

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- .

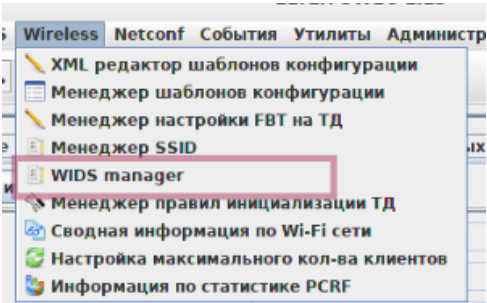
- GUI EMS -, /usr/lib/eltex-ems/conf/licence/licence.xml

Лицензия				
		SFP, WOP-2ac-SFP		
21	WIRELESS devices by external vendors	GenericAp	9000	1
22	Wireless WIPSWIDS		10	9
Bcero		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 " - , . 1. - WIPS/WIDS .
- " WIDS/WIPS" - , . , " WIDS/WIPS " , - , .

The screenshot shows the 'Доступ' (Access) tab in the GUI EMS. The 'Мониторинг' (Monitoring) sub-tab is active, showing the 'Пользователи Wi-Fi' (Wi-Fi Users) section. The 'Мониторинг конкурентных ТД' (Monitoring of competitive TD) section is also visible. The 'Обновить' (Update) and 'Редактировать' (Edit) buttons are at the top. The configuration fields include: Web password, BRAS сервис (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 WIDS/WIPS сервис (checked), and Реальное применение WIDS/WIPS (checked). The 'Параметры инициализации' (Initialization parameters) section is also visible, showing the ФИО (Full Name) field.

, "" , :

- "" - "WIDS/WIPS"

The screenshot shows the 'Конфигурация' (Configuration) tab in the GUI EMS. The 'Мониторинг' (Monitoring) sub-tab is active, showing the 'Пользователи Wi-Fi' (Wi-Fi Users) section. The 'Мониторинг конкурентных ТД' (Monitoring of competitive TD) section is also visible. The 'Обновить' (Update) and 'Редактировать' (Edit) buttons are at the top. The configuration fields include: Сеть (Network), Беспроводной доступ (Wireless access), Доступ (Access), Радио интерфейсы (Radio interfaces), WIDS/WIPS, Виртуальные точки доступа (Virtual access points), Key holder data, Global RADIUS, QoS. Main, QoS. EDCA parameters, Client QoS. Global, Client QoS. Class Map, Client QoS. Policy Map, WIDS (highlighted), Captive Portal. Global, Captive Portal. Instance, Cluster. Main, AirTune сервис (AirTune service), and Системное время (System time).

- "" "" "" WIDS/WIPS

Описание	Пользователи Wi-Fi	Мониторинг конкурентных ТД	Мониторинг	Конфигурация	Статистика RRD	Доступ
Активные аварии						
Общие						
Радиоокружение						
Пользователи Wi-Fi						
Clients summary						
Cluster. State						
Журнал событий						
Журнал syslog						
Статистика ICMP						
Статистика SNMP						

Приоритет:	--- Все ---	Дата:		
OID:		Сообщение		
Страница:	19 / 7027	на странице:	20	

ID	Дата создания	Приоритет	Сообщение
1417858	08.07.2019 17:35:22	CRITICAL	Обнаружена атака "отказ в обслуживании" на wlan0(2.4GHz): слишком много пакетов т
1417857	08.07.2019 17:35:21	INFO	Изменен канал wlan0 на 1
1417856	08.07.2019 17:35:21	INFO	Изменен канал wlan1 на 36
1417855	08.07.2019 17:35:15	CRITICAL	Обнаружена небезопасная конфигурация. system: Стандартный пароль входа: wlan0vap

- " " - , , .
- "" - ,
- "" - , (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" ""

ОписаниеПользователи Wi-FiМониторинг конкурентных ТДМониторингКонфигурацияСтатистика RRDДоступ

СетьБеспроводной доступДоступРадио интерфейсыWIDS/WIPSВиртуальные точки доступаKey holder dataGlobal RADIUSQoS. MainQoS. EDCA parametersClient QoS. GlobalClient QoS. Class MapClient QoS. Policy MapWDSCaptive Portal. GlobalCaptive Portal. InstanceCluster. MainAirTune сервисСистемное времяСистемные событияSNMP trapCLI/telnetCLI/ssh

ОбновитьРедактироватьВ XML

WIDS Parameters

StatusFullShared key1234567890WIDS list URLws://100.110.1.159:9095/MacListsWIDS MAC listWhiteListScan modePassivePassive scan interval, sec20Passive scan duration, ms100Prevention modeNone

DoS Detection Parameters

ModeUpInterval, sec1Assoc threshold50Reassoc threshold50Disassoc threshold50Auth threshold50Deauth threshold50Rts threshold100Cts threshold100Prob threshold100Beacon threshold200Blockack threshold100Blockackreq threshold100Pspoll threshold100

Bruteforce Detection Parameters

Interval, sec5Threshold25



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
... threshld	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" ""

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

Принять

Редактирование объекта

Наименование

★ WhiteList

Наименование списка

Белые адреса

★

a8:f9:4b:11:11:11

a8:f9:4b:11:11:12

a8:f9:4b:11:11:13

Черные адреса

★

Принять

- /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"
```