v1.16_WIDS

-
-
-
- eltex-wids-service

WIPS/WIDS - () .

 , , , , .

 (1.18.0) :

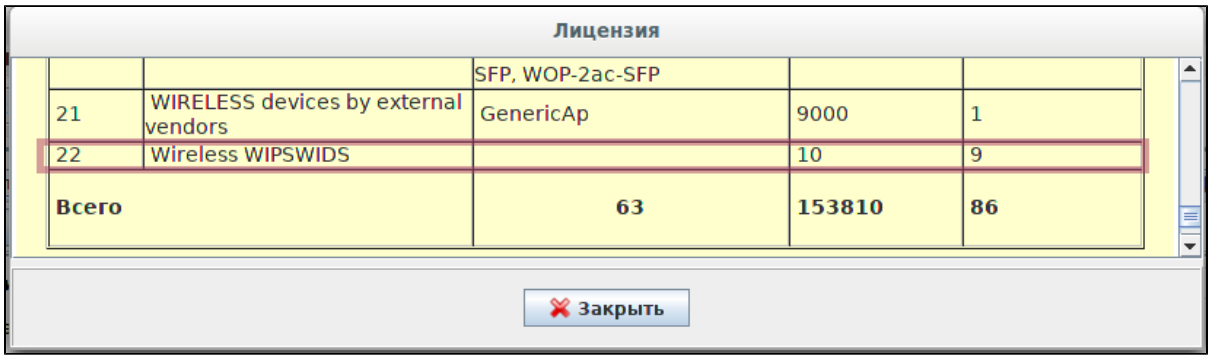
1. DDoS ;
2. ;
3. ;
4. , SSID;
5. , MAC;
6. ;
7. .

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

 WIPS/WIDS .

- EMS (-) 2- .

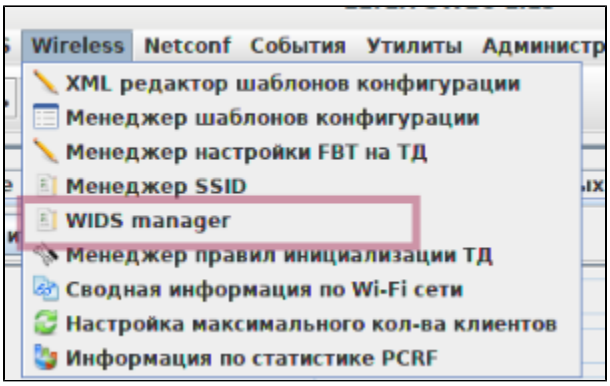
 GUI EMS , */usr/lib/eltex-ems/conf/licence/licence.xml*



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

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

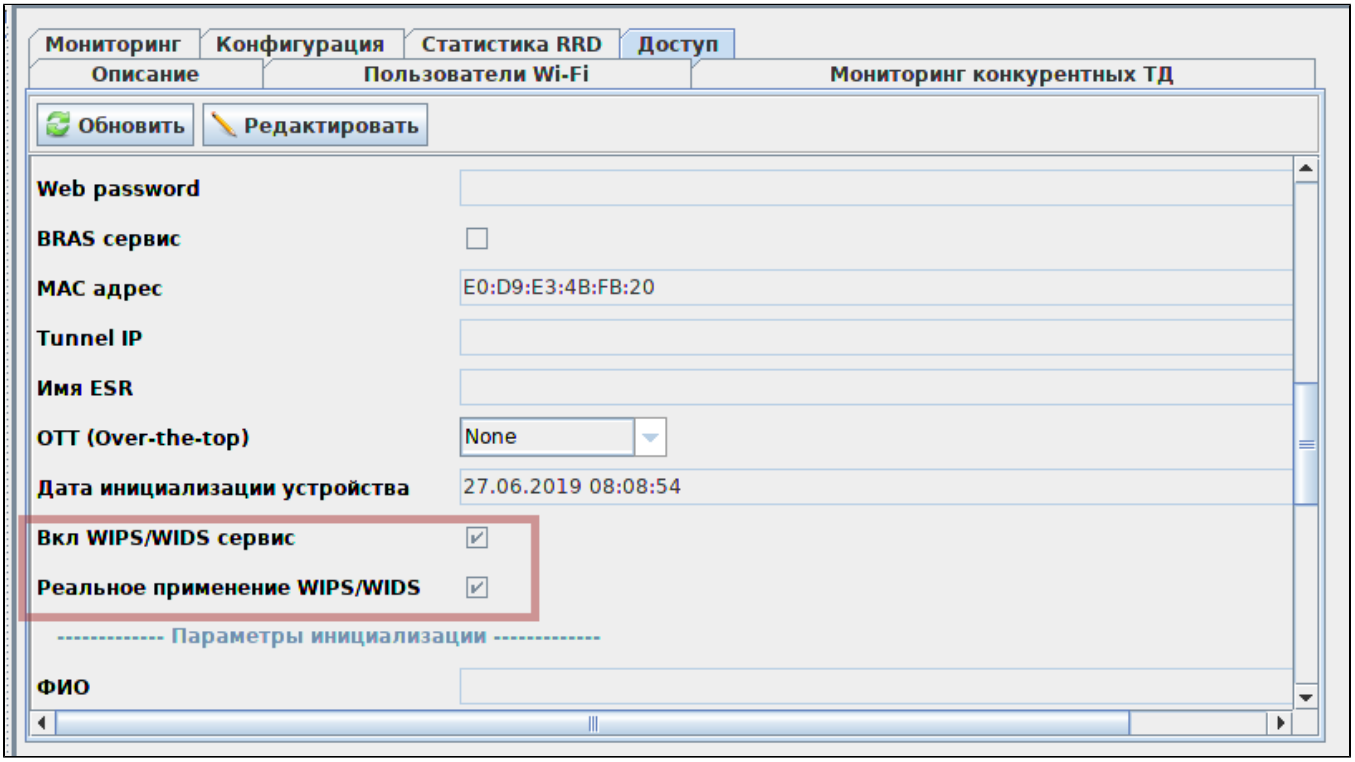
 WIPS/WIDS , GUI EMS "*Wireless*" "*WIDS manager*":



"" .

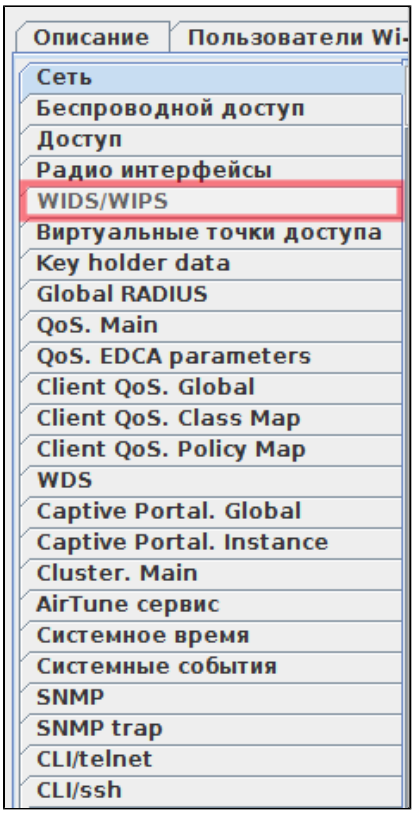
GUI EMS . :

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



, , :

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



:

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

" " , Beacon , WIDS, .

, *Shared key* .

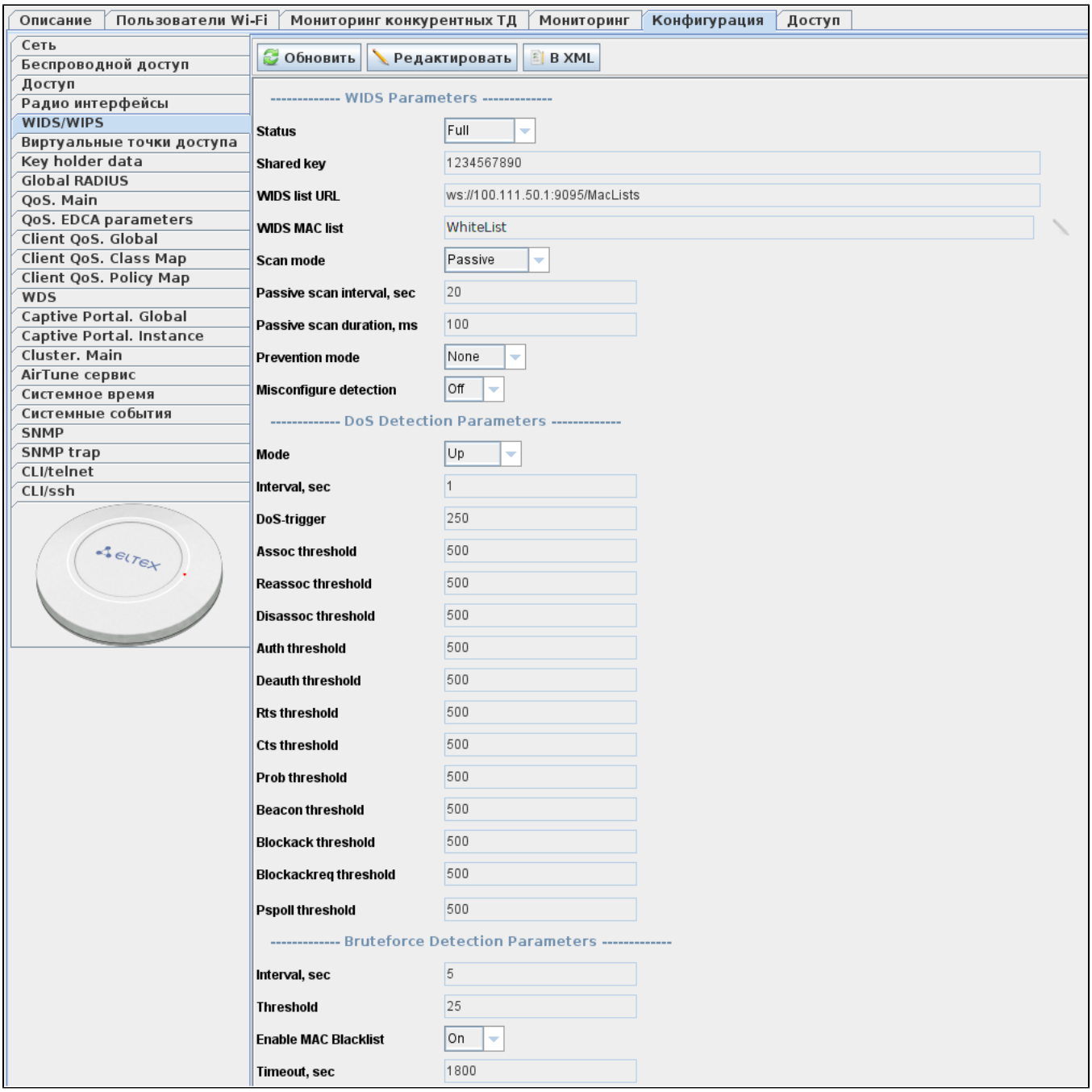
, , , , " ". ""

" " 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*" "*.*



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

WIDS list URL	ws://<ip>:<port>/MacLists	eltex-wids-service. .
WIDS MAC list		MAC-, *"Wireless - WIDS Manager"* .
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* - v1.16_ : 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
DoS Detection Parameters		
Mode	Up/Down	DoS-. -: *down.* DoS . , destination mac mac- . (Beacon)
Interval, sec	1..86400	, . , SNMP- . : 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 -: *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	. SSID (Personal Enterprise) . Threshold , " ". : 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 *-: 5 .* Interval = 0, " " .
Threshold	1..10000	. *-: 25.*
Enable MAC Blacklist	On/Off	MAC- , " ", Timeout. "MAC Blacklist" Timeout, , . *-: off*
Timeout, sec	1..86400	MAC- . *-: 1800*

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
```

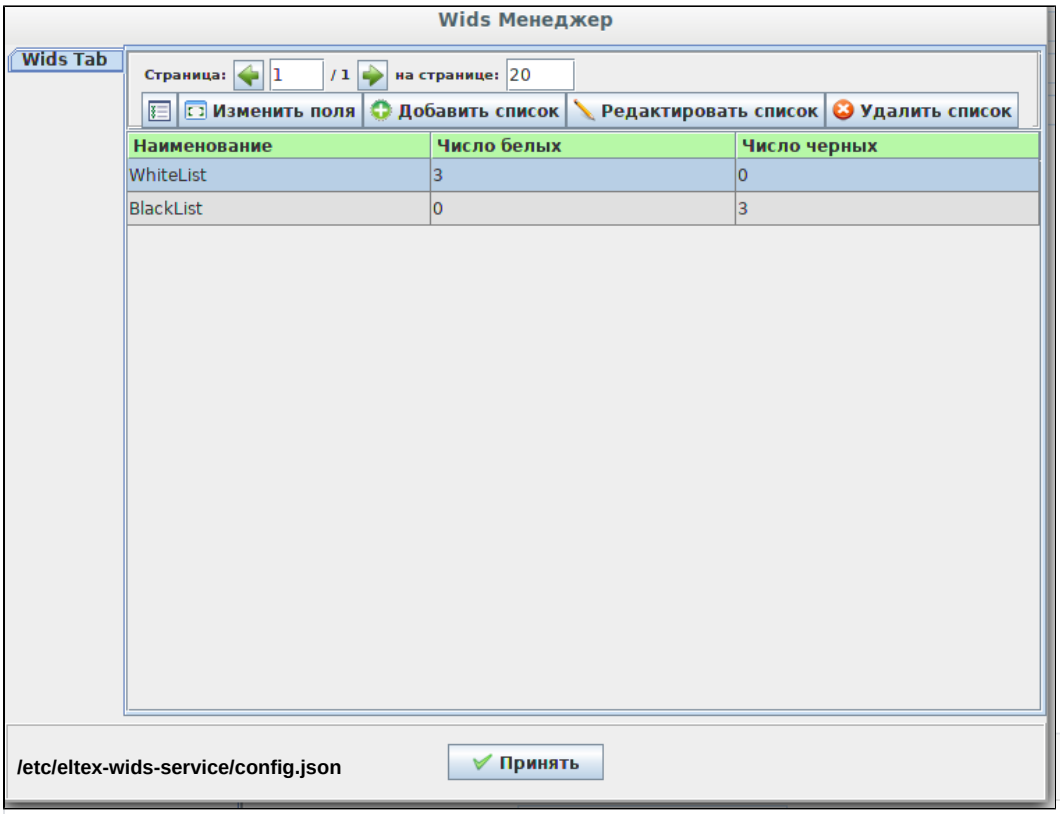
logon-snmp-retries	0..127	, logon-snmp-interval, ip- " ". *: 3*
logon-snmp-interva, sec	1..86400	, . *: 180*
logon-snmp-freeze-interval, sec	0..600	, ip- , , . *: 300*

, / , 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
```

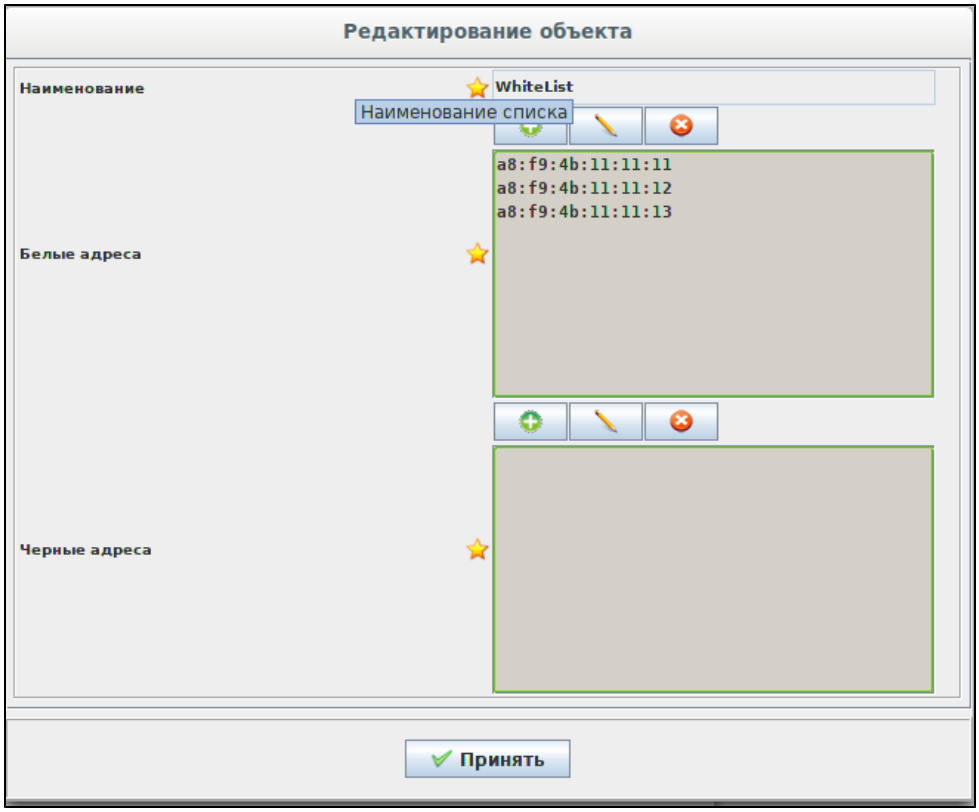
eltex-wids-service

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



- /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
a8:f9:4b:11:11:11
a8:f9:4b:11:11:12
a8:f9:4b:11:11:13
Белые адреса
Черные адреса
Принять