	0..600	<p>, ip-, , .</p> <p>: 300</p>

, / , CLI .

```

: get ap-security
:
Property                               Value
-----
logon-snmp-retries                     3
logon-snmp-interval                    180
logon-snmp-freeze-interval             300

: set ap-security <_> <>
: set ap-security logon-snmp-interval 86400

: set ap-security logon-snmp-retries 0

: save-running

```

eltex-wids-service

"" "" GUI EMS ("Wireless WIDS Manager") " WIDS MAC list" " WIDS/WIPS" "" .

Wids Менеджер

Wids Tab

Страница: / на странице:

Наименование	Число белых	Число черных
WhiteList	3	0
BlackList	0	3

/etc/eltex-wids-
service/config.hocon

Редактирование объекта

/etc/eltex-wids-service/config.hoon

Наименование ★ WhiteList

serviceConfiguration = { Наименование списка ✓ ✎ ✖

ApplicationConfiguration = {

ServicePort = 9095 // service listen port

// if this environment equals to 'production', all logs will transmit to graylog

// else if this environment equals to 'k8s', all logs will be written to stdout

Environment = "production" ★

SleepDaemonQueueTime = 5 // time for sleep (unit: milliseconds)

FoulTime = 60 // time of raw event, they disappear (unit: seconds)

GelfEnabled = false // inclusion of sending logs to graylog ✓ ✎ ✖

DatabaseName = "wids" // database name

MongoConnectionString = "mongodb://172.17.0.2:27017" // database connection string

}

Черные адреса ★

logs = {

LoggerConfiguration = {

LogLevel = "error"

FileLog = "/var/log/eltex-wids/wids.log" // name of log file

MaxSize = 5 // maximal size of log file (unit: megabyte)

MaxAge = 30 // maximum log lifetime (unit: days)

MaxBackups = 10 // maximum number of backups (unit: amount of log files)

Compress = true // the need of compression ✓ ✎ ✖

GelfHostWithPort = "lab3-test.eltex.loc:12201" // address of graylog server

}

}

- , :

ServicePort = 9095

- . 2: "production" - Graylog, "k8s" - stdout.

Environment = "production"

- Graylog:

GelfEnabled = false

- , :

DatabaseName = "wids"

- :

MongoConnectionString = "mongodb://172.17.0.2:27017"

- :

LogLevel = "error"

- :

```
FileLog = "/var/log/eltex-wids/wids.log"
```

- :

```
MaxSize = 5
```

- :

```
MaxAge = 30
```

- :

```
MaxBackups = 10
```

- :

```
Compress = true
```

- Graylog:

```
GelfHostWithPort = "lab3-test.eltex.loc:12201"
```

docker-. .env docker-compose.yml

docker-compose.yml

```
version: "3"

services:
  wids:
    image: hub.eltex-co.ru/softwlc/eltex-wids:1.20-<tag>
    ports:
      - 9095:9095
    volumes:
      - "/var/log/eltex-wids:/var/log/eltex-wids"
      - "/etc/eltex-wids-service/config.hocon:/etc/eltex-wids-service/config.hocon"
    environment:
      - LogLevel=${WIDS_LOG_LEVEL}
      - MongoUrl=${WIDS_MONGO_URL}
      - DBName=${WIDS_DB_NAME}
      - SleepDaemonQueueTime=${WIDS_SLEEP_DAEMON_QUEUE_TIME}
      - FoulTime=${WIDS_FOUL_TIME}
```



<tag> , .

.env

```
WIDS_LOG_LEVEL=error
WIDS_MONGO_URL=mongodb://<IP-address>:27017
WIDS_DB_NAME=wids
WIDS_SLEEP_DAEMON_QUEUE_TIME=5
WIDS_FOUL_TIME=60
```

- **ServicePort** - , .

- **SleepDaemonQueueTime** - ;
- **FoulTime** - .

MongoDB

- **DBName** -
- **MongoUrl** - MongoDB-.

- **LogLevel** - (ERROR, INFO, DEBUG);
- **FileLog** - ;
- **MaxSizeFileLog** - - ;
- **MaxAgeFileLog** - - ;
- **MaxBackupsFileLog** - ;
- **CompressLogs** - -;
- **GelfHostWithPort** - GrayLog;
- **LogEnvironment** - ; , (file/stdout);
- **GelfEnabled** - GrayLog.