Контроллер управления, мониторинга и аналитики Wi-Fi-сетей

QWC-VC

Оглавление

1. ТЕРМИНЫ, СОКРАЩЕНИЯ И УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

ПО – Программное Обеспечение.

AP (Access Point) – ТД (Точка Доступа).

BSSID – Basic Service Set Identifier.

DHCP – Dynamic Host Configuration Protocol.

DNS – Domain Name System.

FW – Firmware (прошивка).

HTTP – HyperText Transfer Protocol.

HTTPS – HyperText Transfer Protocol Secure.

IP – Internet Protocol.

MAC – Media Access Control.

NAS Identifier – Non-Access Stratum Identifier.

NAT – Network Address Translation.

NMS – Network Management System.

QWC-VC – QTECH Platform. Далее по тексту контроллер будем называть платформой.

QWP-FW – QTECH Firmware.

QNMS – QTECH Network Management System.

QWP-Agent – QTECH Customer Premises Equipment Agent.

RADIUS – Remote Authentication in Dial-In User Service.

SSID – Service Set Identifier.

VLAN – Virtual Local Area Network.

WLAN (Wireless Local Area Network) – Беспроводная сеть.

WPA – Wi-Fi Protected Access.

2. СТРУКТУРА QTECH PLATFORM

QTECH Platform состоит из следующих компонент:

- платформа управления и мониторинга (NMS);
- платформа авторизации и монетизации (Portal);
- платформа аналитики (Analytics).

Наполнение конечной поставки зависит от купленной лицензии.

3. ИНТЕРФЕЙС ПЛАТФОРМЫ

3.1. Первый вход в систему

Для доступа к интерфейсу платформы в адресной строке браузера нужно набрать **https://<IP_or_Domain>**. В конфигурации по умолчанию интерфейс доступен по стандартным портам 80 и 443 протоколов HTTP и HTTPS соответственно. Однако, при установке на одном сервере платформы управления (NMS) и портала авторизации (Portal) порты отличаются (Рисунок 1).

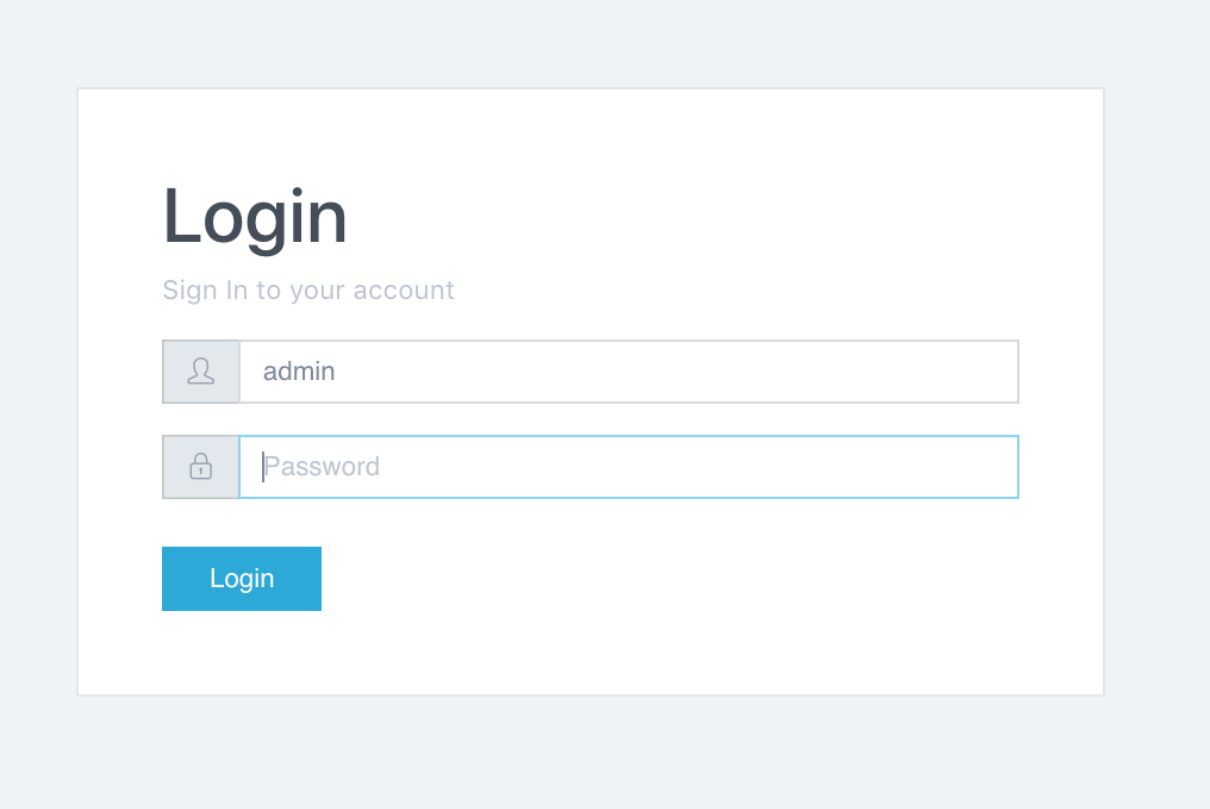


Рисунок 1. Вход в систему платформы

В случае удачной проверки прав доступа NMS перенаправляет вас на страницу состояния системы (Рисунок 2).

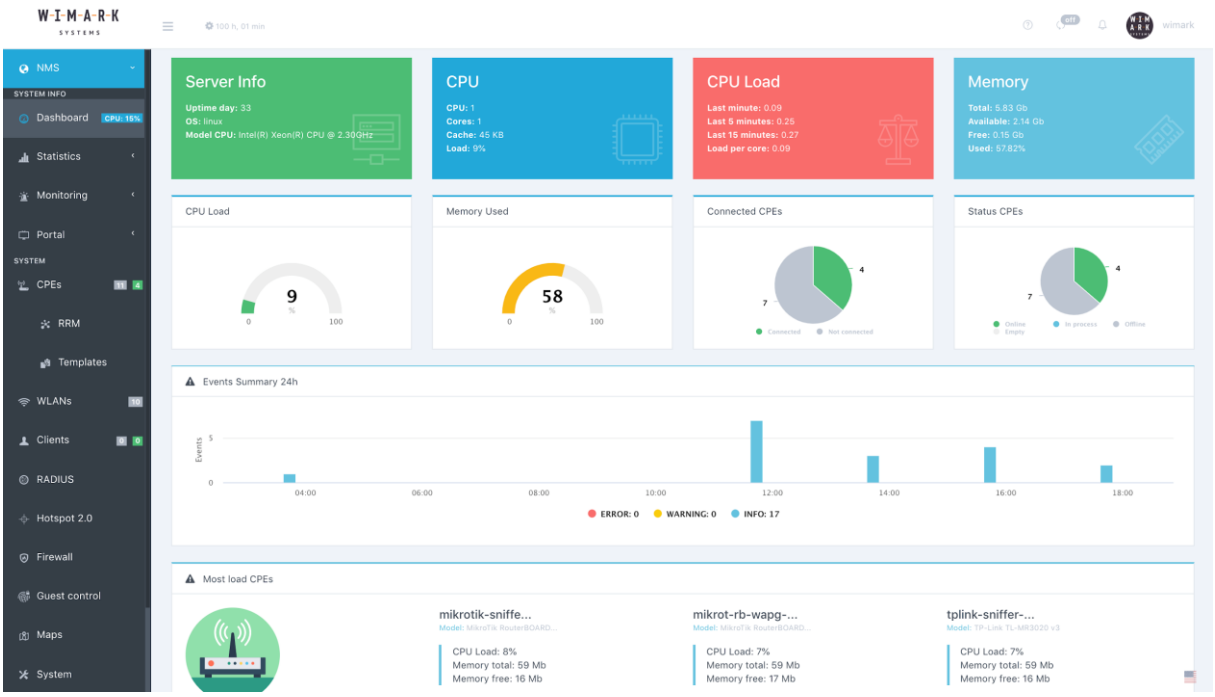


Рисунок 2. Страница состояния системы

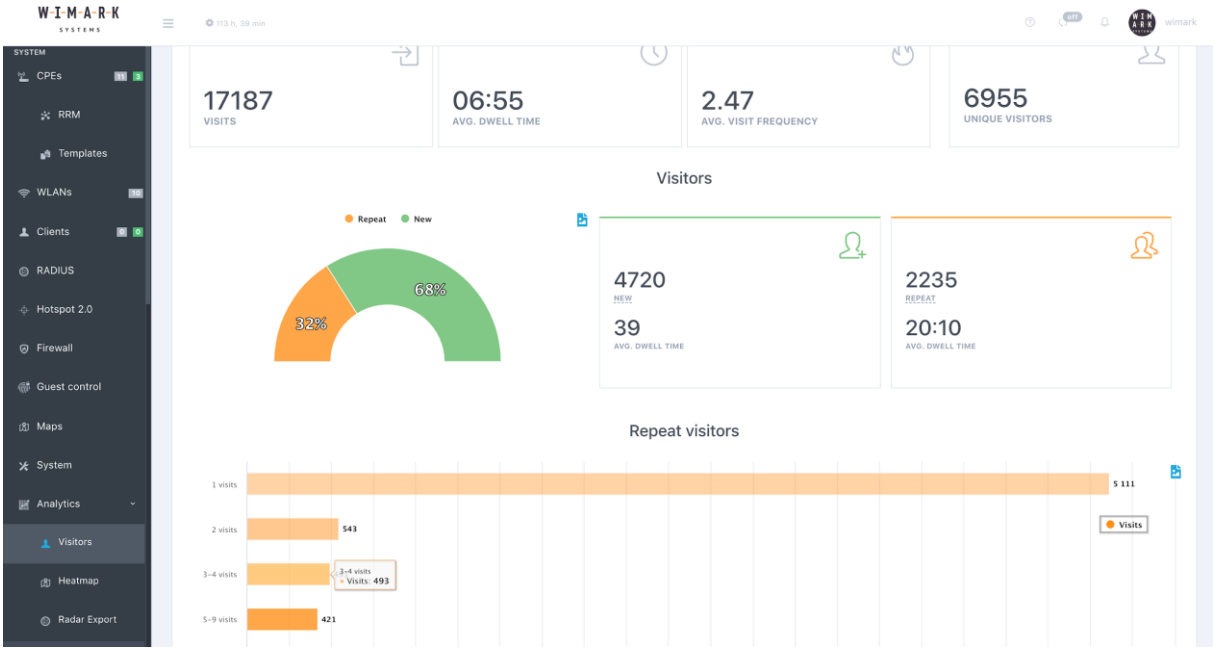


Рисунок 3. Пример интерфейса платформы QTECH

3.2. Общая структура интерфейса

Визуально интерфейс платформы можно поделить на 3 основные части:

- Вертикальная панель слева – основное меню, позволяющее взаимодействовать с объектами NMS (CPE, WLAN, карты и т.д.), объектами портала (в подменю Portal), статистики и мониторинга, а также смотреть аналитические отчеты (карты перемещений, работу Wi-Fi-радара).

- Горизонтальная панель сверху – status-bar, позволяющий в реальном времени просмотреть текущие операции и перейти в меню пользователей Веб-интерфейса, настройку локации и управления доступом.
- Главная рабочая область – панель взаимодействия объектов системы.

3.3. Работа с таблицами

NMS делалась для того, чтобы облегчить работу с большим количеством устройств, подключенных к платформе. Для этого списки объектов, которыми оперирует пользователь QNMS, представлены в виде таблиц. Например, список Точек доступа (CPE-устройств) представлен ниже (Рисунок 4).

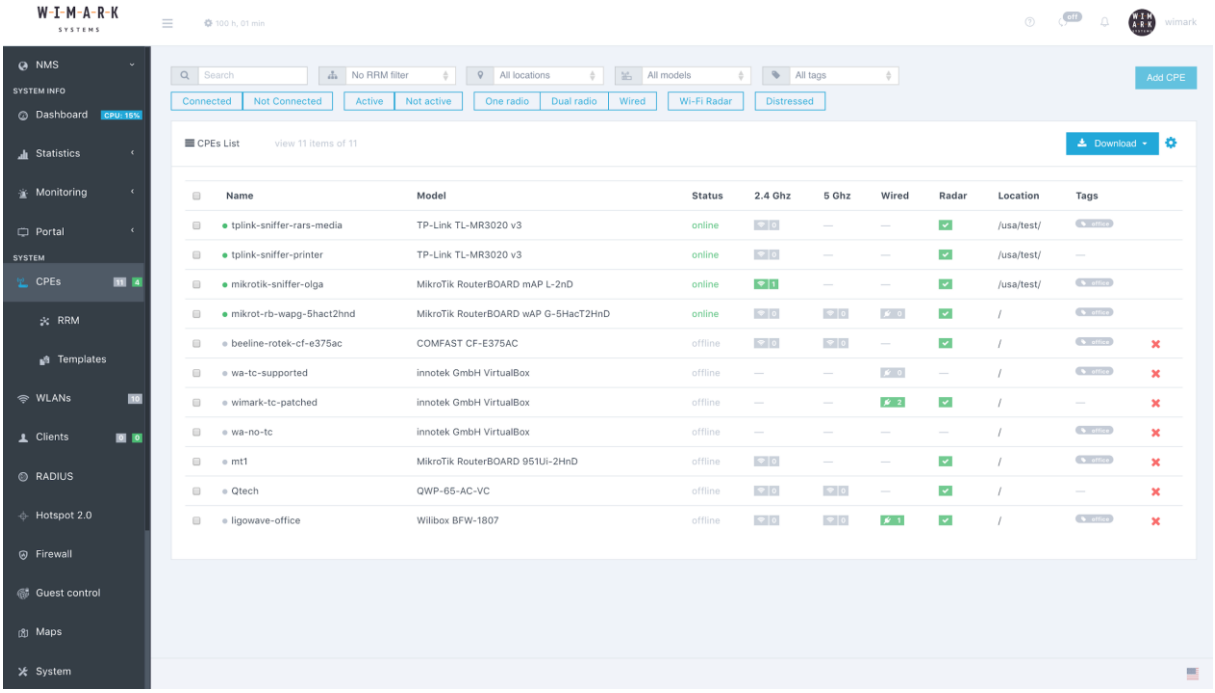


Рисунок 4. Список Точек доступа

Под объектом QNMS понимается структура данных, описывающая ту или иную функциональность. Например, типовыми объектами QNMS являются: устройства CPE, WLAN, локация, шаблон и т.д.

Для того, чтобы удобно работать с большим количеством устройств, QTECH разработала адаптивные фильтры (по локациям, MAC-адресам и т.д.), и теги, которые позволяют фильтровать объекты по признакам и работать с ними, как с группой. Также можно пользоваться строкой поиска (например, в списке устройств CPE будет осуществлен поиск по полям: Имя, MAC, описание, локальный IP-адрес и т.д.).

После фильтрации существует возможность выполнить универсальное действие на множество выбранных объектов. Например, добавить WLAN на все отфильтрованные ТД (Рисунок 5).

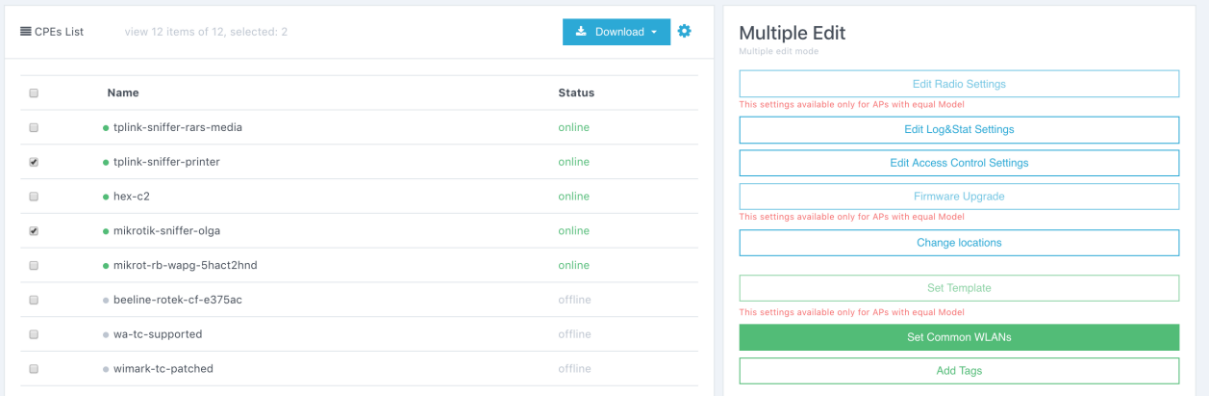


Рисунок 5. Редактирование отфильтрованных ТД

4. ПЛАТФОРМА УПРАВЛЕНИЯ И МОНИТОРИНГА (NMS)

4.1. Подключение точки доступа к платформе

4.1.1. Подключение точки доступа

Для того, чтобы подключить точку доступа (CPE, ТД) к платформе QTECH Platform (QWC-VC) нужно:

- На ТД должно быть установлено Программное Обеспечение (ПО) QTECH Firmware (QWP-FW).
- ТД должна быть настроена на взаимодействие с платформой QWC-VC.
- IP-адреса для ТД с ПО QWP-FW должны выдаваться DHCP-сервером в нативном VLAN.
- Адрес QWC-VC должен быть доступен для ТД (Обязательное условие: связь ТД –> QWC-VC, при которой ТД инициирует подключение к QWC-VC, а не наоборот).
- Обязательно должны быть открыты порты UDP 500/4500 в случае подключения по IPSec, либо TCP 1883 в случае подключения по MQTT без туннелирования.

По умолчанию ТД с ПО QWP-FW настроены на подключение к платформе по адресу **platform.wimark.com.** Подразумевается, что администратор локальной сети может настроить локальный DNS-сервер для того, чтобы все точки доступа с ПО QWP-FW и, настроенные по умолчанию, могут подключиться к платформе автоматически.

Далее, приведены примеры настроек некоторых популярных DNS-серверов с целью поддержки автоматического подключения точек с ПО QWP-FW.

4.1.2. Индикаторы подключенной точки доступа

Благодаря графическим идентификатором в Network Management System (NMS) QTECH NMS (QNMS) можно видеть состояние подключения ТД к QWC-VC.

4.1.2.1. Состояние подключения в таблице точек доступа: Подключено

На изображении ниже можно увидеть “зеленый” индикатор подключения, символизирующий о том, что точка доступа подключилась к QWC-VC и готова к работе.

4.1.2.2. Состояние подключения в таблице ТД: Отключено

На изображении ниже можно увидеть серый индикатор отключения, символизирующий о том, что ТД отключилась от платформы.

4.1.3. Подключение точки доступа. Предконфигурация

В данном разделе рассматривается ситуация, при которой нет возможности организовать схему подключения zero touch provisioning. Поэтому каждую ТД следует подключить по отдельности. Для подключения ТД с установленным ПО QWP-FW нужно выполнить следующие действия:

- Найти IP-адрес ТД для получения доступа к Веб-интерфейсу управления.
- Изменить настройку для подключения к платформе QWC-VC.

4.1.3.1. Как найти IP-адрес точки доступа, полученный по DHCP

Ниже описаны несколько популярных методов получения информации о выданном IP для определенного устройства. Для того чтобы однозначно найти выданный IP-адрес нужно знать MAC-адрес устройства. Обычно MAC-адрес точек доступа можно найти:

- на корпусе самой ТД;
- на упаковке ТД;
- в документации к ТД.

Методы, описанные ниже, основываются на том факте, что MAC-адрес ТД известен.

4.1.3.1.1. Метод fping

Данный метод предполагает наличие на вашей локальной рабочей станции/вашем компьютере установленного приложения *fping*. Утилита *fping* может опрашивать все устройства локальной сети путем посылки icmp-пакета.

Пример использования:

- Предполагается, что подсеть, в которой ТД получила IP, известна (например, 192.168.0.0/24).
- Предполагается, что MAC-адрес ТД известен (например, ab:ab:ab:ab:ab:ab).
- Примерная схема подключения изображена ниже (Рисунок 6).

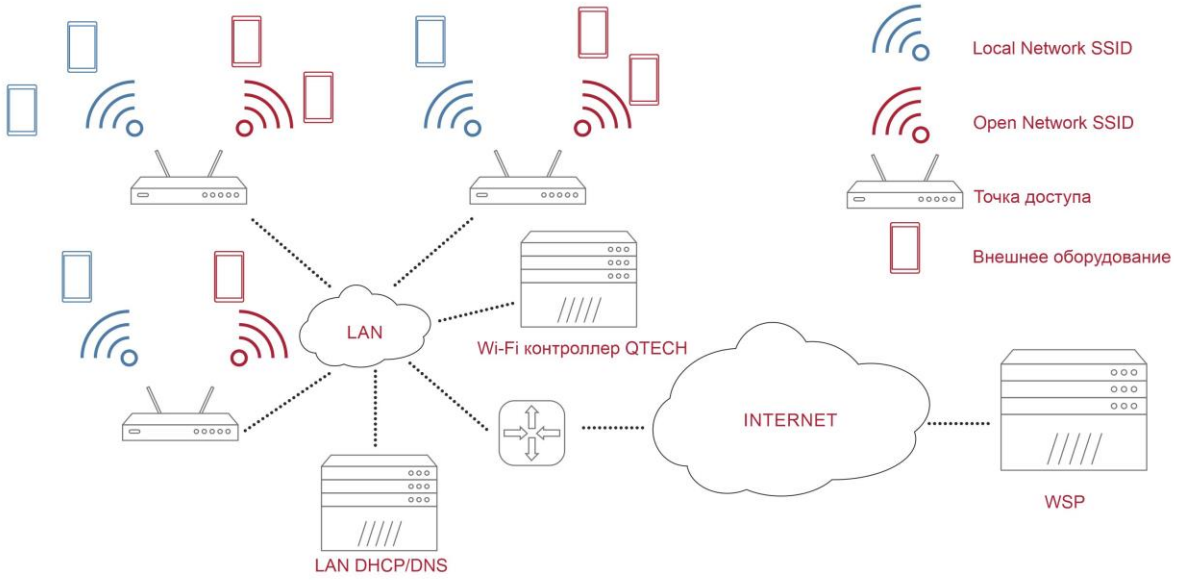


Рисунок 6. Примерная схема подключения ТД

На локальной рабочей станции/компьютере следует открыть терминал и выполнить следующие команды:

```
$ fping -c1 -g 192.168.0.0/24
$ arp -a -n | grep ab:ab:ab:ab:ab:ab
```

4.1.3.2. Последовательность действий при конфигурации точки доступа для подключения к платформе QWC-VC

На данном этапе подразумевается, что нам известно следующее:

- IP-адрес точки доступа (например, 10.30.40.209);
- IP-адрес или доменное имя, по которому доступна платформа QWC-VC (например, 192.168.0.254);
- ТД может находится за NAT относительно расположения QWC-VC.

Для подключения ТД к платформе нужно выполнить следующие шаги:

- Загрузить страницу Веб-интерфейса точки доступа. Для этого в окне браузера надо набрать **https://<IP точки>/** (например, **https://10.30.40.209**). В Веб-браузере появится страница авторизации для точки доступа с ПО QWP-FW (Рисунок 7).

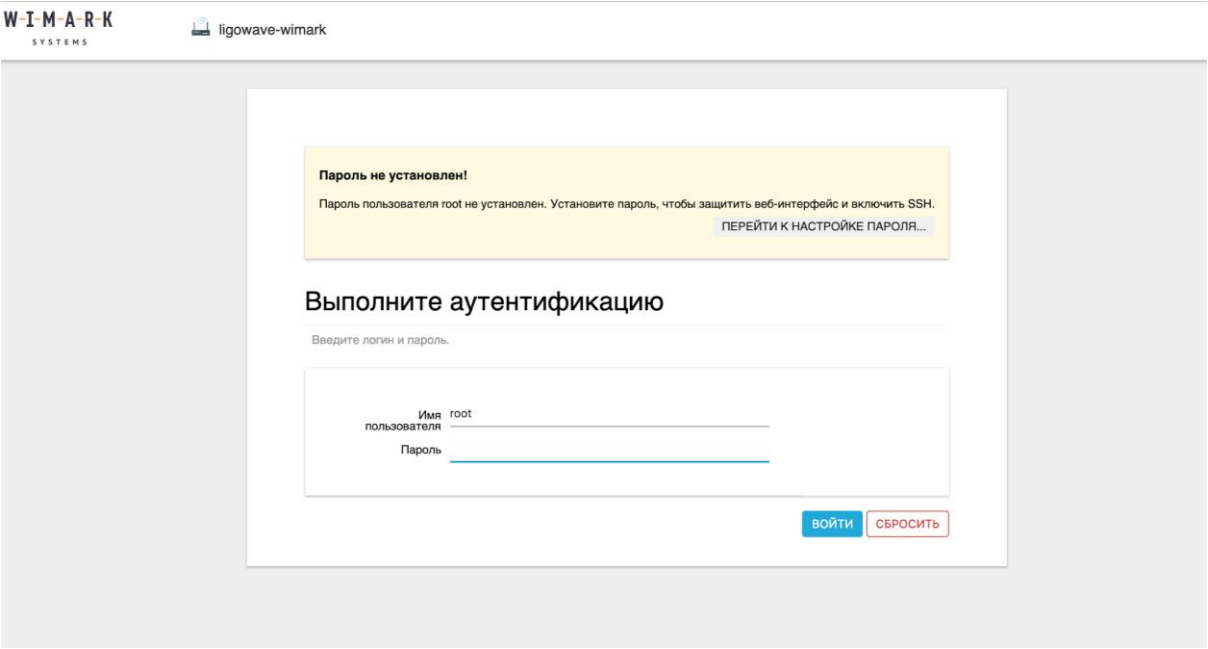


Рисунок 7. Страница авторизации для ТД с ПО QWP-FW

По умолчанию, Веб-интерфейс конфигурации всех ТД с ПО QWP-FW доступен для пользователя **root** с авторизацией **без пароля**.

- Вводим учетные данные и попадаем на страницу статуса точки доступа с ПО QWP-FW и нажимаем “ВВОД” (Рисунок 8).

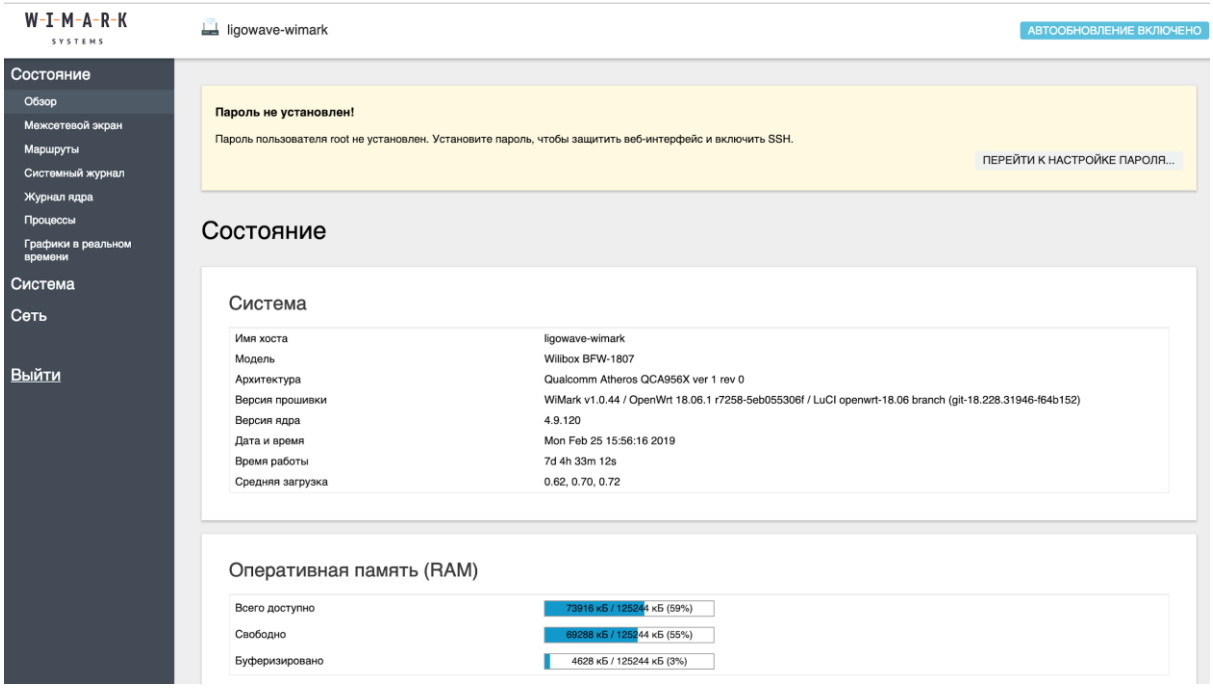


Рисунок 8. Страница статуса ТД с ПО QWP-FW

- Переходим в меню “Сеть” –> “Агент CPE”. QTECH CPE Agent – часть ПО QWP-FW, отвечающая за взаимодействие с QWC-VC (Рисунок 9).

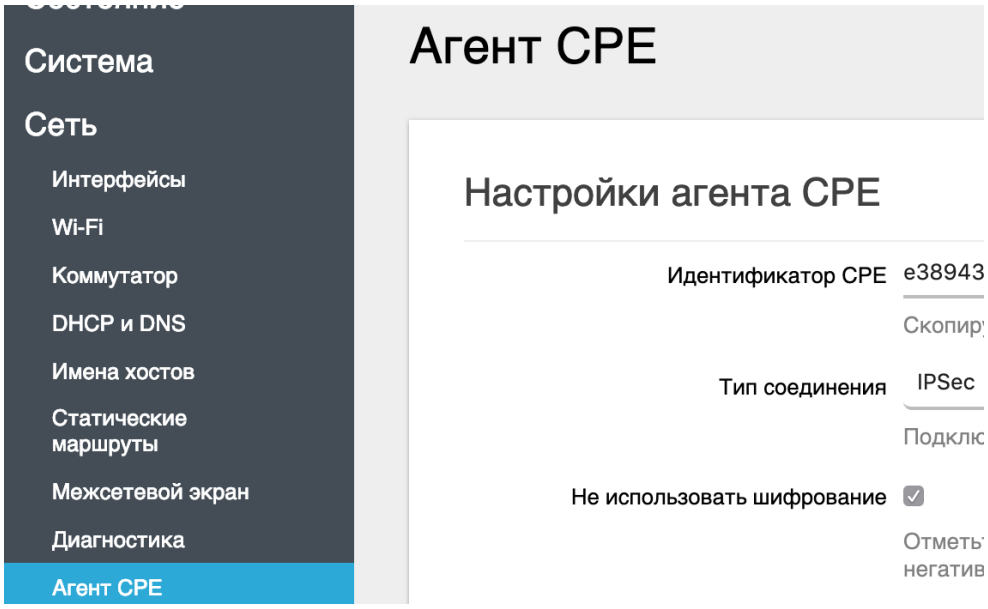


Рисунок 9. Меню “Агент CPE”

- Попадая на страницу конфигурирования связи между ТД и платформой, мы конфигурируем поле “Адрес системы управления” и меняем значения поля на <IP_or_Domain>, где <IP_or_Domain> – IP-адрес или домен, по которому доступна платформа QWC-VC (Рисунок 10).

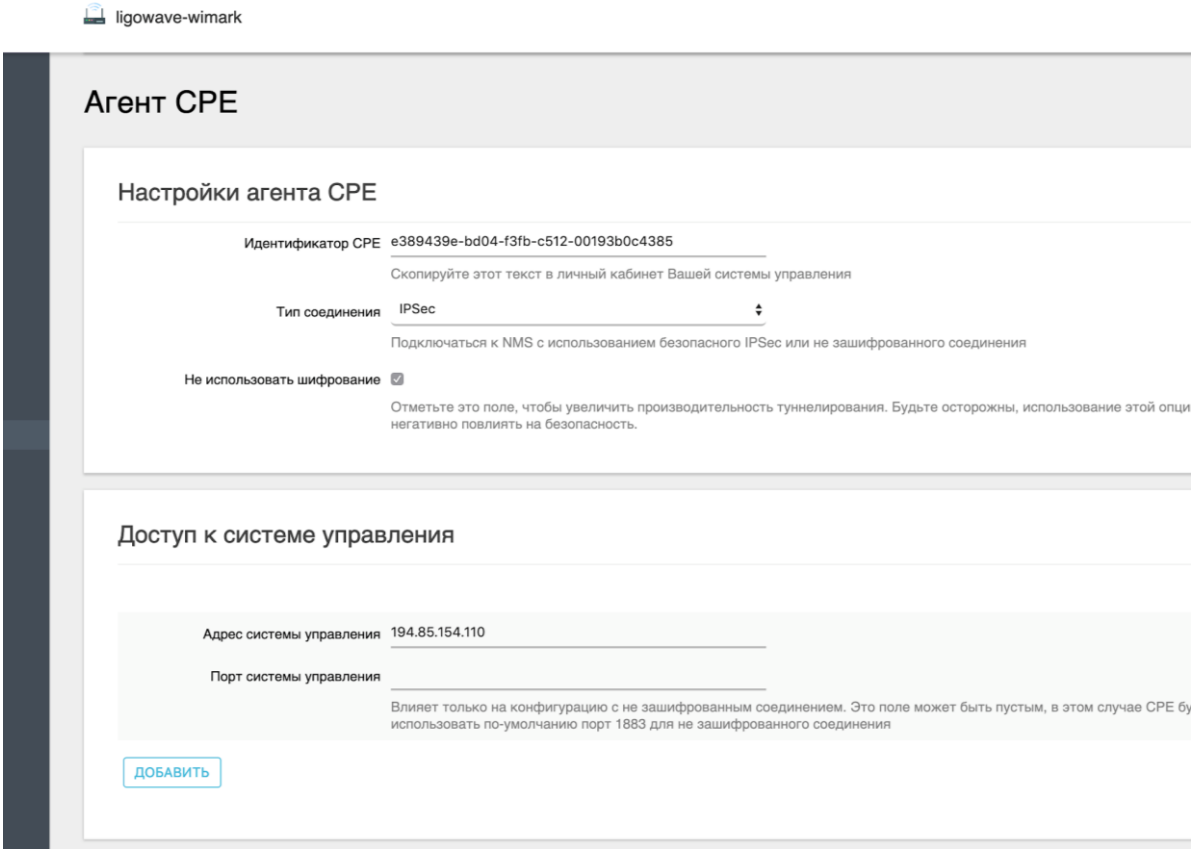


Рисунок 10. Настройка Агента CPE

- Для подтверждения изменений параметров подключения к платформе QWC-VC следует нажать кнопку “Сохранить и применить.”
- Статус подключения точки доступа к платформе следует проверить в QNMS.

Также можно изменить адрес подключения через **ssh**. Для этого требуется выполнить несколько действий:

Зайти на точку: **ssh root@<IP точки>**;

Выполнить изменение адреса: **uci set wimark.broker.host='<IP_or_Domain>'**;

Перезапустить агент для применения конфига: **cpeagent restart**.

4.1.4. Первое подключение точки доступа

Для того чтобы подключить ТД к платформе QWC-VC нужно выполнить действия из пунктов раздела 4.1. При подключении точка регистрируется на платформе и становится доступна для взаимодействия в QNMS.

4.1.5. Повторное подключение точки доступа

При первом подключении ТД проходит процесс регистрации. В процессе регистрации платформа QWC-VC запоминает идентификатор и возможности (capability) каждой ТД, что дает возможность не проходить процесс регистрации повторно.

Вся информация по отключенной ТД сохраняется на платформе и доступна для взаимодействия пользователю.

ТД может отключится от платформы по таким причинам как питание, отключения канала связи и т.д. В случае отключения ТД, отображение ее в QNMS меняется, появляются красные индикаторы отключения ТД (Рисунок 11).

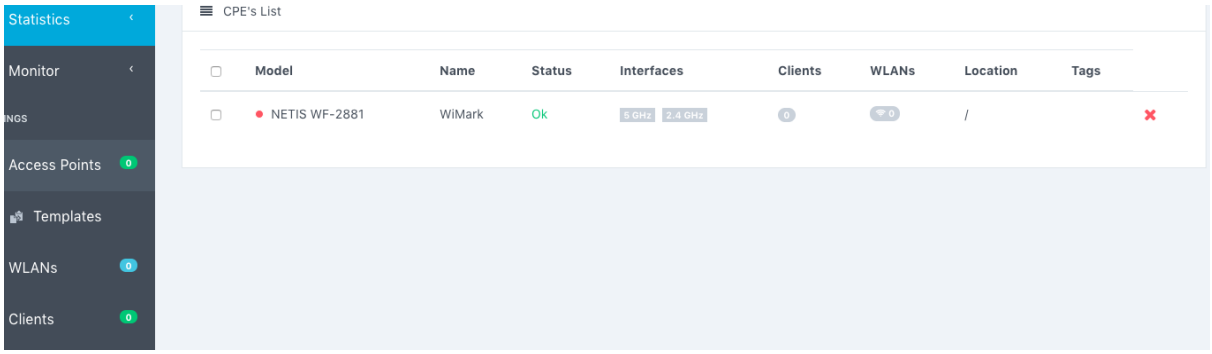


Рисунок 11. Отключение ТД от платформы

При повторном подключении индикаторы подключения ТД меняются и сигнализируют о подключении и конфигурации при подключении (Рисунок 12).

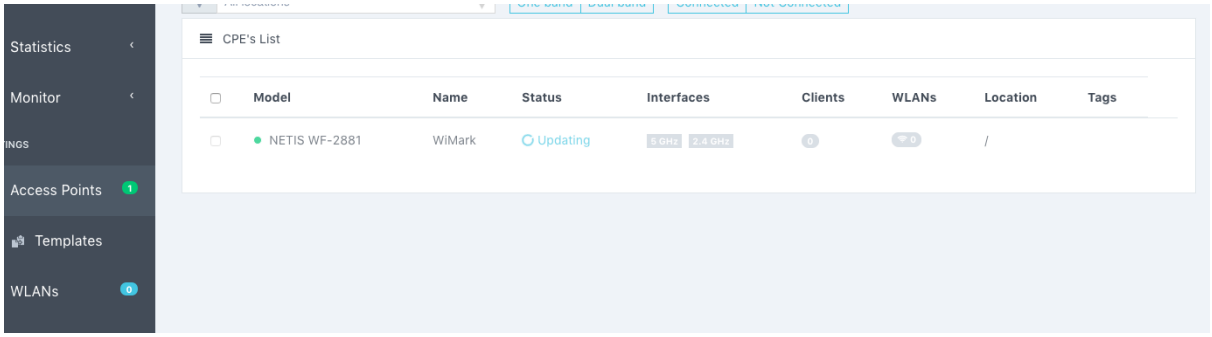


Рисунок 12. Повторное подключение ТД к платформе

4.2. Статусы объектов в платформе

Некоторые объекты QNMS меняют свое состояние при определенных действиях. К таким объектам прежде всего относятся ТД и WLAN.

Точки доступа имеют два типа статусов:

- статус подключения;
  - включен – “зеленый индикатор”, символизирующий о подключении ТД к платформе;
  - выключен – “серый индикатор”, символизирующий об отключении ТД от платформы;
- статус конфигурации;
  - Error – ошибка конфигурации объекта (также рядом описание ошибки);
  - Updating – обновление конфигурации объекта;
  - Pending – состояние, в котором конфигурация “ждет”, когда подключится ТД, и будет применена;
  - Online – точка работает в нормальном режиме;
  - Offline – точка отключена.

4.3. Иерархия доступа к ресурсам платформы

Платформа управления использует иерархию доступа, сформированную посредством следующих объектов доступа:

- объект локации;
- объект роли.

Комбинации объектов роли и локации определяют доступность того или иного ресурса/объекта. Роль и локация – это обязательные параметры доступа пользователя.

4.3.1. Локации и Роли

4.3.1.1. Локации

Локация – объект QNMS, который позволяет выставить уровень доступа. Локация дает возможность работы с находящимися в ней объектами, а также с объектами, находящимися в подлокациях. Локация является обязательным параметром каждого из объектов QNMS.

Систему локаций QNMS можно представить в виде дерева локаций с корнем в локации “*/*”. Структура в целом напоминает иерархию папок в Unix подобных ОС.

4.3.1.2. Роль

Роль – это объект QNMS, описывающий набор доступных действий над всеми объектами QNMS. В данный момент QNMS имеет три предустановленные роли:

Admin – роль администратора, которая позволяет делать всевозможные действия с объектами, находящимися в локации этого пользователя (например, /Russia). Так же всевозможные действия могут быть применены к объектам подлокаций (например, /Russia/Moscow).

Operator – роль оператора, которая позволяет только читать данные объектов локации пользователя и её подлокаций.

Marketer – роль маркетолога, позволяет иметь доступ на чтение и запись для объектов подчастей Portal и Analytics.

4.3.2. Создаем/Удаляем локацию

4.3.2.1. Создание локации

Для создания локации нужно нажать на иконку пользователя в верхнем правом углу и выбрать поле Settings (Настройки) (Рисунок 13).

Рисунок 13. Настройки в поле Профиля

Далее в центральной панели выбираем поле Location (Локация) и добавляем интересующую нас локацию. В настоящее время для локаций можно определить ответственного сотрудника и описание, в котором, например, будет реальный адрес (Рисунок 14).

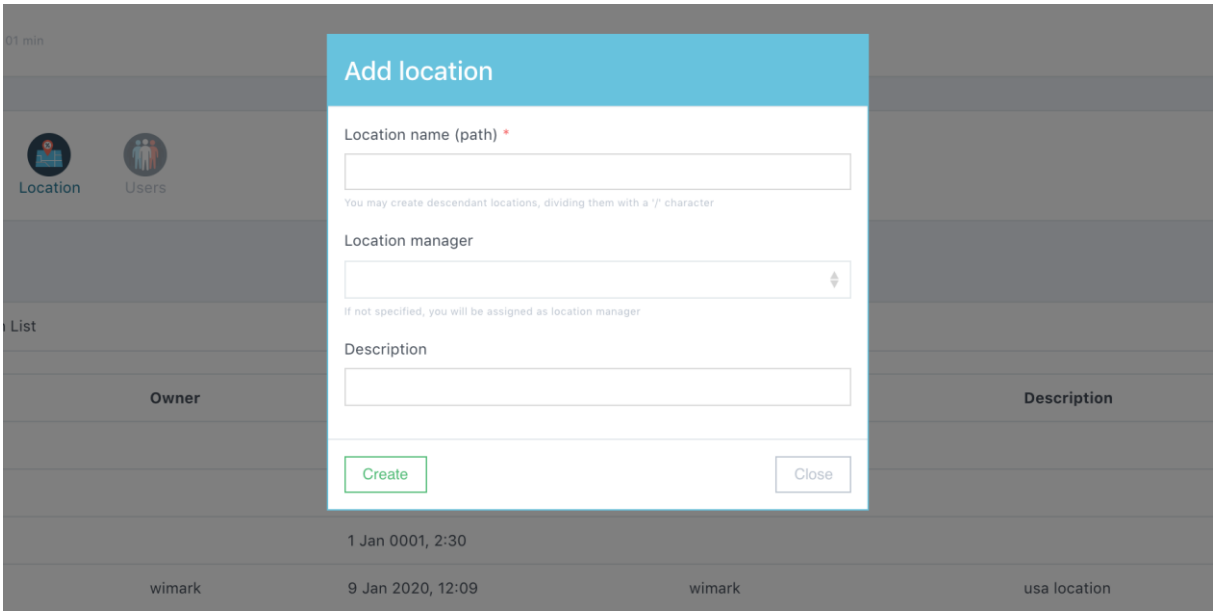


Рисунок 14. Создание локации

4.3.2.2. Удаление локации

Аналогично добавлению локации, нужно перейти в панель “Добавление/Удаление локации” путем нажатия Settings (Настройки) –> Locations (Локации).

Выбрать локацию, которая требует удаления, и удалить, нажав на кнопку Delete (Удалить) (Рисунок 15).

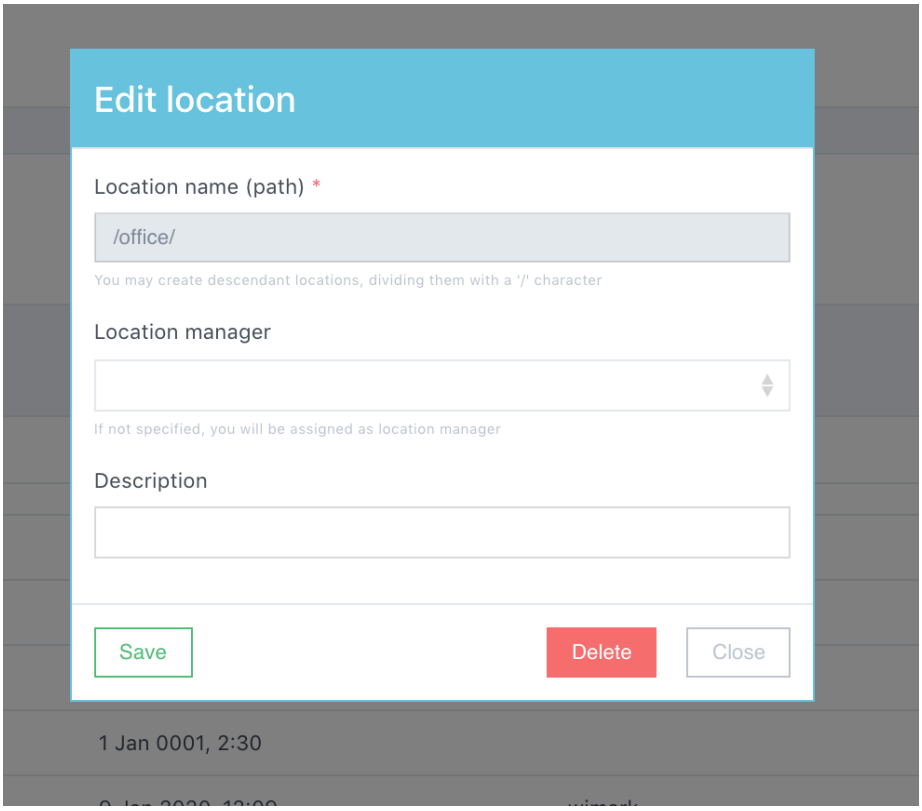


Рисунок 15. Удаление локации

ПРИМЕЧАНИЕ: Все объекты заданной локации переходят на локацию верхнего уровня. (например, при удалении локации /office все ТД локации /office перейдут в локацию /)

4.3.3. Создаем/Удаляем пользователя

4.3.3.1. Создаем пользователя

Для того чтобы получить доступ к QNMS, нужно обладать правами доступа объекта пользователь. По умолчанию система создается с пользователем с логином и паролем **wimark/wimark**. Для того чтобы создать нового пользователя QNMS нужно нажать на иконку пользователя в верхнем правом углу и выбрать поле Settings (Настройки).

Затем на центральной панели выбираем поле Users (Пользователи) (Рисунок 16).

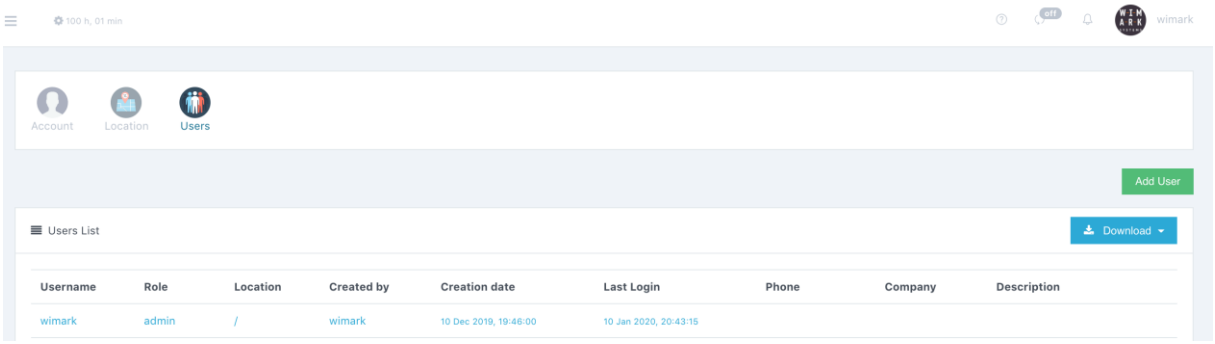


Рисунок 16. Создание пользователя

Нажимаем кнопку Add user (Добавить пользователя) (Рисунок 17).

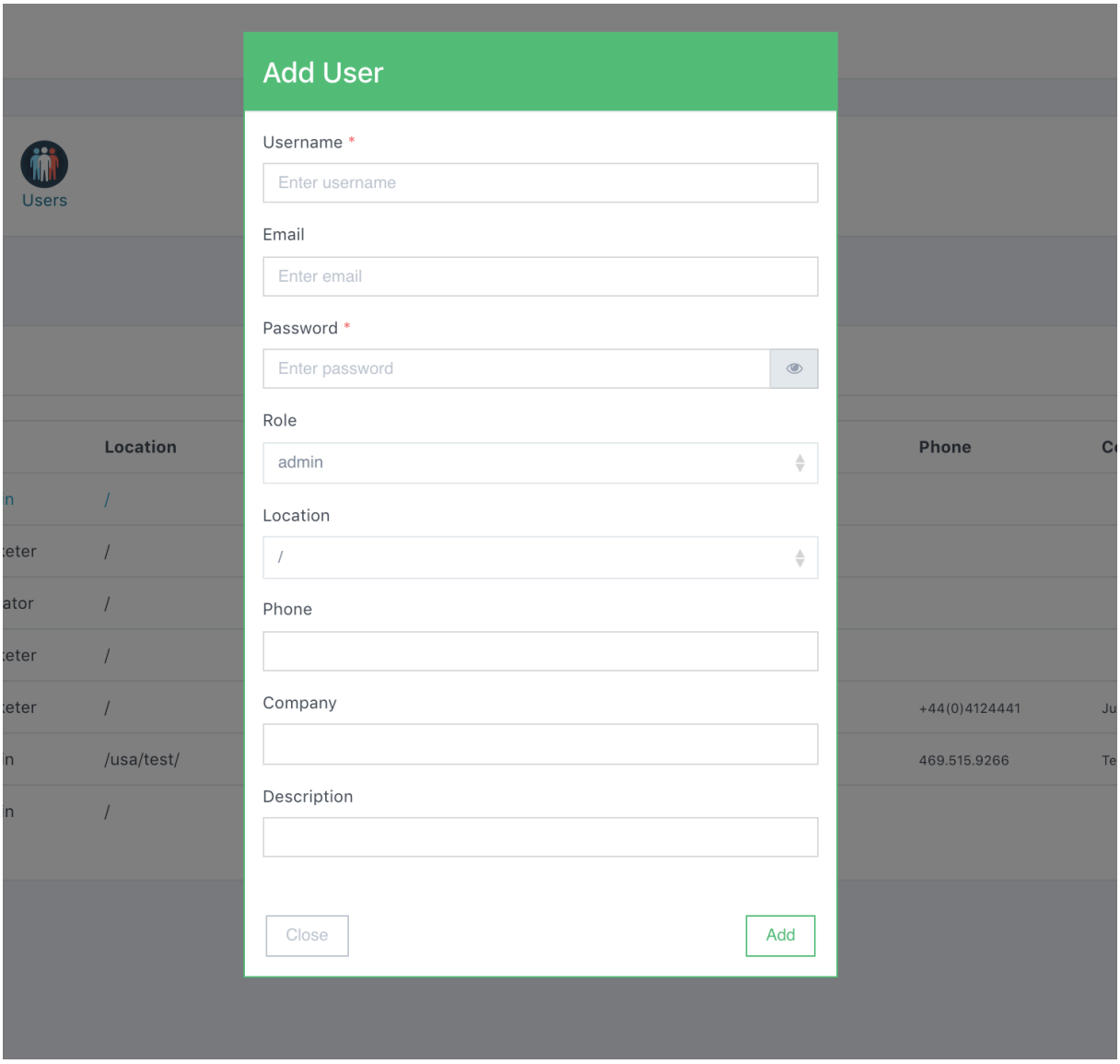


Рисунок 17. Настройка вновь созданного пользователя

После нажатия на кнопку появится модальное окно с полями для заполнения. Нужно заполнить соответствующие поля и перейти к выбору роли и локации – атрибутов ограничения доступа, описанных в разделе 4.3.1. По завершению заполнения формы нажать на кнопку Add (Добавить).

Затем, можно увидеть вновь созданного пользователя в списке (Рисунок 18).

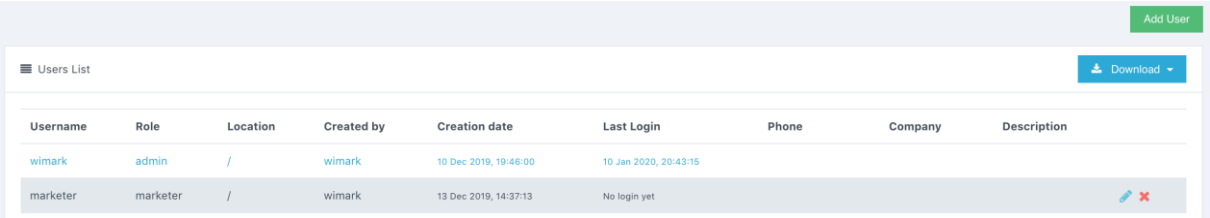


Рисунок 18. Вновь созданные пользователи в списке

4.4. Изменение базовой локации (Base location)

Все объекты на платформе имеют базовую локацию. Базовая локация определяет набор пользователей, которым доступен тот или иной объект. (например, пользователь локации /Moscow имеет доступ к объектам с базисной локацией /Moscow и к объектам с базисной локацией из числа подлокаций /Moscow (например, /Moscow/Chertanovo)).

ПРИМЕЧАНИЕ: Изменение базисной локации может привести к неконсистентности. Например, может поменять локации ТД, но не поменять локации WLAN, и тогда пользователь не сможет изменять уже установленные WLAN на ТД.

4.5. Работа с объектом беспроводной сети (WLAN)

4.5.1. Создание/Удаление беспроводной сети

Для того чтобы начать конфигурировать ТД, нужно создать настройку беспроводной сети (WLAN). Для этого в пункте меню, вертикальная панель с правой стороны, нужно нажать на кнопку WLAN (Беспроводных сетей). Создание многих объектов в QNMS сделано с помощью удобных пошаговых Wizard (Мастеров).

Далее отдельно описано создание разных типов беспроводных сетей.

4.5.2. Конфигурация разных типов беспроводных сетей

4.5.2.1. Конфигурация беспроводной сети без шифрования

Нужно нажать на кнопку Add WLAN (Добавить WLAN), находящуюся в правом верхнем углу (Рисунок 19).

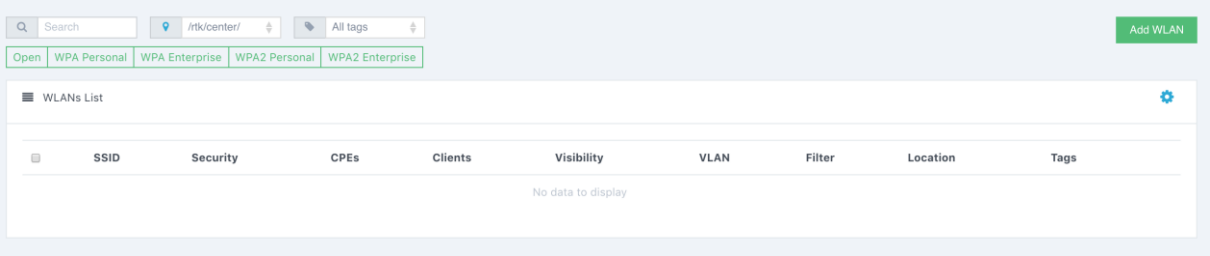


Рисунок 19. Добавление WLAN

Далее мы переходим на страницу Wizard (Мастера) создания WLAN.

На шаге 1 мы выбираем SSID (Service Set Identifier) беспроводной сети, добавляем Description (Описание) и выбираем базисную локацию для этой сети (Рисунок 20).

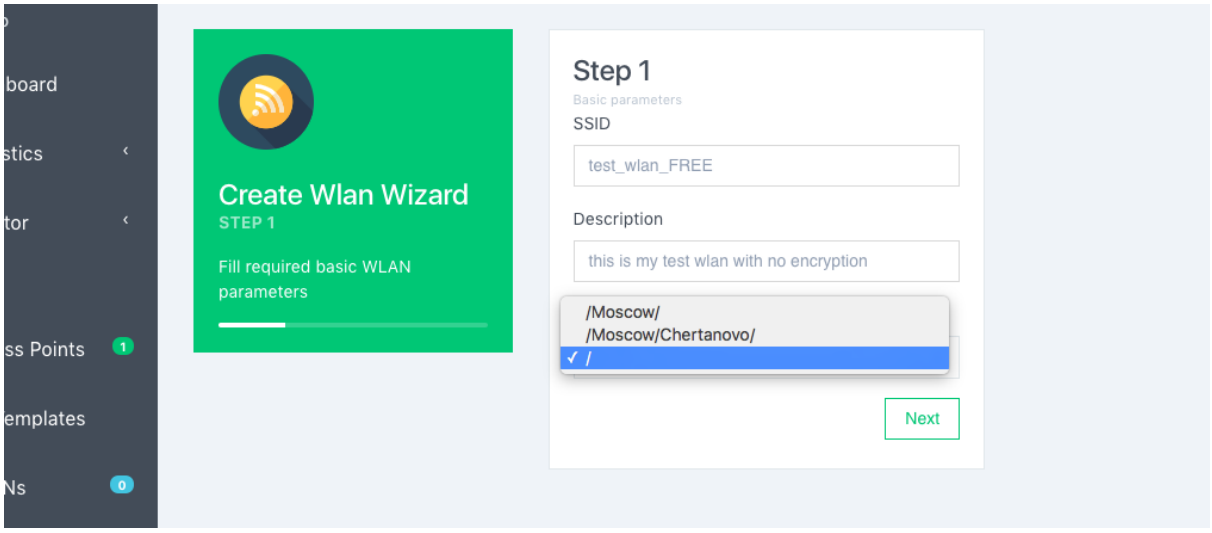


Рисунок 20. Добавление Описание и базисной локации для сети

Нажимаем Next (Далее) и переходим на шаг 2, где выбираем тип шифрования сети. Нас интересует конфигурация открытой сети (Рисунок 21).

Выбираем Security (Безопасность): “Open” и нажимаем Next (Далее).

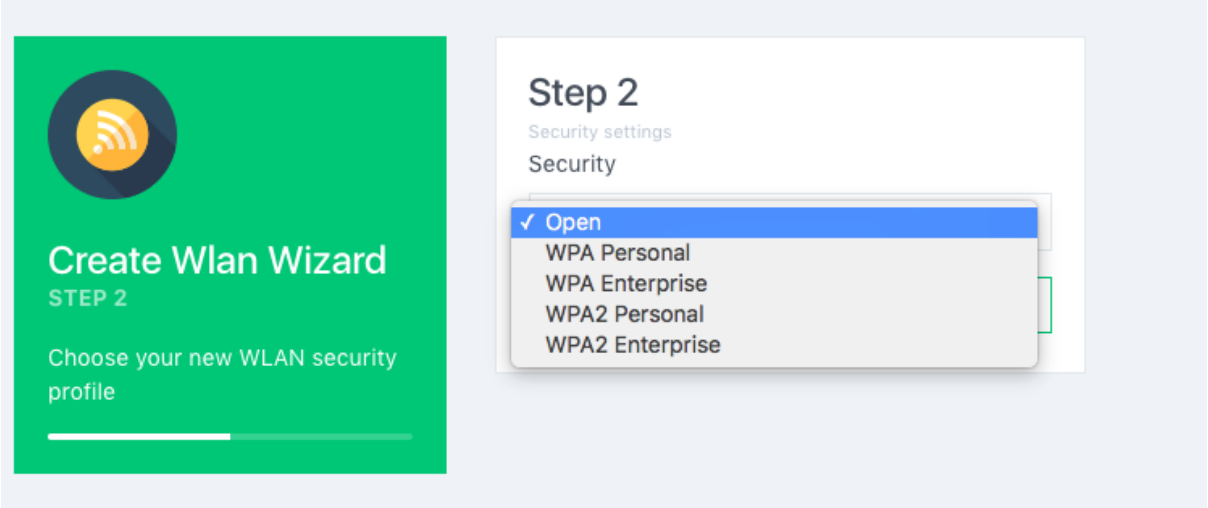


Рисунок 21. Выбор типа шифрования сети

На шаге 3 выбираем VLAN, в который собираемся коммутировать пользовательский трафик (Выбираем VLAN по умолчанию/нативный VLAN 0). Также нужно выбрать в каком режиме будет происходить вещание данной сети.

Существует два режима: Visible и Hidden. Visible – режимы работы ТД, когда в радио эфир распространяется информация о том, что ТД вещает соответствующий SSID (Рисунок 22). В случае с режимом Hidden подобная информация не распространяется. Нажимаем Next (Далее).

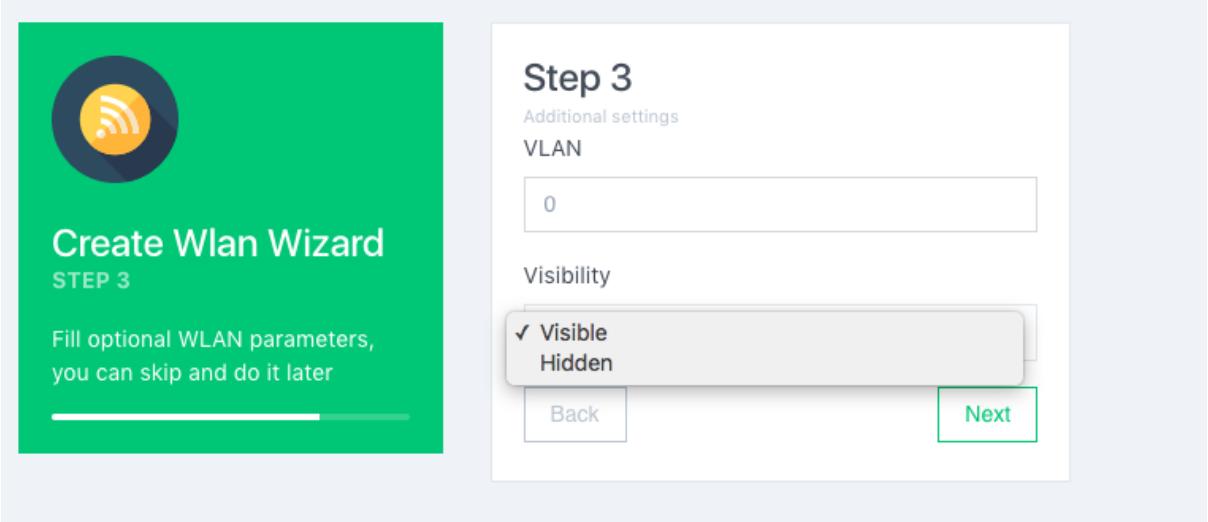


Рисунок 22. Выбор режима работы ТД

Шаг 4. Происходит предпоказ конфигурации нового WLAN (Рисунок 23).

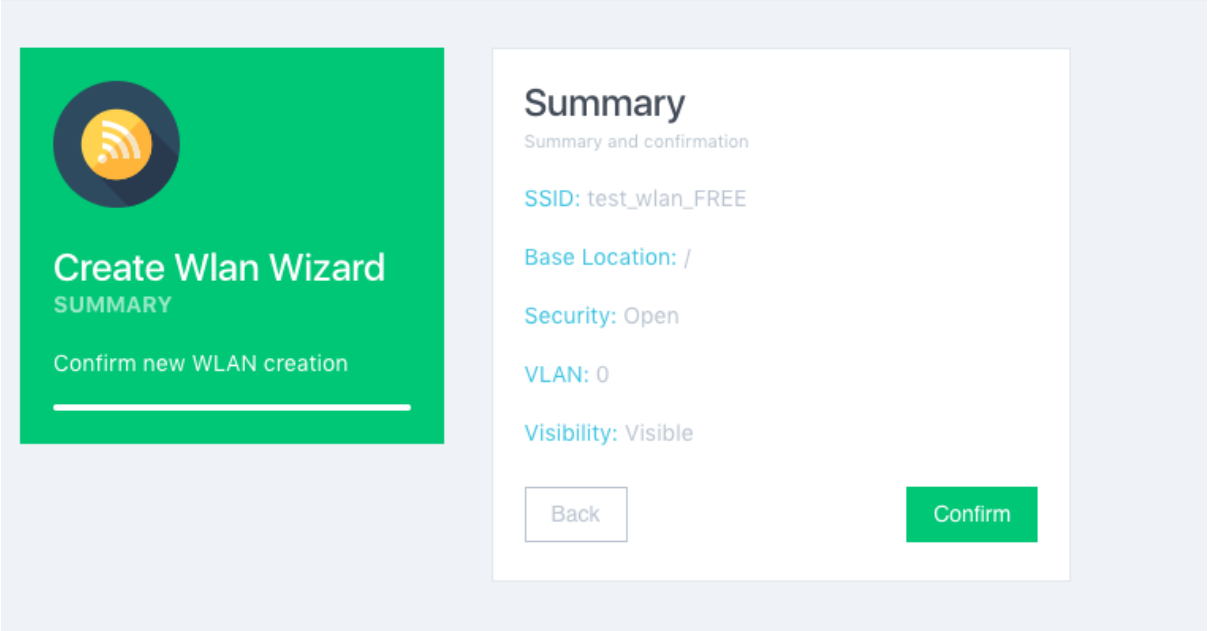


Рисунок 23. Предпоказ конфигурации нового WLAN

Далее при нажатии Confirm (Подтвердить) мы увидим список беспроводных сетей, содержащий только что созданный объект конфигурации беспроводной сети (Рисунок 24).

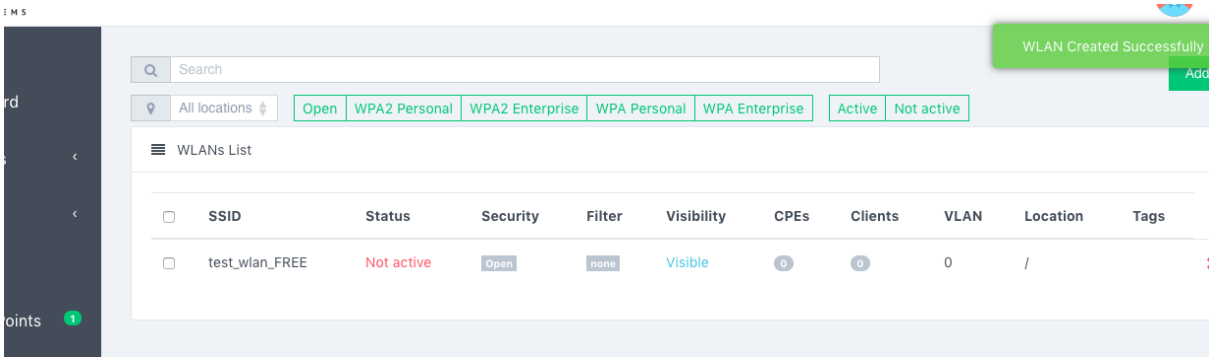


Рисунок 24. Список беспроводных сетей, содержащий только что созданный объект конфигурации беспроводной сети

4.5.2.2. Конфигурация сетей с типом безопасности WPA Personal

Для создания сети WPA Personal проходим аналогичные шаги, что и для открытой сети.

Шаг 1 (Рисунок 25).

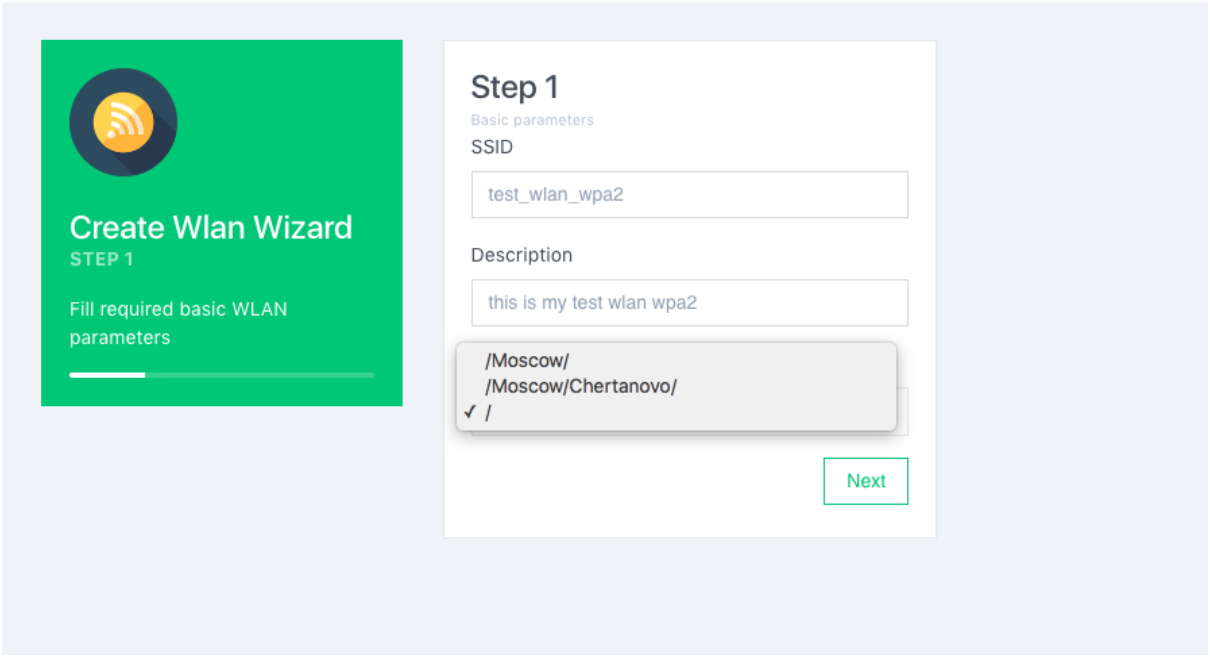


Рисунок 25. Добавление Описание и базисной локации для сети

Шаг 2. Здесь нужно выбрать поддерживаемые типы шифрации (Рисунок 26).

ПРИМЕЧАНИЕ: Для поддержки последних iPhone шифрование типа AES обязательно.

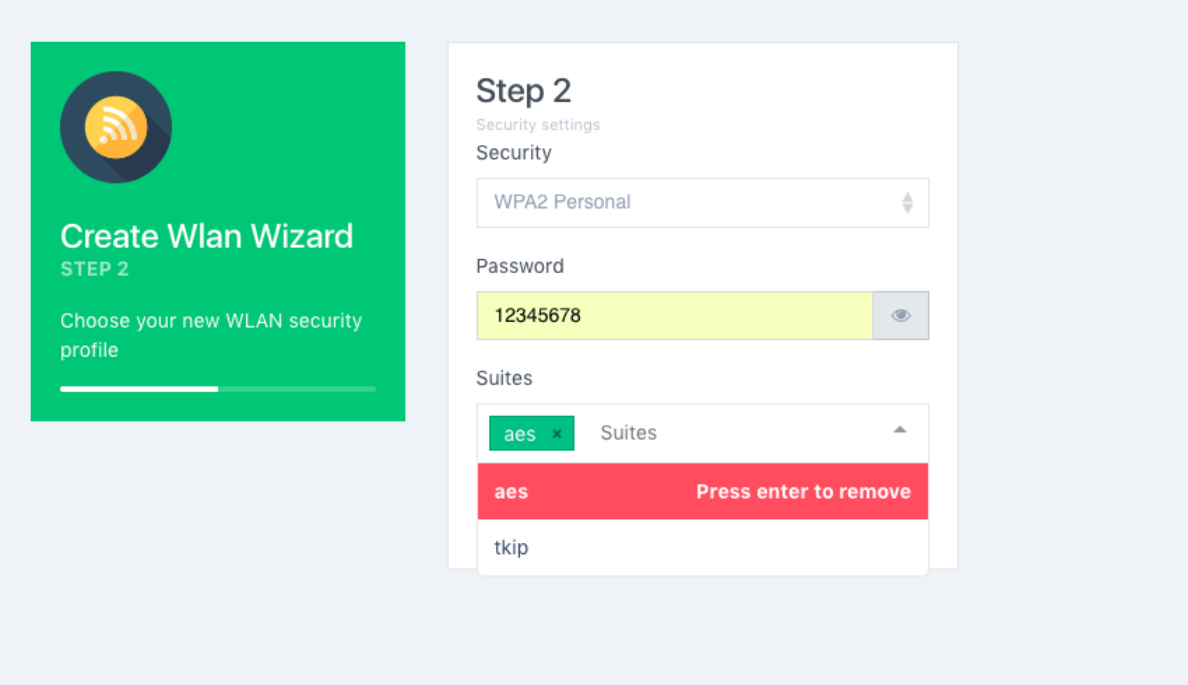


Рисунок 26. Выбор типа шифрования сети

Шаг 3 (Рисунок 27).

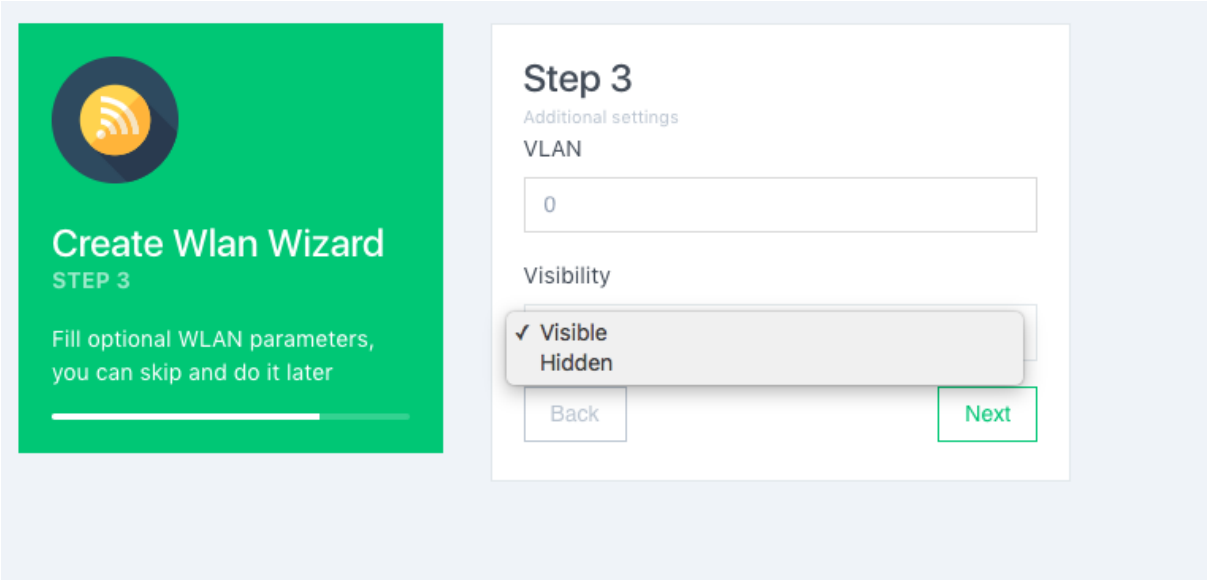


Рисунок 27. Выбор режима работы ТД

Шаг 4 (Рисунок 28).

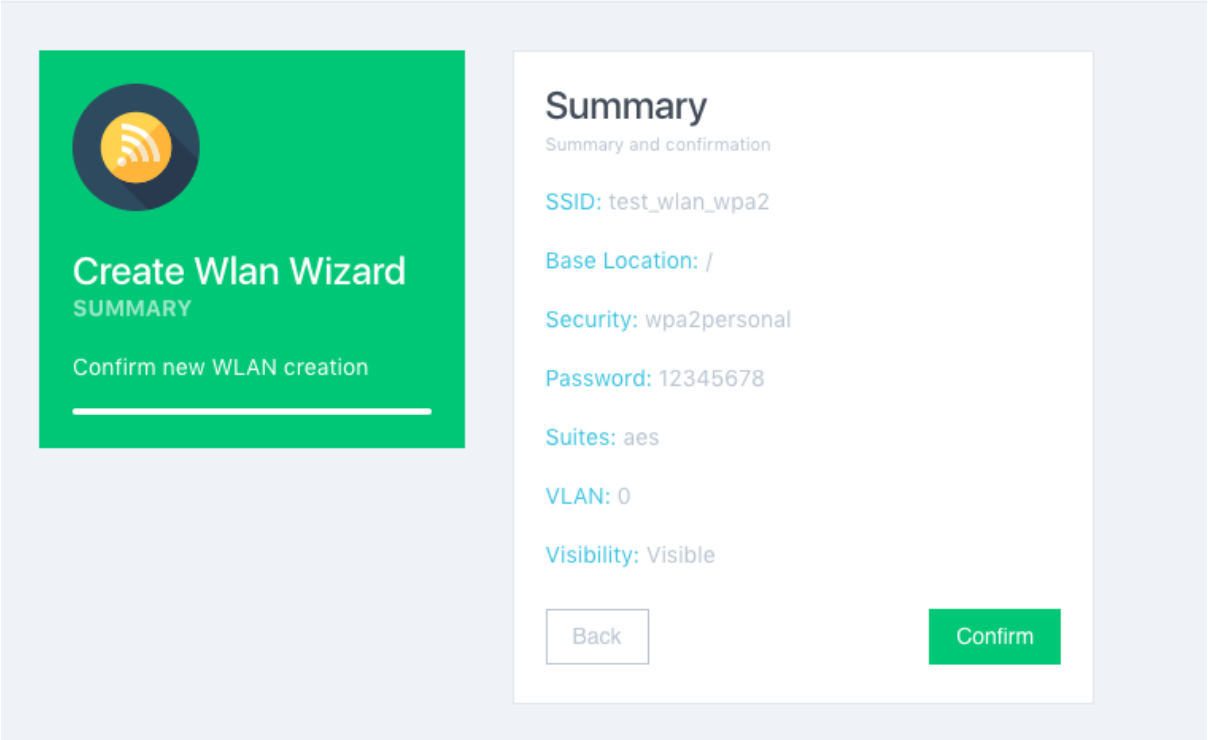


Рисунок 28. Предпоказ конфигурации нового WLAN

Далее при нажатии Confirm (Подтвердить) мы увидим список беспроводных сетей, содержащий только что созданный объект конфигурации беспроводной сети.

4.5.2.3. Конфигурация беспроводной сети с типом безопасности WPA Enterprise

Для того чтобы добавить настройку беспроводной сети с типом безопасности WPA Enterprise, нужно создать связность платформы с сервером аутентификации RADIUS Server. О том, как создать связность с RADIUS-сервером, написано в разделе 4.5.3.

4.5.2.4. Конфигурация беспроводной сети с типом безопасности WPA2 Enterprise

Предполагается, что на данном этапе связность с RADIUS-сервером присутствует и описана в терминах объектов QNMS. Тогда по аналогии с другими типами WLAN начинаем создание WLAN с 1 шага Wizard (Мастера) добавления WLAN.

Шаг 1 (Рисунок 29).

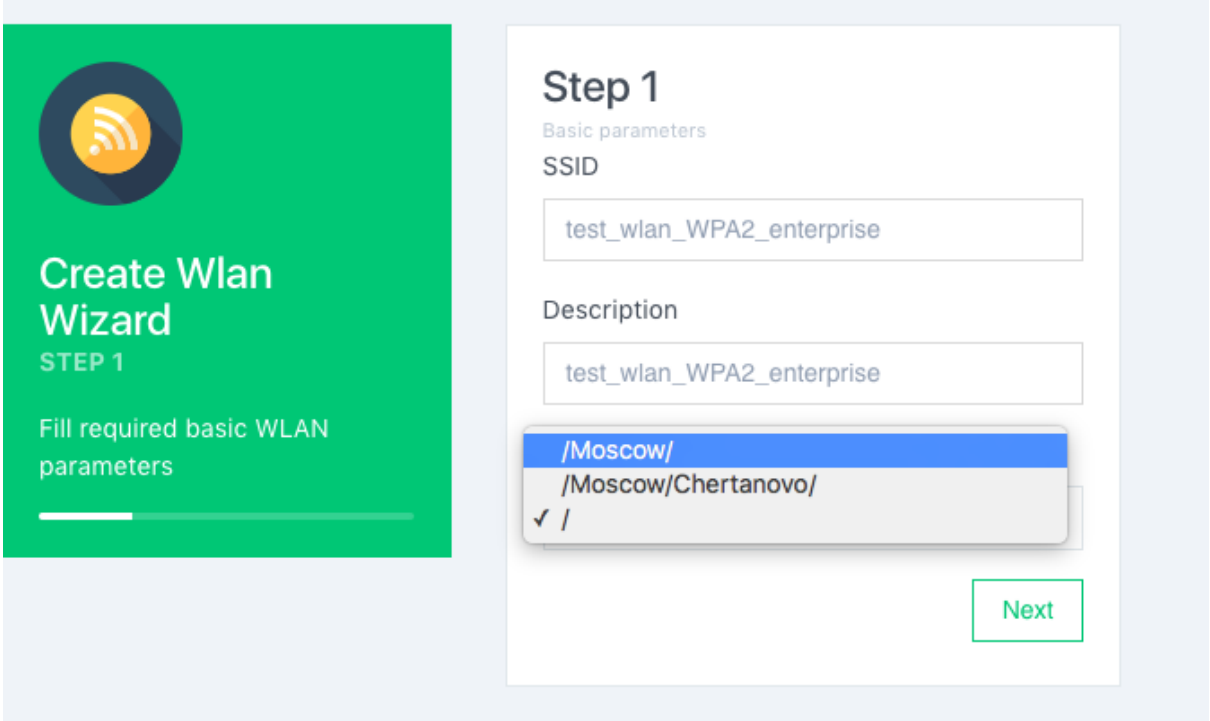


Рисунок 29. Добавление Описание и базисной локации для сети

Шаг 2. Выбираем ранее подготовленный RADIUS-сервер из списка связностей с RADIUS-серверов (Рисунок 30).

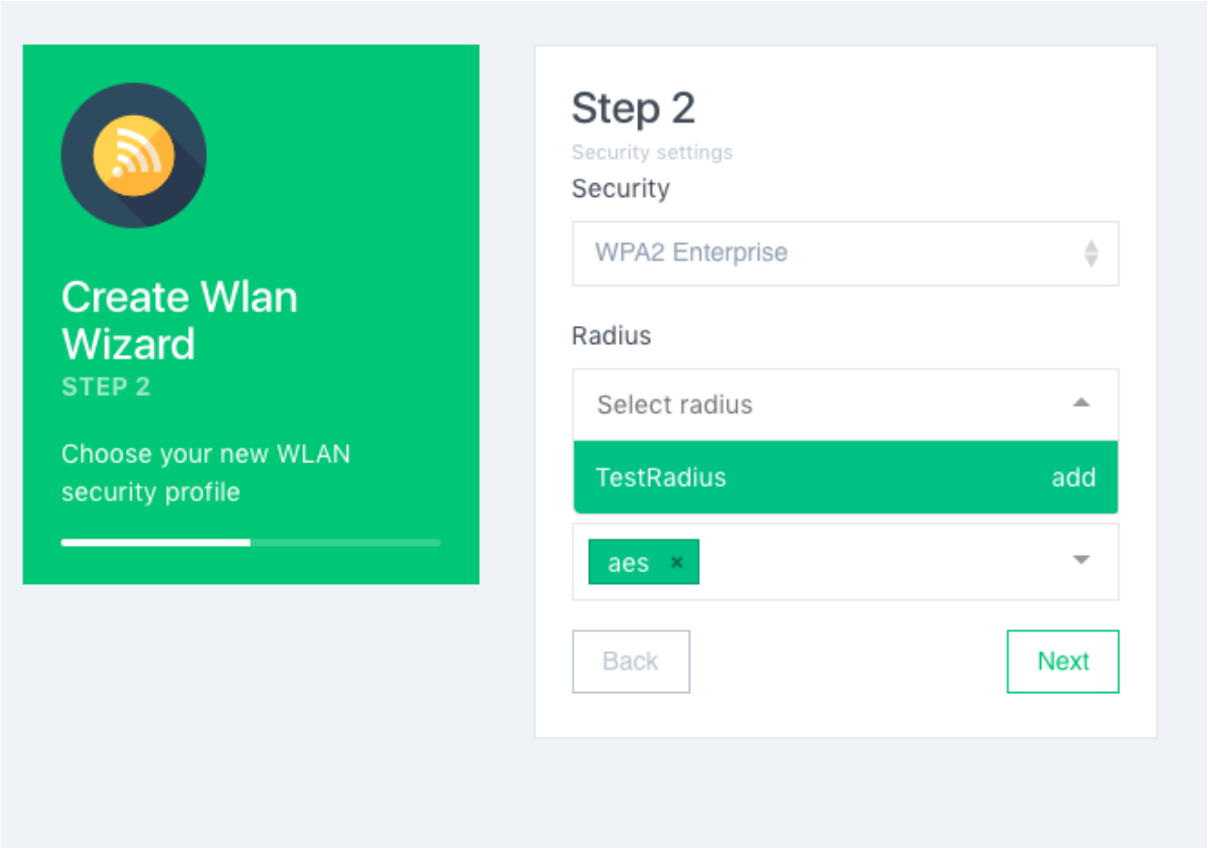


Рисунок 30. Выбор RADIUS-сервера

Шаг 3 (Рисунок 31).

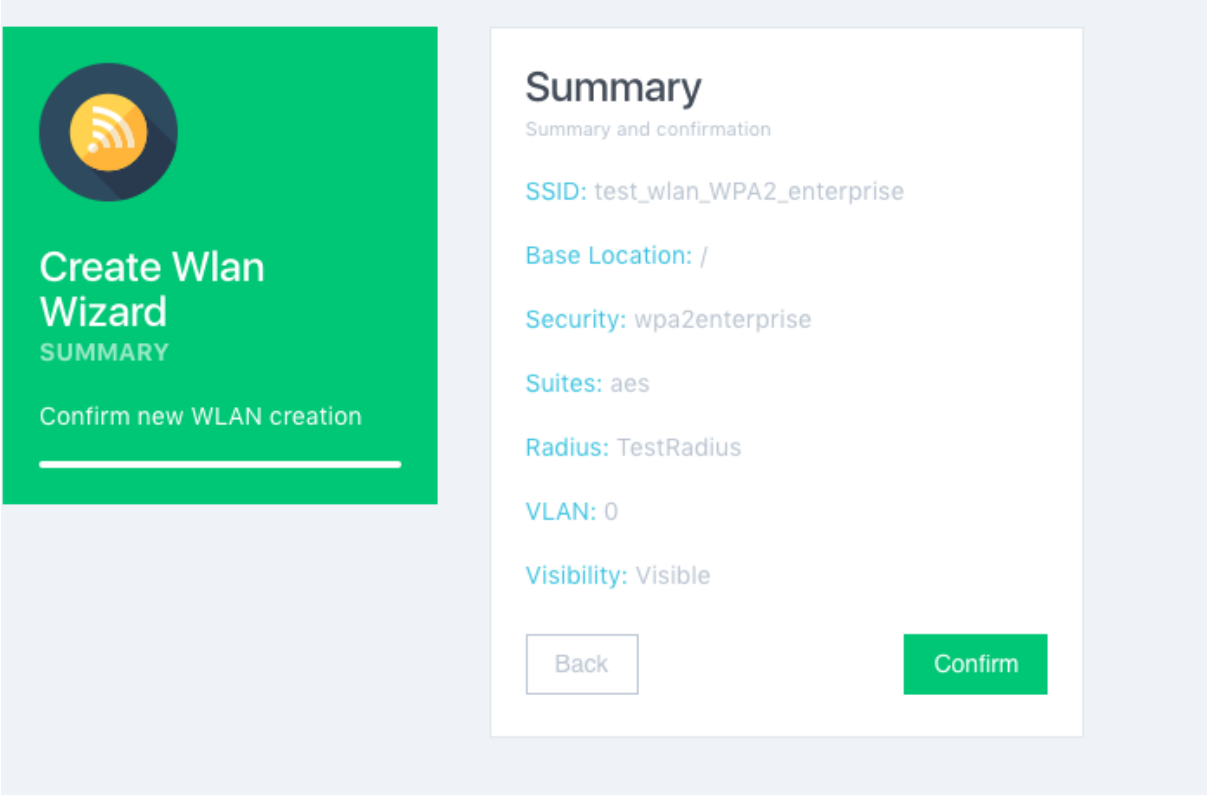


Рисунок 31. Предпоказ конфигурации нового WLAN

Далее при нажатии Confirm (Подтвердить) мы увидим список беспроводных сетей, содержащий только что созданный объект конфигурации беспроводной сети.

4.5.2.5. Дополнительные настройки WLAN

Для того, чтобы перейти в дополнительные настройки беспроводной сети WLAN нужно:

- выбрать в главном меню (вертикальное меню слева) раздел WLANs (Сети Wi-Fi);
- перейдя в таблицы WLANs, нужно нажать на нужный для редактирования WLAN (Рисунок 32).

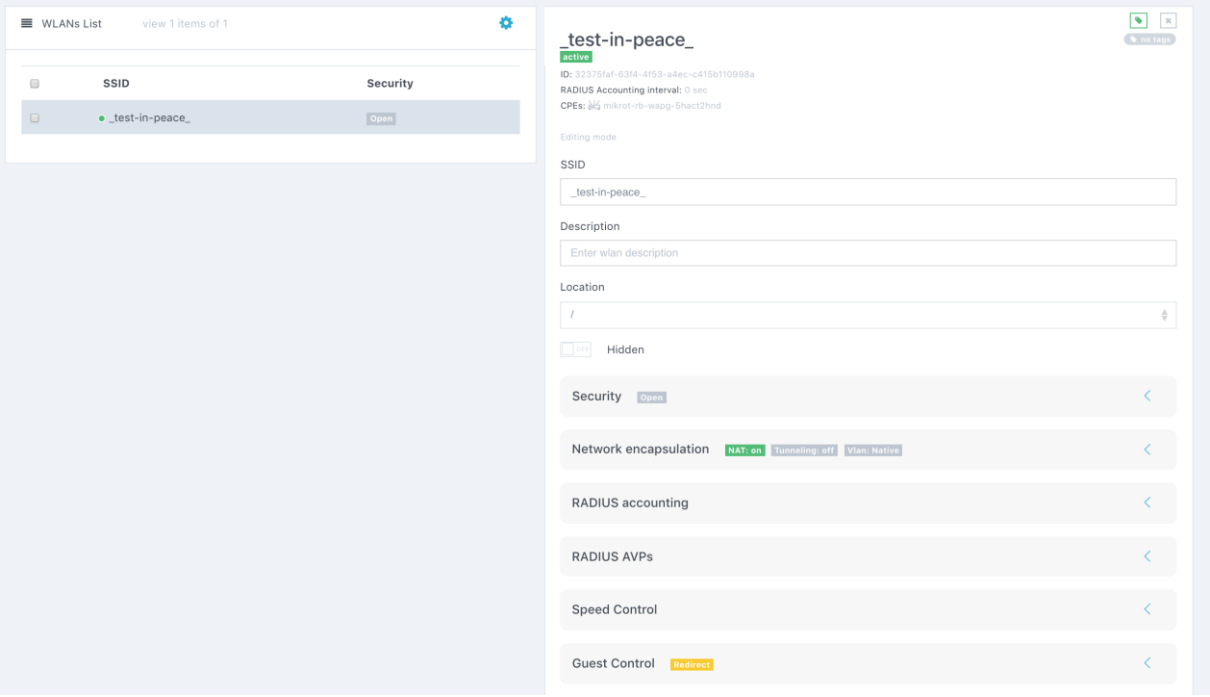


Рисунок 32. Дополнительные настройки беспроводной сети WLAN

После нажатия пользователь попадает в меню настройки отдельной WLAN (Сети Wi-Fi).

Меню настройки беспроводной сети разделено на несколько частей.

Основные настройки – это те самые настройки, которые заполняются при создании WLAN (Рисунок 33).

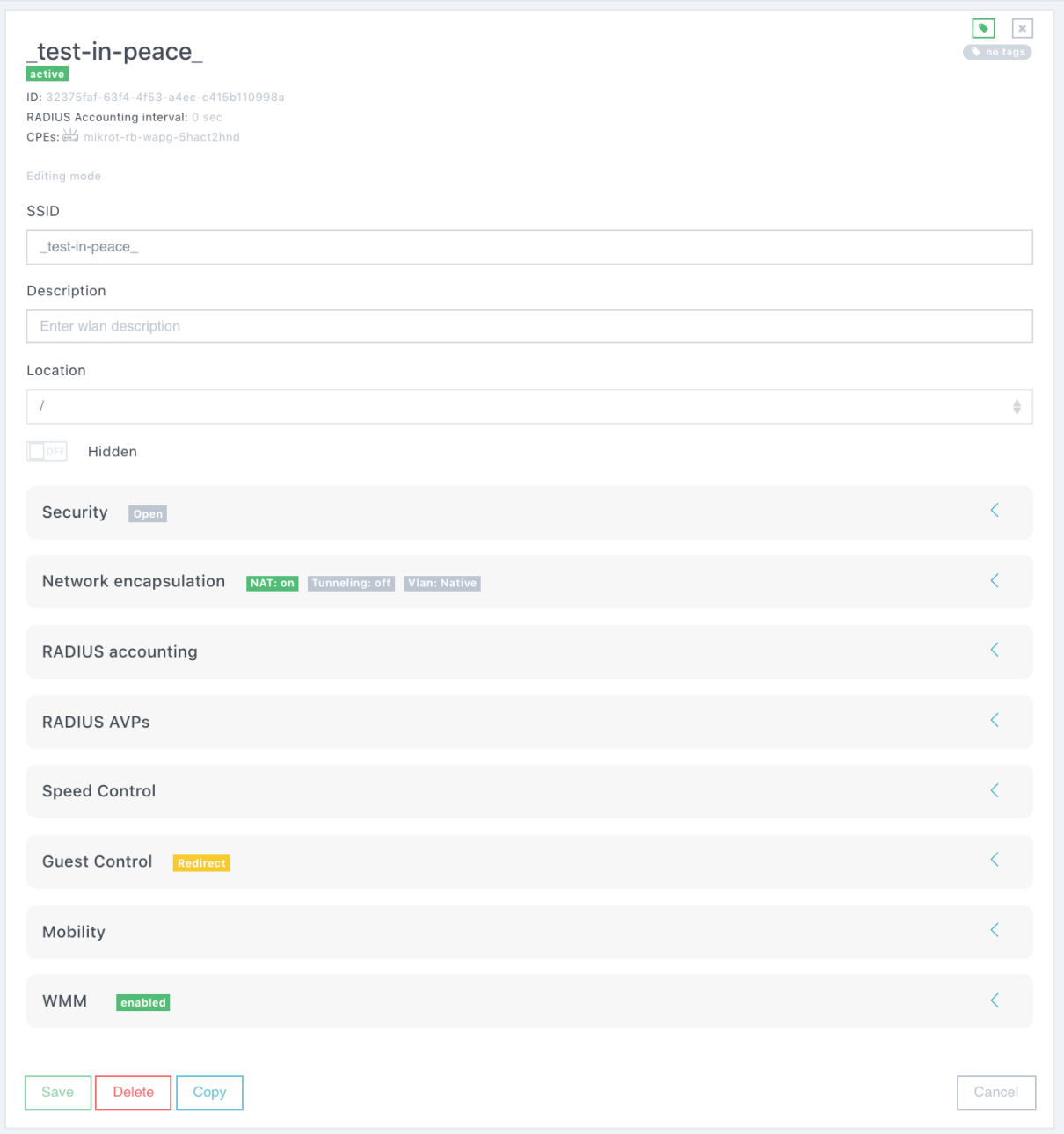


Рисунок 33. Основные настройки WLAN

Помимо стандартной настройки SSID, локации и VLAN здесь представлена информация о статусе (ТД, на которых WLAN активен), WLAN ID в системе. Также присутствует кнопка добавления “Tag” для этой беспроводной сети.

Следующей частью настройки является Security (Безопасность). Для того, чтобы получить доступ к информации, содержащейся в этом блоке, нужно нажать на кнопку, находящуюся в правом верхнем углу блока (Рисунок 34).

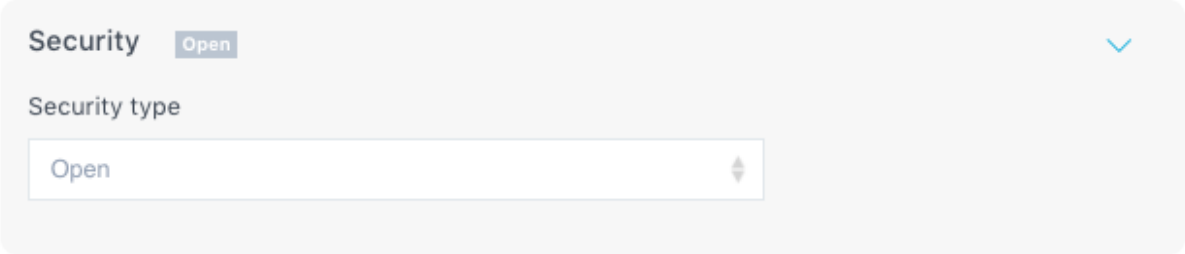


Рисунок 34. Выбор типа настройки безопасности WLAN

В данном блоке можно поменять тип настройки безопасности WLAN.

Следующий блок ответственен за настройку инкапсуляции трафика с WLAN.

Для того чтобы сконфигурировать туннелирование на QWP-VC, нужно включить переключатель туннелирования и выбрать интерфейс хостовой системы, в который предполагается коммутировать трафик беспроводных пользователей (Рисунок 35).

Настройка контроллера для обработки туннелированного трафика приведена в Приложении 1.

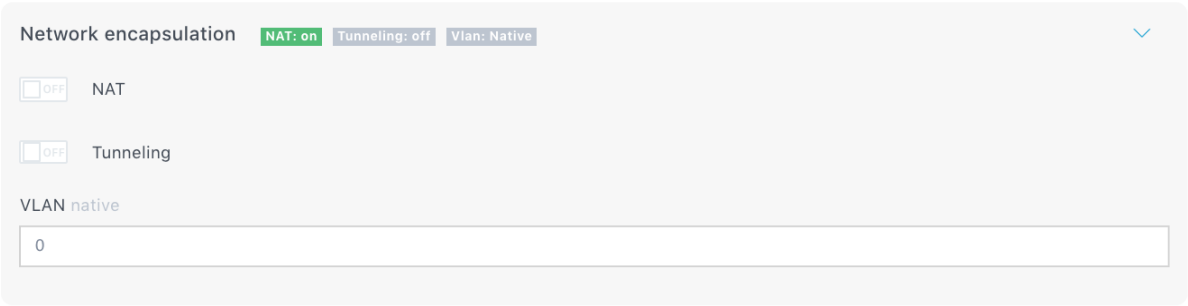


Рисунок 35. Настройка инкапсуляции трафика с WLAN

Также в данном пункте можно настроить тегирование или туннелирование трафика (на платформу), либо использование NAT непосредственно на ТД (Рисунок 36).

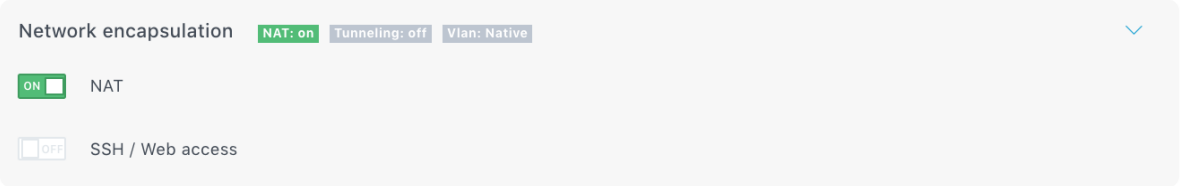


Рисунок 36. Настройка тегирования или туннелирования трафика

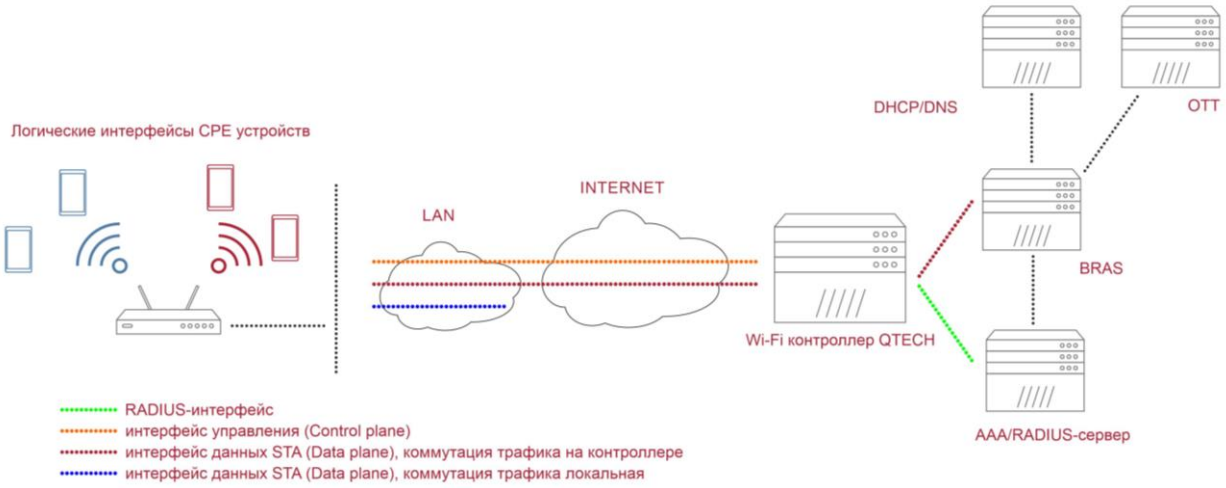


Рисунок 37. Одна из возможных схем туннелирования

Далее идет пункт настройки передачи аккаунтинговой информации на RADIUS-сервер. QWP-VC дает возможность передачи аккаунтинговой информации для любого типа беспроводной сети (Рисунок 38).

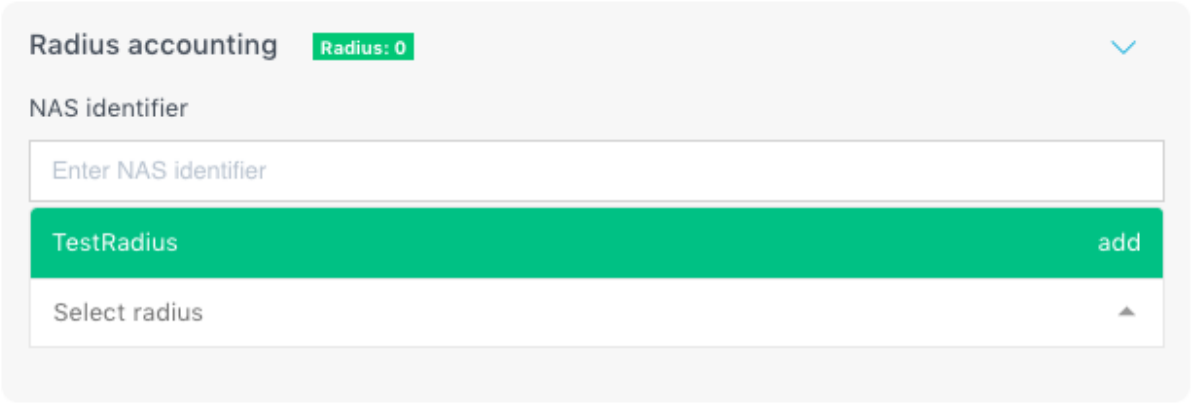


Рисунок 38. Настройка передачи аккаунтинговой информации на RADIUS-сервер

В данном блоке есть возможность выбрать RADIUS-сервер, на который будет передаваться аккаунтинговая информация. Также имеется возможность заполнить поле NAS identifier.

Блок Guest Control (Контроль доступа) осуществляет конфигурацию правил доступа к беспроводной сети (Рисунок 39).

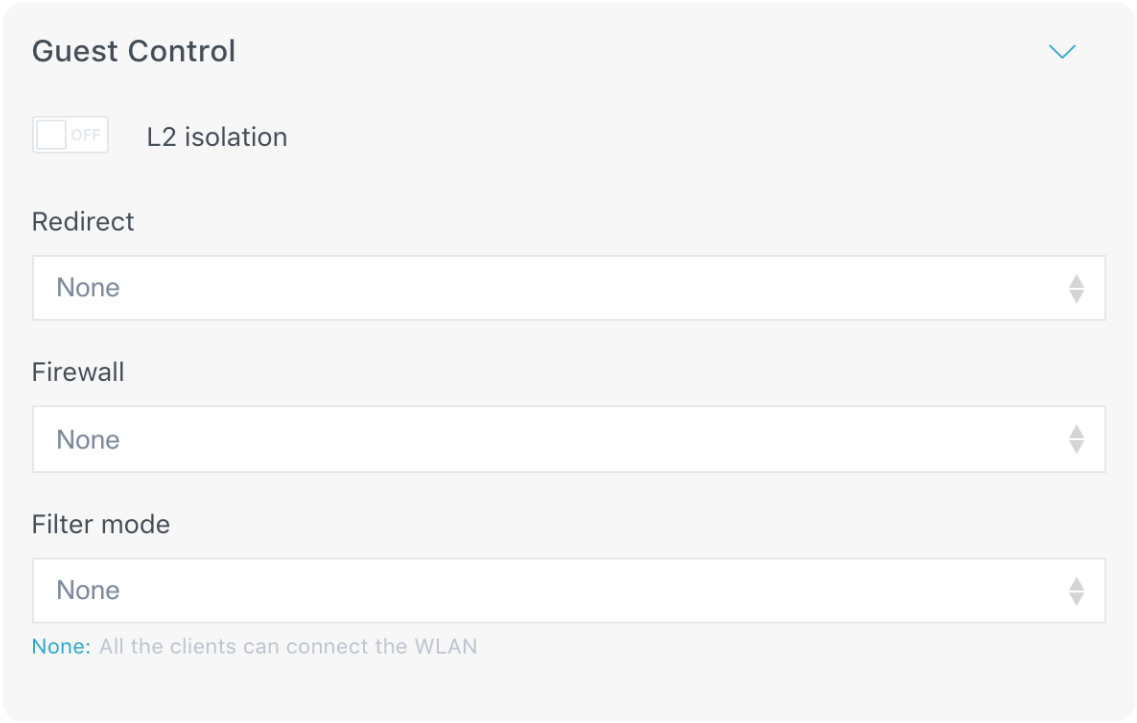


Рисунок 39. Конфигурация правил доступа к беспроводной сети

Блок управления доступом к беспроводной сети дает возможность выставлять ограничение на L2-связность беспроводных клиентов в рамках одной точки доступа (L2 isolation). Также есть возможность конфигурирования Black and White list (Белых и Черных листов) доступа, а также добавлять правило Firewall. В версии 0.10 добавлена возможность управления перенаправлением пользовательского трафика на Портал авторизации (Captive Portal) с помощью установки правила Redirect.

Далее имеются настройки WMM и настройки Roaming (Рисунок 40).

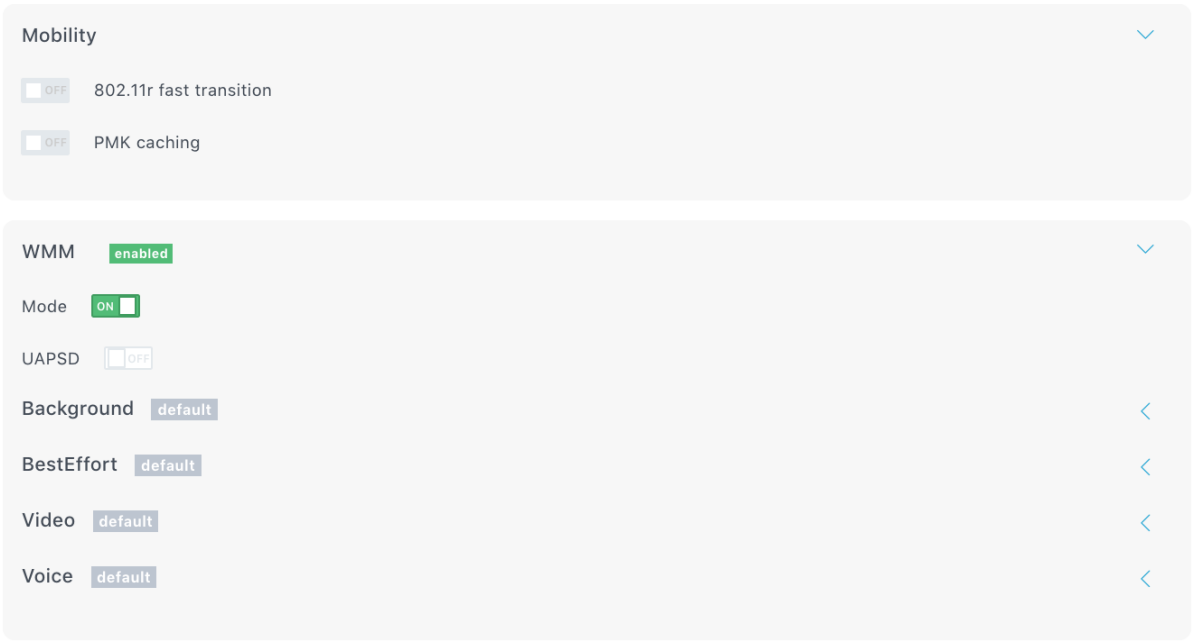


Рисунок 40. Настройки WMM и настройки Roaming

По завершению процедуры нажимаем на кнопку Save (Сохранить). WLAN переходит в состояние Updating (Обновление). Тем временем все ТД, на которых работает данный WLAN, меняют свою конфигурацию в соответствии с переданными настройками WLAN.

4.5.3. Создание и удаление связности с RADIUS-серверами

В это пункте описано создание объекта QNMS, который отвечает за AAA со сторонними RADIUS-серверами.

Для того чтобы создать связность с RADIUS-сервером нужно пройти следующие шаги:

Шаг 1. В главном меню (вертикальный блок в левой части экрана) выбрать поле RADIUS (Радиусы) и нажать (Рисунок 41).

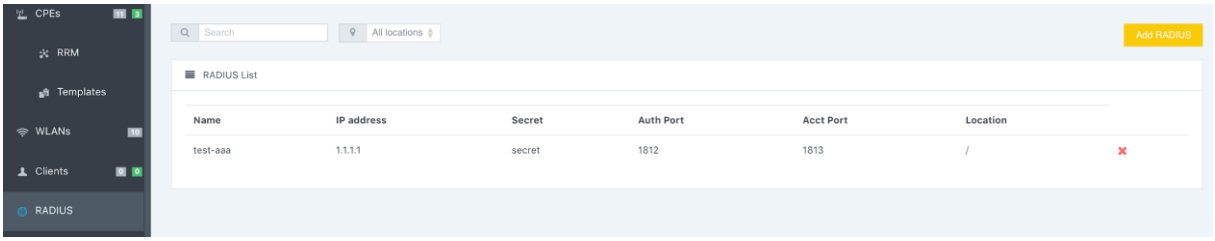


Рисунок 41. Выбор поля меню RADIUS (Радиусы)

Далее в правой части появится таблица, содержащая список всех доступных объектов связности с RADIUS-серверами.

Для того чтобы добавить новый объект RADIUS, нужно нажать на кнопку Add (Добавить) и воспользоваться мастером настройки связности с RADIUS-сервером, пройдя следующие шаги:

Шаг 1. Мы настраиваем название объекта QNMS RADIUS, IP-адрес, по которому QWP-VC будет передавать RADIUS-сообщение и локацию, в которой доступен данный объект (Рисунок 42).

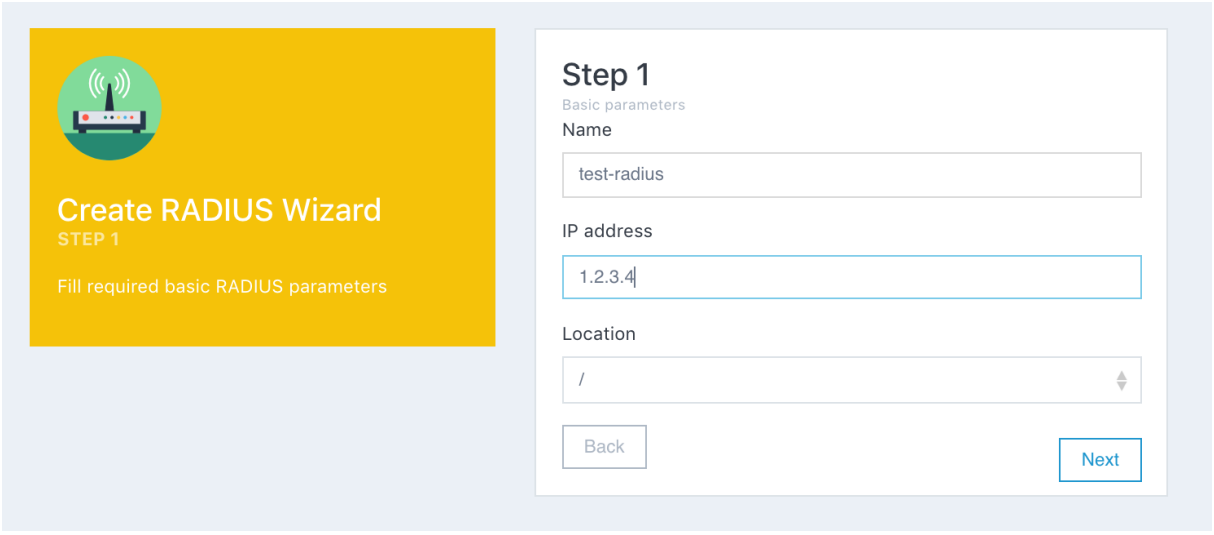


Рисунок 42. Создание и начальные настройки RADIUS

Шаг 2. На данном шаге мы заполняем поля пароля для RADIUS-подключения. Также имеется возможность изменить стандартные порты, которые используются для подключения к RADIUS-серверу (Рисунок 43).

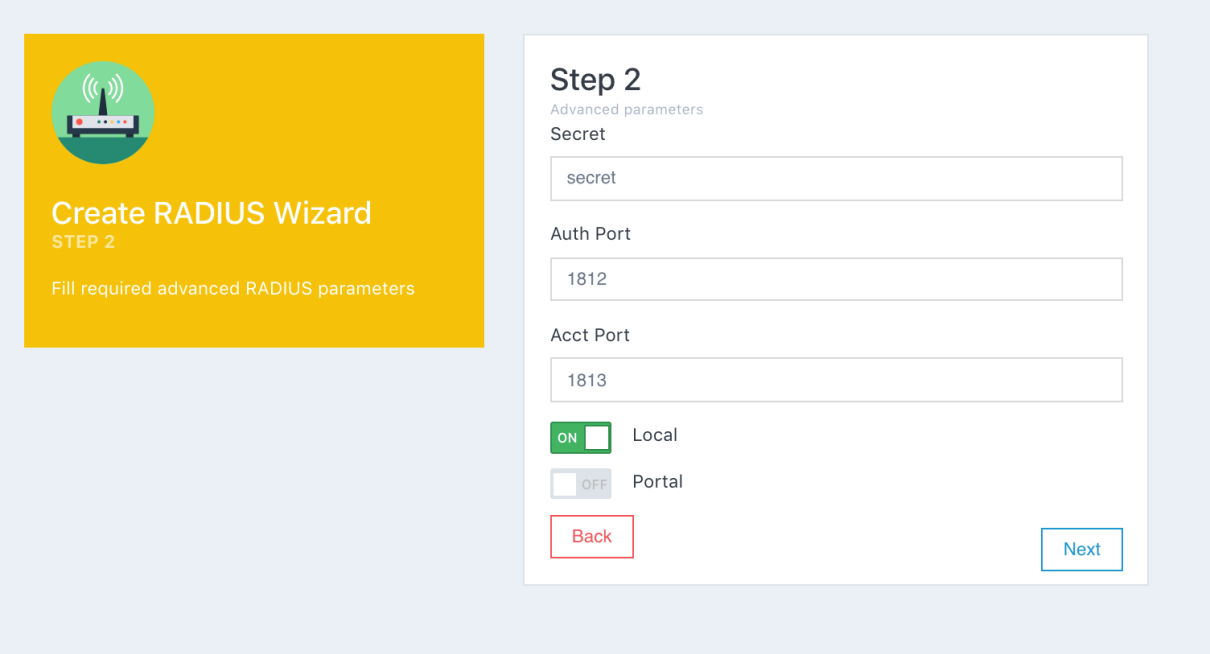


Рисунок 43. Установка пароля для RADIUS-подключения и изменение портов

Шаг 3. На котором мы видим все параметры получившегося объекта QNMS RADIUS (Рисунок 44).

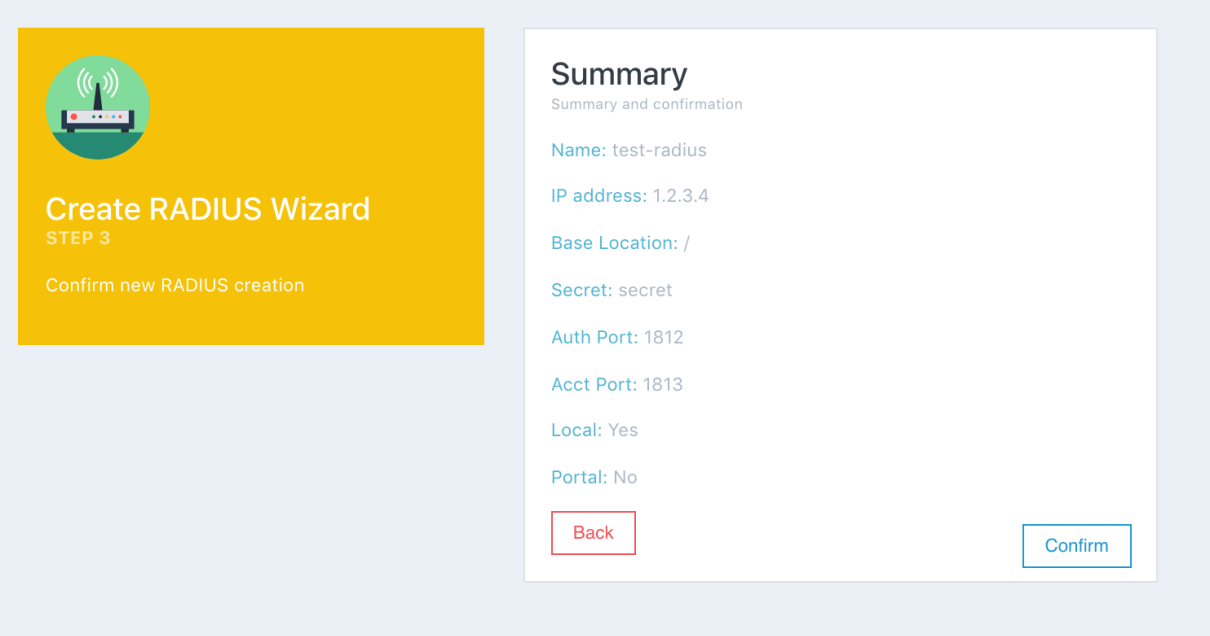


Рисунок 44. Предпоказ параметров получившегося объекта QNMS RADIUS

ПРИМЕЧАНИЕ: Настройка Portal отвечает за связь данного объектами типа RADIUS-сервер с внешним сервером для отправки аккаунтинговой информации при интеграции с внешними порталами авторизации.

Далее при нажатии Confirm (Подтверждения) новый объект успешно создается и добавляется в таблицу.

Для редактирования уже существующего объекта выбираем нужный нам объект QNMS RADIUS и нажимаем на него (Рисунок 45).

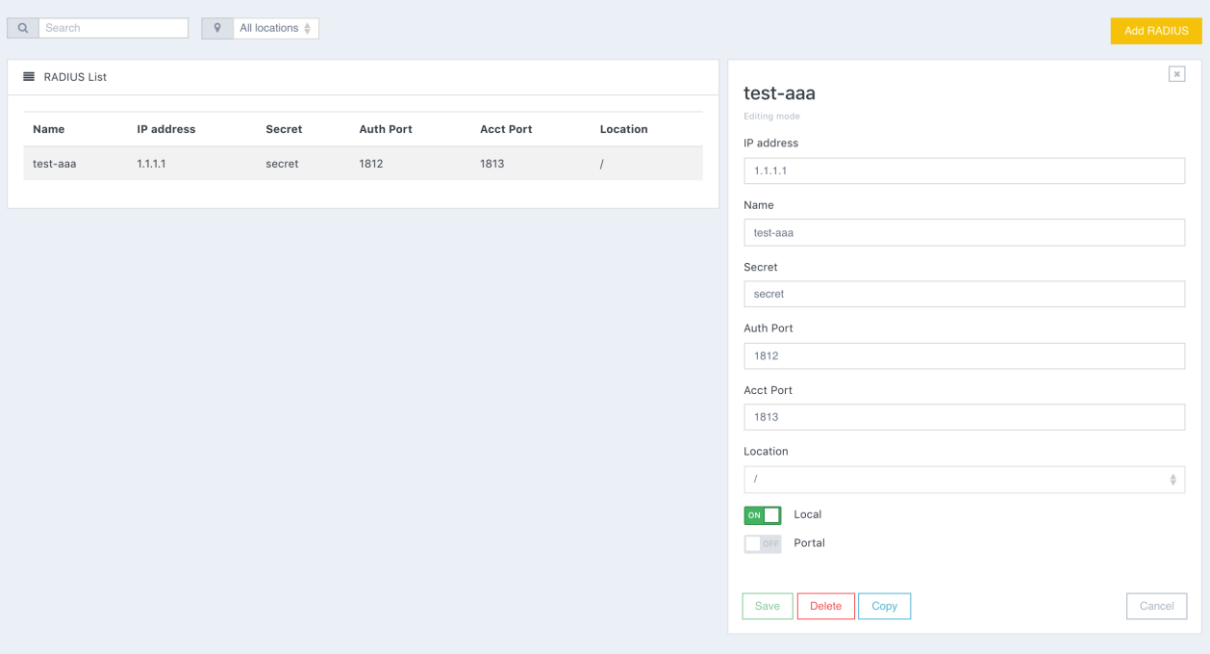


Рисунок 45. Редактирование уже существующего объекта QNMS RADIUS

После нажатия появляется возможность редактировать те же самые поля, что и при создании объекта.

4.6. Добавление WLAN на точки доступа

Для того чтобы сконфигурировать беспроводную сеть (WLAN) на ТД с помощью Веб-интерфейса QNMS, нужно в блоке главного меню (вертикальный блок меню слева) нажать секцию Access Points (Точки доступа) (Рисунок 46).

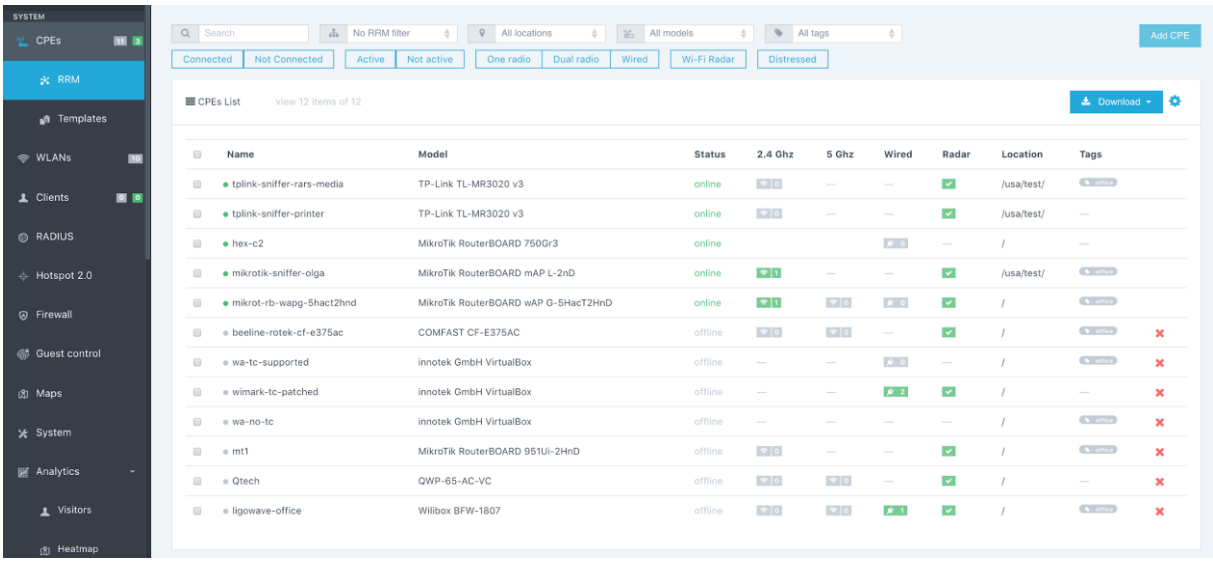


Рисунок 46. Таблица всех точек доступа

При нажатии на меню “Точки доступа” вы переходите в блок с таблицей всех точек доступа из всех доступных локаций вашего пользователя (базисная и подлокации).

Для того чтобы установить беспроводную сеть на беспроводной интерфейс точки доступа, нужно выполнить следующие шаги:

- нажать на объект ТД (ряд в таблице ТД);
- после нажатия в правом углу появится меню конфигурирования отдельной ТД (Рисунок 47).

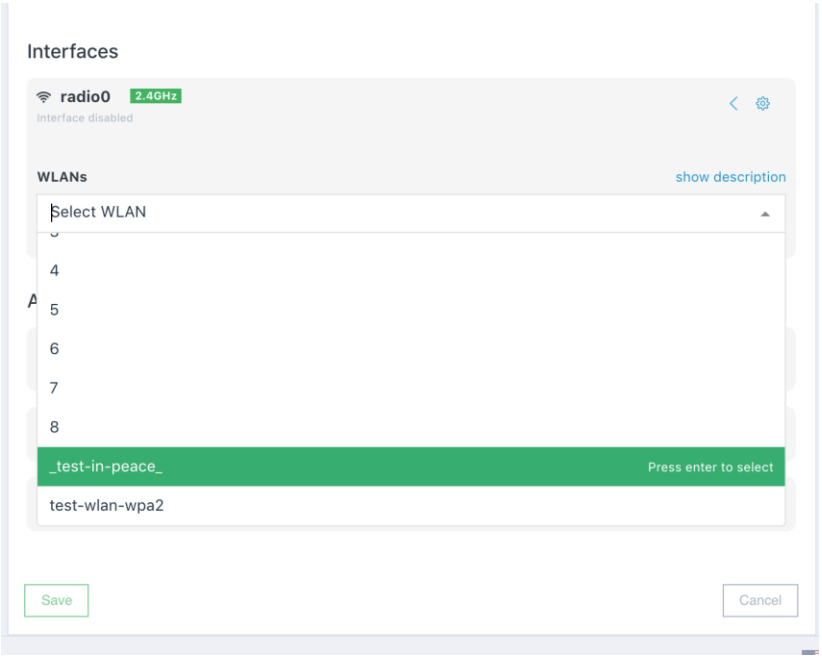


Рисунок 47. Меню конфигурирования отдельной ТД

ТД всегда имеет один или более беспроводных интерфейсов. В конфигурацию беспроводного интерфейса входит добавление WLAN для вещания в радиоэфире. Для этого нужно нажать на выпадающий список “WLAN” и в нем можно выбрать все доступные пользователю объекты WLAN.

ПРИМЕЧАНИЕ: Максимальное количество SSID на один беспроводной интерфейс равно 8 SSID (в некоторых платформах 4).

- Для выполнения конфигурации нужно нажать на кнопку Save (Сохранить). После этого QNMS заблокирует взаимодействие с объектом ТД до тех пор, пока ТД не перейдет в конечный статус Ok/Error.

4.7. Работа с правилами Firewall

4.7.1. Создание/Удаление правил Firewall

Для создания/редактирования/удаления правил Firewall необходимо использовать меню Firewall (Рисунок 48).

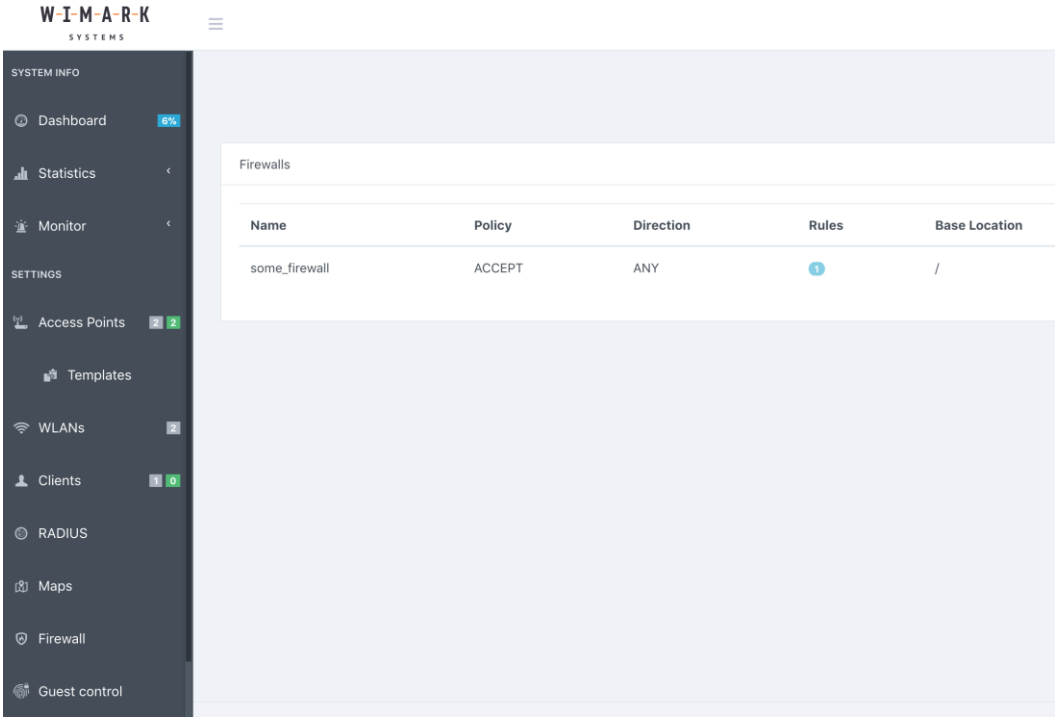


Рисунок 48. Меню Firewall

Правила могут содержать политики управления доступом на уровне L2 (по MAC-адресам устройств), уровне L3 (по IPv4), а также на уровне L4 (по типу IP Protocol).

Создание Firewall осуществляется через Add Firewall с введением имени, базовой политики (ACCEPT/DROP), а также базового Direction (IN/OUT/ANY) (Рисунок 49).

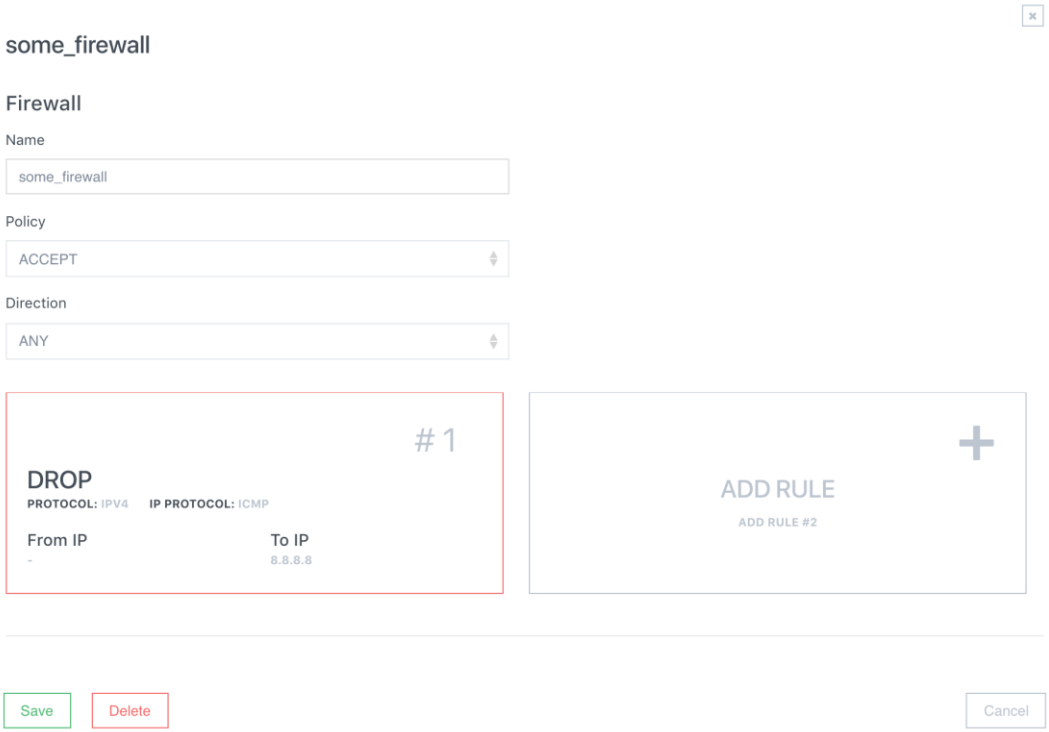


Рисунок 49. Создание Firewall

Для изменения Firewall необходимо нажать на него в таблице, изменить требуемые поля или добавить новые правила в цепочку Firewall (Рисунок 50).

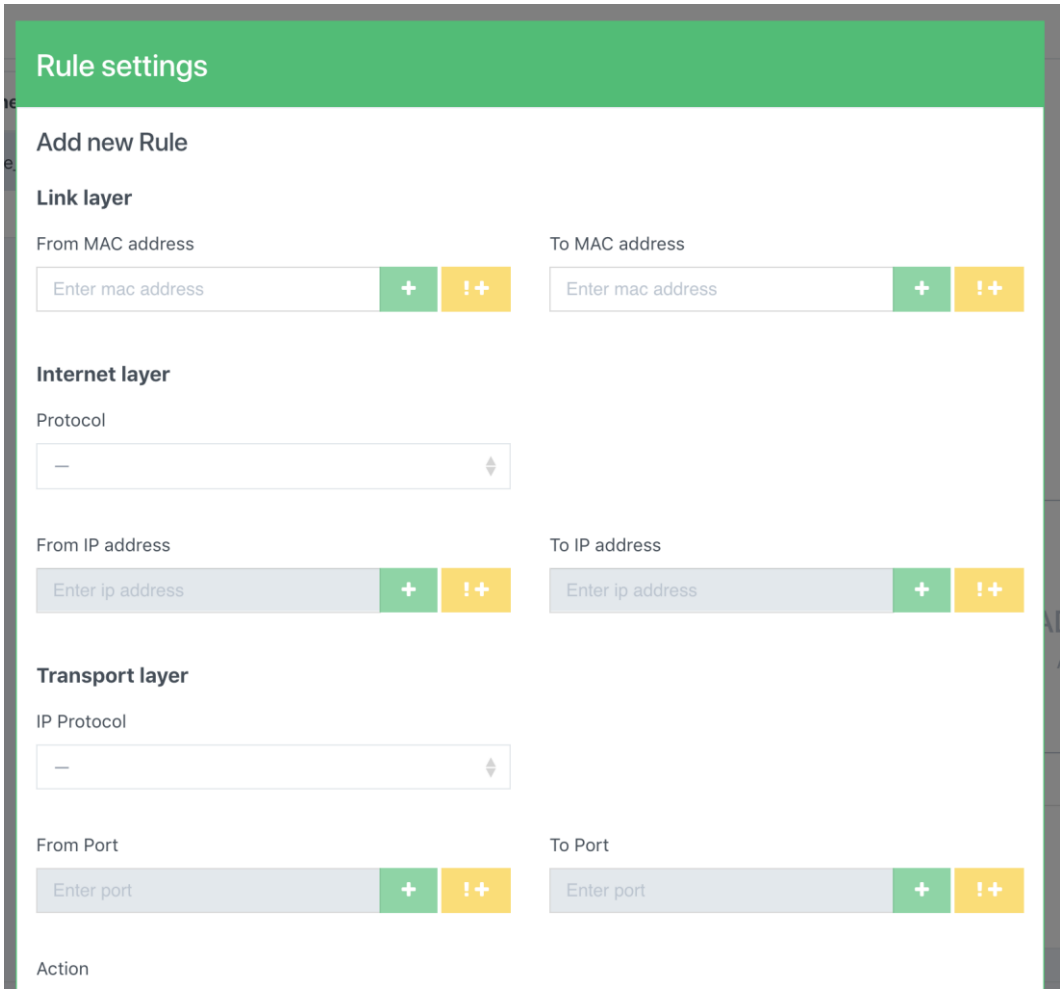


Рисунок 50. Настройка и изменения Firewall

После сохранения цепочки Firewall правило перегружается на связанных WLAN или AP.

Связать Firewall с WLAN можно на странице WLANs –> Edit mode. Связать с Точкой доступа можно на соответствующей странице изменения конфигурации точки доступа.

4.7.2. Создание/Удаление правил Redirect

В версии 0.10 добавлена возможность настраивать перенаправление пользовательского трафика на портал авторизации (Captive Portal). Настройка соответствующих правил находится в меню на странице Guest Control (Рисунок 51).

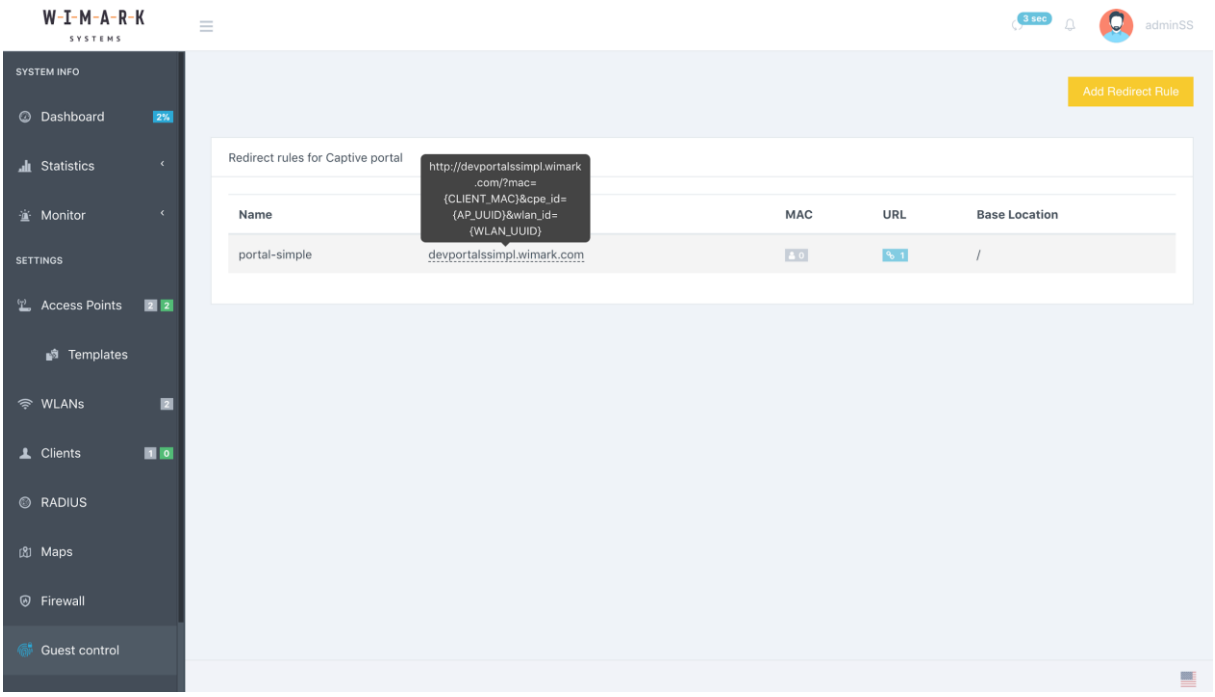


Рисунок 51. Настройка перенаправления пользовательского трафика на портал авторизации

Для создания правила необходимо нажать на кнопку Add Redirect Rule над таблицей (Рисунок 52).

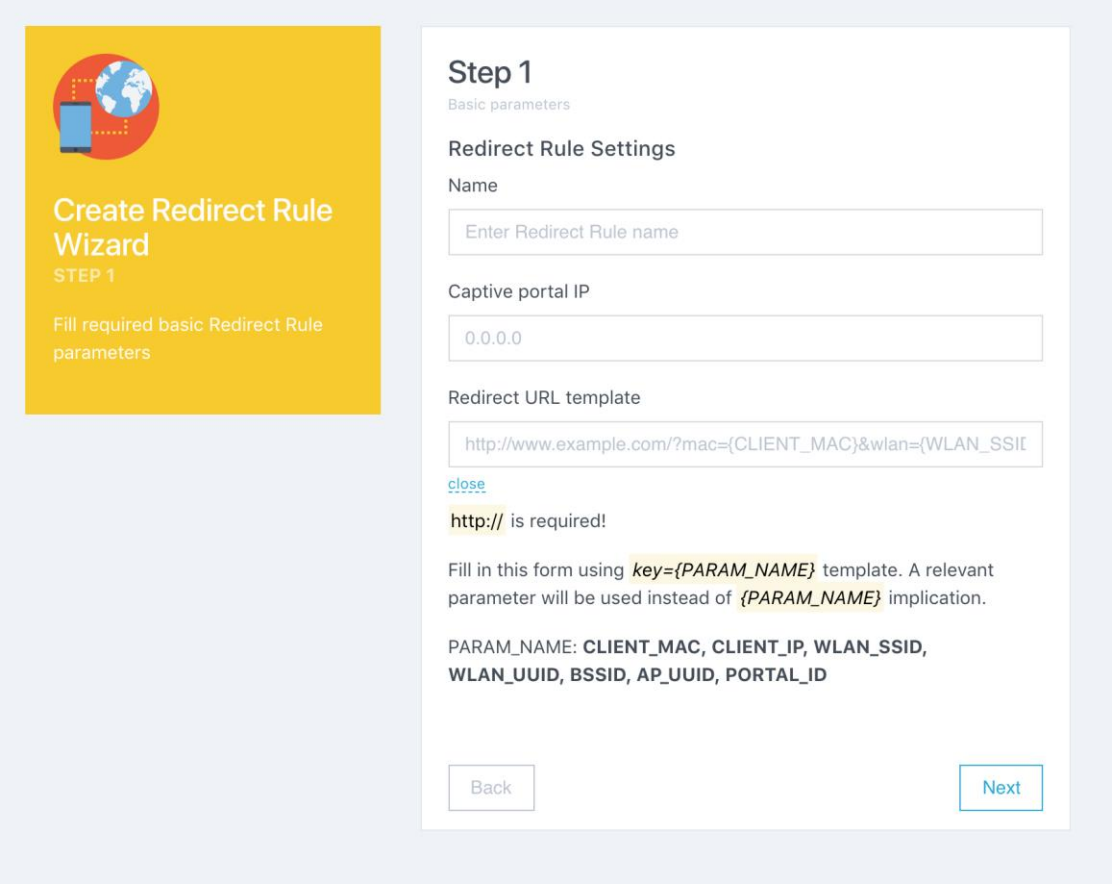


Рисунок 52. Создание правила перенаправления

В соответствующем окне необходимо указать имя правила, IP-адрес портала авторизации, а также URL, с которым пользователи будут перенаправляться на портал, в специальном формате.

Пример URL:
http://portal.wimark.com/?mac={CLIENT_MAC}&cpe_id={AP_UUID}&wlan_id={WLAN_UUID}&switch_url=http://dev.wimark.com/api/authorize&client_ip={CLIENT_IP}

При указании такого URL, на портал авторизации поступит пользователь с реальными MAC, CPE_ID, IP и WLAN_ID, которые могут быть использованы для идентификации пользователя на портале.

На второй странице окна создания правила перенаправления можно указать список белых MAC-адресов, которые не будут перенаправляться на портал авторизации, а также список доступных без авторизации IP.

Рекомендуем для работы IOS устройств добавлять в белый список адрес captive.apple.com с указанием реального текущего IP-адреса этого домена.

Правила перенаправления можно добавлять на WLAN в разделе редактирования в блоке Guest Control. Одно правило можно добавить на один WLAN, при этом несколько WLAN могут использовать одно правило.

4.8. Шаблоны конфигурирования

4.8.1. Общие принципы работы шаблонов

Шаблон – набор параметров конфигурации конечного оборудования (ТД), который может быть установлен на одно или группу устройств. Шаблоны WNMS можно классифицировать следующим образом:

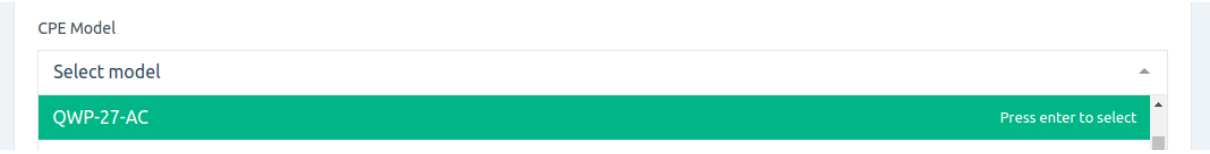
- Шаблоны, применяемые при первом подключении устройства. То есть набор настроек, описанных в шаблоне, применяется только при первом подключении устройства к WNMS. Данная функция регулируется параметром Always apply и должна быть выставлена в OFF.

- Шаблоны, применяемые при каждом подключении. Для применения конфигурации, описанной в шаблоне, при каждом подключении требуется переключить параметр Always apply в состоянии ON.

- Используемые шаблоны. То есть те, которые используются при конфигурации. Неиспользуемые шаблоны нужны лишь для хранения информации о конфигурации и не используются при конфигурировании устройств. Для того чтобы перевести шаблон в состояние “используемый”, нужно поменять параметр Auto configuration и выставить значение ON.

Шаблоны конфигурации для определенной модели. При использовании параметра Model CPE шаблон приобретает функциональность устанавливать соответствующую ему

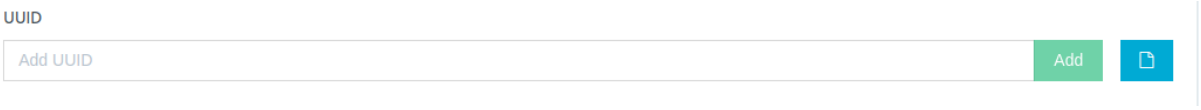
конфигурацию на соответствующую модель конечного оборудования, что также дает возможность конфигурировать специфические настройки беспроводных интерфейсов конечного оборудования.



- Шаблоны конфигурации без указания определенном модели. То есть те шаблоны, которые применяются ко всем CPE и соответственно имеют более общие настройки.

В таком типе шаблона нельзя конфигурировать специфические настройки радио интерфейса. В данном шаблоне возможно лишь определить, какие WLAN будут добавлены по умолчанию и некоторые общие дополнительные настройки CPE.

- Шаблоны конфигурации группы устройств. Для того, чтобы шаблон применялся для конфигурации группы устройств нужно определить группу устройств, как список их идентификаторов (CPE UUID доступны из WEB UI QWP-FW).



Для того чтобы создавать и менять шаблоны, нужно перейти в подменю Settings.CPES.Templates, находящееся в левой вертикальной панели WEB UI QNMS.

4.8.2. Создание шаблона с помощью помощника

Для создания шаблона в меню templates нужно нажать на кнопку Add Template (Рисунок 53).

Создание состоит из нескольких шагов:

Выбор условий срабатывания шаблона и его идентификаторов (имя, локация).

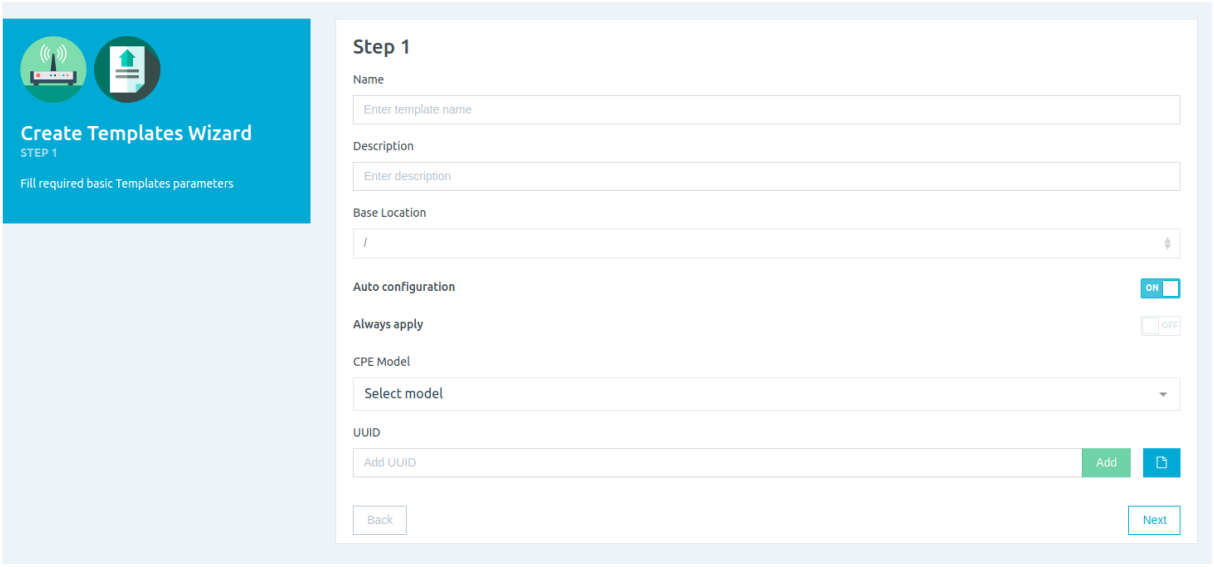


Рисунок 53. Создание шаблона и определение его идентификаторов (имя, локация)

Выбор специфических настроек характерных только определенным моделям (Рисунок 54).

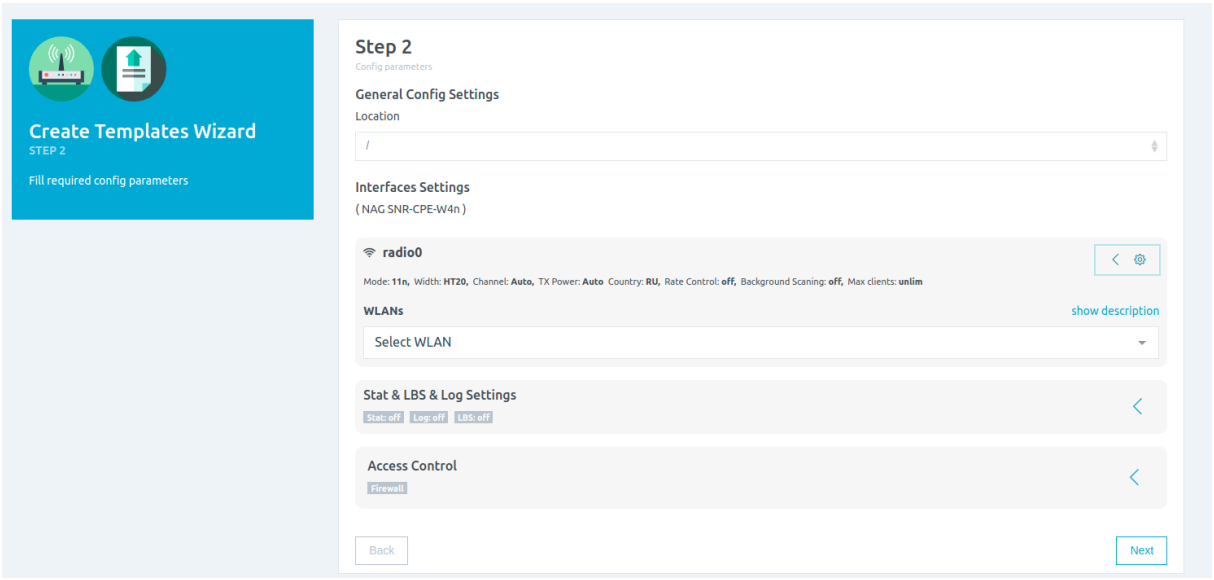


Рисунок 54. Выбор специфических настроек для определенных моделей

Настройка конфигурации подобна настройке конфигурации отдельной CPE.

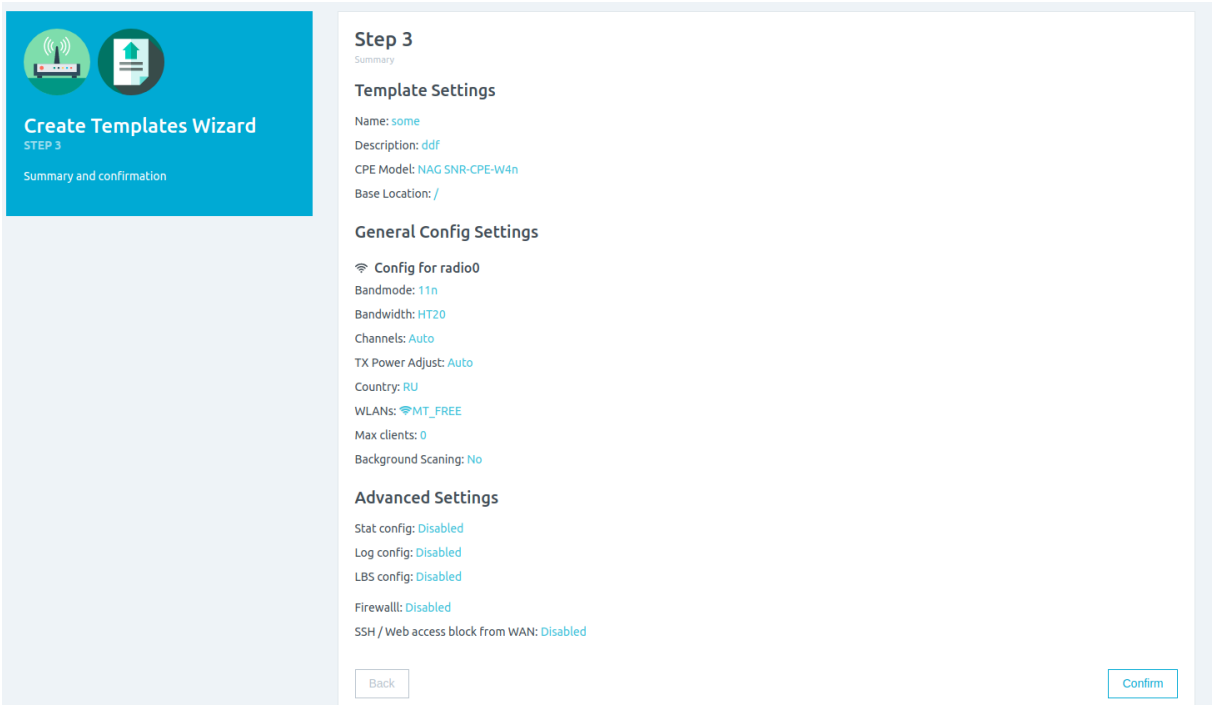


Рисунок 55. Подтверждение выбранных настроек

Сохраненные шаблон появляется в списке шаблонов (Рисунок 56).

Рисунок 56. Список шаблонов

4.8.3. Создание шаблона из уже имеющейся конфигурации

Для создания шаблона конфигурации из уже имеющейся конфигурации, подключенной ТД, нужно выполнить следующую последовательность действий:

Выбрать соответствующую CPE в списке подключенных CPE (Рисунок 57).

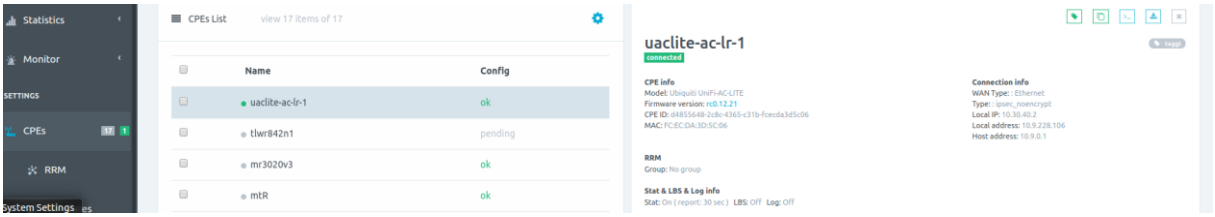


Рисунок 57. Список подключенных CPE

Нажать на кнопку генерации шаблона из конфигурации CPE. Create Template (Рисунок 58).

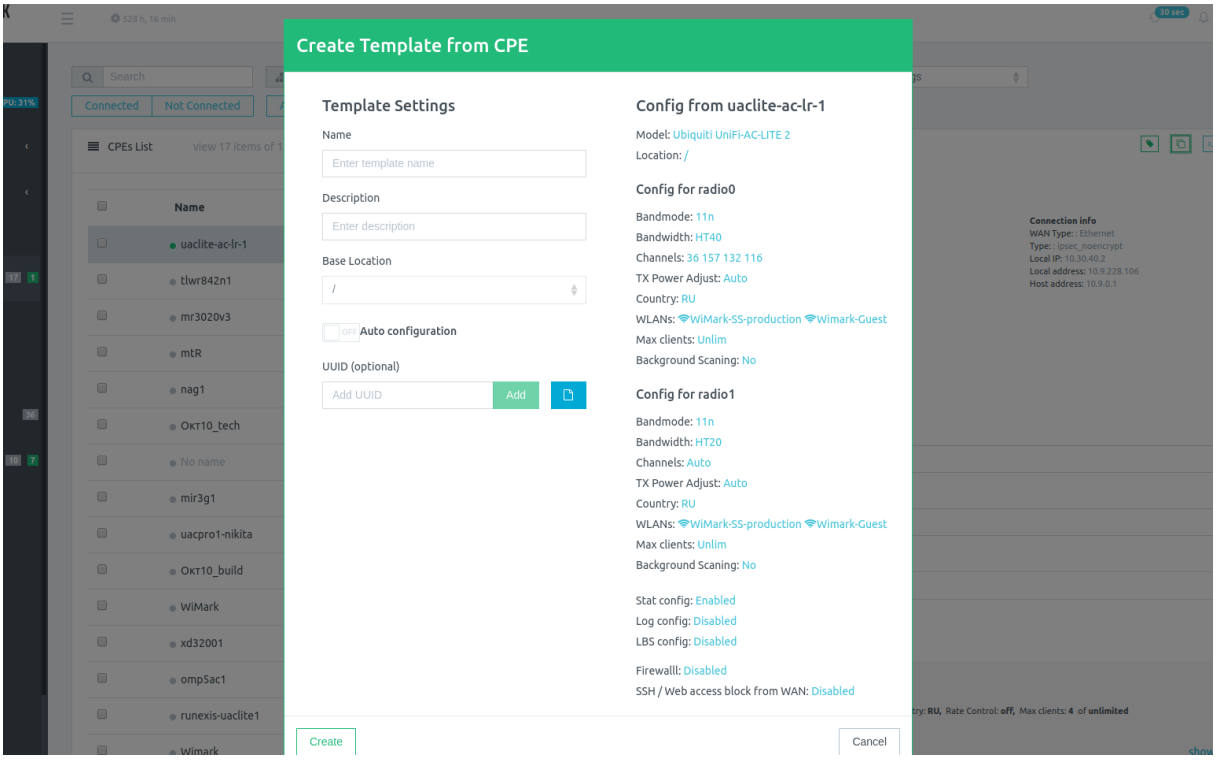


Рисунок 58. Генерация шаблона из конфигурации CPE

Далее нужно заполнить идентификаторы нового шаблона конфигурации, дополнив общими параметрами триггеров конфигурации и нажать кнопку save.

4.9. Работа с группами RRM

Ниже представлена последовательность действий для конфигурирования работы RRM-алгоритма на группе конечных ТД.

Подключаемся к платформе управления и переходим в меню RRM-групп (Рисунок 59).

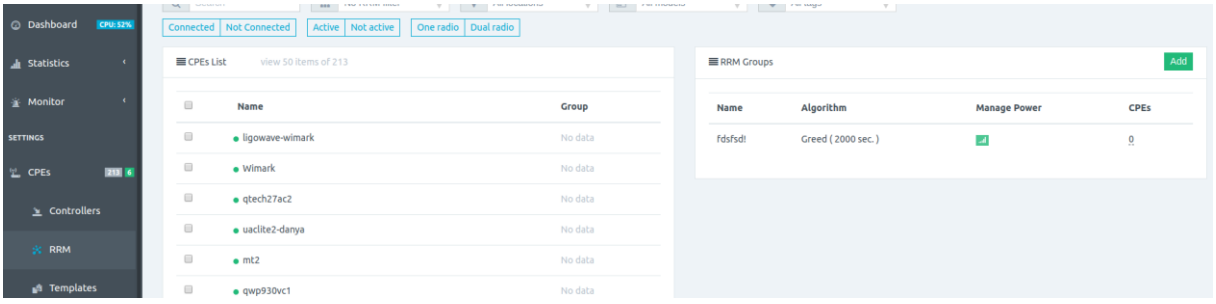


Рисунок 59. Список RRM-групп

Нажимаем кнопку Add (добавить) (Рисунок 60).

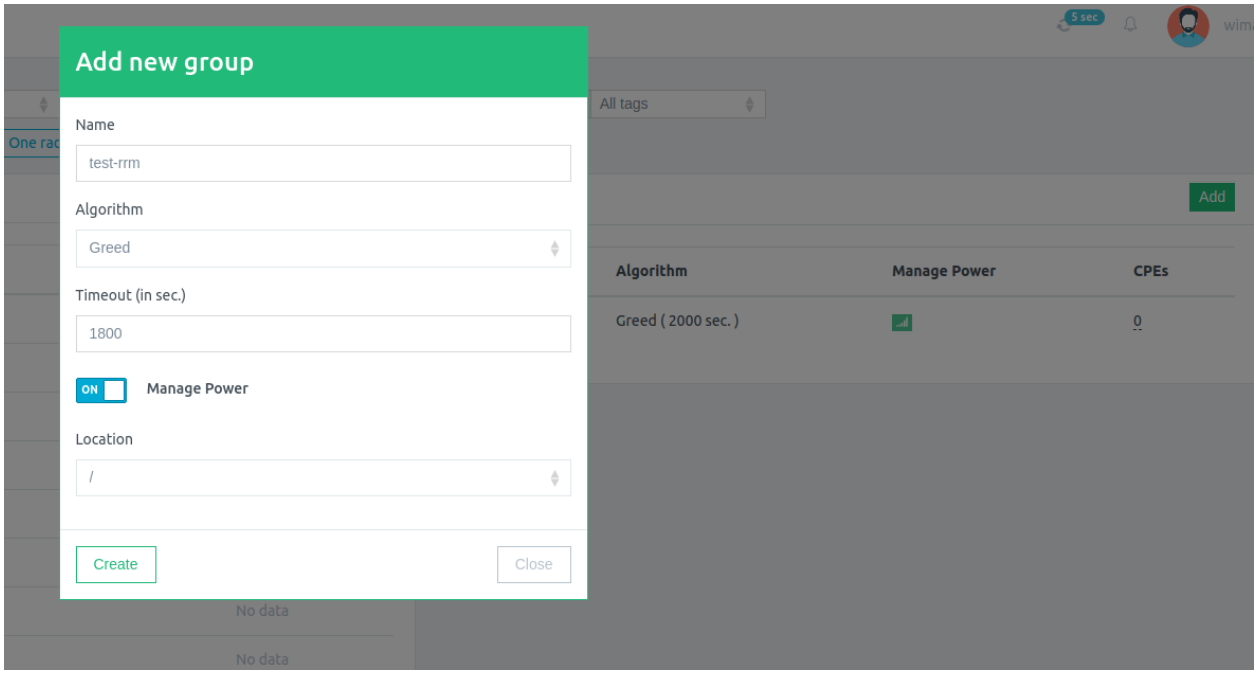


Рисунок 60. Создание новой группы RRM

Заполняем соответствующие поля:

Имя – имя объекта группы.

Алгоритм – алгоритм, который применяется для динамического конфигурирования мощностью и канала передачи конечного устройства.

Dummy – тестовый алгоритм, который не воздействует на устройства и используется для отладочного тестирования.

Greed – жадный алгоритм. В соответствующий момент времени выбирается оптимальный канал передачи для каждой из ТД. Метода выбора: канал, на котором ТД испытывает минимальную интерференцию. Алгоритм вычисляет оптимальную конфигурацию канала передачи для всей группы ТД.

Blind – алгоритм, который минимизирует вероятность пересечения каналов передачи конечных устройств.

Manage power – включить или выключить управление мощностью. Алгоритм оптимизирует мощность устройств в группе, работающих на одном канале передачи.

Location – к какой локации относится данный объект.

Timeout – период, через который происходит проверка радиообстановки и перенастройка (при надобности) радио модулей конечных устройств.

Нажимаем на кнопку create (создать).

Далее добавляем устройства в созданную группу.

Выбираем устройства в таблице (Рисунок 61).

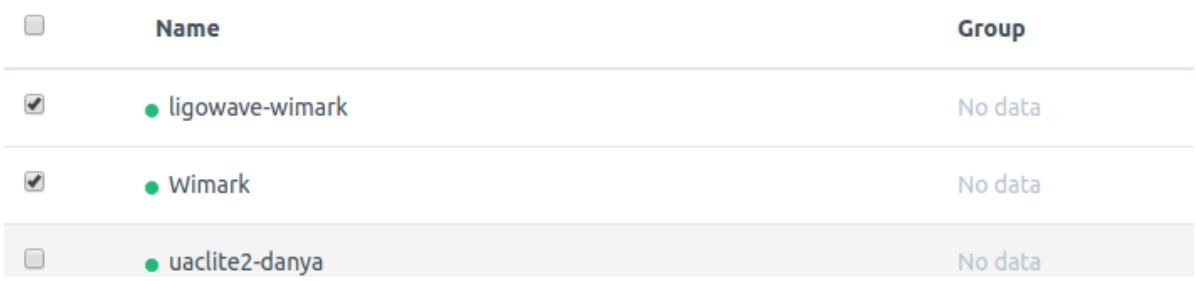


Рисунок 61. Выбор устройств для добавления в группу

Выбираем группу, в которую добавляем устройства (Рисунок 62).

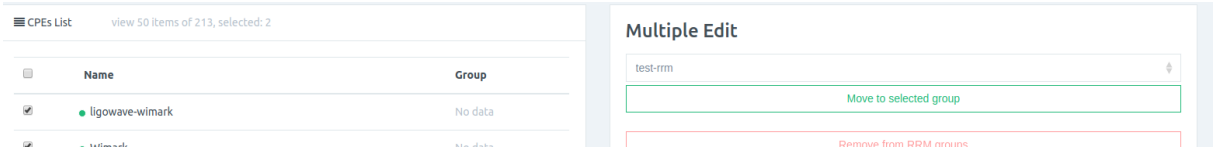


Рисунок 62. Выбор группы, в которую добавляем устройства

Нажимаем move to selected group.

Модуль RRM-платформы управления начинает действовать в соответствии с настройками RRM-группы.

4.10. Работа с картами

Объект Карты используется для визуального представления информации о точках доступа, таких как:

- статистика подключенных клиентов;
- статистика по трафику за указанный период;
- статистика о проходящих пользователях;
- тепловая карта проходящих пользователей.

4.10.1. Создание карт

Для создания карт необходимо перейти на страницу Maps и создать карту с помощью модального окна, открывающегося при клике на кнопку “Add Map”.

Предварительно необходимо подготовить картинку местности/офиса, а также указать примерный масштаб (выбрав 2 точки и указав кол-во метров).

После создания необходимо открыть новую карту и расставить на ней точки доступа.

ПРИМЕЧАНИЕ: Проходящие клиенты собираются только для точек, на которых активирован режим радара (Wi-Fi Radar).

4.10.2. Просмотр статистики

После расстановки точек на карте будет отображена информация по трафику, пользователям, а также проходящие клиенты и тепловая карта их местоположений. Данные постоянно добавляются, для обновления необходимо использовать кнопку “Refresh”.

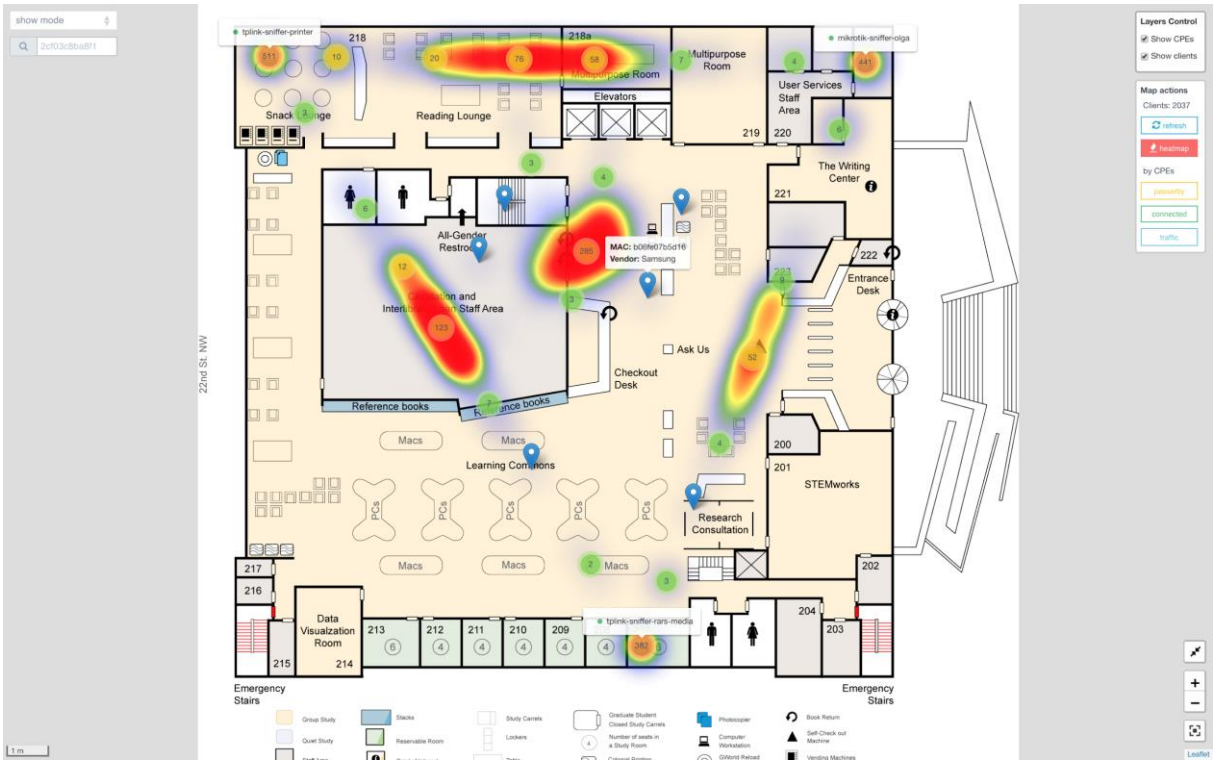


Рисунок 63. Пример карты

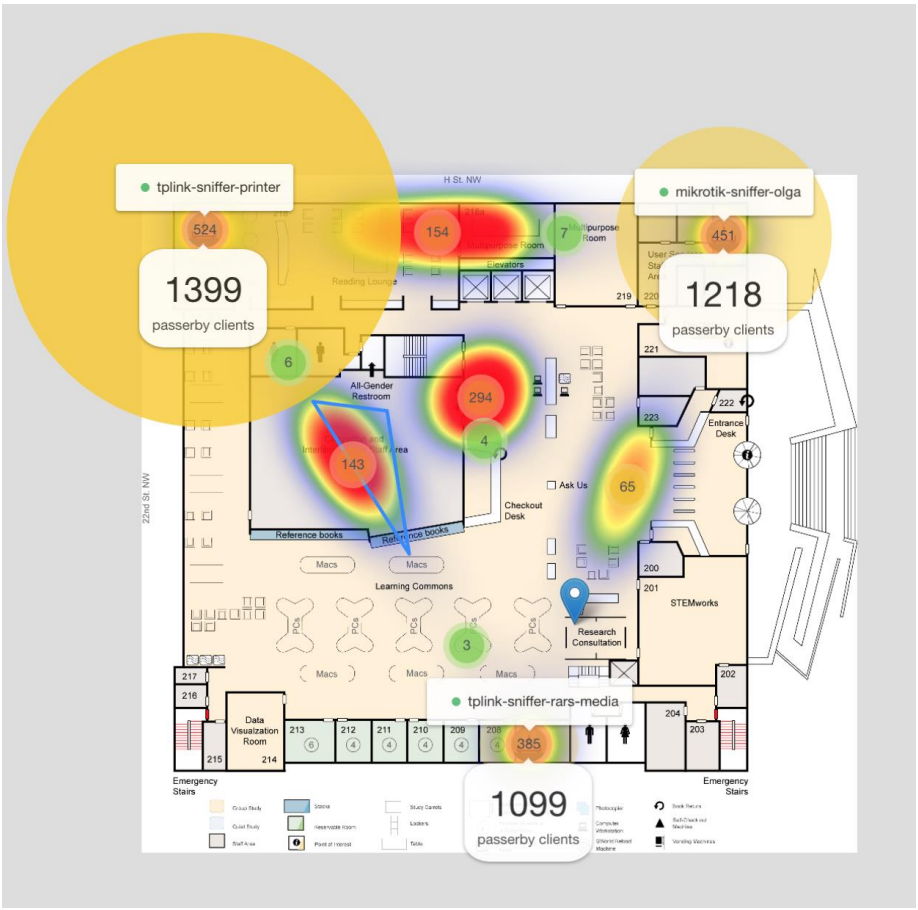


Рисунок 64. Пример карты

4.10.3. Просмотр пути пользователей

В режиме показа можно использовать строку поиска для поиска клиентских адресов. После можно выгрузить данные об его перемещении относительно расставленных точек доступа. Триангуляция работает при числе точек от 3-х.

Рисунок 65. Пример путей пользователей на карте

4.11. Просмотр общей статистики

QNMS позволяет просматривать статистику по следующим объектам:

- точки доступа;
- локации;
- WLAN-сети;
- клиенты беспроводных сетей.

Для просмотра необходимо использовать вкладку “Statistics” с необходимыми объектами (Рисунок 66). В настоящее время можно просматривать среднюю или суммарную статистику за период по:

- использованию CPU;
- использованию RAM;
- количество клиентов беспроводных сетей;
- количество уникальных проходящих клиентов.

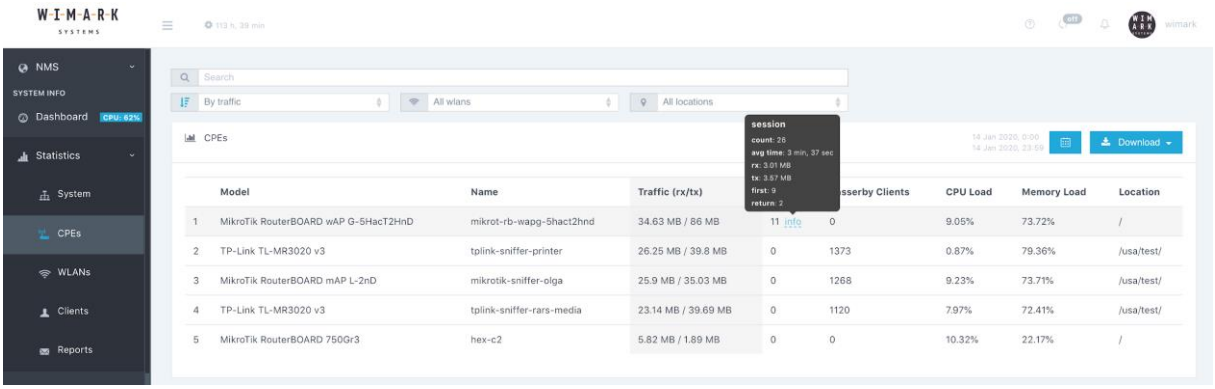


Рисунок 66. Просмотр статистики по объектам

По клику на точку можно перейти в раздел с временной диаграммой по данным метрикам (Рисунок 67), а также сохранить отчет на локальный диск:

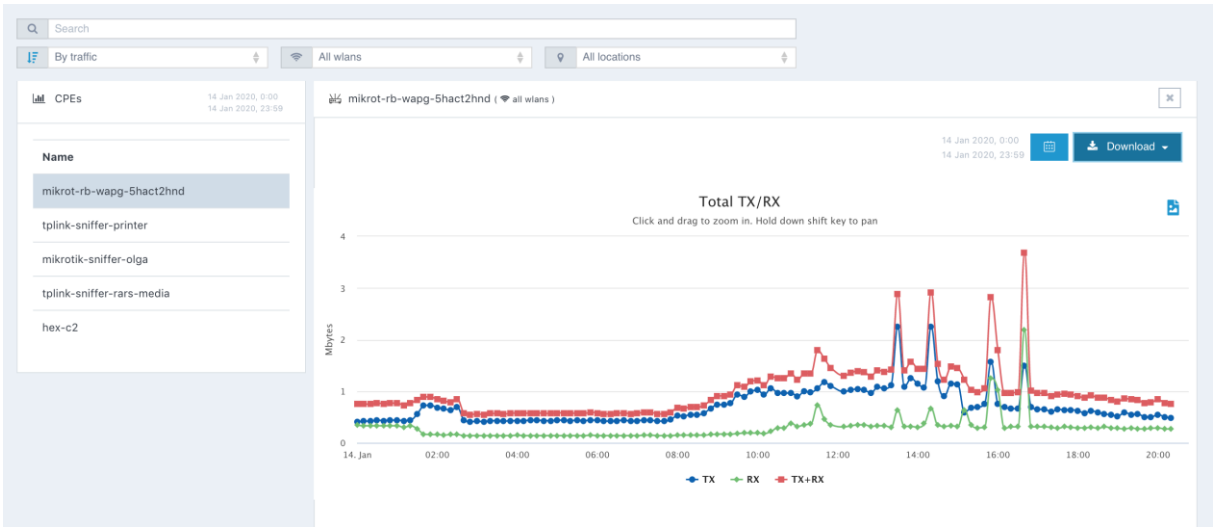


Рисунок 67. Просмотр статистики с временной диаграммой по метрикам

В разделе “Reports” можно сформировать отчеты о событиях, клиентах в системе, для выгрузки на e-mail (Рисунок 68).

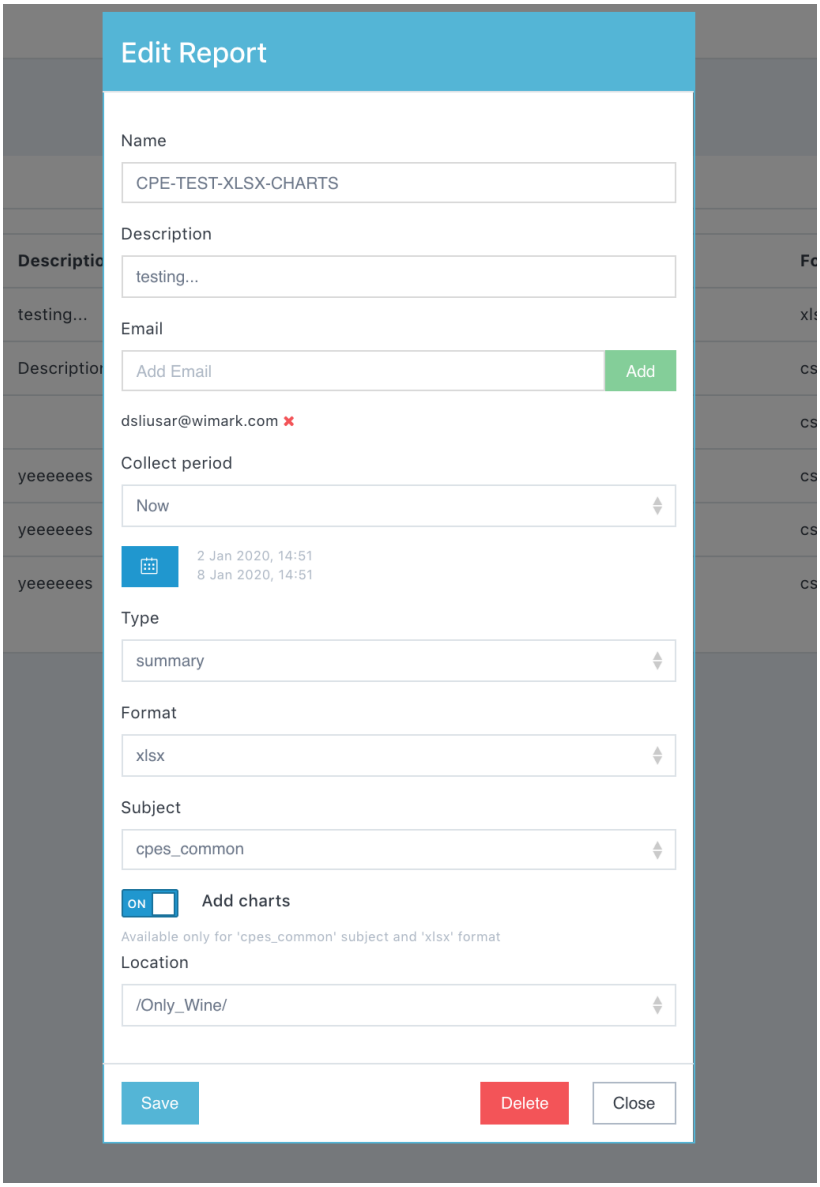


Рисунок 68. Формирование отчетов о событиях, клиентах в системе, для последующей выгрузки на e-mail

4.12. Мониторинг и определение проблем

В разделе мониторинг можно смотреть данные о внутренних сообщениях в системе, времени подключения точек доступа, создавать правила для триггеров по типам (Рисунок 69):

- высокое показание CPU, RAM;
- подключение, отключение ТД;
- ошибки конфигурирования.

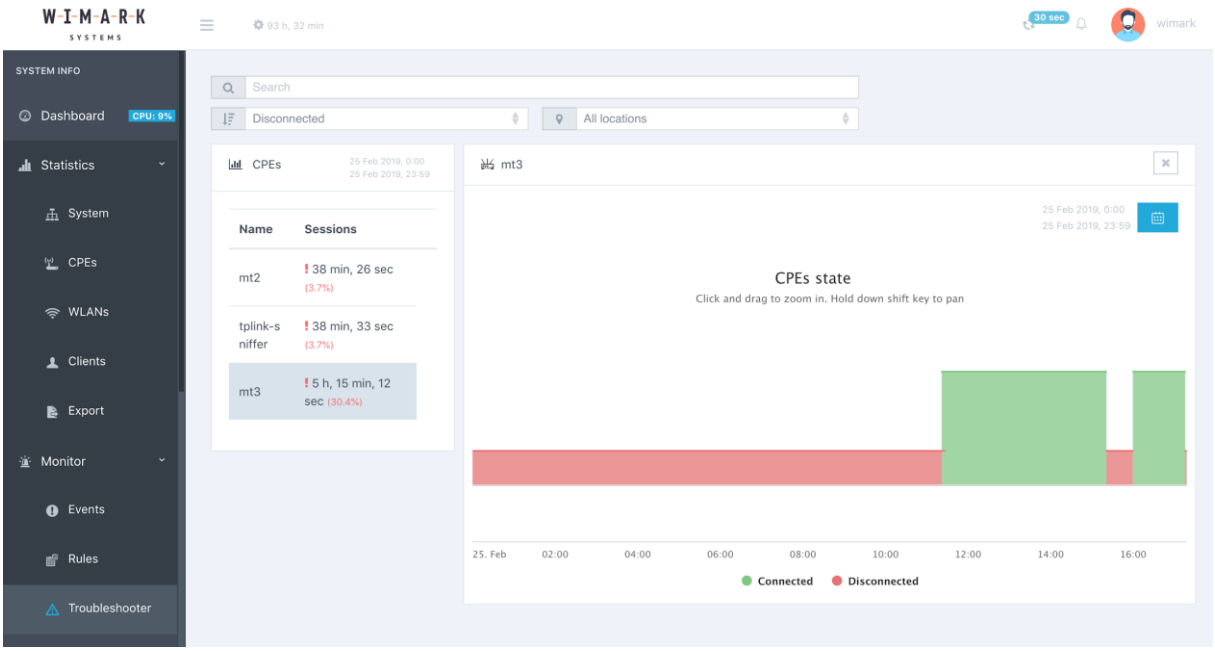


Рисунок 69. Раздел мониторинга

4.13. Работа с событиями (Events)

На странице сообщений можно видеть список событий системы, сервисов, подключения клиентов, пользовательские отчеты и т.д. (Рисунок 70).

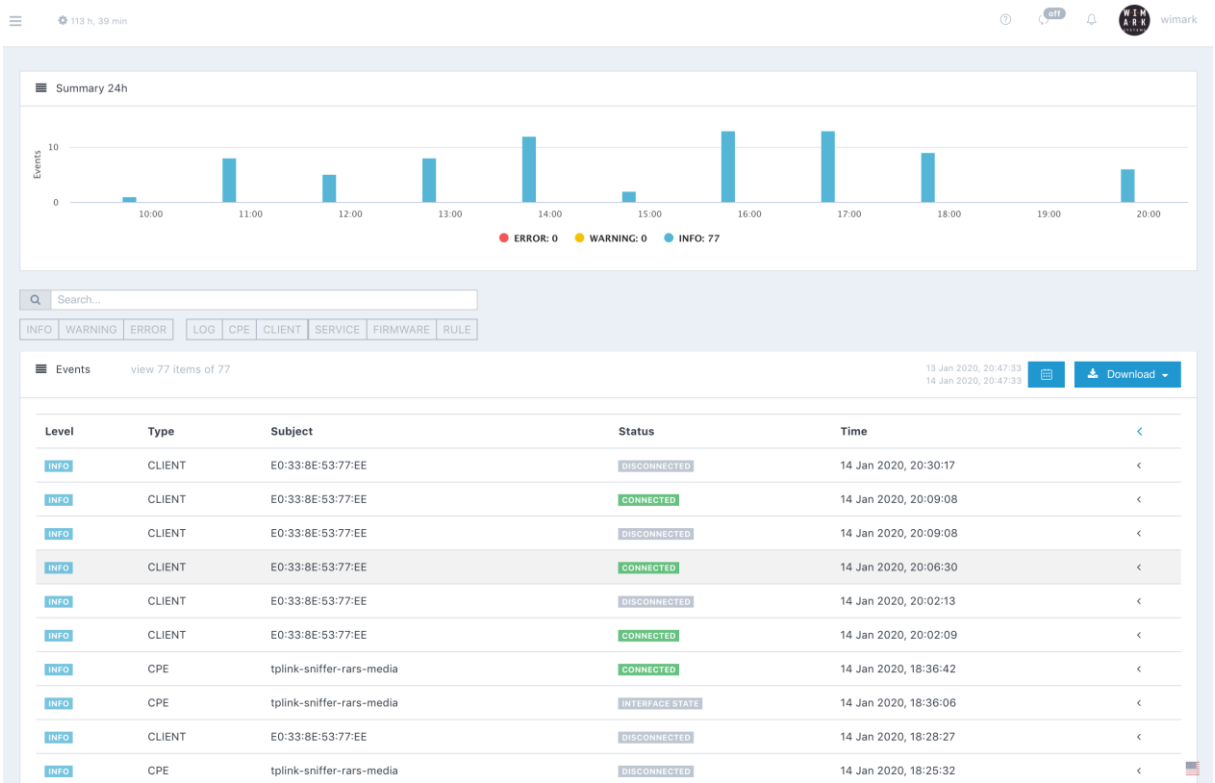


Рисунок 70. Список событий

4.14. Работа с данными Wi-Fi Radar

Для включения сбора данных Wi-Fi Radar необходимо перейти в раздел CPEs, выбрать точку доступа и включить Wi-Fi Radar Config (Рисунок 71). Таймаут сбора и время клиента рекомендуем сделать одинаковыми. Параметры задаются в секундах.

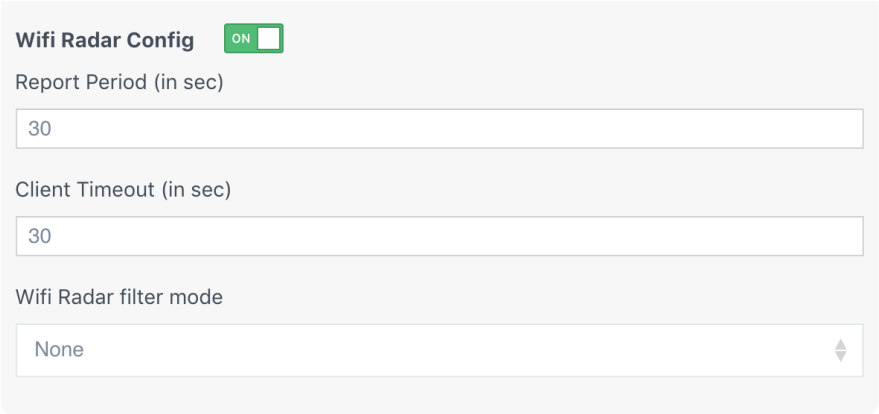


Рисунок 71. Настройка Wi-Fi Radar

После настройки собираемые данные можно выгрузить через интерфейс экспорта данных аналитики (на email, Yandex или myTarget) (Рисунок 72).

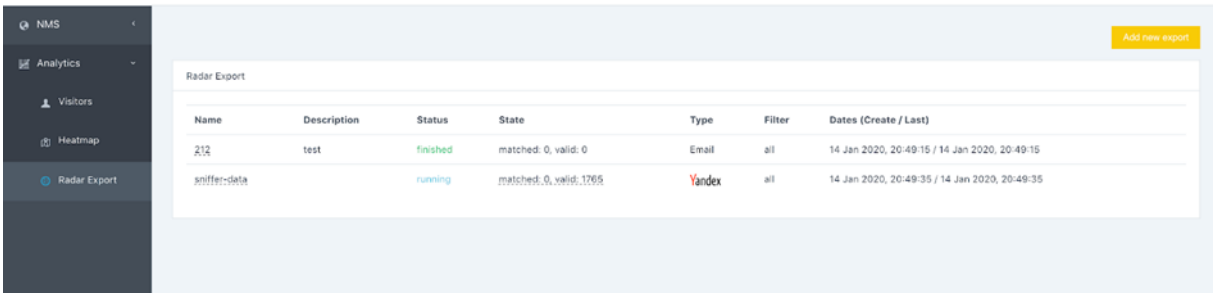


Рисунок 72. Выгрузка данных аналитики

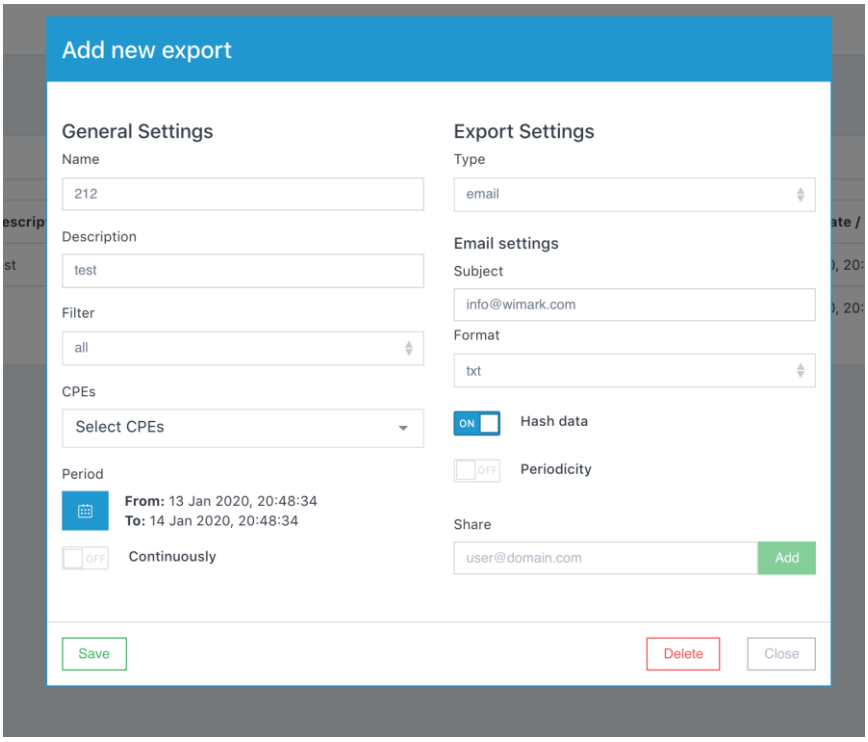


Рисунок 73. Пример создания экспорта данных Wi-Fi Radar

5. ПЛАТФОРМА АВТОРИЗАЦИИ И МОНЕТИЗАЦИИ (PORTAL)

Платформа авторизации и монетизации QTECH состоит из следующих компонентов:

- агент на точке доступа с функциями NAS (Network Access Server);
- правило редиректа (Redirect Rule), настраиваемое с помощью платформы управления и мониторинга (NMS);
- непосредственно Веб-страниц порталов авторизации и их бекенда;
- сервис показа рекламы;
- сервис управления ваучерами и платежами пользователей;
- сервис настройки страниц, объектов, баннеров, рекламы и т.д.;
- сервис интеграции с Cisco WLC для показа портала авторизации.

5.1. Интерфейс управления авторизацией и монетизацией

Меню в Веб-интерфейсе управления представлено объектами, указанными на изображении ниже (Рисунок 74).

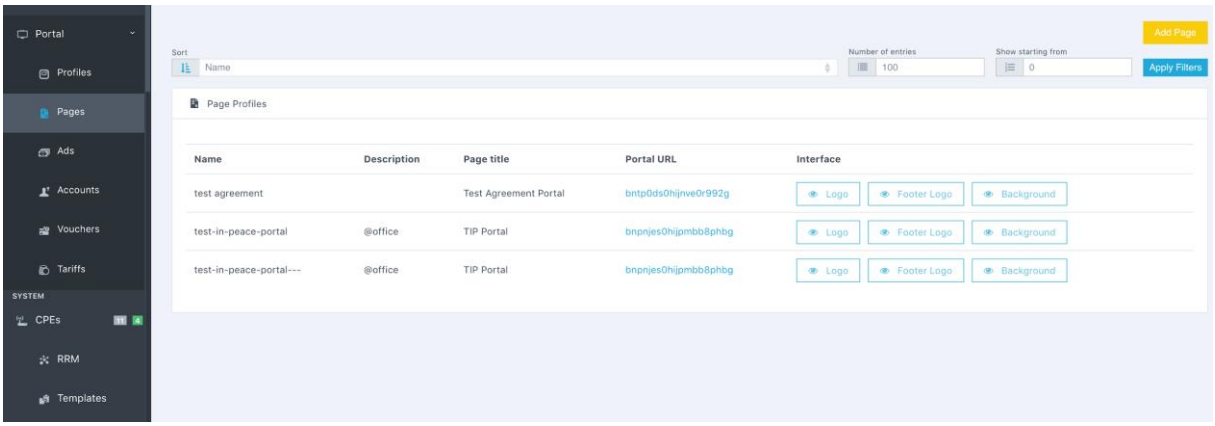


Рисунок 74. Интерфейс управления авторизацией и монетизацией

Это портальные профили, страницы, реклама (баннеры, видео и опросы), а также части для управления платным Wi-Fi: аккаунты, ваучеры и тарифы.

5.2. Связь между объектами портала

Правило перенаправления (Redirect rule) может быть добавлено для перенаправления неавторизованных пользователей на портал. Правило может быть добавлено на WLAN или сразу на проводной интерфейс CPE (во втором случае требуется явно задавать CPE ID в настройках правила). Правило добавляет в URL перенаправления специальные параметры.

Страница портала (Page) принимает пользователя и отображает интерфейс (логотипы, цвета). Логики не содержит.

Логика работы портала авторизации сосредоточена в профиле портала (Portal Profile). Здесь осуществляется связь WLAN, CPE и отображение типов аутентификации (по нормам гос. законов) и авторизации (с рекламой, ограничением на длину сессий, блокировками и платным Wi-Fi). Важно, что связь WLAN-CPE должна быть одна среди всех профилей портала для их корректной работы.

Реклама и опросы (Ads) – статические файлы или простые опросы, которые можно добавить для отображения в конкретный профиль, в конкретный тип авторизации.

Пользовательские аккаунты (Accounts) – связь между идентификаторами пользователей (номером телефона или e-mail), портальным профилем и списком MAC-адресов. Также содержит баланс пользователя. Баланс одного пользователя для каждого профиля различен.

Тариф – набор настроек сессии пользователя с привязкой к цене тарифа.

Ваучер – единоразовая покупка определенного тарифа с привязкой к конкретному пользовательскому аккаунту. Имеет строгое время действия.

Тарифы, баланс и ваучеры видны в личном кабинете пользователя конечного сети с порталом авторизации на Веб-странице портала.

5.3. Добавление WLAN с порталом авторизации

Для добавления WLAN (беспроводной сети) с порталом авторизации, необходимо:

1. Создать WLAN без указания правила перенаправления (Redirect Rule).
2. Создать страницу портала (на странице Pages), либо выбрать имеющуюся.
3. На странице Pages скопировать адрес портала.
4. Создать правило редиректа (Redirect Rule), указав скопированный адрес из Веб-страницы и открыв доступ до портала (указав доменное имя и IP-адрес платформы).
5. Указать в ранее созданном WLAN созданное правило редиректа.
6. Добавить WLAN на необходимые точки доступа.
7. Создать профиль портала, связав WLAN, точки доступа и логику работы портала (такую как набор типом аутентификации, авторизации и выбрав рекламу, если это необходимо).

Для открывания портала авторизации на устройствах iOS/MacOS сразу в браузере, а не во всплывающем окне, требуется добавить домен **captive.apple.com** с указанием IP-адреса платформы в правиле перенаправления.

5.4. Добавление портала авторизации на проводной интерфейс

Для добавления портала авторизации на проводной интерфейс, необходимо:

1. Создать WLAN без указания правила перенаправления (Redirect Rule) (сам WLAN не будет использован, он нужен только для работы логики).
2. Создать страницу портала (на странице Pages), либо выбрать имеющуюся.
3. На странице Pages скопировать адрес портала.
4. Создать правило редиректа (Redirect Rule), указав скопированный адрес из Веб-страницы и открыв доступ до портала (указав доменное имя и IP-адрес платформы). А также **важно** указать CPE (точку доступа) и WLAN.
5. Указать в ранее созданном WLAN созданное правило редиректа.
6. Добавить правило редиректа на проводные интерфейсы на необходимых точках доступа (CPE).
7. Создать профиль портала, связав WLAN, точки доступа и логику работы портала (такую как набор типом аутентификации, авторизации и выбрав рекламу, если это необходимо).

Для открывания портала авторизации на устройствах iOS/MacOS сразу в браузере, а не во всплывающем окне, требуется добавить домен **captive.apple.com** с указанием IP-адреса платформы в правиле перенаправления.

5.5. Работа с рекламой и опросами

Работа с рекламой и опросами (создание, редактирование, просмотр статистики) реализован на странице Ads (Рисунок 75).

В настоящий момент поддерживаются в качестве рекламы изображения, видео (mp4) и опросы.

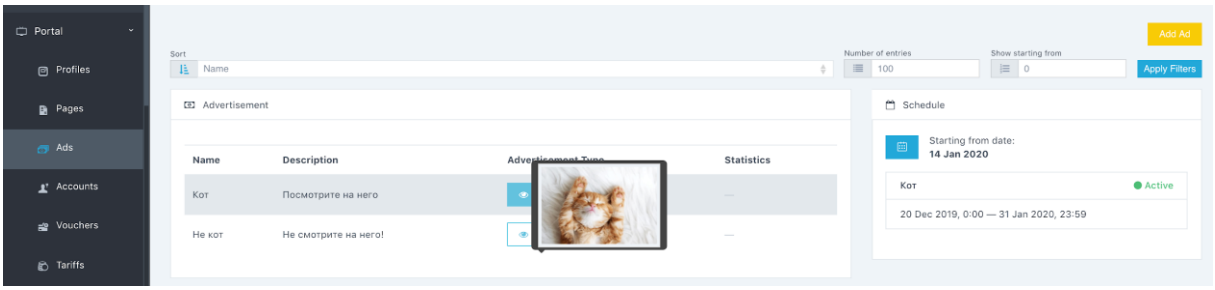


Рисунок 75. Меню настройки рекламы

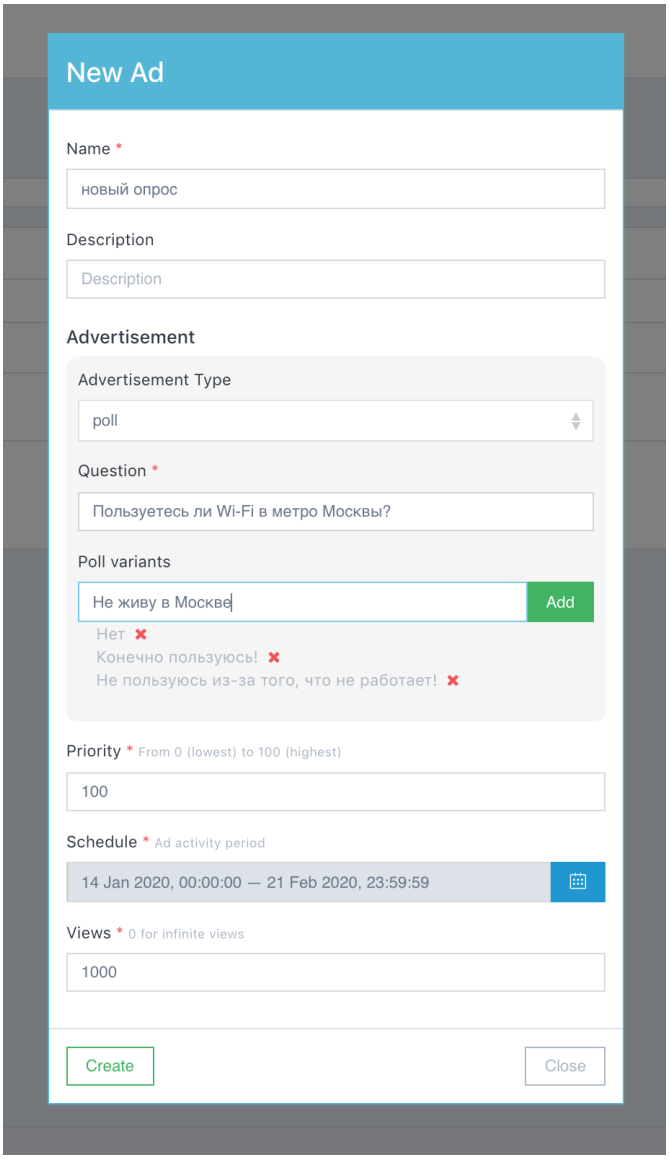


Рисунок 76. Форма создания рекламы

После создания рекламы ее следует добавить для отображения в портальный профиль на конкретный тип авторизации (например, на тип Бесплатный интернет).

5.6. Работа со страницами авторизации

Интерфейс/визуальную составляющую страниц авторизации можно настраивать на странице Pages.

Данная страница содержит список Веб-страниц, предпросмотр и, что главное, уникальный URL, который используется для перенаправления пользователей (с помощью правил перенаправления) и работы авторизации у клиентов.

Интерфейс таблицы страниц представлен ниже. Для создания страниц нужно нажать Add Page и загрузить лого, фон, установить выводимое имя и т.д. (Рисунок 77)

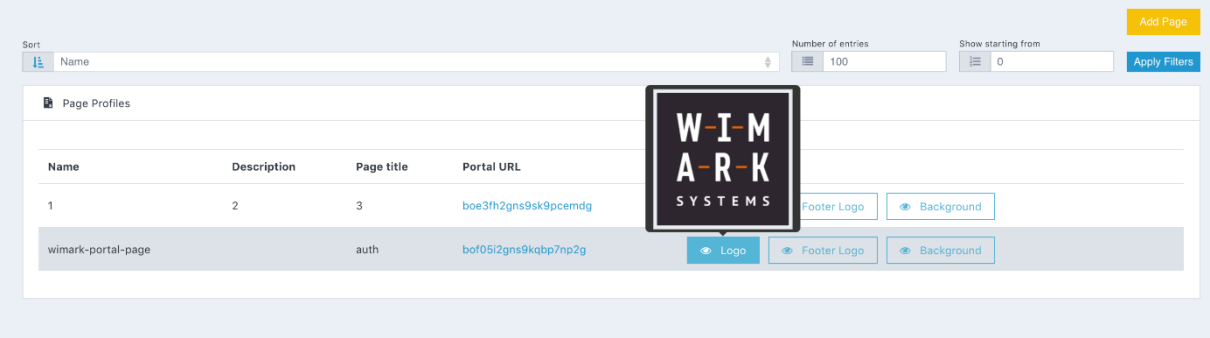


Рисунок 77. Интерфейс таблицы страниц

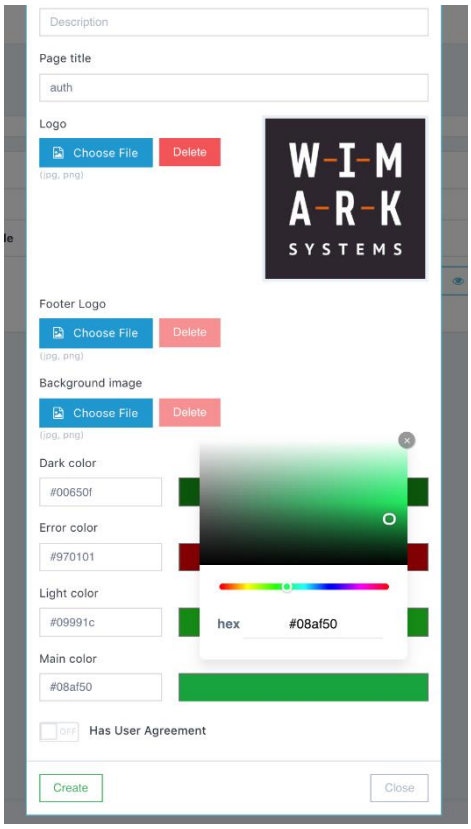


Рисунок 78. Интерфейс создания новой страницы.

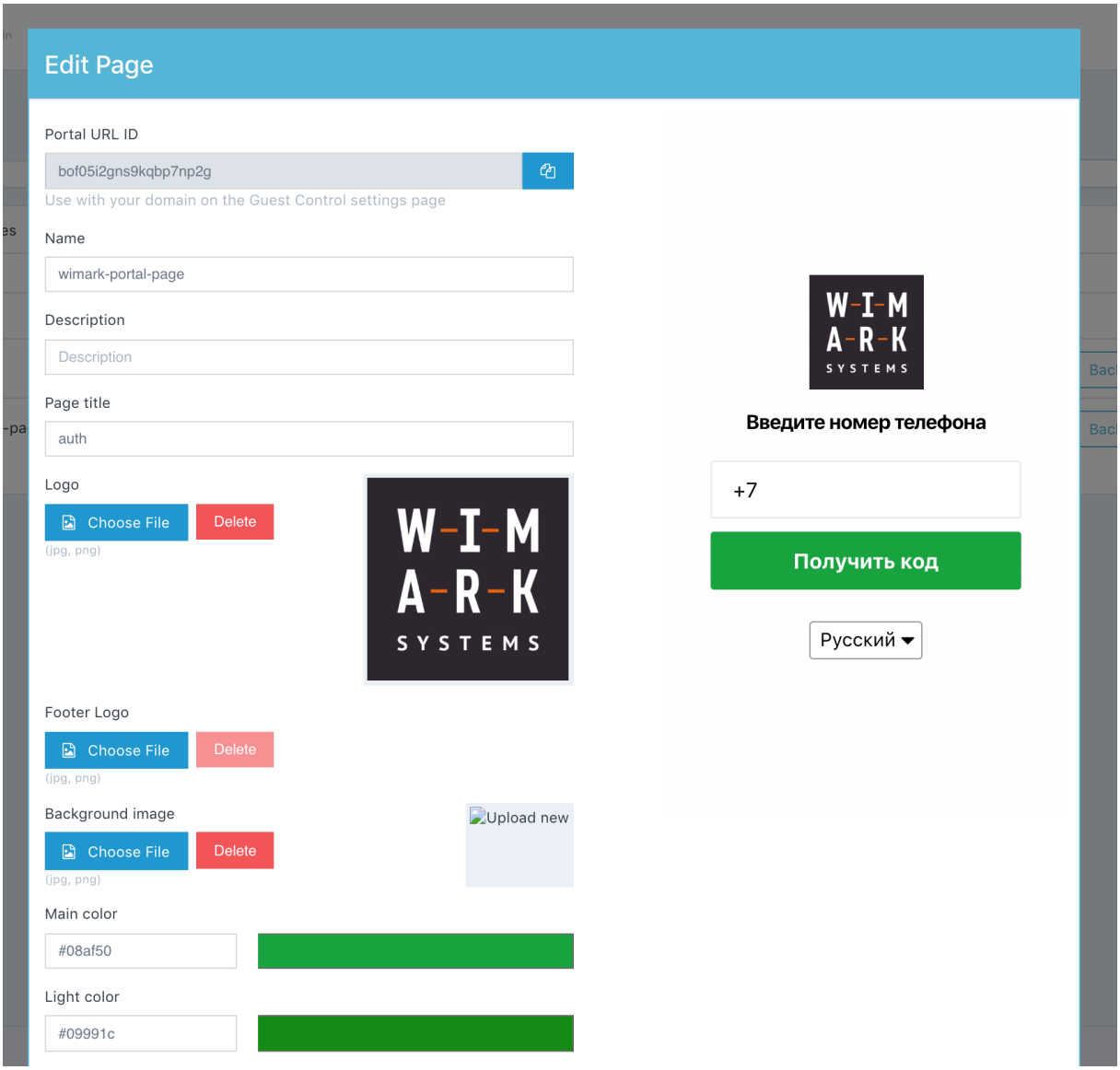


Рисунок 79. Интерфейс создания новой страницы.

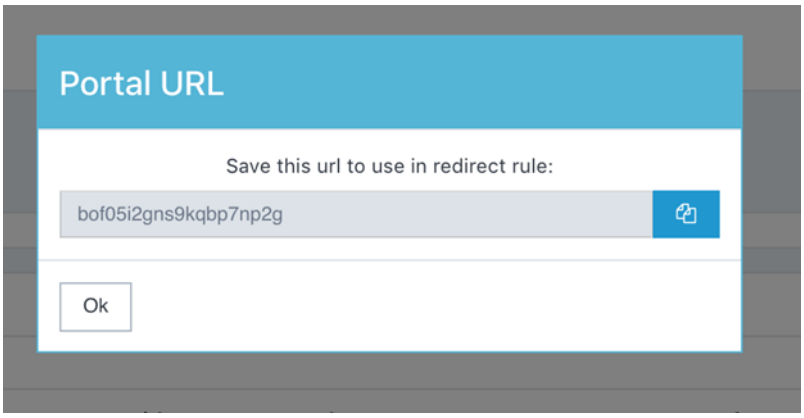


Рисунок 80. Адрес страницы для правила редиректа

После создания страницы следует скопировать ее адрес, который будет использован на странице управления правилами редиректа (Рисунок 80).

6. ПЛАТФОРМА АНАЛИТИКИ (ANALYTICS)

Платформа аналитики работает с данными, полученными с Wi-Fi-радара. В частности, аналитика может быть построена:

- с целью оценки посетителей локаций (рядом с точками доступа);
- с целью проверки и отображения мест скопления людей;
- с целью сбора массива пользователей и последующего показа рекламы с помощью онлайн сервисов, типа Yandex.Audience и myTarget.

6.1. Оценка посетителей

Данная страница содержит информацию о посетителях локаций, времени посещения, количестве уникальных, соотношение новых и повторных посетителей (Рисунок 81).

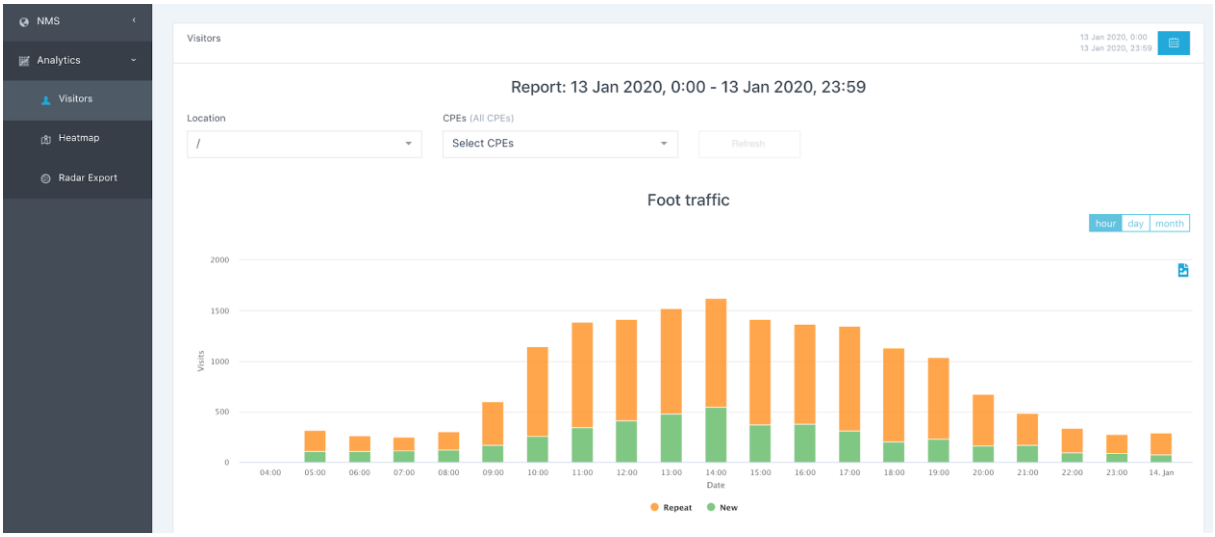


Рисунок 81. Страница Оценка посетителей

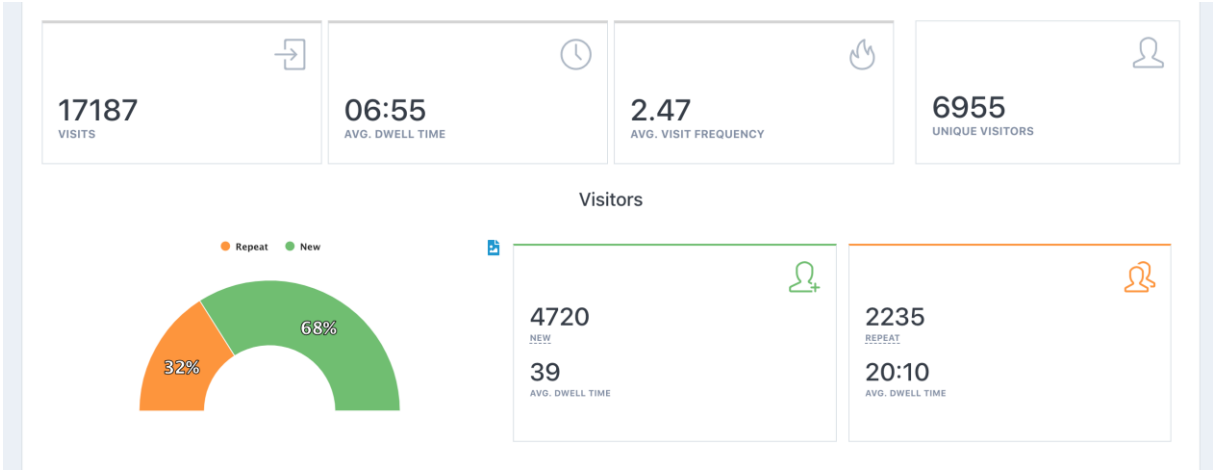
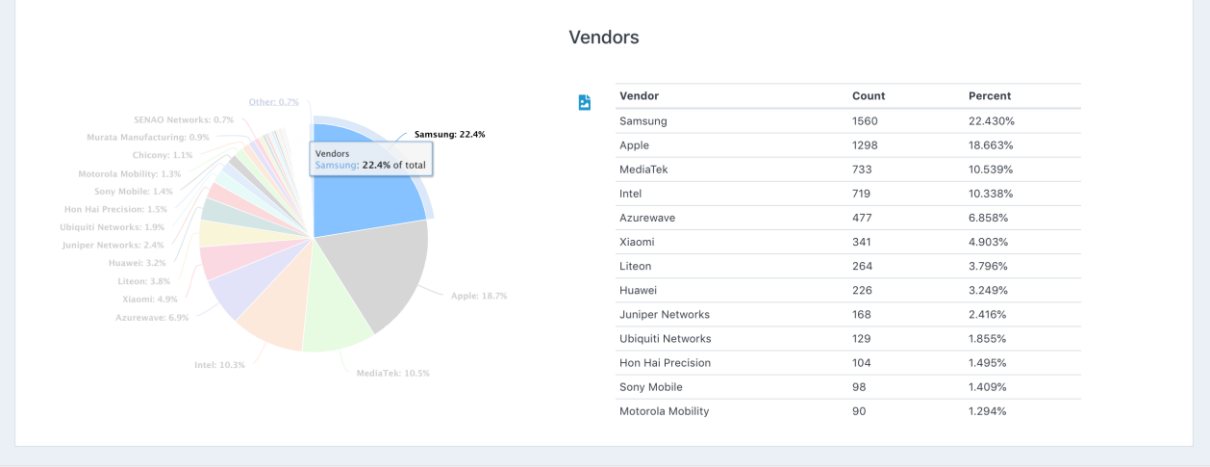


Рисунок 82. Информация о посетителях

Repeat visitors by visit frequency

Repeat	Visits	Avg. dwell time
1 visits	5111	5 min. 55 sec.
2 visits	543	9 min. 33 sec.
3-4 visits	493	8 min. 33 sec.
5-9 visits	421	9 min. 48 sec.
>= 10 visits	387	11 min. 23 sec.

Рисунок 83. Информация о повторных посетителях



Vendor	Count	Percent
Samsung	1560	22.430%
Apple	1298	18.663%
MediaTek	733	10.539%
Intel	719	10.338%
Azurewave	477	6.858%
Xiaomi	341	4.903%
Liteon	264	3.796%
Huawei	226	3.249%
Juniper Networks	168	2.416%
Ubiquiti Networks	129	1.855%
Hon Hai Precision	104	1.495%
Sony Mobile	98	1.409%
Motorola Mobility	90	1.294%

Рисунок 84. Информация об устройствах посетителей

Также собираются данные о поставщике клиентского оборудования и количестве визитов каждым из уникальных пользователей (позволяет оценить лояльность или отсечь персонал) (Рисунок 84).

6.2. Работа с картами

Работа с картами в режиме аналитики аналогично описанной в разделе NMS.

Далее приведены некоторые примеры интерфейса.

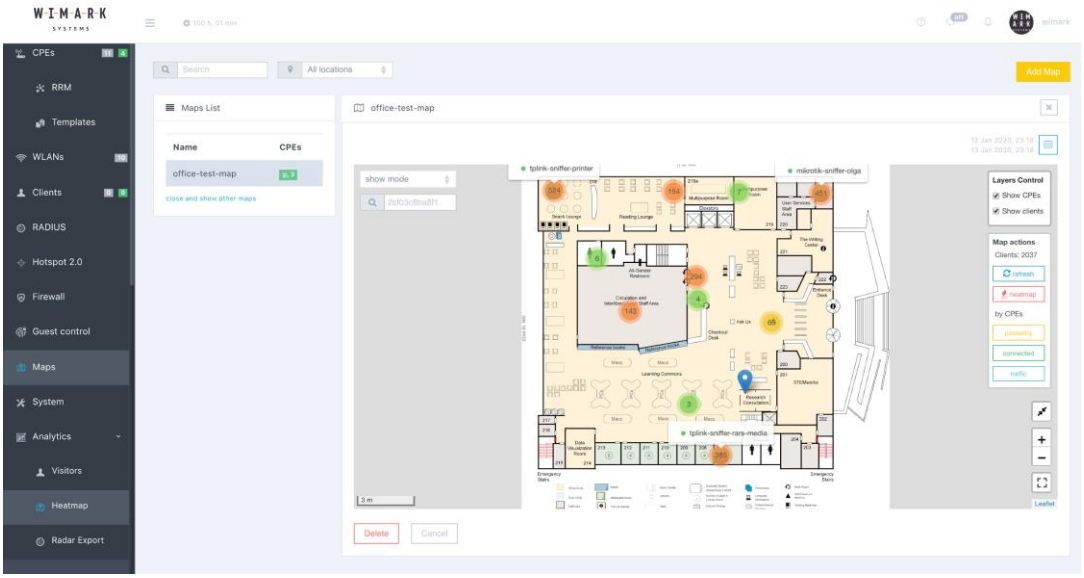


Рисунок 85. Базовый интерфейс карты с отображением проходящих пользователей

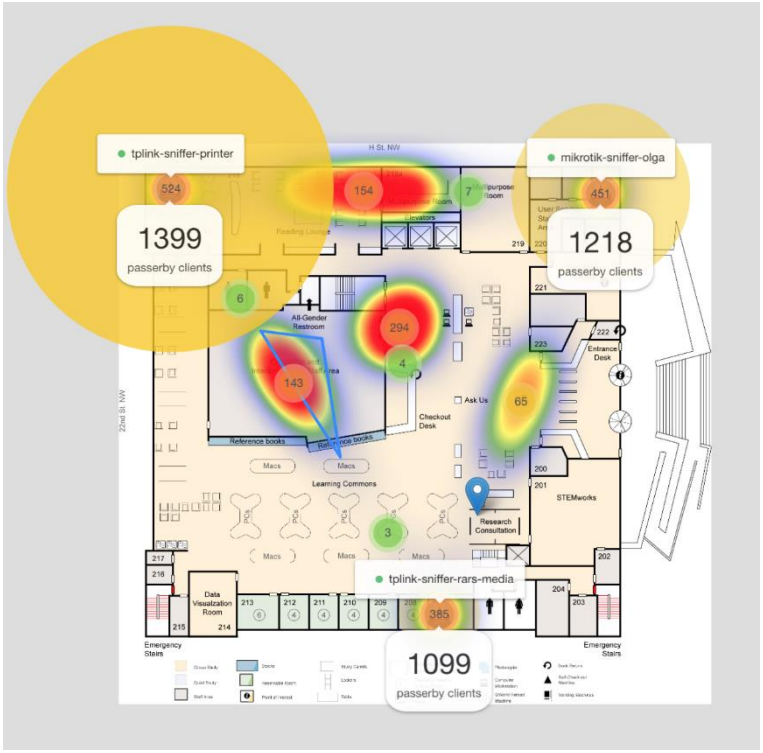


Рисунок 86. Карта с отображением проходящих пользователей

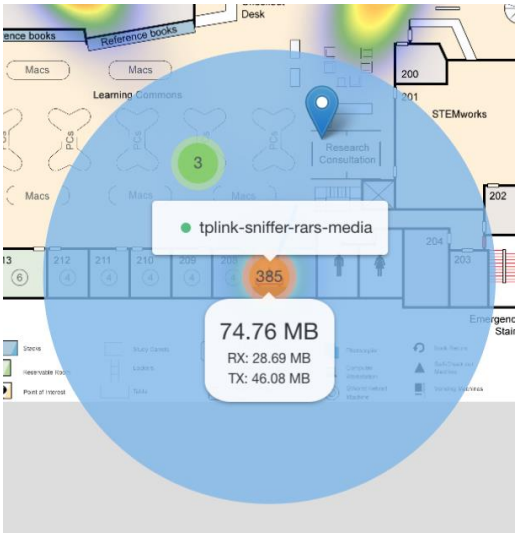


Рисунок 87. Режим отображения трафика ТД

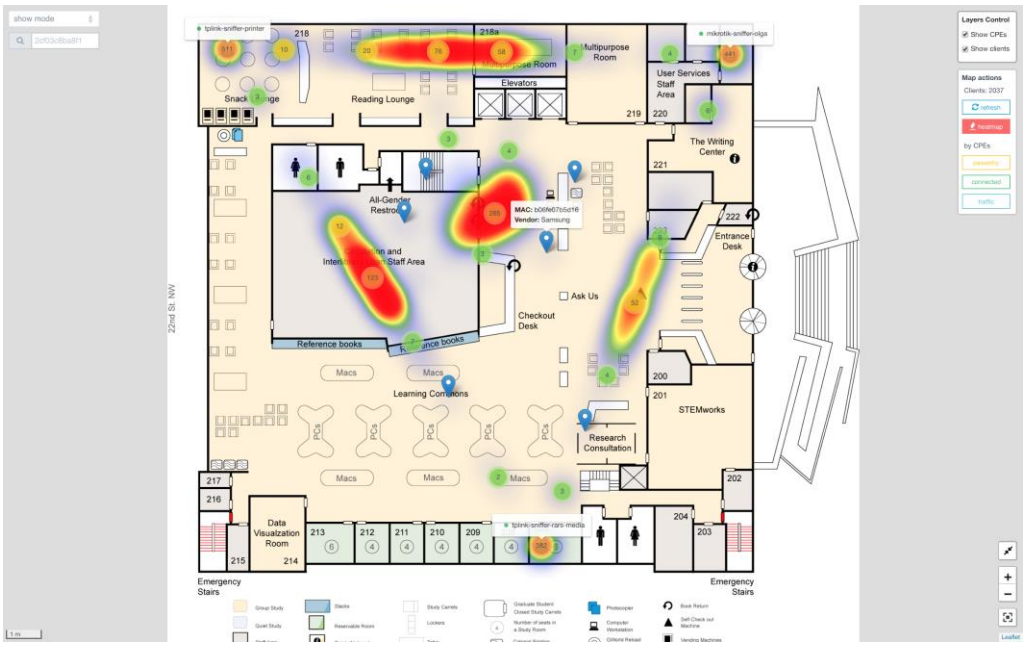


Рисунок 88. Работа с картой горячих пятен (Heatmap)

Рисунок 89. Работа с картой горячих пятен (Heatmap) и отслеживание конкретного пользователя

Рисунок 90. Отслеживание конкретного пользователя

6.3. Выгрузка данных Wi-Fi-радара

На данной странице находится выгрузка собранных Wi-Fi-радаром данных (Рисунок 91). Списки MAC-адресов могут быть выгружены на e-mail, Yandex, myTarget, что впоследствии может быть использовано как сегмент для таргетированной рекламы (Рисунок 92).

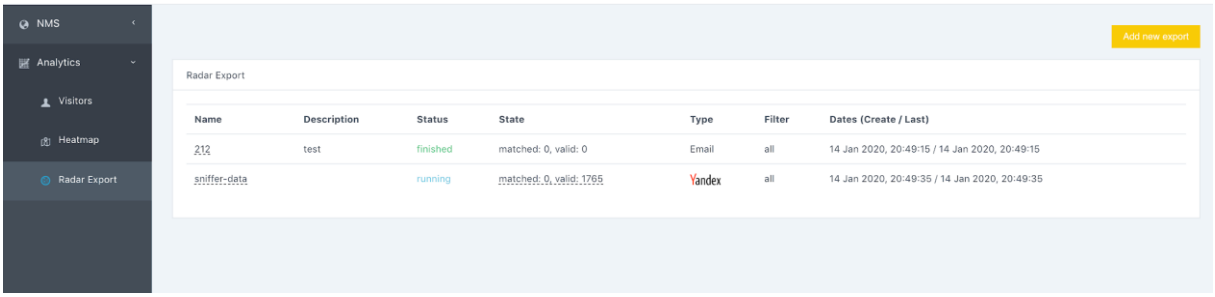


Рисунок 91. Страница выгрузок данных, собранных Wi-Fi-радаром

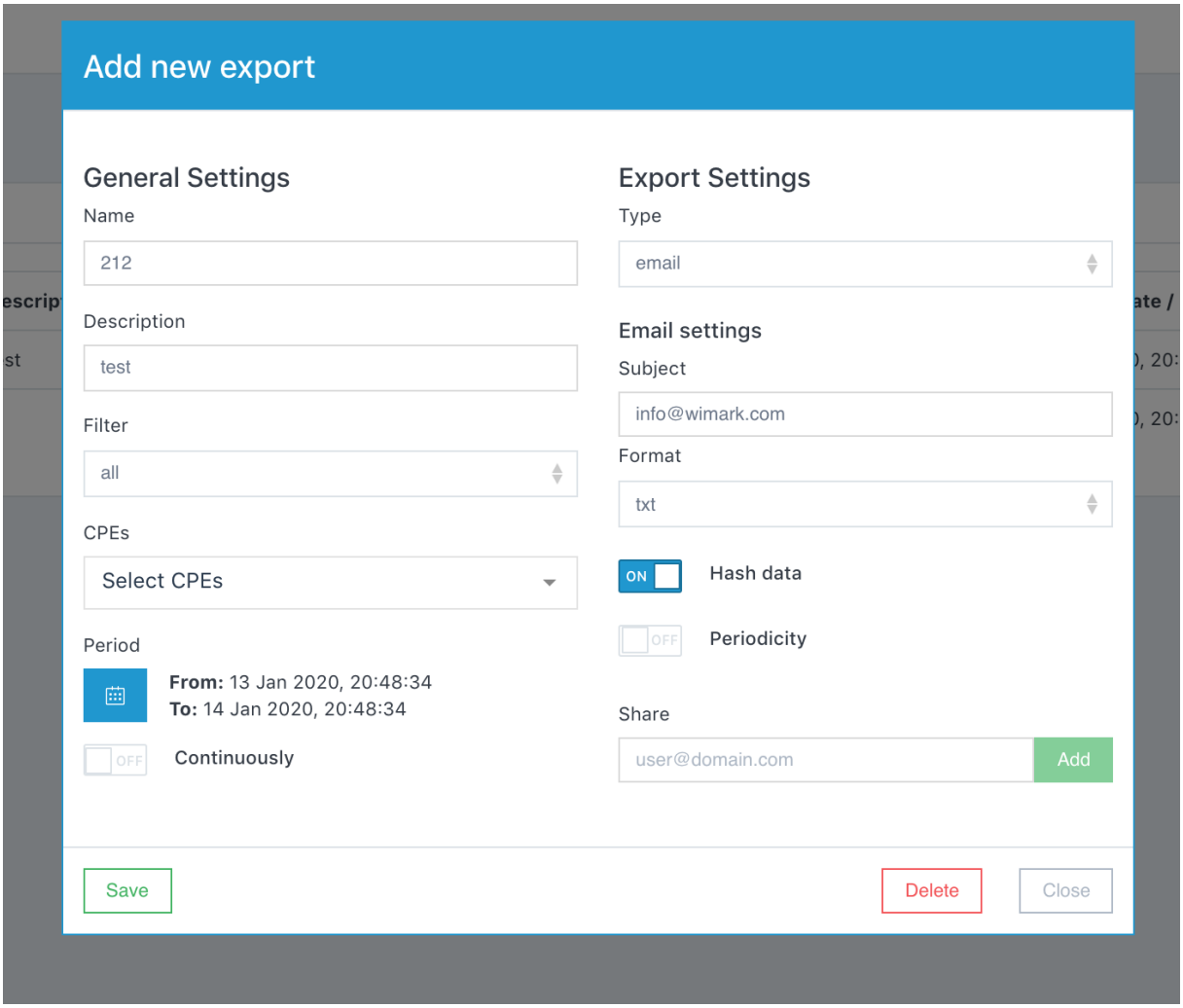


Рисунок 92. Пример создания выгрузки на e-mail хешированных данных

ПРИЛОЖЕНИЕ 1.

Туннелирование через контроллер.

Данные настройки производятся в cli контроллера.

1. Включить форвардинг трафика:

$ sudo iptables -P FORWARD ACCEPT

2. Отредактировать **/etc/sysctl.conf**, убрать # в начале строк и сохранить файл:

net.ipv4.ip_forward=1

net.bridge.bridge-nf-call-iptables = 1

net.bridge.bridge-nf-filter-vlan-tagged = 1

3. Выполнить команду:

$ sudo sysctl -p /etc/sysctl.conf

4. Установить дополнительные пакеты:

$ sudo apt install bridge-utils

$ sudo apt install vlan

$ sudo modprobe --first-time 8021q

$ modinfo 8021q

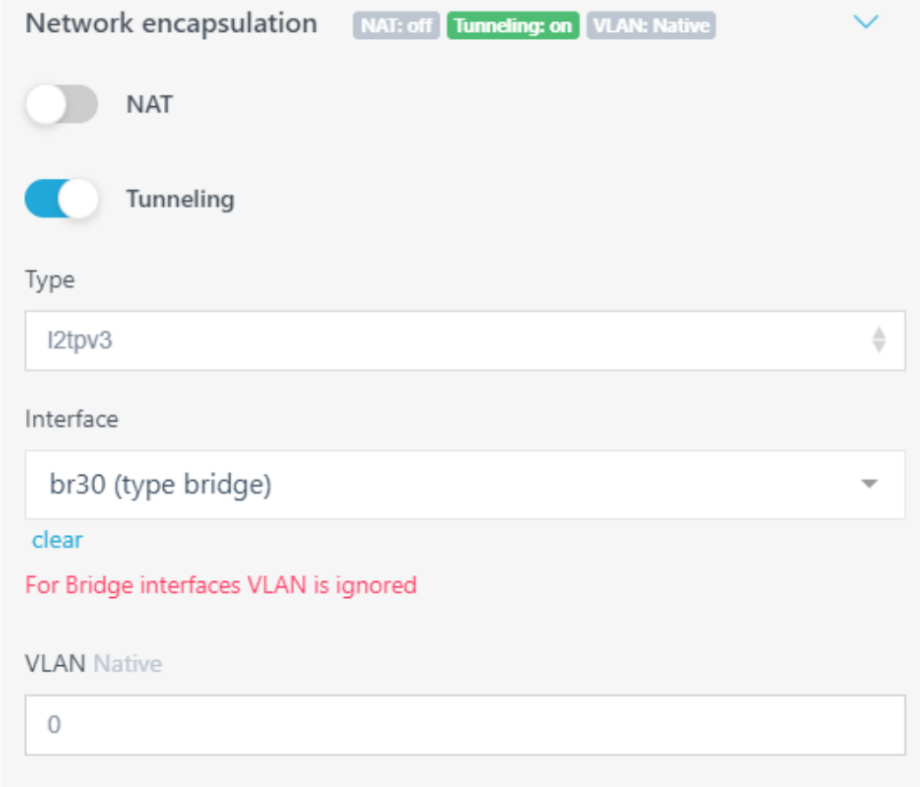
5. Отредактировать файл сетевых настроек (пример для транкового порта в контроллер с управлением native vlan и пользовательским VLAN30). Создается новый bridge br30 с VLAN-интерфейсом. В случае использования гипервизора коммутатор гипервизора необходимо перевести в promiscuous mode.

```
$ sudo nano /etc/netplan/00-installer-config.yaml

network:
  ethernets:
    enp1s0:
      dhcp4: true
  version: 2

  vlans:
     enpls0.30:
         id: 30
         link: enp1s0
         dhcp4: false

  bridges:
        br30:
          interfaces: [ enpls0.30 ]

$ sudo netplan apply
```

6. Выполнить перезагрузку tunnel manager (либо новый мост появится в Веб-интерфейсе контроллера через 10 минут).

$ sudo docker container restart $(sudo docker ps | grep tunnel-manager | awk '{print $1}')

7. Создать WLAN с L2TP на br30.



8. Привязать WLAN в радиоинтерфейсу.
9. Проверить подключение туннеля ТД к мосту можно командой:

```
brctl show

br30        8000.000c2900290b     no          ens160.30       #созданный интерфейс
                                                t35656-s35689  #туннель ТД
```

7. ОБЩАЯ ИНФОРМАЦИЯ

7.1. Замечания и предложения

Мы всегда стремимся улучшить нашу документацию и помочь вам работать лучше, поэтому мы хотим услышать вас. Мы всегда рады обратной связи, в особенности:

- ошибки в содержании, непонятные или противоречащие места в тексте;
- идеи по улучшению документации, чтобы находить информацию быстрее;
- неработающие ссылки и замечания к навигации по документу.

Если вы хотите написать нам по поводу данного документа, то используйте, пожалуйста, форму обратной связи на qtech.ru.

7.2. Гарантия и сервис

Процедура и необходимые действия по вопросам гарантии описаны на сайте QTECH в разделе «Поддержка» –> «Гарантийное обслуживание».

Ознакомиться с информацией по вопросам тестирования оборудования можно на сайте QTECH в разделе «Поддержка» –> «Взять оборудование на тест».

Вы можете написать напрямую в службу сервиса по электронной почте sc@qtech.ru.

7.3. Техническая поддержка

Если вам необходимо содействие в вопросах, касающихся нашего оборудования, то можете воспользоваться нашей автоматизированной системой запросов технического сервис-центра helpdesk.qtech.ru.

Телефон Технической поддержки +7 (495) 477-81-18 доб. 0

7.4. Электронная версия документа

Дата публикации 21.11.2022

https://files.qtech.ru/upload/wireless/QWC-VC/QWC-VC_config_guide.pdf