

# v1.17\_WIDS

- 
- 
- 
- eltex-wids-service

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

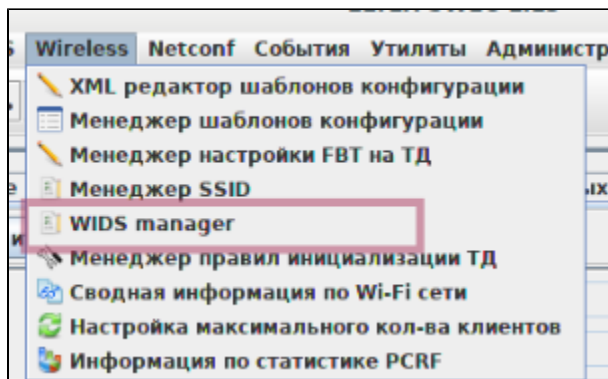
Лицензия					
			SFP, WOP-2ac-SFP		
21	WIRELESS devices by external vendors	GenericAp	9000	1	
22	Wireless WIPSWIDS		10	9	
Всего		63	153810	86	

Закреть

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

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

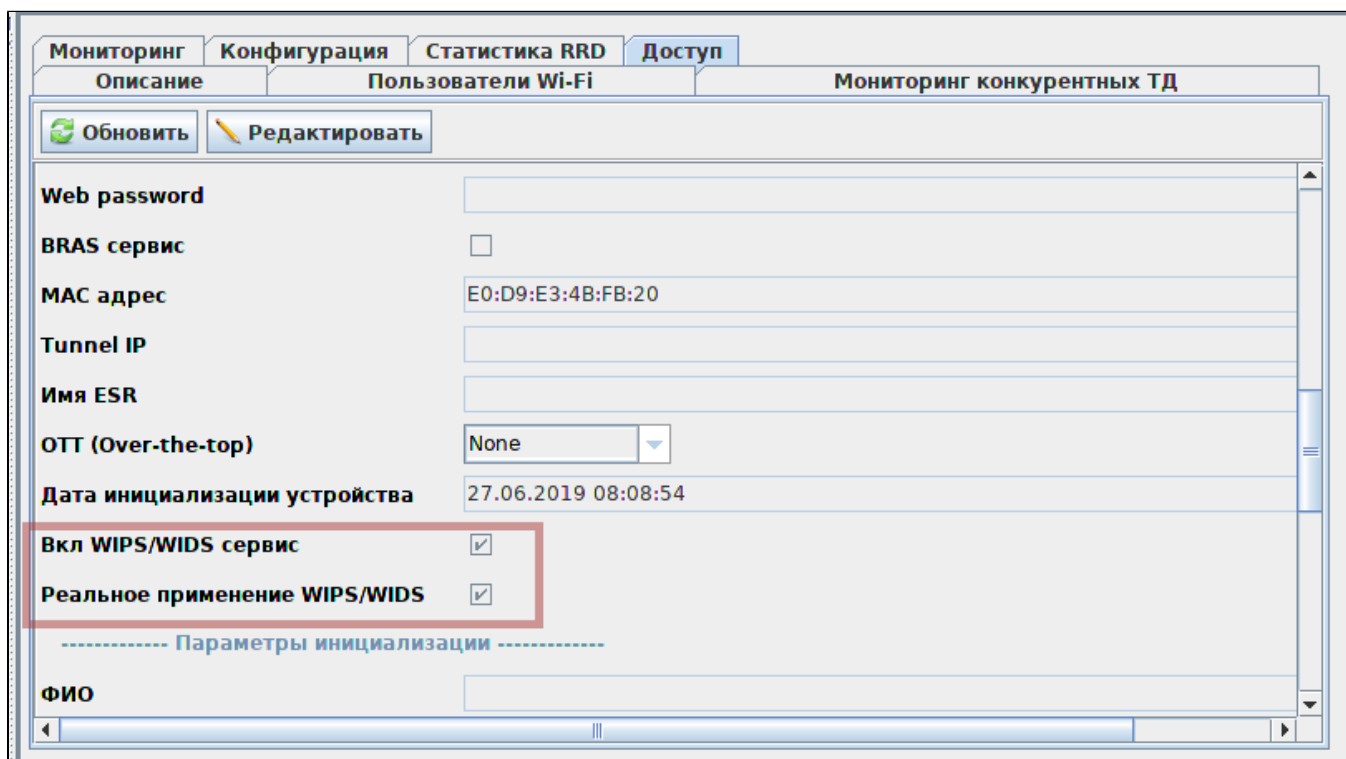
WIPS/WIDS , GUI EMS "Wireless" "WIDS manager":



" "

GUI EMS :

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



, , :

- " " :  
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

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 - . <b>Down</b> - . . 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	. <b>Passive</b> - (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	. <b>None</b> - . . 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> <div> : 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 </div> <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	, logon-snmp-interval, ip- "". : 3
logon-snmp-interva, sec	1..86400	, . : 180
logon-snmp-freeze-interval, sec	0..600	, ip-, , . : 300

, / , 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: 1 / 1 на странице: 20

Изменить поля

Добавить список

Редактировать список

Удалить список

Наименование	Число белых	Число черных
WhiteList	3	0
BlackList	0	3

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

Принять

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

```

{
  "ServicePort": 9095,
  "Database": "wids",
  "MongoConnectionString": "mongodb://localhost:27017",
  "FileLog": "/var/log/eltex-wids-service/log.log",
  "Environment": "production",
  "LogLevel": "debug",
  "MaxAge": 7,
  "MaxSize": 5,
  "MaxBackups": 14,
  "SleepDaemonQueueTime": 50000,
  "FoulTime": 60,
  "GelfHost": "lab3-test.eltex.loc:12201"
}

```

## Редактирование объекта

Наименование

★ WhiteList

Наименование списка

а8:f9:4b:11:11:11  
а8:f9:4b:11:11:12  
а8:f9:4b:11:11:13

Белые адреса



Черные адреса



✓ Принять