

v1.24_WIDS

-
-
-
-
- "WIDS/WIPS" Fastpath- (WEP/WOP-2ac/12ac)
- "WIDS/WIPS" ESDK (WEP/WOP-3ax)
- eltex-wids-service
- /etc/eltex-wids-service/config.hocon
-
-
-
-
- MongoDB
-

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
<div>✖ Закрыть</div>				

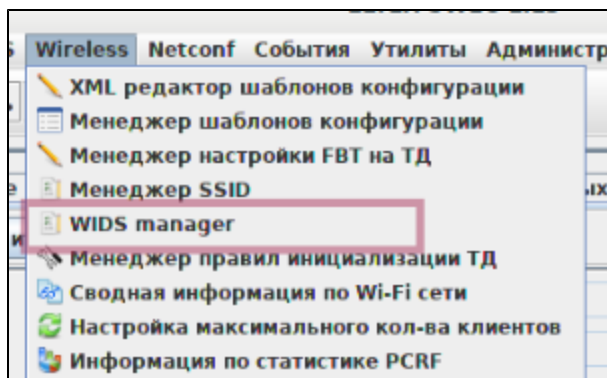
/licence.xml:

/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" Fastpath- (WEP/WOP-2ac/12ac)

"*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

StatusFull

Shared key1234567890

WIDS list URLws://100.111.50.1:9095/MacLists

WIDS MAC listWhiteList

Scan modePassive

Passive scan interval, sec20

Passive scan duration, ms100

Prevention modeNone

Misconfigure detectionOff

DoS Detection Parameters

ModeUp

Interval, sec1

DoS-trigger250

Assoc threshold500

Reassoc threshold500

Disassoc threshold500

Auth threshold500

Deauth threshold500

Rts threshold500

Cts threshold500

Prob threshold500

Beacon threshold500

Blockack threshold500

Blockackreq threshold500

Pspoll threshold500


Bruteforce Detection Parameters

Interval, sec5

Threshold25

Enable MAC BlacklistOn

Timeout, sec1800



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 - v1.23_ <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

```

"WIDS/WIPS" ESDK (WEP/WOP-3ax)

"config" " ".

Описание

Пользователи Wi-Fi

Мониторинг

Консоль

Управление

Доступ

WEP-3ax

config

monitoring

Get

Edit config

Apply config

Save

Backup Config

Настройка WIDS

Включить WIDS

Enable

Общий сетевой ключ

Режим сканирования WIDS

none

Интерфейс сканирования WIDS

all

Период пассивного сканирования, сек

20

Продолжительность сканирования канала для пассивного режима, мс

110

Продолжительность сканирования канала для активного режима, мс

200

Режим подавления (WIPS)

none

URL-адрес службы WIDS-service

ws://192.168.1.1:9095/MacLists

Имя списка службы WIDS

Default_list

Включить обнаружение небезопасной конфигурации

Enable

Bruteforce-detection

Включить обнаружение атак "перебор пароля"

Enable

Порог количества неудачных попыток авторизаций

25

Интервал подсчета неудачных попыток авторизаций, сек

5

Включить блокировку клиентов, уличенных в атаке

Enable

Продолжительность блокировки клиентов, сек

1800

Описание	Пользователи Wi-Fi	Мониторинг	Консоль	Управление	Доступ
<div> <div> <div>WEP-Зах</div> <div>config</div> <div>monitoring</div> </div> <div> <div>Get</div> <div>Edit config</div> <div>Apply config</div> <div>Save</div> <div>Backup Config</div> </div> </div>					
<div> <div>Продолжительность блокировки клиентов, сек</div> <div>1800</div> </div>					
<div>DoS-Detection</div>					
<div> <div>Включить обнаружение атак "отказ в обслуживании"</div> <div>Enable</div> </div>					
<div> <div>Интервал подсчета пакетов в радиоэфире, сек</div> <div>1</div> </div>					
<div> <div>Порог резкого изменения кол-ва пакетов относительно предыдущего периода времени</div> <div>250</div> </div>					
<div> <div>Период отправки сообщения о детектировании атаки в секундах (0-604800)</div> <div>20</div> </div>					
<div> <div>Пороговое значение пакетов типа "Association request"</div> <div>500</div> </div>					
<div> <div>Пороговое значение пакетов типа "Reassociation request"</div> <div>500</div> </div>					
<div> <div>Пороговое значение пакетов типа "Disassociation request"</div> <div>500</div> </div>					
<div> <div>Пороговое значение пакетов типа "Probe request"</div> <div>500</div> </div>					
<div> <div>Пороговое значение пакетов типа "Beacon"</div> <div>500</div> </div>					
<div> <div>Пороговое значение пакетов типа "Block Ack request"</div> <div>500</div> </div>					
<div> <div>Пороговое значение пакетов типа "Block Ack"</div> <div>500</div> </div>					
<div> <div>Пороговое значение пакетов типа "PS poll"</div> <div>500</div> </div>					
<div> <div>Пороговое значение пакетов типа "Authentication"</div> <div>500</div> </div>					
<div> <div>Пороговое значение пакетов типа "Deauthentication"</div> <div>500</div> </div>					
<div> <div>Пороговое значение пакетов типа "RTS"</div> <div>500</div> </div>					
<div> <div>Пороговое значение пакетов типа "CTS"</div> <div>500</div> </div>					

		WIDS
WIDS	/	/ WIDS. -:- off
	ASCII 10 32	, . - , .
WIDS	none/passive/sentry	None - . . Passive - () () () , Sentry - - . .
WIDS	all/wlan0/wlan1	all - 2,4 5 . . wlan0 - 2,4 . wlan1 - 5 .
,	1..3600	. -:- 20.
,	10..2000	. -:- 110.

,	100..2000	, . - : 200.
(WIPS)	none/rogue/all	None - . . Rogue - MAC- , "" , DeAuth "" "" . All - DeAuth , "" , , "" .
URL- WIDS-service	ws://<IP>:<Port>/MacLists	eltex-wids-service. . / MAC
WIDS	Default_list	MAC-, "Wireless - WIDS Manager" . - : Default_list
	/	, , WIDS . - : off
Bruteforce-detection		
" "	/	/ . - : off
	1..10000	. - : 25.
,	0..86400	SSID (Personal Enterprise) . , "" . - : 5. 0, "" .
,	/	MAC- , "" , Timeout. "MAC Blacklist" Timeout, , . - : off
,	1..86400	MAC- . - : 1800
DoS-Detection		
" "	/	DoS- - : off DoS . , destination mac mac- . (Beacon)
,	0..86400	, . , SNMP- . - : 1.
	0..86400	, , DoS- . - : 250.
	0..604800	- : 20
"Association request"	0..86400	- : 500
"Reassociation request"	0..86400	- : 500
"Diassociation request"	0..86400	- : 500
"Probe request"	0..86400	- : 500
"Beacon"	0..86400	- : 500
"Block Ack request"	0..86400	- : 500
"Block Ack"	0..86400	- : 500
"PS poll"	0..86400	- : 500
"Authentication"	0..86400	- : 500
"Deauthentication"	0..86400	- : 500
"RTS"	0..86400	- : 500

"CTS"	0..86400	~: 500
-------	----------	--------

eltex-wids-service

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

Wids Менеджер

Wids Tab

Страница: 1 / 1 на странице: 20

Изменить поляДобавить списокРедактировать списокУдалить список

Наименование	Число белых	Число черных
WhiteList	3	0
BlackList	0	3

Принять

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

Редактирование объекта

Наименование

WhiteList

Наименование списка

Белые адреса

Черные адреса

Принять

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

```
serviceConfiguration = {
  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://127.0.0.1:27017" // database connection string
  }
}

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 = "localhost:12201" // address of graylog server
  }
}
```

- , :

```
ServicePort = 9095
```

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

```
Environment = "production"
```

- Graylog:

```
GelfEnabled = false
```

- , :

```
DatabaseName = "wids"
```

- :

```
MongoConnectionString = "mongodb://127.0.0.1:27017"
```

- :

```
LogLevel = "error"
```

- :

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

- :

```
MaxSize = 5
```

- :

```
MaxAge = 30
```

- :

```
MaxBackups = 10
```

- :

```
Compress = true
```

- Graylog:

```
GelfHostWithPort = "localhost:12201"
```

docker-. .env docker-compose.yml

docker-compose.yml

```
version: "3"

services:
  wids:
    image: hub.eltex-co.ru/softwlc/eltex-wids:1.21-<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.