Комплексные решения для построения сетей

SoftWLC

Инструкция по настройке системы, инициализации и первоначальному конфигурированию точек доступа

Приложение к руководству по эксплуатации

Система конфигурирования AP

Версия ПО 1.5

http://eltex.nsk.ru/support/documentations
http://mc240.ru/support/documentations

Оглавление

Ведение

В данной инструкции рассмотрена схема организации на точке доступа WEP-12ac двух беспроводных сетей: сети с шифрованием WPA2-PSK и сети Hotspot с авторизацией на WEB-портале.

Обычно для управления точкой доступа используется отдельная Management VLAN, а для абонентов – другие VLAN. В данной схеме для упрощения допустим, что управление точкой доступа осуществляется без использования VLAN (трафик управления от SoftWLC до точки идет нетегированным), а абонентский трафик данных будет идти в VLAN 1000, как показано на схеме. Для организации коммутирования устройств и обработки VLAN потребуется L2-коммутатор, а также выход в интернет во VLAN 1000 для проверки услуги с абонентского устройства. При этом во VLAN 1000 должен быть настроен DHCP-сервер для выдачи адресов абонентам Wi-Fi.

На *Рисунке 1* приведена схема стенда.

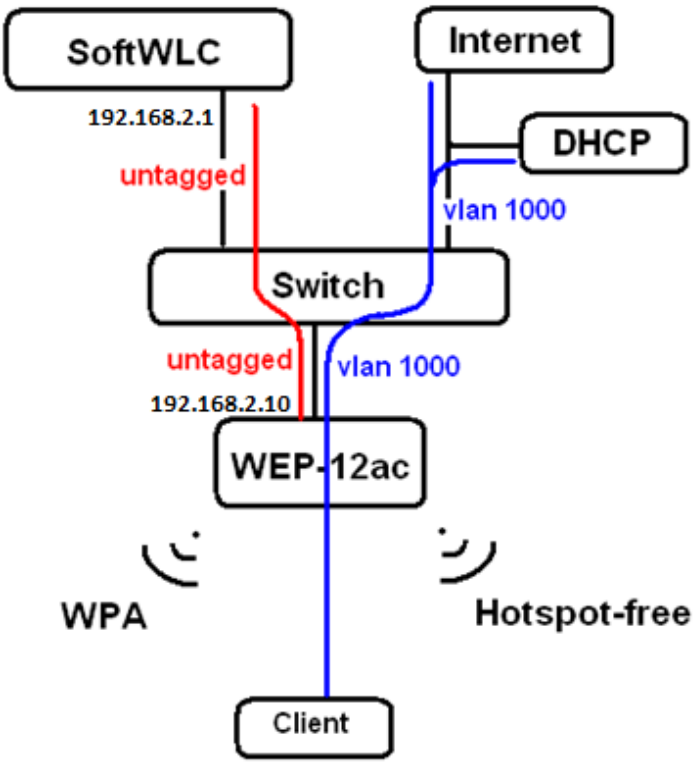


Рисунок 1- Схема стенда

1 Первоначальная настройка EMS-сервера

Для открытия графического интерфейса EMS (GUI EMS) можно воспользоваться браузером с установленным плагином Java или приложением Java Web Start. В отличие от апплетов, приложения Web Start запускаются не в окне браузера и не имеют с ним прямой связи.

1.1. В строке браузера введите адрес (Рисунок 2).

192.168.2.1:8080/ems/

Рисунок 2 – Адресная строка браузера

При загрузке страницы может потребоваться разрешение на выполнение Java-приложения, дайте постоянное разрешение, чтобы сообщение не возникало повторно.

Либо запустите приложение Java Web Start (должен быть установлен Oracle-Java8). Для этого введите:

192.168.2.1:8080/ems/jws/

Чтобы на рабочем столе появился ярлык для открытия GUI EMS, необходимо включить хранение временных файлов в Java Control Panel.

1.2. Для авторизации на EMS сервере введите логин **«admin»** без пароля (Рисунок 3).

Рисунок 3 – Подключение к EMS серверу

1.3. После авторизации откроется графический интерфейс EMS-сервера (Рисунок 4).

Обратите внимание, что при использовании браузера закрытие страницы, с которой был открыт интерфейс, или закрытие браузера приведет к тому, что работа GUI EMS будет завершена.

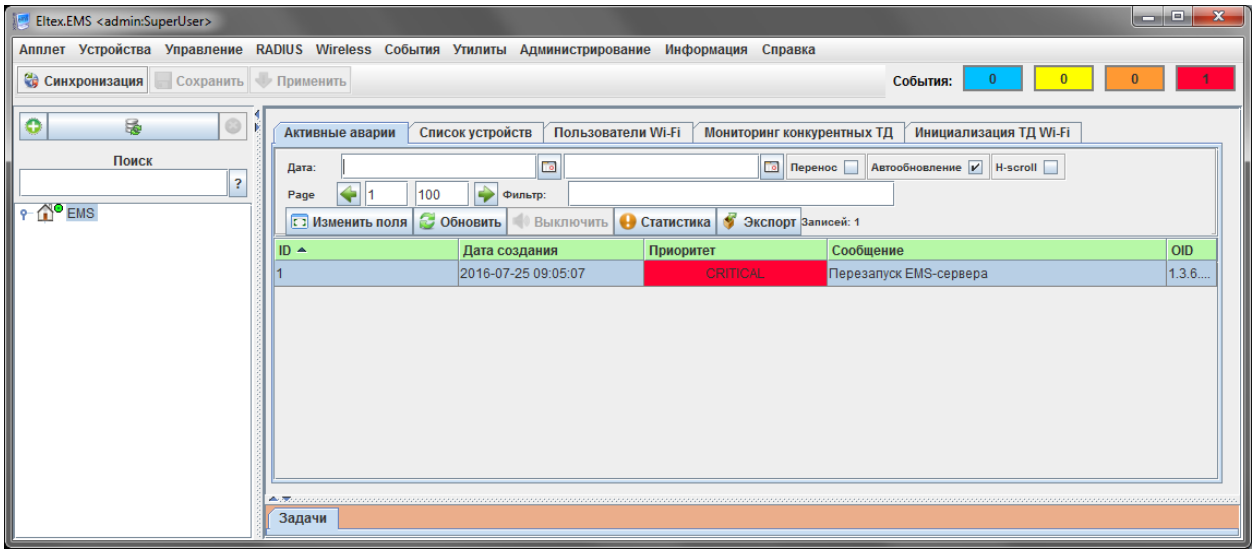


Рисунок 4 – Графический интерфейс EMS

Под заголовком окна расположено главное меню и элементы управления.

1.4. Выполните первоначальную настройку контроллера.

Зайдите в меню «*Администрирование/Настройка сервера/Системные модули*». Откройте вкладку *«System»* и укажите:

- IP-адрес EMS сервера в управляющей сети станции: **192.168.2.1**;
- Tomcat URL: **http://192.168.2.1:8080**;
- тип доступа к устройствам системы: **BY_DOMAIN**.

Перейдите на вкладку *«tftpserver»,* сохранив сделанные изменения. Задайте IP-адрес для станционных устройств: **192.168.2.1.** Нажмите кнопку *«Принять»* и сохраните сделанные изменения.

Перезапустите EMS командой **sudo service eltex-ems restart** либо через меню *«Администрирование/Настройка сервера/Перезапуск EMS сервера».*

Создайте в системе домены. Для этого выберите пункт меню *«Администрирование»,* затем *«Права и пользователи»* и *«Домены».* Создайте корневой домен *«root»* и поддомены при необходимости (Рисунок 5).

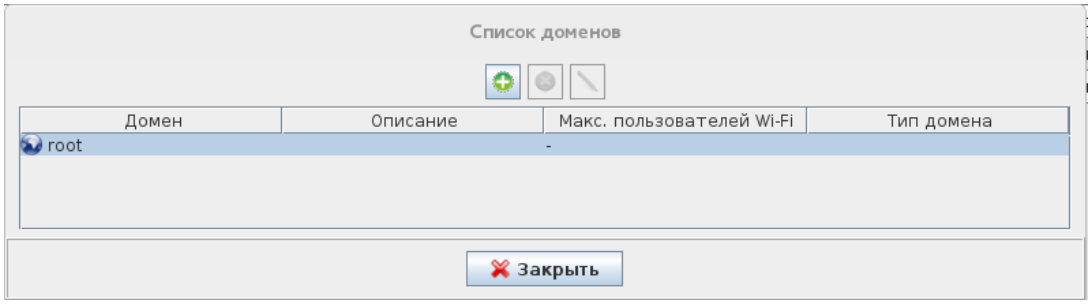


Рисунок 5 – Список доменов

1.5 Добавьте объект «RADIUS» в дерево объектов.

Удалите все устройства из дерева объектов, находящегося в левой части GUI. Нажмите кнопку «+» на панели управления, чтобы добавить объект в дерево устройств.

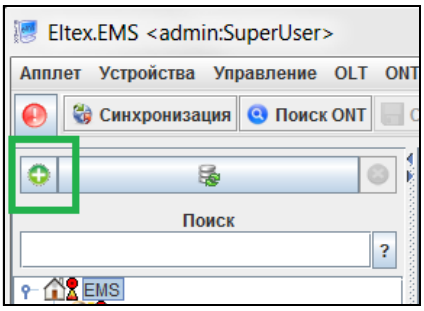


Рисунок 6 – Добавление объекта в дерево устройств

В появившемся окне введите имя объекта, выберите тип «RADIUS» и укажите IP-адрес. Если RADIUS-сервер установлен локально на вашем сервере, введите адрес 127.0.0.1.

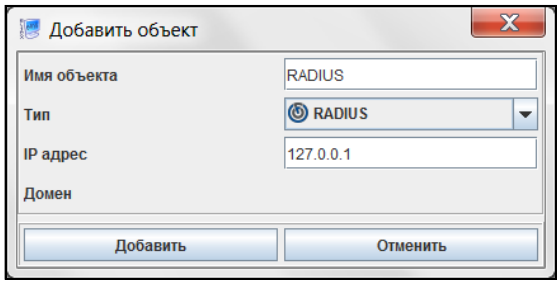


Рисунок 7 – Параметры объекта

Нажмите кнопку *«Добавить»,* после этого объект «RADIUS» появится в дереве объектов.

Выделите объект *«RADIUS»* в дереве и откройте вкладку *«Доступ»,* нажмите кнопку *«Редактировать»* и введите логин и пароль для доступа к серверу. В данном случае:

Telnet/SSH login: tester
Telnet/SSH password: tester

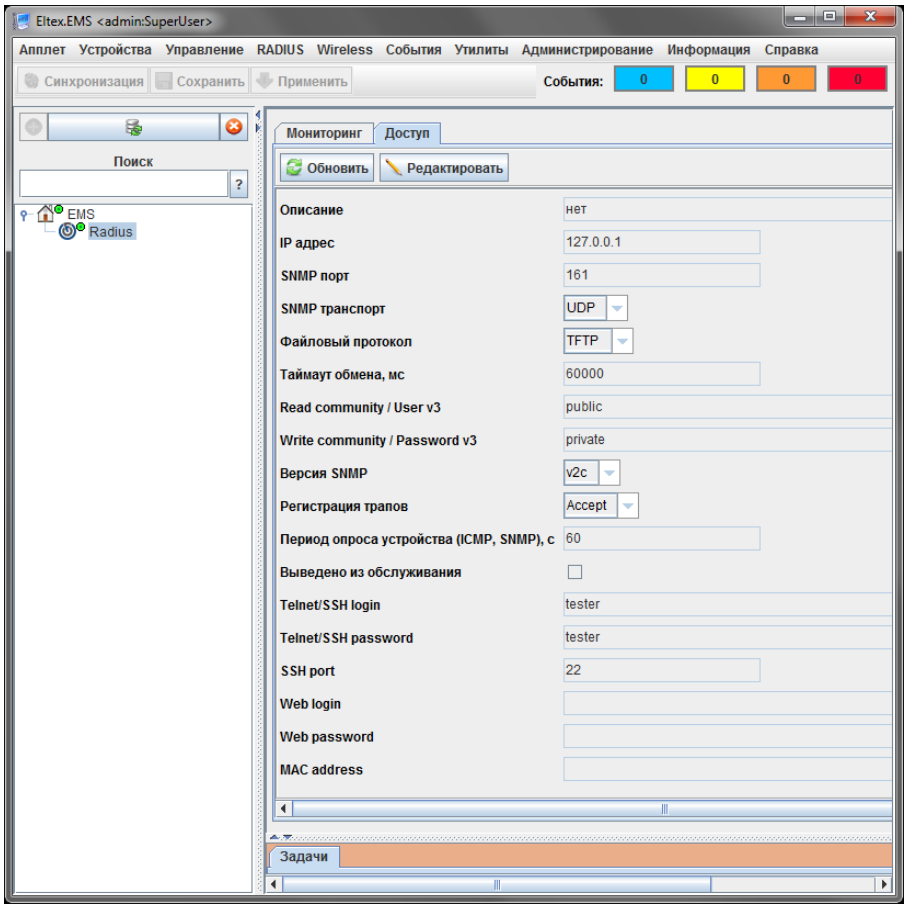


Рисунок 8 – Вкладка доступ

2 Обновление прошивки точки доступа через WEB-конфигуратор

Прежде чем устанавливать точку доступа на сеть, необходимо обновить ее на актуальную версию прошивки для обеспечения совместимости с обновленной версией SoftWLC.

По умолчанию (default) точки доступа имеют IP адрес 192.168.1.10.

2.1. Подключите точку доступа к компьютеру при помощи Ethernet-кабеля и напишите в адресной строке браузера 192.168.1.10 (Рисунок 9).

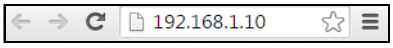


Рисунок 9 – Адресная строка в браузере

2.2. Пройдите авторизацию на открывшейся странице (Рисунок 10).

User Name: admin
Password: password

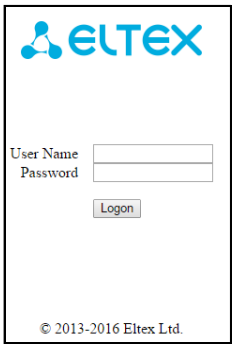


Рисунок 10 – Ввод логина и пароля

2.3. Зайдите в меню *«Maintenance/Upgrade».*

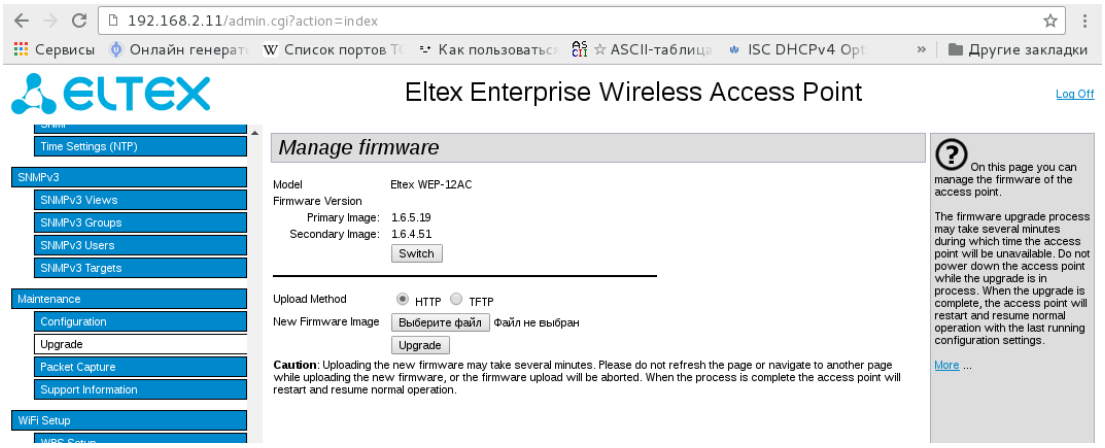


Рисунок 11 – Меню «Maintenance/Upgrade»

2.4. Нажмите кнопку *«Выберите файл»* в строке *«New Firmware Image»,* откроется окно для выбора файла. Укажите прошивку и нажмите *«Ok».*

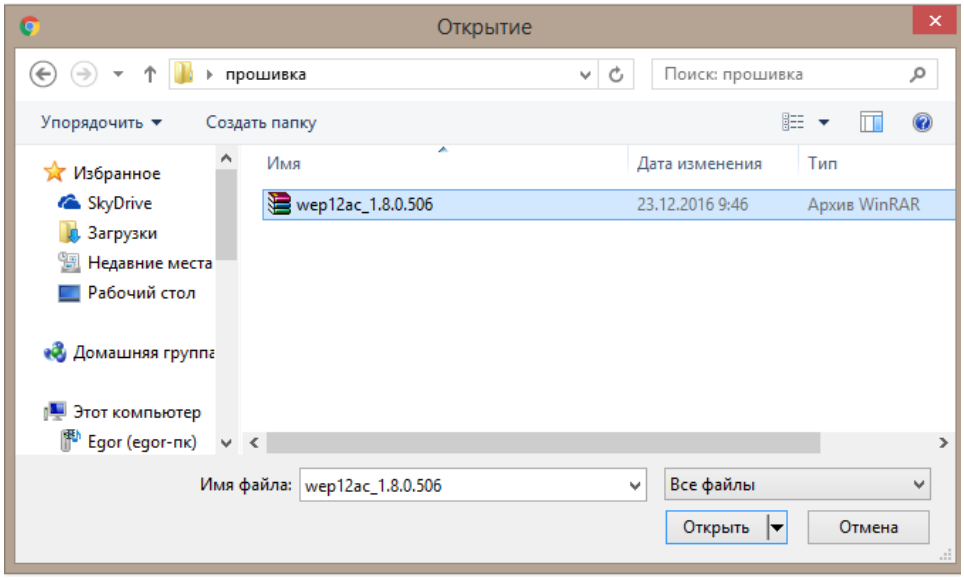


Рисунок 12 – Выбор файла

2.5. После этого в строке *«New Firmware Image»* появится название выбранной прошивки (Рисунок 13).

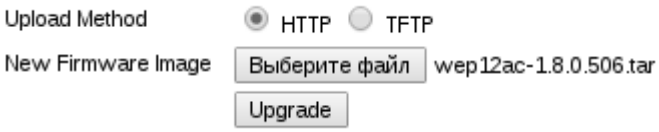


Рисунок 13 – Отображение выбранной прошивки на странице «Manage firmware»

2.6. Нажмите кнопку *«Upgrade»*. Система предупредит, что при обновлении потребуется перезагрузка и будет потеряна связь с точкой (Рисунок 14).

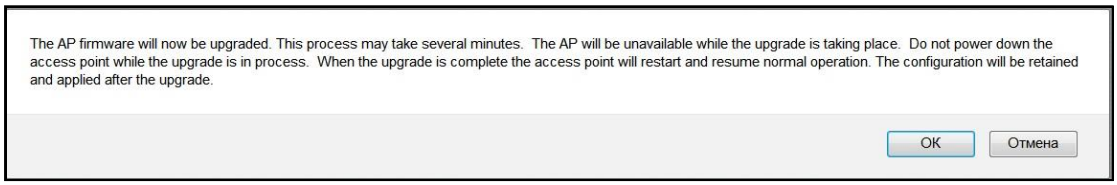


Рисунок 14- Предупреждение о перезагрузке точки доступа

Нажмите *«Ok»* и подождите, пока будет происходить загрузка и установка новой прошивки (Рисунок 15).

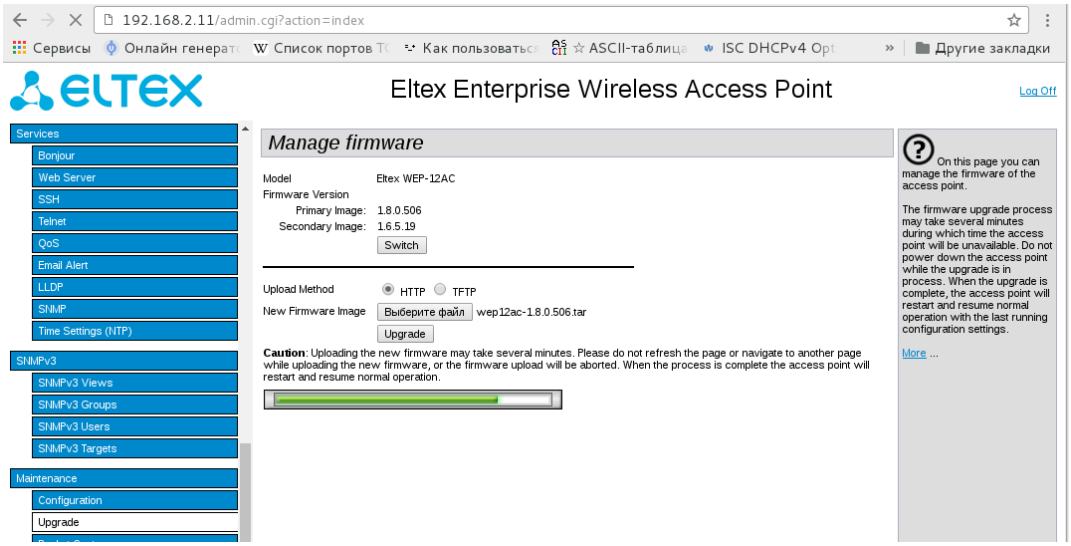


Рисунок 15 – Загрузка новой прошивки на точку доступа

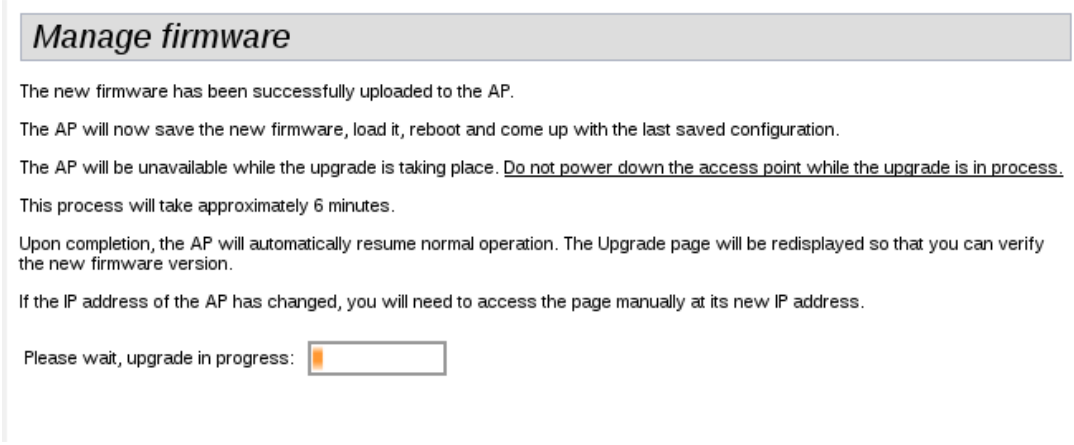


Рисунок 16 – Обновление точки доступа

Через несколько минут точка доступа перезагрузится и к ней можно будет вновь подключиться.

3 Добавление точек доступа

Подключите точку доступа к сети в соответствии со схемой. При включении точка доступа получит адрес по DHCP, а также IP SoftWLC и сообщит ему о своем появлении. Точка доступа автоматически появится в EMS во вкладке *«Инициализация ТД Wi-Fi».*

3.1. Создайте правила инициализации в меню *«Wireless/Менеджер правил инициализации ТД».* Добавьте правило, выберите тип устройства, укажите имя и домен правила (Рисунок 17).

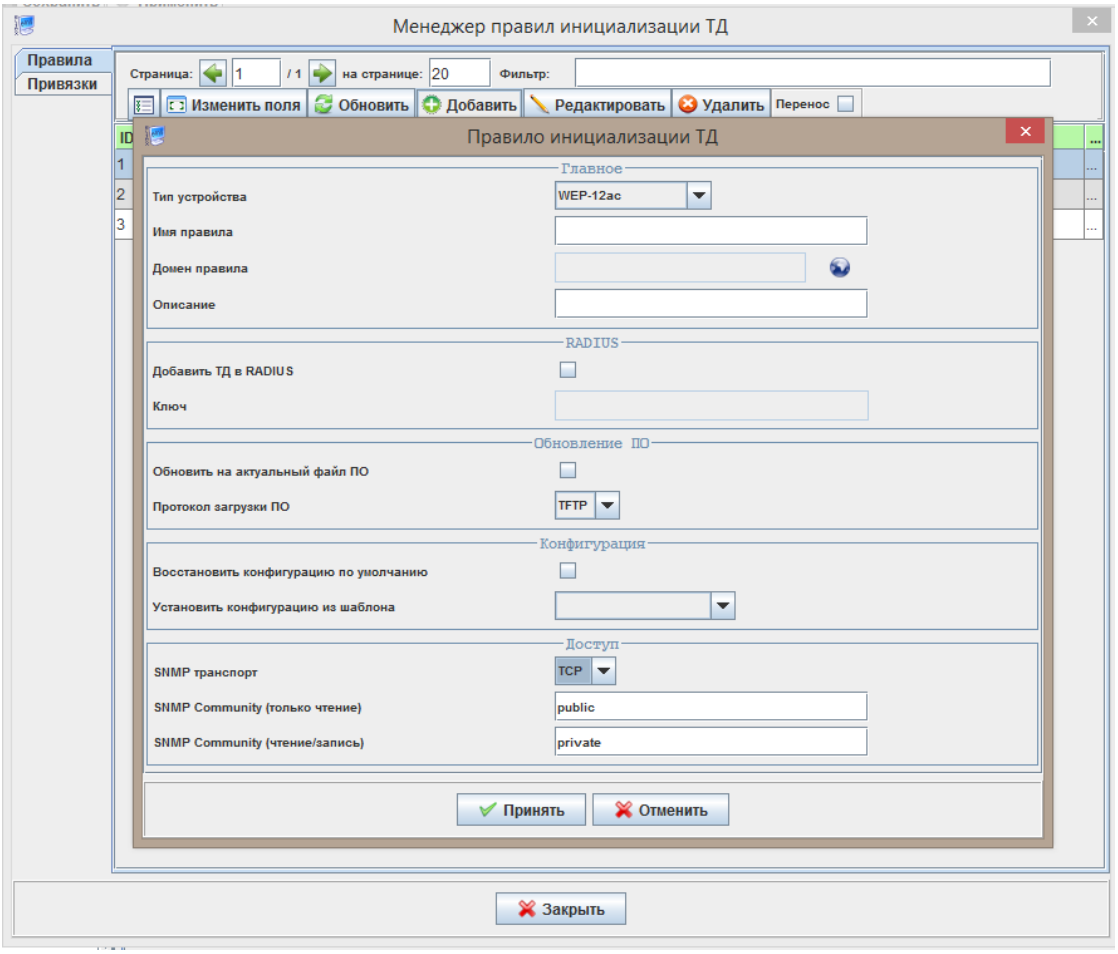


Рисунок 17 – Добавление правила инициализации

В правиле инициализации требуется активировать добавление ТД в базу данных RADIUS и указать пароль авторизации ТД в RADIUS: "eltex" (поле «ключ»). В противном случае абоненты ТД не смогут пройти авторизацию на RADIUS.

Для автоматического обновления ПО на ТД при инициализации укажите актуальный файл ПО и протокол передачи файла ПО (TFTP или HTTP). В рамках данной демонстрации пропустим этот пункт и выберем *«Не обновлять ПО».*

Для восстановления на ТД конфигурации по умолчанию перед добавлением ТД в дерево необходимо установить флаг «Восстановить конфигурацию по умолчанию».

Также в правиле инициализации имеется возможность выбрать заранее созданный шаблон конфигурации, который будет назначен на ТД. Поскольку при первом запуске системы конфигурационный файл еще отсутствует, не будем выбирать шаблон конфигурации.

Выберите транспортный протокол передачи SNMP-сообщений между точкой доступа и EMS: TCP или UDP, а также значения поля *«Community».* Нажмите кнопку *«Принять»,* созданное правило отобразится в менеджере правил инициализации ТД (Рисунок 18).

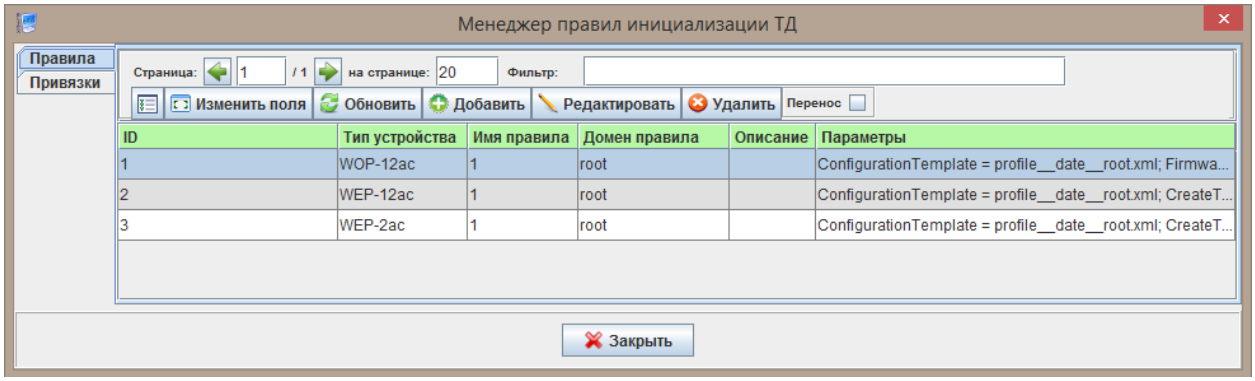


Рисунок 18 – Менеджер правил инициализации ТД

Сконфигурируйте привязку MAC-адреса устанавливаемой точки доступа к правилу инициализации. Для этого откройте вкладку *«Привязки».* MAC-адрес точки доступа указывается в поле *«Ключ».* Можно задать "Имя устройства", с которым точка появится в дереве. Если оставить поле пустым, то в качестве имени будет отображаться MAC адрес и тип устройства. Также требуется указать имя привязываемого правила инициализации (нажмите кнопку  в конце строки, чтобы выбрать из существующих правил), домен правила, а также домен узла, в который будет помещена точка доступа. При этом при сложной иерархии домена узла будут созданы все необходимые узлы и подузлы.

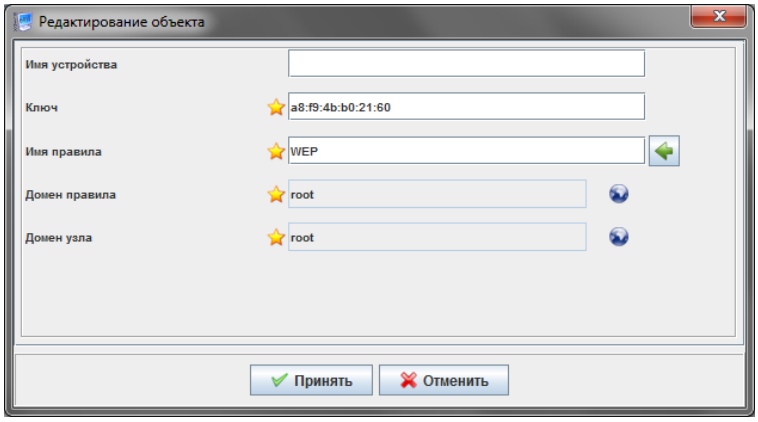


Рисунок 19 – Добавление привязки

Созданная привязка отобразится в менеджере правил инициализации ТД (Рисунок 20).

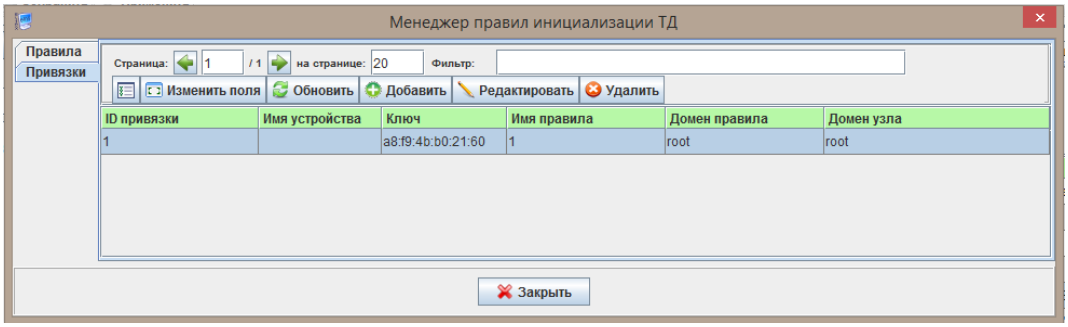


Рисунок 20 – Менеджер правил инициализации ТД

3.2. Чтобы выполнить инициализацию точки доступа с указанными параметрами, в левой части окна выделите корневой узел, в правой части окна откройте вкладку *«Инициализация ТД Wi-Fi»*, выберите точку и нажмите кнопку *«Инициализировать»* (Рисунок 21).

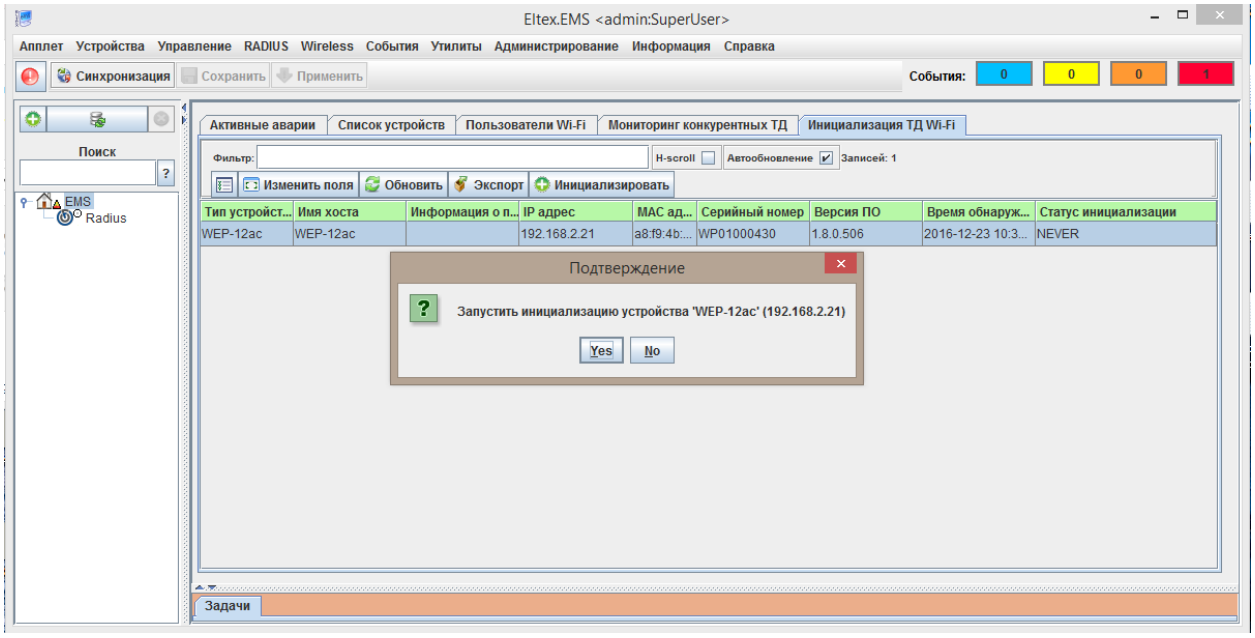


Рисунок 21 – Запуск инициализации ТД

Процесс инициализации можно увидеть на вкладке "Задачи", которая может быть открыта из меню *«Апплет/Вид/Интерактивная панель»* или комбинацией клавиш «Alt+F6»(Рисунок 22). После того, как процесс закончится, точка доступа отобразится в дереве устройств согласно домену узла, указанному в правиле инициализации.

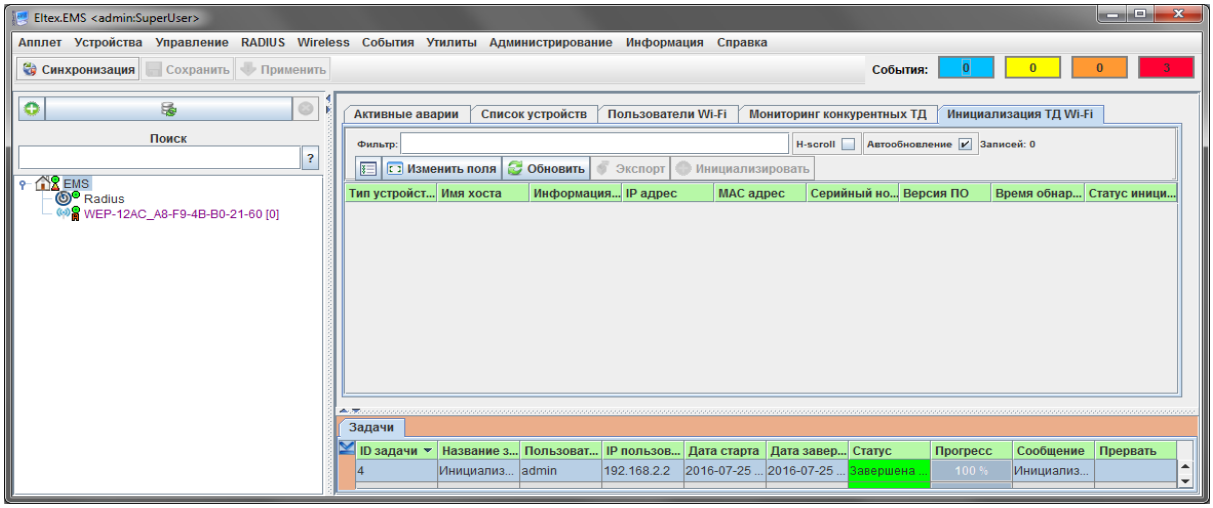


Рисунок 22 – Вкладка «Задачи»

После добавления точек доступа отключите режим кластера, для этого выделите точку в дереве, откройте вкладку «Конфигурация/Cluster.main», нажмите кнопку «Редактировать» и измените режим «Cluster mode» на «SoftWLC».

4 Настройка точки доступа при помощи SoftWLC

Перед настройкой ТД необходимо получить от нее данные о текущих параметрах, для этого выполните синхронизацию точки доступа. Выделите ТД в дереве и нажмите кнопку *«Синхронизация»,* обычно этот процесс длится несколько секунд (Рисунок 23).

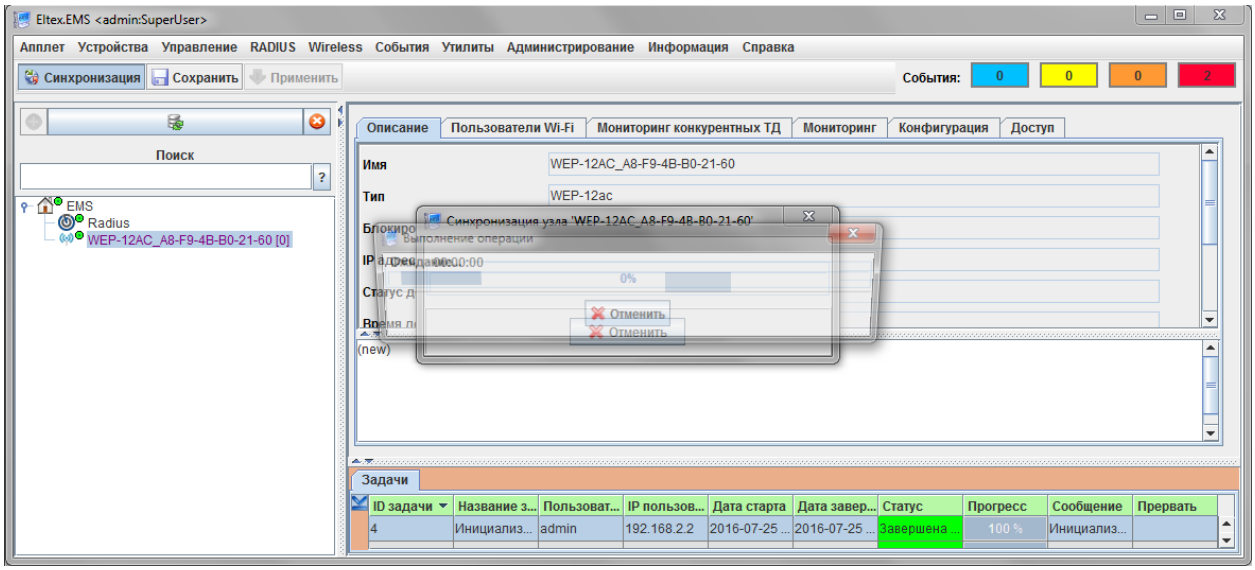


Рисунок 23 – Синхронизация точки доступа

Справа откройте вкладку *«Конфигурация».* Настройте основные параметры радио интерфейсов: выберите режим работы, способ выбора канала (статически или автоматически), ширину полосы канала, мощность передатчика. Нажмите кнопку *«Сохранить».*

4. 1 Настройка виртуальной точки доступа Enterprise с шифрованием WPA2

4.1.1. Откройте меню *«Wireless/Менеджер SSID»* (Рисунок 24).

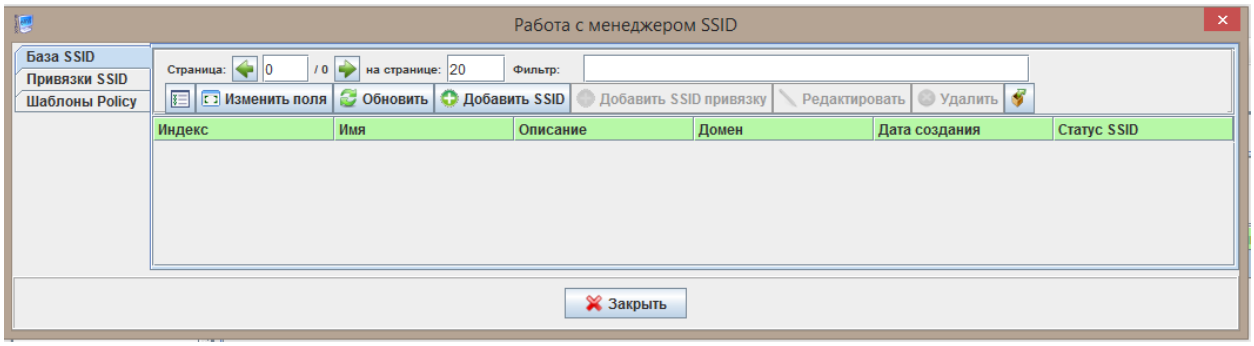


Рисунок 24 – Менеджер SSID

4.1.2. Создайте SSID, для этого нажмите кнопку *«Добавить SSID».* В открывшемся окне укажите следующие параметры (Рисунок 25):

Имя = Test_enterprise Domain = root Статус VAP = up Режим безопасности = WPA Enterprise VLAN-ID = 1000 Установите флаг: Use global RADIUS server settings

Выберите радио интерфейсы (Radio), на которые будет назначен созданный SSID.

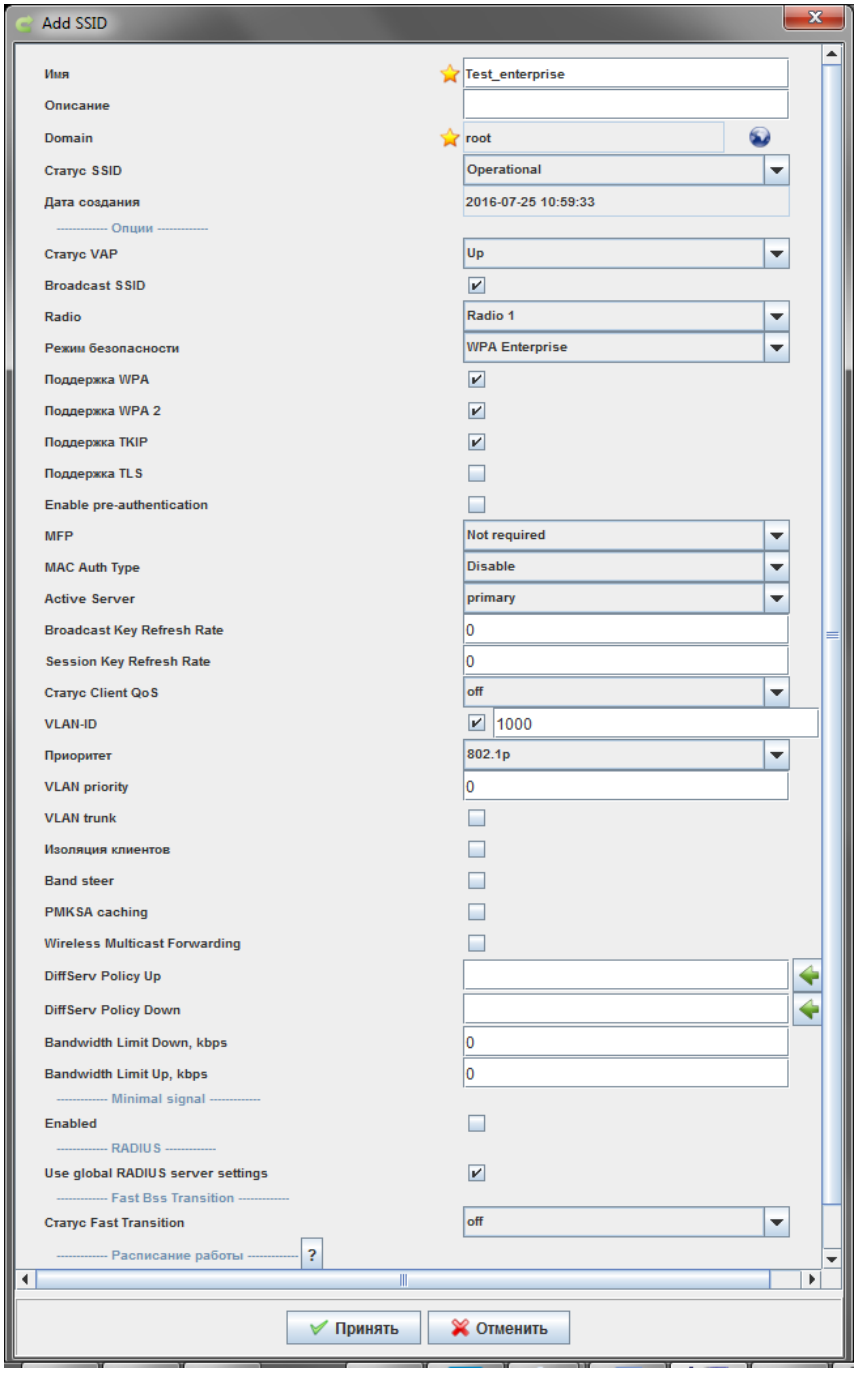


Рисунок 25 – Задание параметров SSID

После нажатия кнопки *«Принять»* созданный SSID отобразится в *«Базе SSID»* (Рисунок 26).

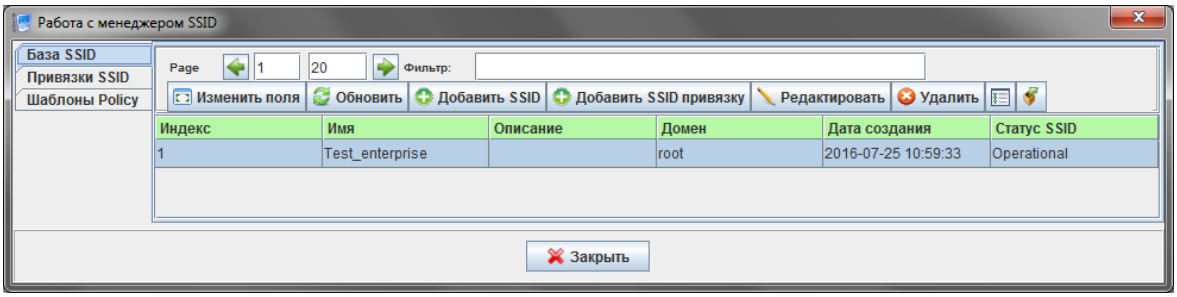


Рисунок 26 – База SSID

4.1.3. Назначьте SSID на точки доступа, для этого выберите созданный SSID и нажмите кнопку *«Добавить SSID привязку».*

В появившемся окне выберите ключ для привязки (Рисунок 27). Привязка может осуществляться по MAC-адресу ТД, по IP-адресу ТД или по домену узла. Затем выделите объекты для привязки (точки доступа или узлы) и нажмите кнопку *«Создать привязку»,* индикатор в дереве сменится с желтого на зеленый. Нажмите кнопку *«Принять».* Появится окно с вопросом "Исправить привязки SSID?". Если необходимо сразу же назначить на точки созданный SSID, то ответьте "да", если необходимо, чтобы привязка существовала только в БД, но не применилась сейчас на точку доступа - нажмите кнопку "Нет". Потом по необходимости можно зайти на вкладку "Привязки SSID" и нажать кнопку "Исправить", чтобы привязка применилась на точку доступа, либо же она применится по срабатыванию соответствующего монитора, который по дефолту срабатывает раз в сутки. Процесс назначения SSID можно контролировать на вкладке *«Задачи».*

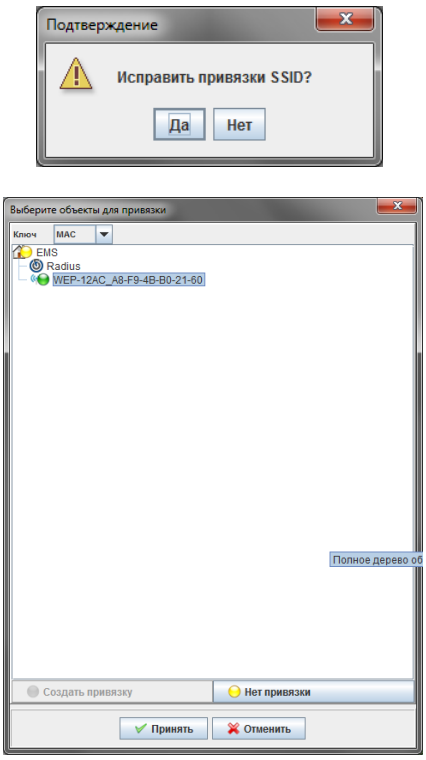


Рисунок 27 – Назначение привязки

Созданная привязка отобразится на вкладке *«Привязки SSID» (Рисунок 28).*

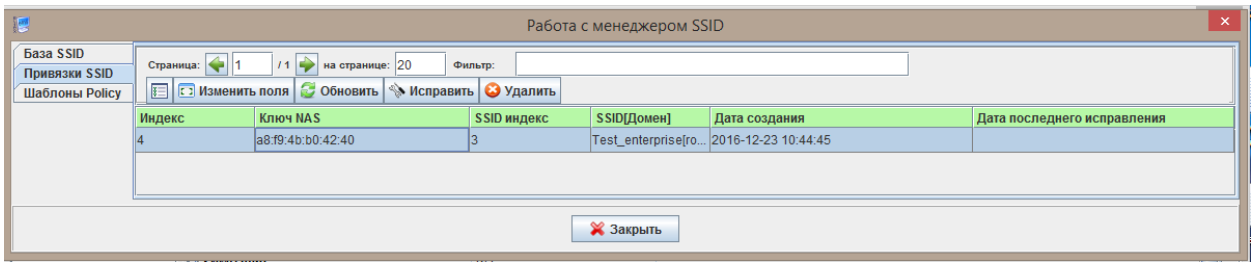


Рисунок 28 – Привязки SSID

SSID будет назначен на первую выключенную VAP на точке доступа. Результат можно увидеть во вкладке *«Конфигурация/Виртуальные точки доступа»* (Рисунок 29).

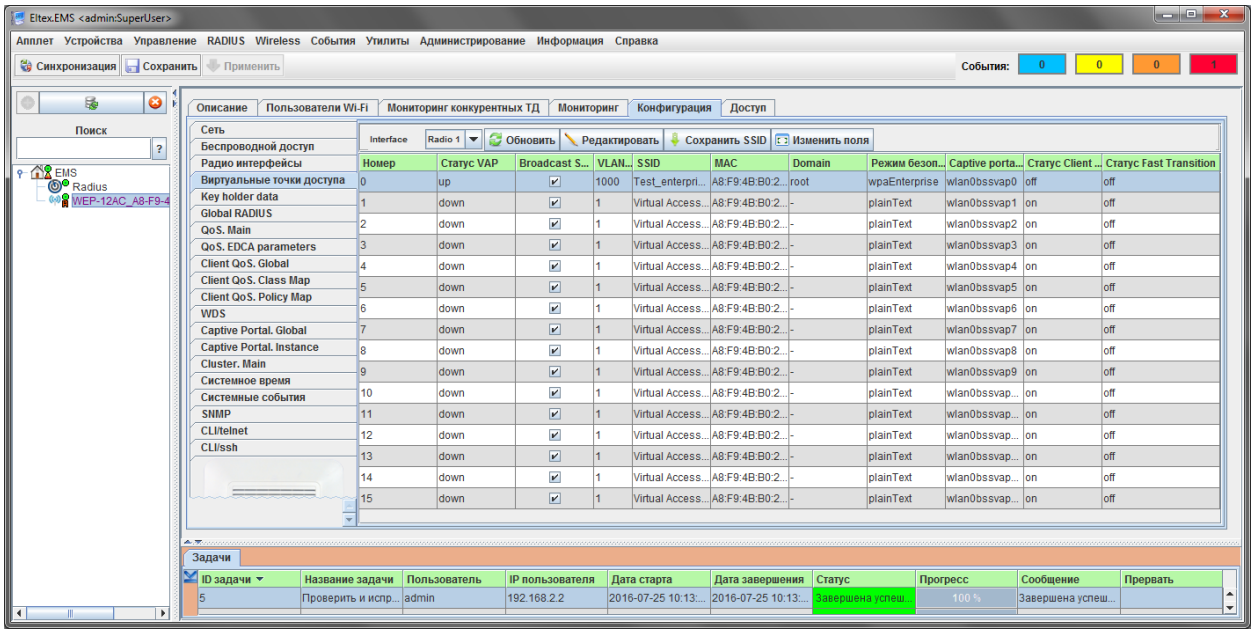


Рисунок 29 – Виртуальные точки доступа

4.1.4. В меню параметров выберите пункт «Global RADIUS». Нажмите кнопку *«Редактировать»* (Рисунок 30).

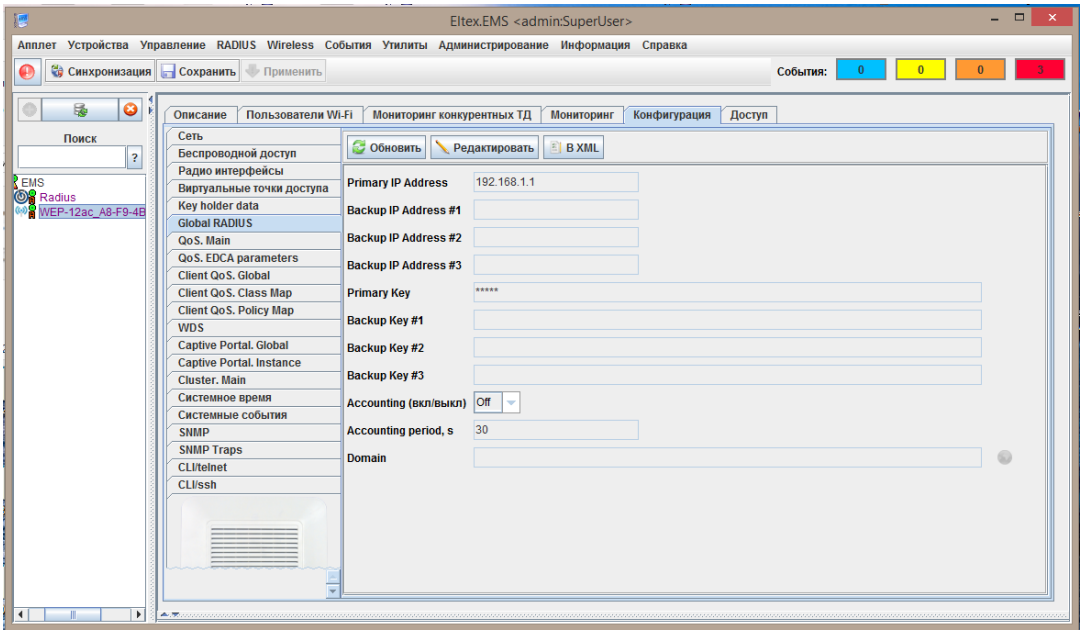


Рисунок 30 – Поле настроек «Global RADIUS»

В появившемся окне (Рисунок 31) укажите параметры:

Primary IP Address = 192.168.2.1 Primary Key = eltex Accounting = on Domain = root

Нажмите кнопку *«Принять».*

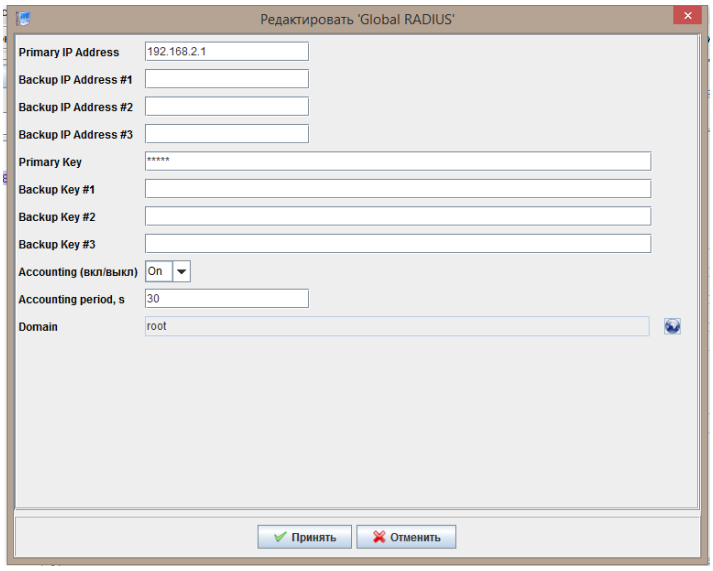


Рисунок 31 – Параметры «Global RADIUS»

4.1.5. В меню параметров выберите пункт *«Client QoS. Global».* Нажмите кнопку *«Редактировать»* и в появившемся окне установите *«Client QoS Global Admin Mode» = «on»* (Рисунок 32).

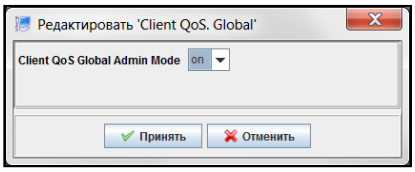


Рисунок 32 – Настройка «Client QoS Global»

4.1.6. Добавьте точку доступа в раздел *«RADIUS»,* если это не произошло автоматически при инициализации ТД. Откройте подменю *«Управление точками доступа»* в панели управления GUI. Укажите параметры:

Адрес = <IP адрес ТД>,
Домен = root,
Имя = имя ТД,
Тип = WEP
Ключ = eltex.

Если Вы используете ТД уличного исполнения, то в поле «Тип» необходимо указать WOP.

4.1.7. Добавьте аккаунты Wi-Fi-пользователей в том же разделе в подменю *«Управление пользователями»* (Рисунок 33).

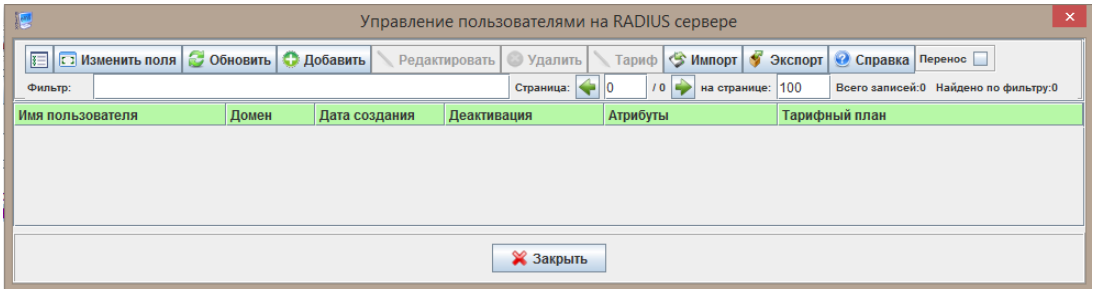


Рисунок 33 – Управление пользователями на RADIUS сервере

Основные атрибуты, доступные при создании пользователя (Рисунок 34):

- *имя пользователя* и *пароль* для аутентификации на RADIUS;
- *домен пользователя* (выбирается из дерева доменов при нажатии кнопки в конце строки);
- *срок действия сертификата* (для авторизации по TLS);
- *деактивация* – при установленном флаге аккаунт не активен;
- *тарифный план* – группа, в которую может быть включен пользователь. В тарифных планах задаются ограничения доступа. Все пользователи тарифного плана будут иметь указанные ограничения (по времени, скорости, трафику);
- *срок действия* – срок действия учетной записи с момента создания;
- *ограничение доступа* – указывает число пользователей, которые одновременно могут быть авторизованы под данным аккаунтом;
- *MAC-адрес* – ограничение доступа по MAC-адресам для авторизации под данным аккаунтом;

- *макс. скорость входящего/исходящего трафика* – максимальная скорость передачи трафика в битах в секунду в downstream и upstream;
- *Policy для входящего/исходящего трафика* – профиль Policy для определенного клиента. Профиль Policy создается ранее в меню Client QoS точки доступа;
- *продолжительность сессии* – длительность сессии пользователя в минутах;
- *Квота по трафику – общее ограничение по количеству входящих данных для пользователя, в мегабайтах;*
- *Квота по времени – общее ограничение времени для всех сессий пользователя, в минутах;*
- *CVLAN* – индивидуальный VLAN для абонента (при этом должны быть включены атрибуты «*Tunnel-Type*» и «*Tunnel-Medium-Type*» с выставленными по умолчанию значениями «13» и «6» соответственно);
- *Eltex-Additional-Vlans* – дополнительные сервисные VLAN. Если используется более одной сервисной VLAN, список номеров задается через запятую («,»).

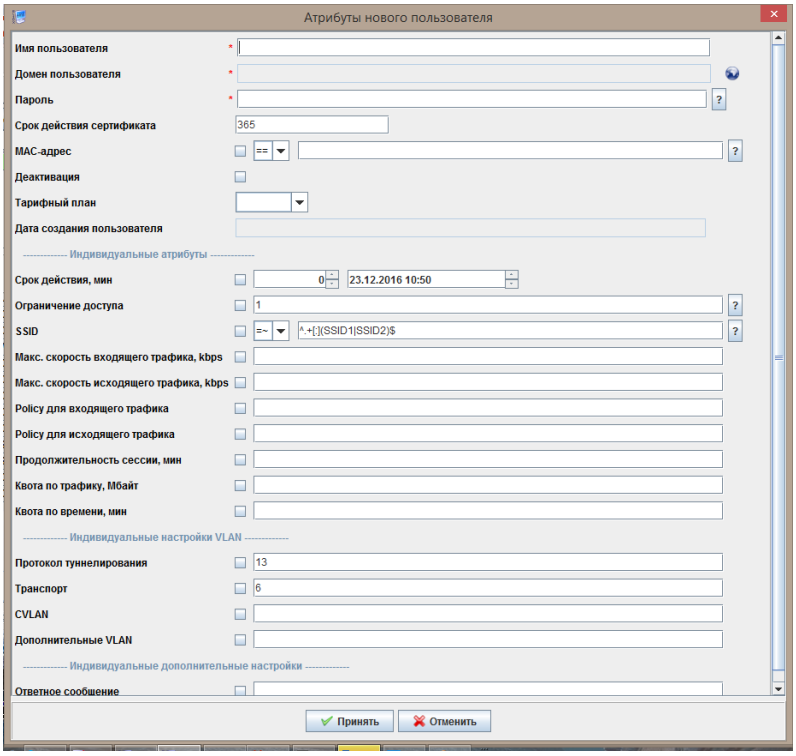


Рисунок 34 – Атрибуты пользователя

4. 2 Настройка виртуальной точки доступа в режиме Hotspot

4.2.1. Включите режим *«Captive Portal».* Для этого во вкладке *«Конфигурация»* выберите пункт *«Captive Portal. Global»,* нажмите кнопку *«Редактировать»* и установите *«Captive Portal Mode» - «on».* Задайте *«Roaming service URL»* в формате *ws://host:port/path.* Нажмите кнопку *«Принять».*

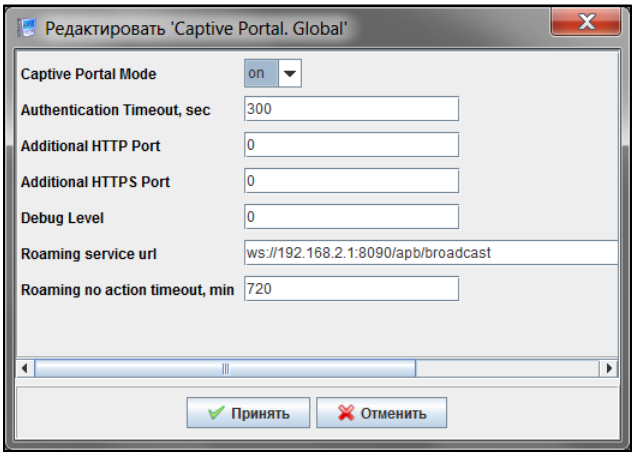


Рисунок 35 – Настройки «Captive Portal. Global»

4.2.2. Откройте Менеджер SSID и создайте еще один SSID. Укажите следующие параметры:

Имя = Test_hotspot
Domain = root Статус VAP = upРежим безопасности = без шифрования
Статус Client QoS = on
VLAN-ID = 1000Поставьте флаг "Captive portal"/ "Enabled"
Уберите флаг «Radius»/ «Use global RADIUS server settings»
RADIUS IP Address = 192.168.2.1
RADIUS key = eltex
Radius Accounting = up
Virtual portal name = default[1]
Verification = CaptivePortal
Поставьте флаг "External"
External URL = http://192.168.2.1:8080/eltex_portal/
User mobility domain = root[2]

[1] На портале по умолчанию присутствуют страница *«default»*,,которая для примера кастомизирована под *ООО «Предприятие «Элтекс»*.

[2] Название группы, в пределах которой может быть осуществлен роуминг.

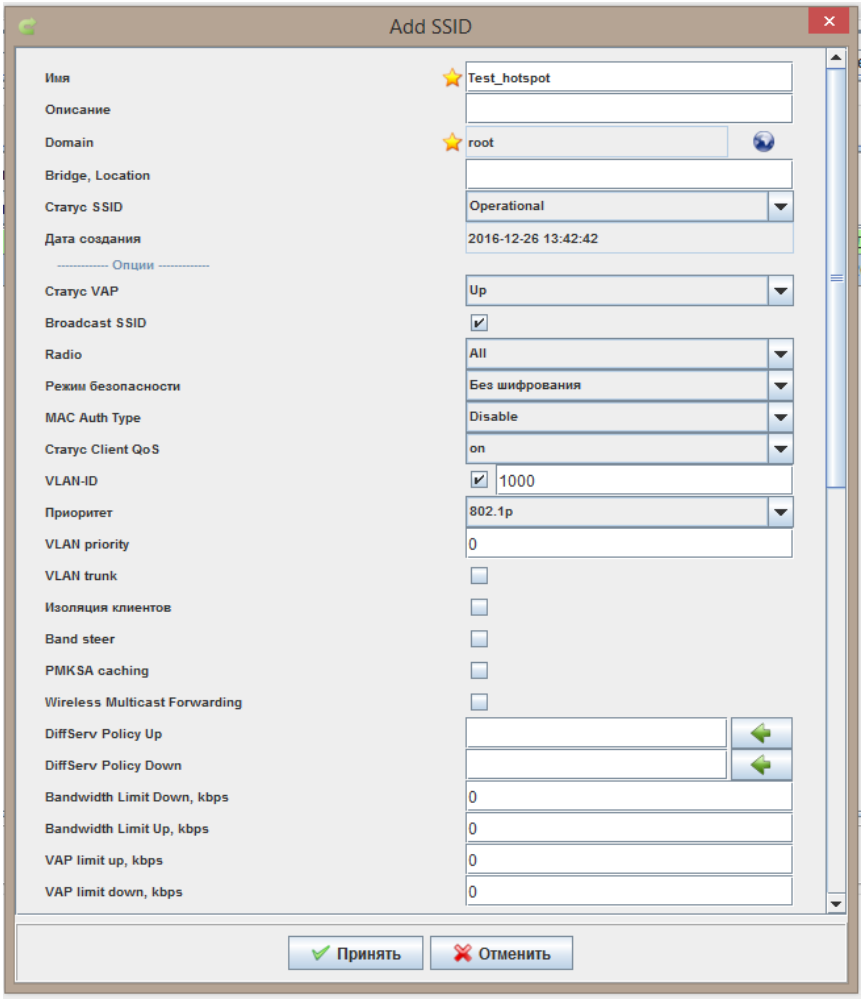


Рисунок 36 – Параметры SSID

Для того чтобы при подключении клиента к Hotspot SSID происходило перенаправление его на определенную страницу для авторизации, необходимо имя этой страницы указать в *«Virtual portal name»*.

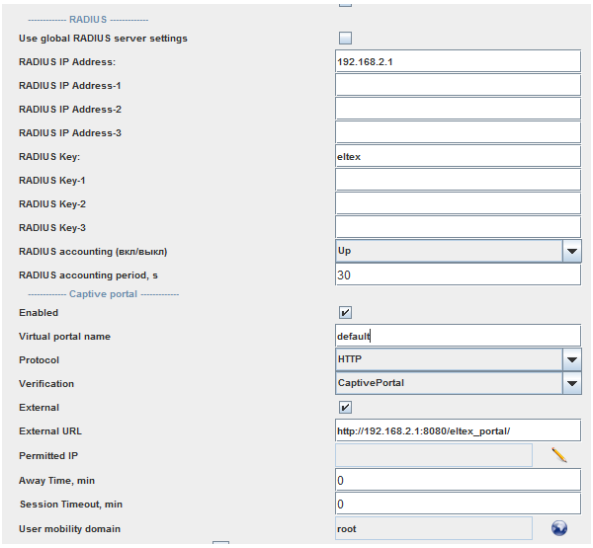


Рисунок 37 – Параметры SSID Captive portal

После нажатия кнопки *«Принять»* созданный SSID отобразится в *«Базе SSID»* (Рисунок 38).

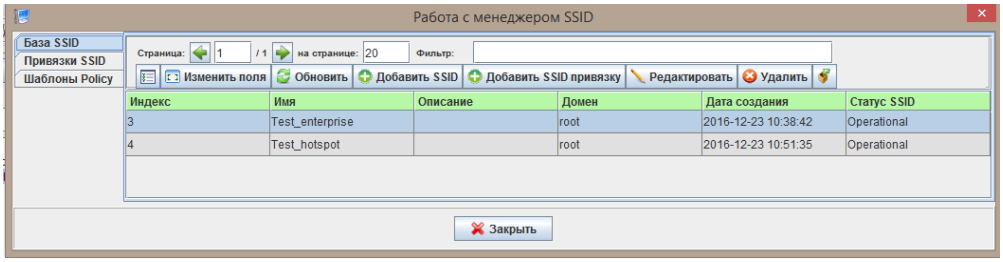


Рисунок 38 – Менеджер SSID

4.2.3. Назначьте SSID на точки доступа через кнопку *«Добавить SSID привязку».*

SSID будет назначен на первую выключенную VAP на точке доступа. Результат можно увидеть во вкладке *«Конфигурация/Виртуальные точки доступа»* (Рисунок 39).

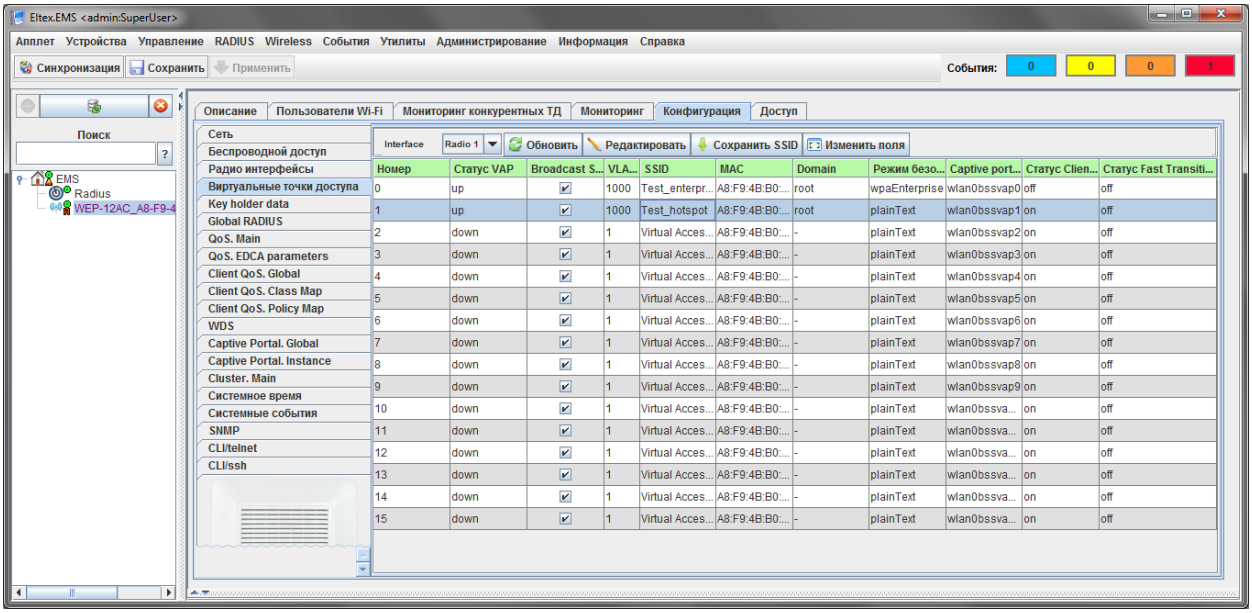


Рисунок 39 – Виртуальные точки доступа

4.2.4. Добавьте тарифный план.

В меню *«RADIUS/ Управление тарифными планами»* нажмите кнопку *«Добавить»* и укажите основные параметры тарифного плана:

- Название: tarif1;
- Код: 2;
- Домен: root.

Установите флаг *«Портальная аутентификация».*

Примеры использования тарифных планов можно посмотреть в статье «SoftWLC. Настройка тарифных планов для портальной авторизации», которая доступна по ссылке http://kcs.eltex.nsk.ru/articles/899

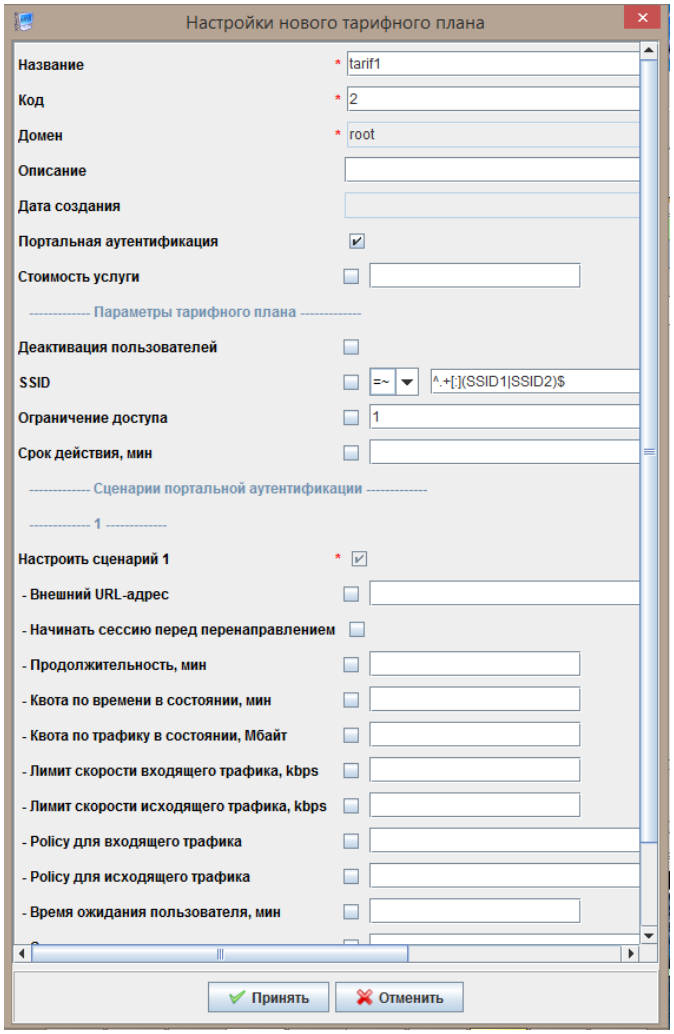


Рисунок 40 – Настройки тарифного плана

4.2.5. Активируйте тарифный план на портале.

Для активации откройте портал по ссылке: 192.168.2.1:8080/epadmin.

Login: admin
Password: password

На панели слева выберите портал, на который настроено перенаправление (default). Откройте вкладку *«Тарифные планы»* и отметьте флагом созданный тарифный план «tarif1». Введите его название, которое будет отображаться клиенту на странице авторизации в случае использования нескольких тарифных планов.

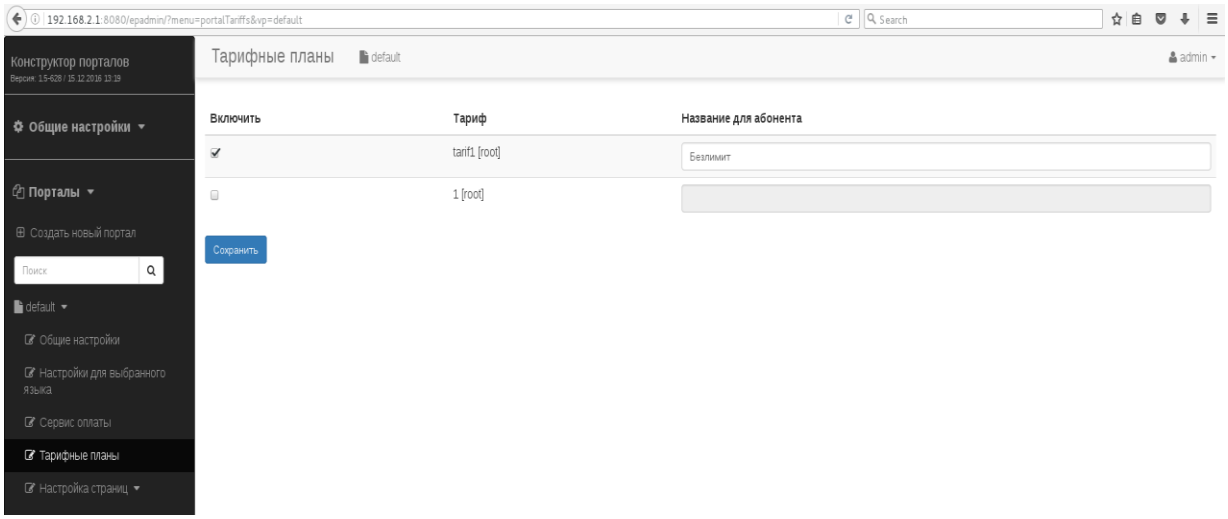


Рисунок 41 – Активация тарифного плана

По умолчанию для портальной авторизации используется демо-режим, в котором после ввода номера телефона генерируется код и автоматически подставляется в форму. Для настройки авторизации через smsc-шлюз выберите на панели слева вкладку *«Общие настройки» и в поле «Режим отправки»* установите «Notification Gate». Далее сконфигурируйте файл /etc/eltex-notification-gw/notification.properties. При использовании смс шлюза smsc.ru поле sms.gate.config необходимо заполнить следующим образом:

```
sms.gate.config=smsc_gate.conf
```

В этом же файле редактируются настройки для отправки писем.
Содержимое файла notification.properties:

```
#Common gates settings
#Current gate used (config name, for example smpp_gate.conf)
sms.gate.config=smsc_gate.conf

#Gate pool size
sms.gate.pool.size=50

#Regex for valid phone format
phone.regexp=\+?\d+

#============================
#=======email settings========
#============================
mail.smtp.submitter=test@email.com
mail.smtp.password=
mail.smtp.auth=true
mail.smtp.host=email.com
mail.smtp.port=587
mail.smtp.sendpartial=true
mail.smtp.connectiontimeout=5000
mail.gate.pool.size=20
mail.pool.wait.millis=10000
```

Отредактируйте конфигурационный файл smsc_gate.conf. Заполните поля: **SMSC_LOGIN, SMSC_PASSWORD**, полученные на сайте **smsc.ru,** и **SMSC_PROTOCOL (http или https).**

Содержимое файла smsc_gate.conf:

```
# SMSC settings

#any Gate name for logging
GATE_NAME=SMSC
SMSC_USE_TRANSLIT=false
# smsc accounting (api) settings
SMSC_LOGIN=
# password for smsc account. If also using this account with smpp, password should be no
longer
# that 8 symbols according to specification of smpp protocol. Russian symbols are not allowed
SMSC_PASSWORD=
# encoding for transferring sms via http protocol
SMSC_CHARSET=utf-8
SMSC_DEBUG=false
SMSC_USE_POST=false
# choosing protocol (http|https)
SMSC_PROTOCOL=http
# project settings
FACTORY=org.eltex.softwlc.notification.sms.SMSCGateFactory
```

Для использования протокола SMPP необходимо заполнить данные в конфигурационном файле smpp_gate.conf: логин, пароль, адрес сервера, порт и другие параметры, необходимые для использования данного протокола. В конфигурационном файле notification.properties поле sms.gate.config необходимо заполнить следующим образом:

```
sms.gate.config= smpp_gate.conf
```

Содержимое файла smpp_gate.conf:

```
# SMPP Gate settings

#Gate name for receiving delivery reports (SMSC|SMSC_SMPP|CRAFT|SMS_TRAFFIC) If other name,
reports won`t be described, but will show error codes
GATE_NAME=SMSC_SMPP
# smsc accounting (api) settings
SMSC_LOGIN=
# password for smsc account. should be no longer that 8 symbols according
# to specification of smpp protocol. Russian symbols are not allowed
SMSC_PASSWORD=
# project settings
FACTORY=org.eltex.softwlc.notification.sms.SMSCGateFactory

# for enabling smpp via smsc.ru need to enable smpp-sending in smsc.ru
# private account settings and connect with smsc.ru support and tell them
# ip-address(es) from which connection(s) will be established and
# which port to open: regular or secured (ssl) (or both)

# host - name or IP
SMSC_SMPP_HOST=smpp.smsc.ru
SMSC_SMPP_PORT=3700
# reserved host for sending sms
SMSC_SMPP_RESERV_HOST=smpp2.smsc.ru
SMSC_SMPP_SSL_PORT=
# seconds between sending ENQUIRE_LINK packet to maintain connection with SMPP server
# for SMSC SMPP 15 seconds is OK
SMSC_SMPP_ENQUIRE_LINK_INTERVAL=15
# Seconds waiting response from SMPP server on SUBMIT_SM packet
SMSC_SMPP_TRANSACTION_INTERVAL=5
# type of number for ESME address - better use UNKNOWN (UNKNOWN|INTERNATIONAL|
# NATIONAL|NETWORK_SPECIFIC|SUBSCRIBER_NUMBER|ALPHANUMERIC|ABBREVIATED)
```

```
SMSC_ESME_TYPE_OF_NUMBER=UNKNOWN
# numbering plan indicator for ESME address - better use UNKNOWN (UNKNOWN|ISDN|
# DATA|TELEX|LAND_MOBILE|NATIONAL|PRIVATE|ERMES|INTERNET|WAP)
SMSC_ESME_NUMBERING_PLAN_INDICATOR=UNKNOWN
# service type - better leave empty for default (|CMT|CPT|VMN|VMA|WAP|USSD)
SMSC_SERVICE_TYPE=
# source address type of number when sending (UNKNOWN stands for 0|INTERNATIONAL stands for 1|
# NATIONAL - 2|NETWORK_SPECIFIC - 3|SUBSCRIBER_NUMBER - 4|ALPHANUMERIC - 5|ABBREVIATED - 6)
SMSC_SOURCE_ADDR_TYPE_OF_NUMBER=ALPHANUMERIC
# source address numbering plan indicator when sending (UNKNOWN stands for 0|ISDN - 1|
# DATA - 2|TELEX - 3|LAND_MOBILE - 4|NATIONAL - 5|PRIVATE - 6|ERMES - 7|INTERNET - 8|WAP - 9)
SMSC_SOURCE_ADDR_NUMBERING_PLAN_INDICATOR=ISDN
# source address to indicate in smsc.ru log, can give any name or leave empty, max length is
20 symbols
# russian symbols will be converted to translit
SMSC_SOURCE_ADDRESS=
# destination address type of number when sending (UNKNOWN stands for 0|INTERNATIONAL -
1|NATIONAL - 2|
# NETWORK_SPECIFIC - 3|SUBSCRIBER_NUMBER - 4|ALPHANUMERIC - 5|ABBREVIATED - 6)
SMSC_DEST_ADDR_TYPE_OF_NUMBER=INTERNATIONAL
# destination address numbering plan indicator when sending (UNKNOWN stands for 0|ISDN -
1|DATA - 2|
# TELEX - 3|LAND_MOBILE - 4|NATIONAL - 5|PRIVATE - 6|ERMES - 7|INTERNET - 8|WAP - 9)
SMSC_DEST_ADDR_NUMBERING_PLAN_INDICATOR=ISDN
# protocol ID
SMSC_PROTOCOL_ID=0
# flag shows priority of sms in smsc queue (0|1|2|3) 3 - the highest
SMSC_PRIORITY_FLAG=3
# encoding (1 stands for 8-bit ASCII|2 for UCS2 (UTF-16)|0 for 7-bit in data coding, but for
text will be used UTF-8).
# For sending messages with cyrillic text use 2
SMSC_ENCODING=2
# concat long text on smpp server into 1 message (TRUE|FALSE). May pay less money of
concatting
SMSC_CONCAT_LONG_TEXT_ON_SMPP_SERVER=TRUE
# ESME settings
# MessageMode (DEFAULT stands for 0|DATAGRAM - 1|TRANSACTION - 2|STORE_AND_FORWARD - 3)
SMSC_MESSAGE_MODE=DATAGRAM
#MessageType
(DEFAULT|ESME_DEL_ACK|ESME_MAN_ACK|SMSC_DEL_RECEIPT|SME_DEL_ACK|SME_MAN_ACK|CONV_ABORT|INTER_D
EL_NOTIF)
SMSC_MESSAGE_TYPE=DEFAULT
# GSMSpecificFeature (DEFAULT|UDHI|REPLYPATH|UDHI_REPLYPATH)
SMSC_GSM_SPECIFIC_FEATURE=DEFAULT
# GeneralDataCoding settings
# ignore these settings (for proper data coding 0x08, for ex.) (TRUE|FALSE)
SMSC_IGNORE_OPTIONAL_DATA_CODING_SETTINGS=FALSE
# compressed (FALSE|TRUE)
SMSC_COMPRESSED=FALSE
# messageClass (0|1|2|3)
SMSC_MESSAGE_CLASS=1tester
```

Сохраните настройки и перезапустите службу командой:

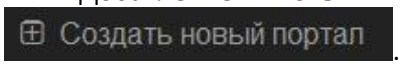
```
sudo service eltex-notification-gw restart.
```

4. 3 Создание и редактирование страниц на WEB-портале

Для того чтобы создать на WEB-портале новую страницу или отредактировать внешний вид текущей, необходимо перейти по ссылке: 192.168.2.1:8080/epadmin/.

Для авторизации используйте:

Login: admin
Password: password

Добавление новых страниц портала осуществляется нажатием на кнопку 

. В диалоговом окне нужно указать название нового портала и домен видимости:

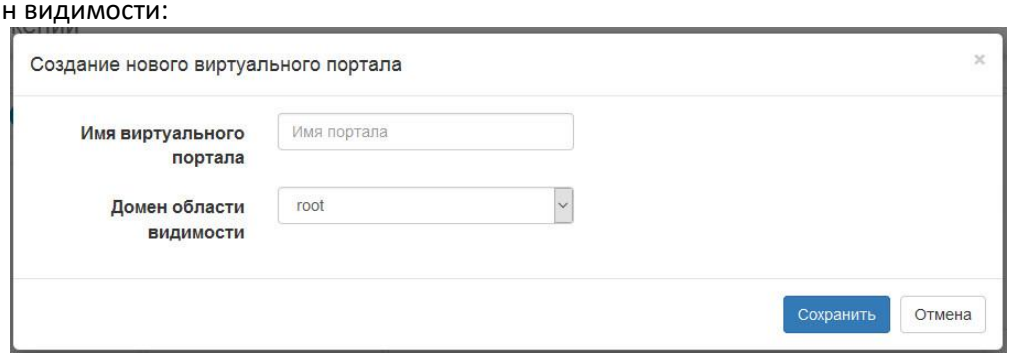


Рисунок 42 – Создание виртуального портала

Чтобы удалить ненужный портал, необходимо нажать на пиктограмму  напротив названия портала. Чтобы изменить имя или домен портала нажмите  .

Следует обратить внимание на имя создаваемой страницы – данное имя потребуется при конфигурировании параметра Virtual Portal Name SSID точки доступа, чтобы привязать этот SSID к созданному кастомизированному под клиента WEB-порталу.

На вкладке *«Внешний вид»* (Рисунок 42) демонстрируется внешний вид WEB-портала для пользователя. Кроме того, на странице производится редактирование баннеров и текста, заполняющих основное пространство портала.

Рекомендуемые размеры загружаемых изображений:

Фоновое изображение – 1024 x 1024;
Баннер слева – 200 x 800 пикселей;
Баннер в шапке – 400 x 200 пикселей:

В качестве изображений можно использовать файлы форматов .png, .jpeg, .gif, .bmp.

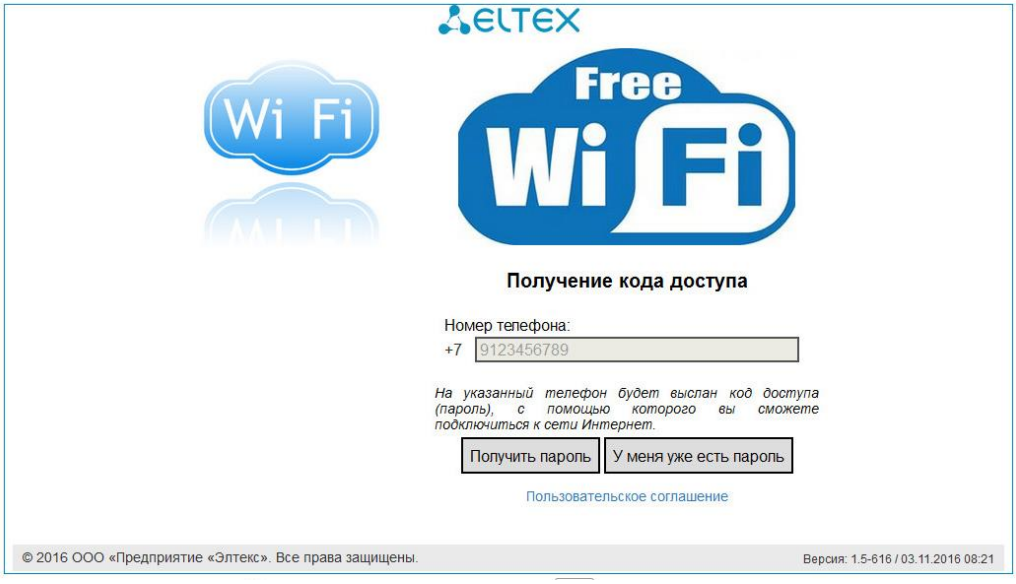


Рисунок 42 – Вкладка «Внешний вид» на WEB-портале

Более подробная инструкция по настройке портала *«WEB портал SoftWLC»* доступна в разделе *«SoftWLC»* на сайте http://www.eltex.nsk.ru/catalog/softwlc.php.

5 Настройка сервиса Eltex-APB

Данный сервис предназначен для настройки корректной работы роуминга клиентов в hotspot-сетях. С его помощью точки доступа, находящиеся в одном роуминговом домене, получают информацию о клиентах, подключенных к другим точкам, а также параметры их тарифных планов, список разрешенных до авторизации ip-адресов и т.д.

Откройте закладку *«Конфигурация»,* выберите вкладку *«Captive Portal Global»* и в строке *«Roaming service URL»* укажите адрес сервера, на котором установлен сервис, а также настройте *«Roaming no action timeout»* (время, через которое ТД отправляет запрос на подключение к Service APB в случае неудачной попытки подключения) в виде:

```
ws://[service_host]:[service_port]/apb/broadcast
```

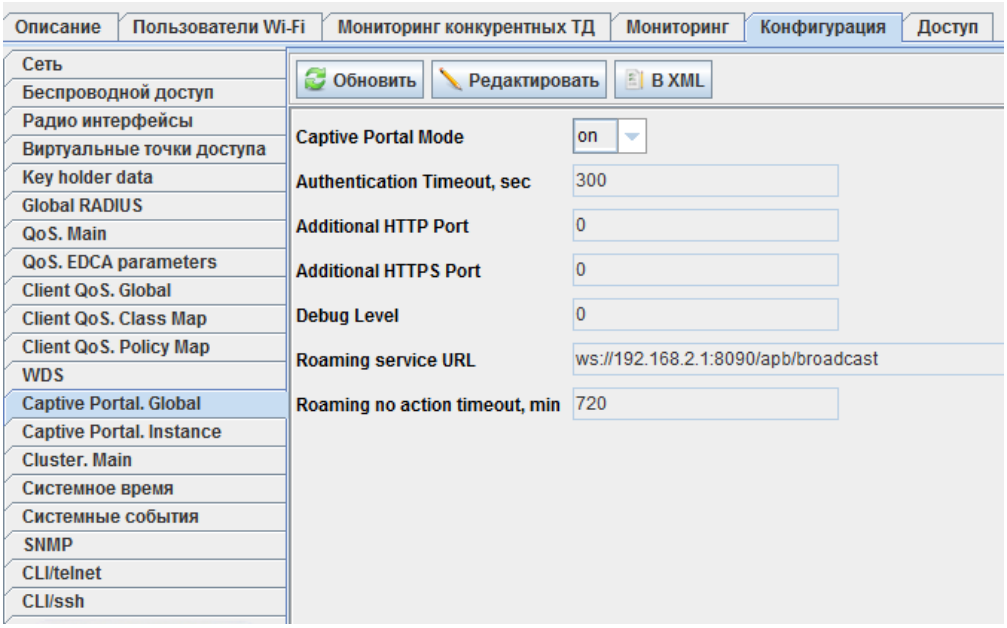


Рисунок 43 – Настройка APB во вкладке «Captive Portal Global»

Затем во вкладке *«Виртуальные точки доступа»* необходимо открыть настраиваемый SSID и в блоке настроек Captive Portal указать *«User Mobility Domain»* (должен быть одинаковым для всех точек доступа, которые будут участвовать в роуминге).

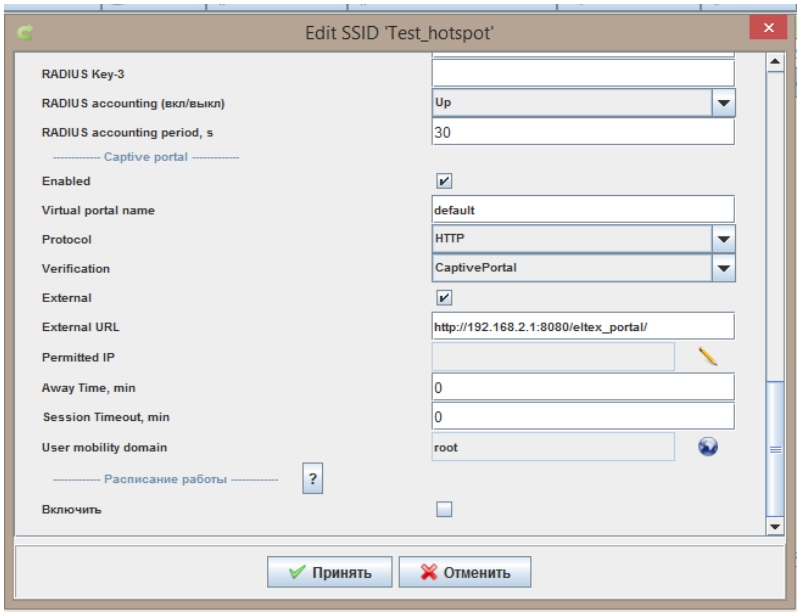


Рисунок 44 – Настройка User mobility domain

Последним шагом является настройка конфигурационного файла APB, который находится на сервере с APB в директории **/etc/eltex-apb**. Название файла — **hosts.json**. Он отвечает за применение списков разрешенных для перехода до авторизации IP-адресов.

Содержание файла hosts.json:

```
[
]
```

Уникальность клиентов может обеспечиваться тремя ключами: mobility-domain, radius-domain и ssid. При подключении клиента к определенному SSID точки доступа, которая настроена на работу с APB, происходит сравнение полученных параметров клиента с шаблонами в конфигурационном файле APB.

Шаблон может содержать пункты «mobility-domain-list» и «permitted-ip-list», для объединения которых используются символы {}.

В «mobility-domain-list» задаются списки ключей, необходимых для идентификации клиента.

В «permitted-ip-list» задаются списки IP-адресов, доступ до которых разрешен клиенту до авторизации.

```
{
    "mobility-domain-list": [
      {
        "mobility-domain": "nsk.ru",
        "radius-domain": "root",
        "ssid": "Eltex-Local"
      }
    ],
    "permitted-ip-list": [
      "eltex.nsk.ru",
      "eltex.org"
    ]
  }
```

Запись в приведенном выше конфигурационном файле говорит о том, что если на сервис поступит информация о клиенте, чьим mobility domain является nsk.ru, radius-domain является root, а ssid – Eltex-Local, данному клиенту в список разрешенных для перехода до авторизации IP-адресов добавятся адреса eltex.nsk.ru и eltex.org. То есть адреса, находящиеся в «permitted-ip-list», применятся для клиента в случае полного совпадения всех ключей, описанных в рамках одного «mobility-domain-list».

Если в правиле указан только список «permitted-ip-list», а «mobility-domain-list» отсутствует, данный список будет применен к каждому клиенту, который подключается к точке доступа с настроенным APB. Пример подобной конфигурации:

```
{
   "permitted-ip-list": [
     "213.222.201.16",
     "213.222.198.16",
     "213.180.193.51",
     "192.225.158.3",
     "180.97.33.83",
     "178.162.216.178" ….....
   ]
 }
```

Если параметры клиента удовлетворяют критериям нескольких правил, ему будут разрешены для доступа IP-адреса из всех таких правил.