v1.14_WIDS

-
-
-
- eltex-wids-service

WIPS/WIDS - () .

, , .

(1.17.0) :

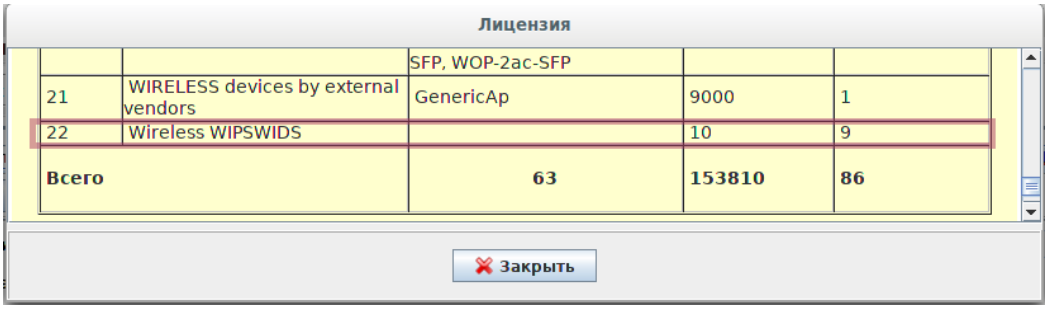
1. DDoS ;
2. ;
3. ;
4. , SSID;
5. , MAC;
6. .

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

WIPS/WIDS .

(-) 2- .

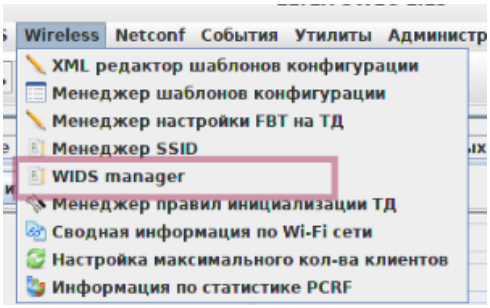
- GUI EMS - , */usr/lib/eltex-ems/conf/licence/licence.xml*



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

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

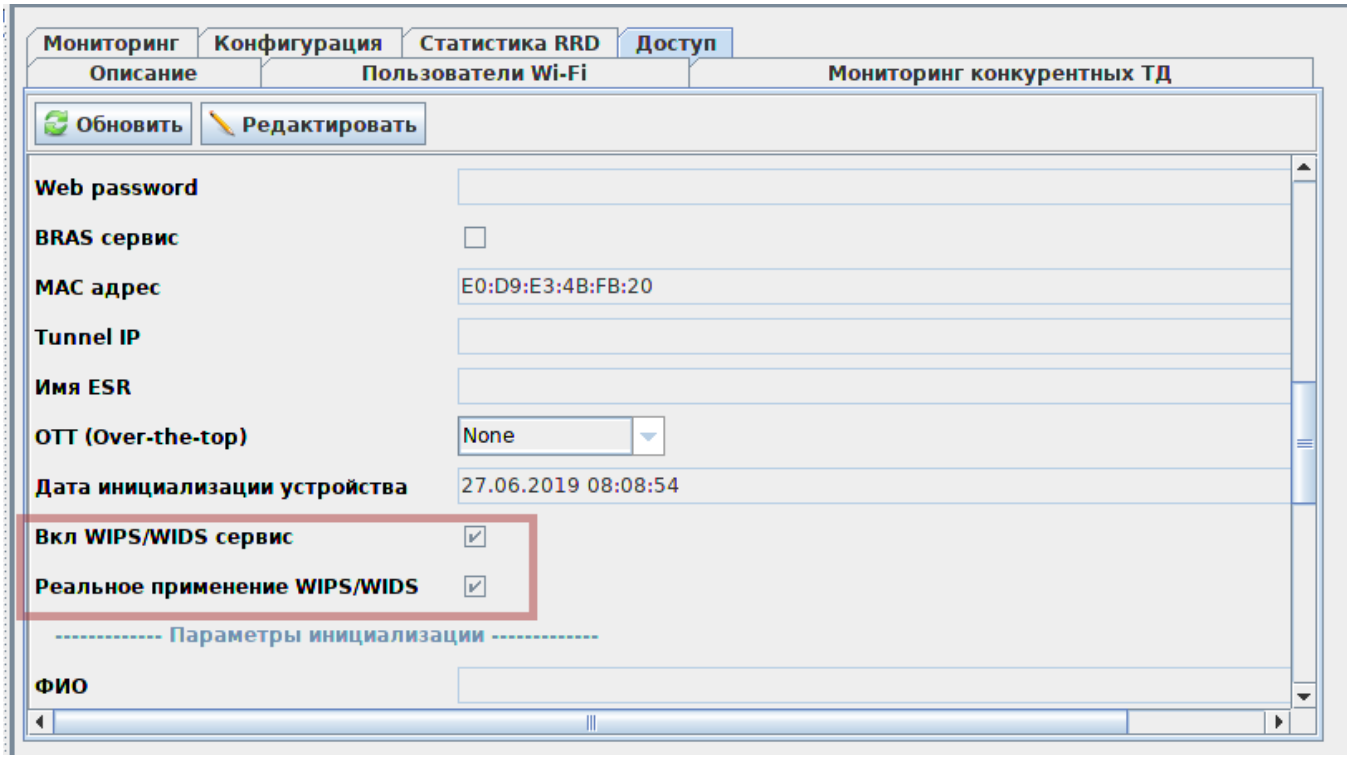
WIPS/WIDS , GUI EMS "*Wireless*" "*WIDS manager*":



"" .

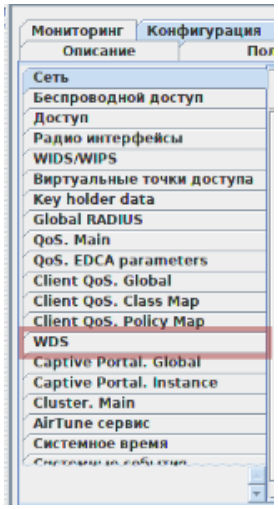
GUI EMS . :

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

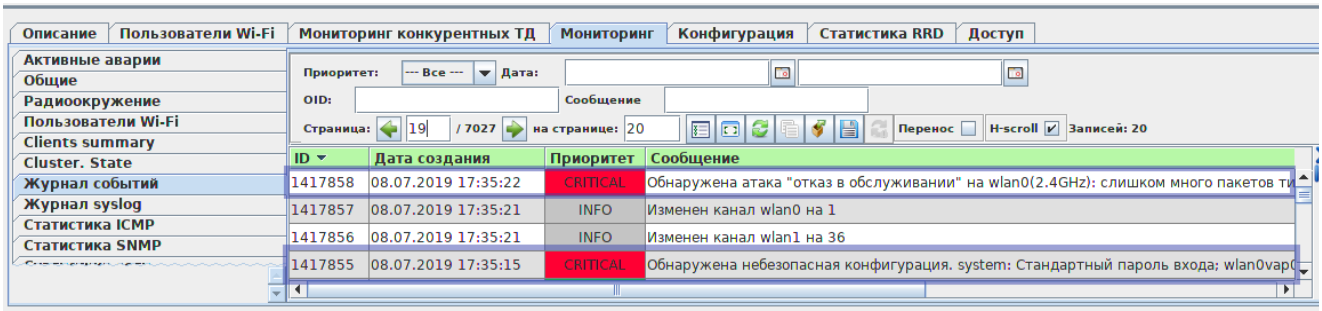


, "" , :

- "" - "*WIDS/WIPS*"



- "" " " " " WIDS/WIPS



:

- " " - , , .
- "" - ,
- "" - , (MAC- SSID).

" " , Beacon , WIDS, .

, *Shared key* .

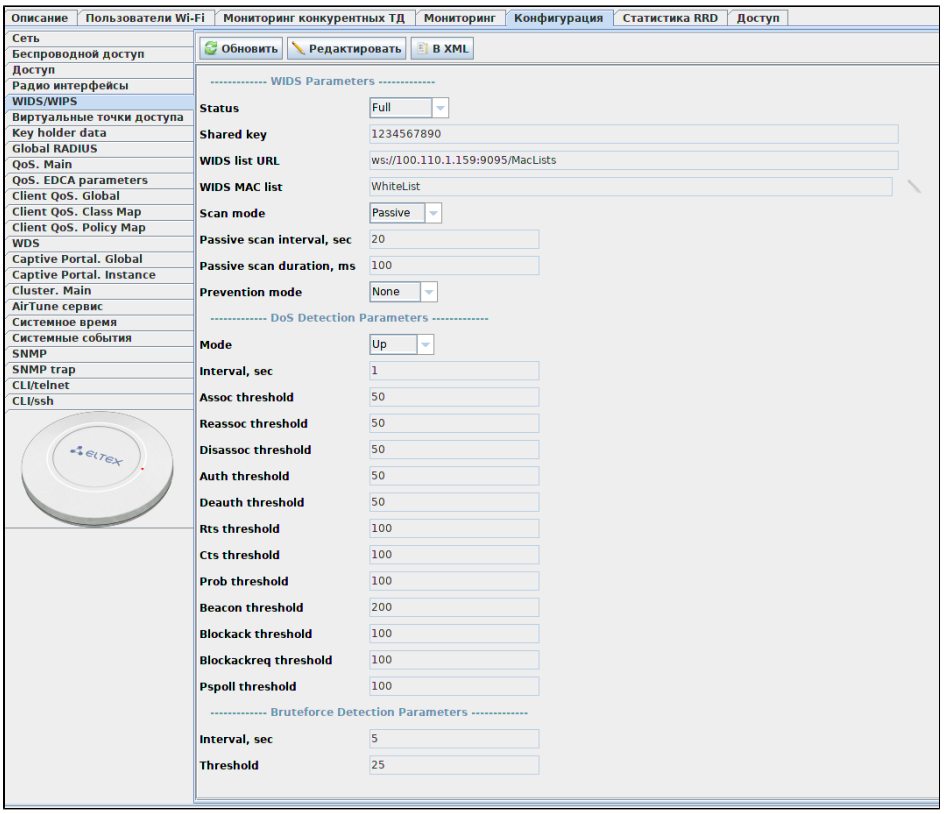
, , , , " ". ""

" " 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.*

eltex-wids-service "WIDS/WIPS" "



WIDS Parameters		
Status	Down/Full/Key-only	Down - (-). Full - . Key-only - , . "Key-only" Beacon , "", . *Shared key.*
Shared key	ASCII 10 32	, . - . , Shared key , .
WIDS list URL	ws://<ip>:<port>/MacLists	eltex-wids-service. .
WIDS MAC list		, *"Wireless - WIDS Manager"* .
Scan mode	Passive/Sentry	. Passive - (*Passive scan interval*) (*Passive scan duration*) ( ) , . (-) Sentry - - . .
Passive scan interval, sec	5..3600	(-: 20)
Passive scan duration, ms	10..2000	(-: 100)

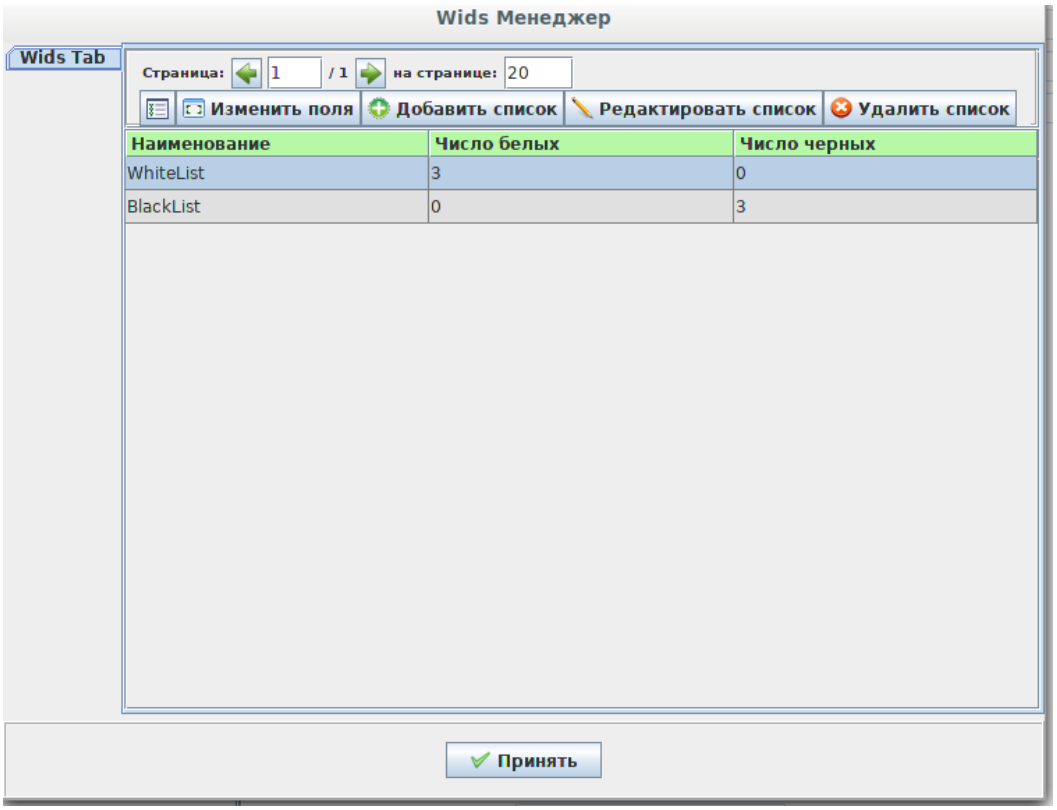
Prevention mode	None/Rogue/All	. None - (-) Rogue - , "" , DeAuth "" , "" . All - DeAuth " ", " " .
DoS Detection Parameters		
Mode	Up/Down	Down - DoS (-) Up - DoS DoS . , destination mac mac- . (Beacon)
Interval, sec	1..86400	, . - SNMP- . : 08.07.2019 17:30:20 : WEP-12ac_13 : " " wlan1(5GHz): Beacon (159 99). 40 : CRITICAL OID : 1.3.6.1.4.1.35265.1.60.1.8.3.0.1 - - 1
... treshlold	1..10000	(Assoc, ReAssoc, DiAssoc, Auth, DeAuth, RTS, CTS, Prob, Beacon, BlockAck, BlockAckReq, Pspoll) -: Assoc, ReAssoc, DiAssoc, Auth, DeAuth - 50 RTS, CTS, Prob, BlockAck, BlockAckReq, Pspoll - 100 Beacon - 200
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 . 0 - " " .
Threshold	1..10000	. -: 25

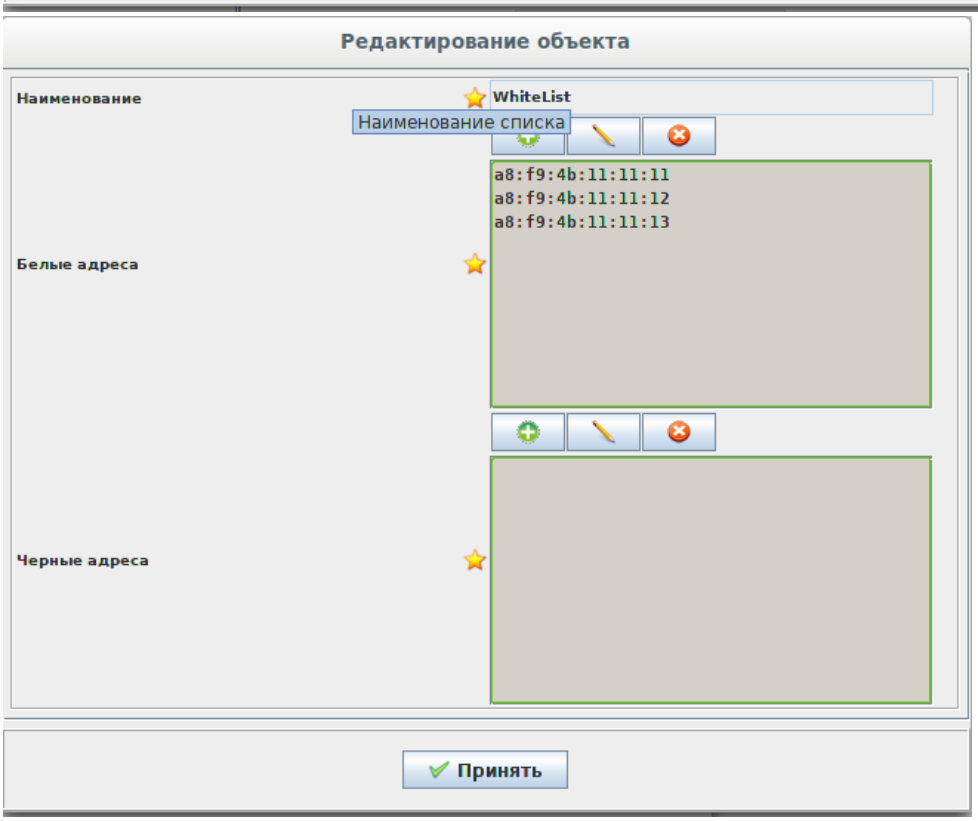
WIPS/WIDS - , .

```
: 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
```

eltex-wids-service

"" "" GUI EMS - "Wireless - WIDS Manager" "*WIDS MAC list*" "*WIDS/WIPS*" "*"*





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

/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"
```