



Руководство пользователя QTECH Atlas



Оглавление

1. ВВЕДЕНИЕ	7
1.1. ПРИМЕЧАНИЯ	7
1.2. ОСНОВНЫЕ ТЕРМИНЫ И СОКРАЩЕНИЯ	7
2. ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ И НАСТРОЙКА СЕТИ	9
2.1. Системные требования для установки	9
2.2. Требования к настройкам сети	9
3. УСТАНОВКА КОНТРОЛЛЕРА	11
3.1. Установка контроллера на ESXi	11
3.1.1. Предварительные настройки	11
3.1.2. Установка	11
3.2. Установка контроллера на VirtualBox	14
3.2.1. Установка VirtualBox	14
3.2.2. Установка контроллера	14
3.3. Установка контроллера на Hyper-V	16
3.3.1. Предварительные настройки	16
3.3.2. Установка контроллера	17
4. РАБОТА С ПРЕДУСТАНОВЛЕННЫМИ ПЛАТФОРМАМИ	20
4.1. Порядок работы	20
5. НАЧАЛО РАБОТЫ С КОНТРОЛЛЕРОМ	21
6. ПЕРЕНОС ВИРТУАЛЬНОЙ МАШИНЫ С КОНТРОЛЛЕРОМ	22
7. ИНТЕРФЕЙС ПЛАТФОРМЫ	24
7.1. Домашняя страница	24
7.2. Управление	25
8. ПРИМЕНЕНИЕ АКТИВАЦИОННОГО КЛЮЧА	28
8.1. Правила применения активационного ключа	28
8.2. Применение активационных ключей в НА-паре.	28
8.3. Порядок применения активационного ключа	28
8.4. Проверка применения активационного ключа	30
9. СИСТЕМНЫЕ НАСТРОЙКИ КОНТРОЛЛЕРА	31
9.1. Переключение языка веб-интерфейса	31
9.2. Изменение IP-адреса контроллера	31
9.3. Настройка времени и NTP-сервера	31
9.4. Обновление ПО контроллера	33
9.5. Создание и восстановление резервной копии конфигурации через WEB-интерфейс	34
9.6. Сброс до заводских настроек	35



10. НАСТРОЙКА РЕЗЕРВИРОВАННОЙ ПАРЫ (HIGH AVAILABILITY)	36
10.1. Конфигурация резервированной пары	36
10.2. Мониторинг состояния	37
10.3. Логика использования IP-адресов	38
10.4. Остановка НА	38
11. ПОДКЛЮЧЕНИЕ ТД К КОНТРОЛЛЕРУ	40
11.1. Подключение точек доступа к контроллеру через опцию 43	40
11.2. Подключение точек доступа через веб-интерфейс ТД	41
11.3. Подключение ТД к нескольким контроллерам	41
11.4. Проверка подключения ТД к контроллеру	42
12. СЕТЕВАЯ БЕЗОПАСНОСТЬ	44
12.1. Требования к TCP/UDP портам	44
12.2. Доступ к управлению ТД	45
12.3. Доступ к управлению контроллером	45
12.4. Принудительное отключение клиента от SSID	46
12.5. Загрузка SSL-сертификата	47
13. УПРАВЛЕНИЕ ТД	48
13.1. Редактирование информации о ТД	48
13.2. Перезагрузка ТД	48
13.3. Перезагрузка ТД по расписанию	48
13.4. Обновление ПО на ТД	49
13.5. Настройка LAN порта точки доступа	50
14. СОЗДАНИЕ И НАЗНАЧЕНИЕ ОРГАНИЗАЦИИ	51
14.1. Основные параметры организации	51
14.2. Дополнительные параметры организации	51
14.3. Настройка радиоинтерфейсов	51
14.4. Удаленный доступ к ТД	52
14.5. Смена организации на ТД	52
15. СОЗДАНИЕ БЕСПРОВОДНОЙ СЕТИ	54
15.1. Создание беспроводной сети. Основные параметры.	54
15.2. Дополнительные настройки SSID	54
15.2.1. Настройка изоляции клиентов	55
15.2.2. Настройка режима безопасности	55
15.2.3. Настройка 802.11r (fast transition)	55
15.2.4. Ограничение пропускной способности	55
15.2.5. Настройка расписания вещания SSID	56
15.2.6. Настройка черного списка MAC-адресов	56



16. БЕЗОПАСНОСТЬ И АУТЕНТИФИКАЦИЯ	57
16.1. Настройка WPA-EAP	57
16.2. Динамическое назначение VLAN (DVA)	57
16.3. Настройка RADIUS-атрибутов для ограничения и приоритезации трафика	59
16.4. MAC-аутентификация	60
16.4.1. Настройка белого списка MAC-адресов	60
16.4.2. Создание локальной учетной записи для MAC-аутентификации	61
16.5. Группы пользователей	62
16.6. Создание локальных учетных записей для пользователей Wi-Fi	64
16.7. Настройка внутреннего портала авторизации.	65
17. НАСТРОЙКА ВНЕШНЕГО ПОРТАЛА АВТОРИЗАЦИИ	68
17.1. Интеграция с системой WNAME	68
17.2. Диагностика взаимодействия с внешним порталом	73
18. НАСТРОЙКИ РАДИО	74
18.1. Настройка регуляторного домена (при необходимости)	74
18.2. Изменение номера и ширины канала и мощности	74
18.3. Включение/выключение радиомодулей	74
18.4. Настройка частотного плана	75
18.5. Настройка Band Steering	75
19. МОНИТОРИНГ	76
19.1. Мониторинг системных ресурсов	76
19.2. Просмотр информации о ТД	76
19.3. Просмотр информации о клиентских устройствах	76
19.4. Включение LLDP на точках доступа	77
19.5. Настройка работы с syslog	77
20. ЖУРНАЛ СОБЫТИЙ	78
20.1. Информация о клиентских устройствах	78
20.2. Информация о состоянии ТД	78
20.3. История действий пользователя	78
21. НАСТРОЙКА SNMP	79
21.1. Включение SNMP	79
21.2. Настройка SNMP трапов	79
22. НАЧАЛО РАБОТЫ С CLI	80
22.1. Основные режимы CLI	80
Настройка профиля выполняется в режиме конфигурации профиля:	81
22.2. Организация и ap profile	81
22.3. SSID и network	81



23. НАСТРОЙКА ЧЕРЕЗ CLI	83
23.1. Настройка RADIUS-атрибутов для ограничения и приоритезации трафика	83
23.2. Настройка частотного плана	84
23.3. Включение LLDP на точках доступа	84
23.4. Настройка работы с syslog	85
23.4.1. Отправка логов контроллера	85
23.4.2. Отправка логов точек доступа	85
23.5. Добавление дополнительных AAA-серверов через CLI	86
23.6. Изменение времени автоматической настройки каналов	87
23.7. Настройка SNMP трапов	87
23.8. Настройка Band Steering	88
23.9. Настройка режима WPA3-SAE (only)	88
24. ДИАГНОСТИКА ЧЕРЕЗ CLI	89
24.1. Процедура диагностики в CLI	89
24.2. Вывод отладочной информации (debug)	89
24.2.1. Диагностика проблем с подключением ТД к контроллеру	89
24.2.2. Диагностика проблем с конфигурацией ТД	89
24.2.3. Диагностика проблем с подключением КУ к SSID	89
24.2.4. Диагностика работы опции «Динамический канал»	90
24.3. Команды show	90
24.3.1. Просмотр информации о подключенных точках доступа	90
24.3.2. Просмотр информации о радиоинтерфейсах ТД	91
24.3.3. Проверка применения активационных ключей	91
24.3.4. Просмотр информации о подключении пользователей	92
25. СКАНИРОВАНИЕ РАДИОЭФИРА	93
25.1. Настройка сканирования	93
25.2. Просмотр информации об обнаруженных SSID	93
26. ROGUE AP DETECTION	95
26.1. Обнаружение Rogue AP	95
26.2. Настройка SNMP трапов для Rogue AP	96
27. MULTICAST TO UNICAST (M2U)	97
28. СЦЕНАРИИ РАЗВЕРТЫВАНИЯ	98
28.1. Общие настройки для всех сценариев	98
28.2. Сценарий 1. Отдельно стоящая инфраструктура	99
28.3. Сценарий 2. High Availability	100
28.4. Сценарий 3. Распределенная сеть с филиалами	101
28.5. Сценарий 4. Георезервирование	101



29. ОБЩАЯ ИНФОРМАЦИЯ	103
29.1. Гарантия и сервис	103
29.2. Техническая поддержка	103
29.3. Электронная версия документа	103



1. ВВЕДЕНИЕ

Данное руководство ставит целью выделить основные этапы конфигурации беспроводной локальной вычислительной сети (БЛВС) на базе оборудования QTECH. Документ содержит описание основных функций контроллера, порядок его установки, а также пошаговые инструкции по настройке беспроводного контроллера и конфигурированию точек доступа.

! ВАЖНО:

- Всё конфигурирование происходит посредством контроллера. Выполнение любых настроек локально на точке, за исключением описанных в настоящем руководстве, по умолчанию **не рекомендуется**.
- Данное руководство включает в себя разделы тонкой настройки через CLI, дополняющие общее руководство в отдельных вопросах. Руководство по CLI в данный момент находится в разработке. Любые действия в CLI, кроме описанных в данном руководстве, могут привести к **ошибкам** в работе контроллера. Настройка контроллера только через CLI в данный момент невозможна.

1.1. ПРИМЕЧАНИЯ

- Настоящее руководство описывает работу контроллера версии 1.1.6. Все примеры, скриншоты и инструкции актуальны для этой версии.
- В приведенных примерах команд для CLI значения, которые необходимо заменить, обозначены **бордовым цветом**.
- В данном руководстве приведены скриншоты русскоязычной версии веб-интерфейса. Версия веб-интерфейса на английском языке выглядит аналогично.

1.2. ОСНОВНЫЕ ТЕРМИНЫ И СОКРАЩЕНИЯ

БЛВС – беспроводная локальная вычислительная сеть

ВМ – виртуальная машина

КУ – клиентское устройство

ЛВС – локальная вычислительная сеть

ОС – операционная система

ПО – программное обеспечение

ТД – точка доступа

ЦОД – центр обработки данных

AP – Access Point

GUI – Graphical User Interface

HA – High Availability

SA – Standalone

SSID – Service Set Identifier



VIP – Virtual IP

Организация – шаблон конфигурации точек доступа, позволяющий задать единые настройки для группы ТД

Нода – одна из виртуальных машин контроллера в составе резервированной пары (НА)

НА-пара / резервированная пара – две ноды контроллера, синхронизированные между собой и объединенные логически в один контроллер, имеющий виртуальный IP-адрес



2. ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ И НАСТРОЙКА СЕТИ

2.1. Системные требования для установки

Таблица 1 – Системные требования для установки

Параметр	до 300 ТД	до 5000 ТД	до 10000 ТД
Совместимый гипервизор	см. примечания к версии: https://www.qtech.ru/catalog/wireless/lan_controllers/kontroller_atlas/#documentation		
vCPU	2	4	8
RAM	8 ГБ	16 ГБ	32 ГБ
Дисковое пространство	60 ГБ	100 ГБ	200 ГБ
Сетевые интерфейсы	1Гбит/с	1Гбит/с	1Гбит/с

❗ ВАЖНО: необходимо обеспечить **резервирование электропитания** серверов, на которых развернут беспроводной контроллер QTECH Atlas!

2.2. Требования к настройкам сети

IP-АДРЕСАЦИЯ И DHCP

- В локальной сети должен быть настроен DHCP-сервер для автоматической выдачи IP-адресов точкам доступа и беспроводным клиентским устройствам.
- Контроллеру должен быть выделен статический IP-адрес в менеджмент-сети или закрепленный по MAC-адресу IP-адрес в DHCP-пуле.
- Для подключения ТД к контроллеру рекомендуется использовать опцию 43 DHCP.

СЕТЕВАЯ ИНФРАСТРУКТУРА

- Контроллер может быть расположен в локальной сети и L2-доступности с точками доступа.
- Должна быть обеспечена L3-доступность точек доступа и контроллера.

❗ При L3-сценарии необходимо убедиться, что трафик разрешен на межсетевых экранах.

VLAN-КОНФИГУРАЦИЯ

- Менеджмент IP-адрес точек доступа должен находиться в нетегированном VLAN.



- Пользовательские VLAN, связанные с SSID, должны быть сконфигурированы на портах ЛВС для точек доступа в тегированном (tagged) режиме.

Сценарии развертывания и примеры сетевых настроек см. в разделе [Сценарии развертывания](#).



3. УСТАНОВКА КОНТРОЛЛЕРА

3.1. Установка контроллера на ESXi

Ниже описан процесс установки контроллера на примере ESXi 7.0.

3.1.1. Предварительные настройки

❗ ВАЖНО! После развертывания виртуальной машины контроллера, при первом запуске она должна получить IP-адрес по DHCP!

Перейдите в раздел **Networking** и создайте или отредактируйте port group в соответствии с примером ниже (рис. 3-1). **Обязательно:**

- в поле **VLAN ID** впишите число **4095**, что означает, что разрешены все VLAN;
- переключатель **Promiscuous mode** установите на **Accept**.

Рисунок 3-1. Настройки в ESXi

3.1.2. Установка

1. Перейдите в **Virtual Machines** и нажмите кнопку **Create / Register VM**

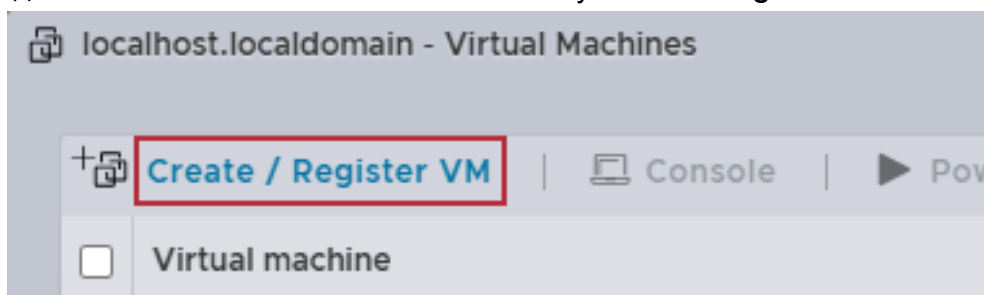


Рисунок 3-2. Создание виртуальной машины



2. Выберите **Deploy a virtual machine from an OVF or OVA file**

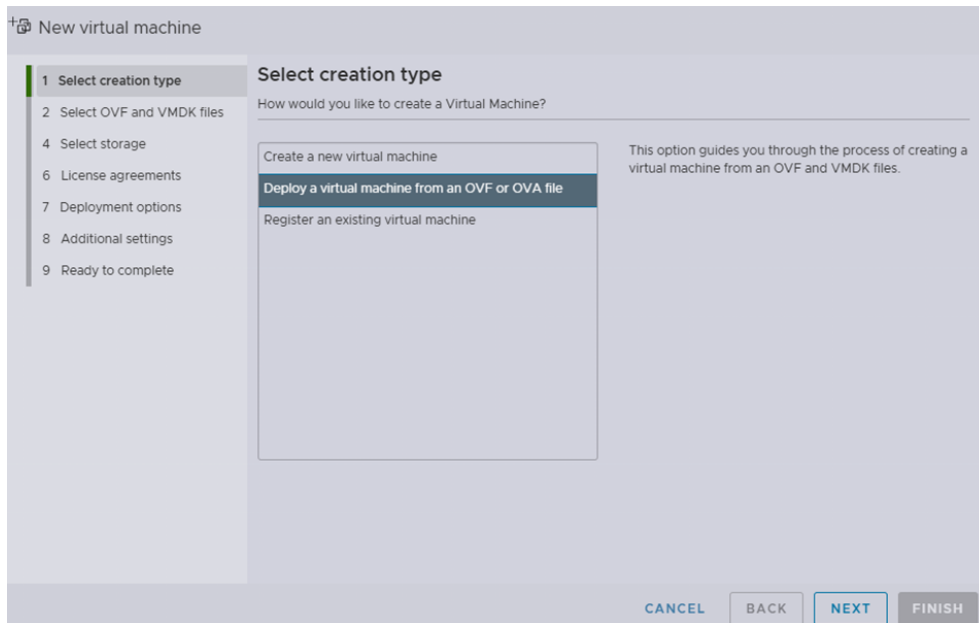


Рисунок 3-3. Создание виртуальной машины

3. Загрузите OVF и VMDK файлы

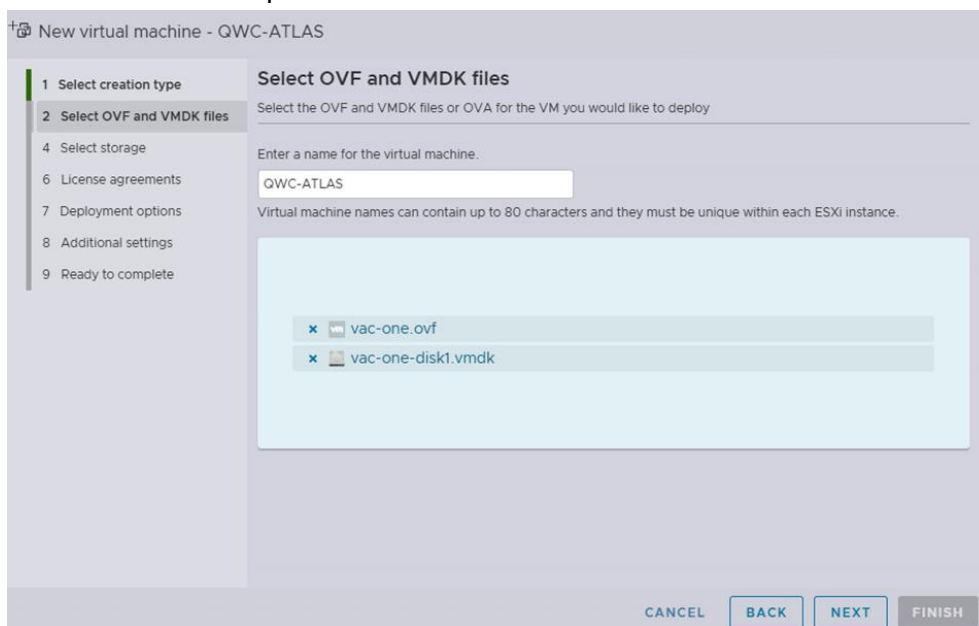


Рисунок 3-4. Создание виртуальной машины

4. Выберите хранилище и port group. Проверьте настройки и нажмите **FINISH**.

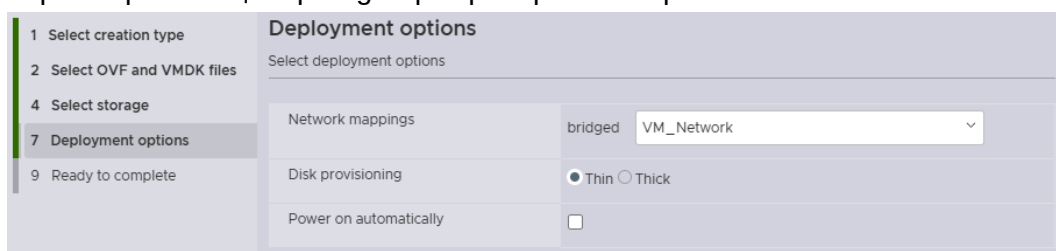
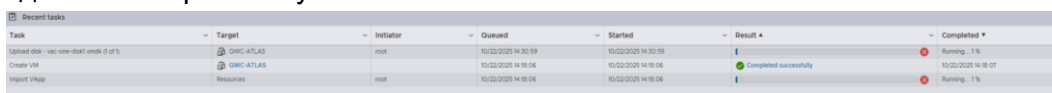


Рисунок 3-5. Создание виртуальной машины

5. Дождитесь завершения установки



Task	Target	Initiator	Queued	Started	Result	Completed
Update disk - vnc-one-disk mode 0 of 5	QWIC-ATLAS	root	10/22/2025 14:30:59	10/22/2025 14:30:59	Completed successfully	Running - 1%
Create vnc	QWIC-ATLAS	root	10/22/2025 14:30:59	10/22/2025 14:30:59	Completed successfully	Running - 1%
Import vnc	Resources	root	10/22/2025 14:30:59	10/22/2025 14:30:59	Completed successfully	Running - 1%

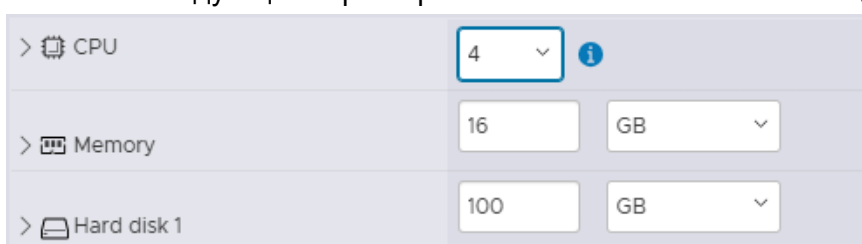
Рисунок 3-6. Завершение установки

6. После завершения установки нажмите на созданную виртуальную машину. Нажмите **Edit** на верхней панели.



Рисунок 3-7. Изменение параметров виртуальной машины

7. Измените значения следующих характеристик в соответствии в табл. 1 ([раздел 2.1](#))



> CPU	4	
> Memory	16	GB
> Hard disk 1	100	GB

Рисунок 3-8. Изменение параметров виртуальной машины

8. Настройте автозапуск VM. Для этого перейдите в **Manage > System > Autostart**. Выберите нужную VM, и нажмите **Enable** на верхней панели.

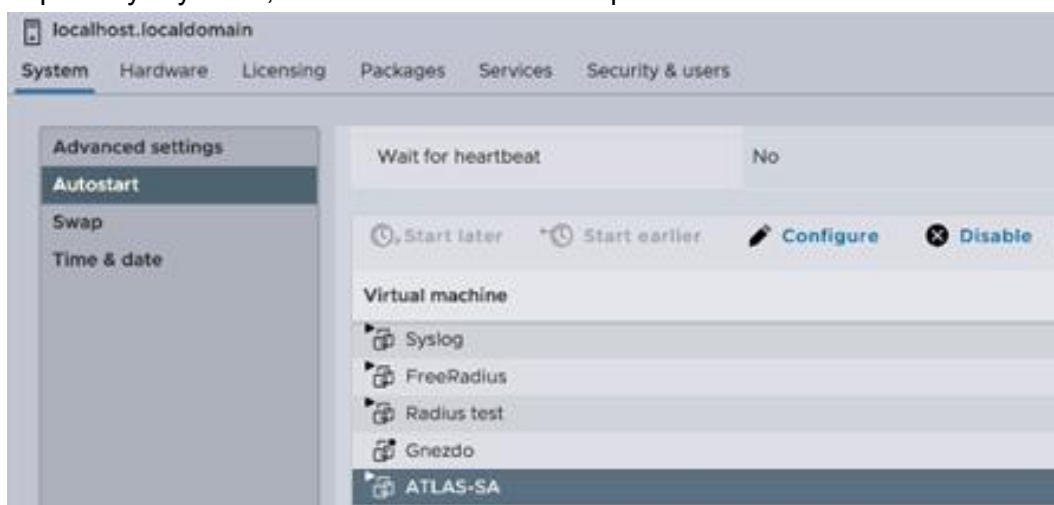


Рисунок 3-9. Настройка автозапуска виртуальной машины

❗ После завершения установки выполните шаги, описанные в [разделе 5](#).

❗ **ВНИМАНИЕ!** В случае необходимости переноса VM с контроллером на другой сервер, ознакомьтесь с инструкцией в [разделе 6](#).



3.2. Установка контроллера на VirtualBox

В этом разделе описана установка на VirtualBox в РЕД ОС и Windows.

3.2.1. Установка VirtualBox

Для РЕД ОС

1. Откройте терминал и выполните следующую команду:

```
sudo dnf install VirtualBox
```

2. Добавьте пользователя в группу vboxusers, чтобы предоставить доступ к функциям VirtualBox.

```
sudo usermod -aG vboxusers username
```

username - имя созданного при установке РЕД ОС пользователя

3. Перезагрузите, чтобы применить изменения.

```
reboot
```

Для Windows

Скачайте VirtualBox с официального сайта и установите.

3.2.2. Установка контроллера

❗ ВАЖНО! После развертывания виртуальной машины контроллера, при первом запуске она должна получить IP-адрес по DHCP!

1. Нажмите **Импортировать**, выберите .ovf файл. Нажмите **Далее**, затем **Готово**.

❗ Убедитесь, что в папке с .ovf файлом присутствуют связанные файлы .mf и .vmdk, поскольку они являются частью образа виртуальной машины и необходимы для корректного завершения импорта.

2. Дождитесь завершения импорта конфигурации.

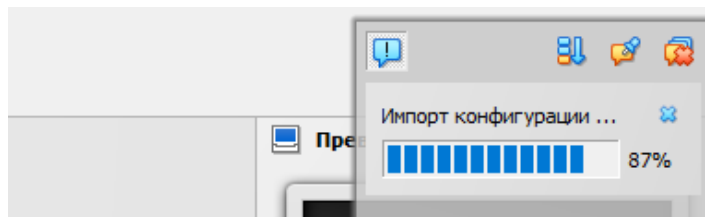


Рисунок 3-10. Импорт конфигурации

3. Перейдите в **Инструменты > Носители**.

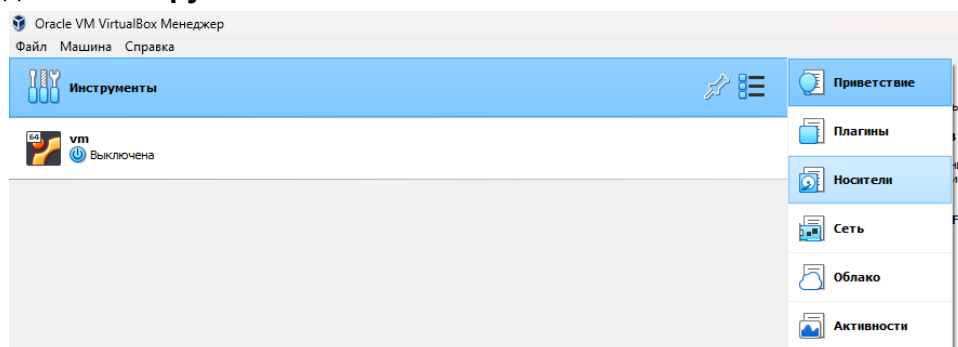


Рисунок 3-11. Переход в настройки носителей

- Нажмите на импортированную VM, затем Свойства на верхней панели. Измените размер диска в соответствии с Таблицей 1. Нажмите **Применить**.

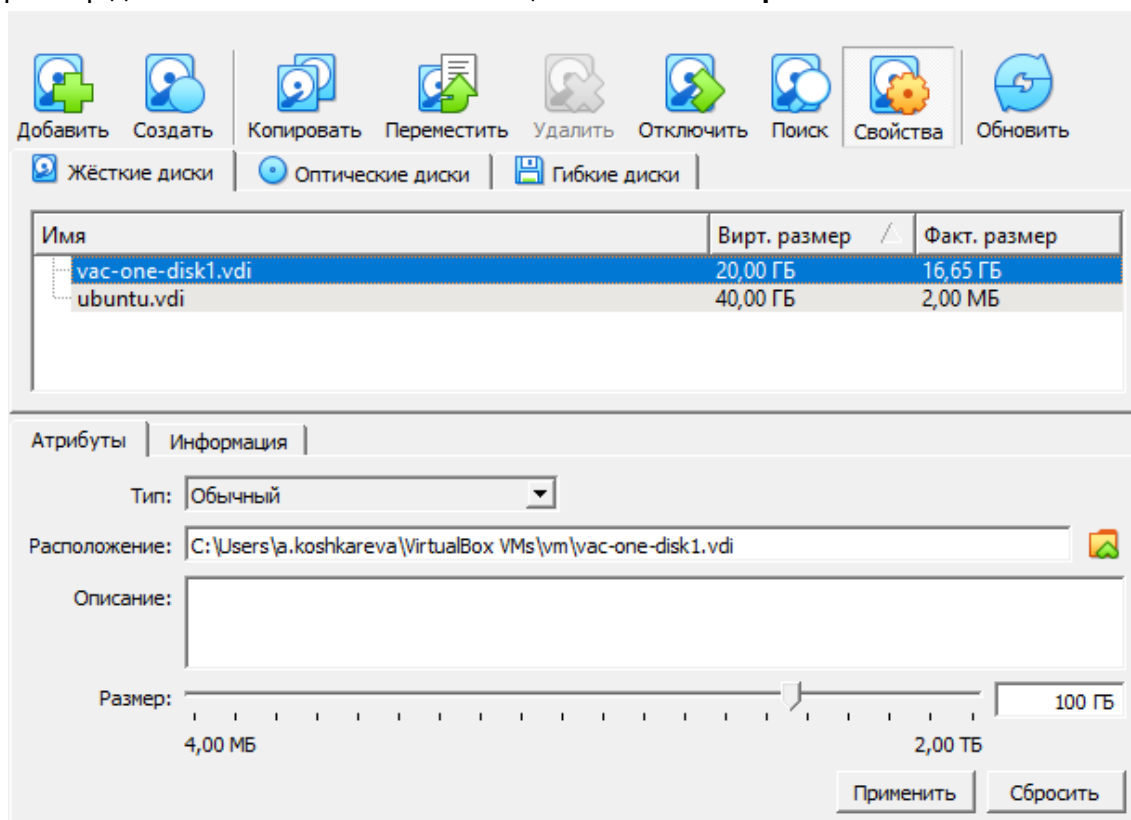


Рисунок 3-12. Настройка размера диска

- Нажмите на VM, затем **Настроить**.

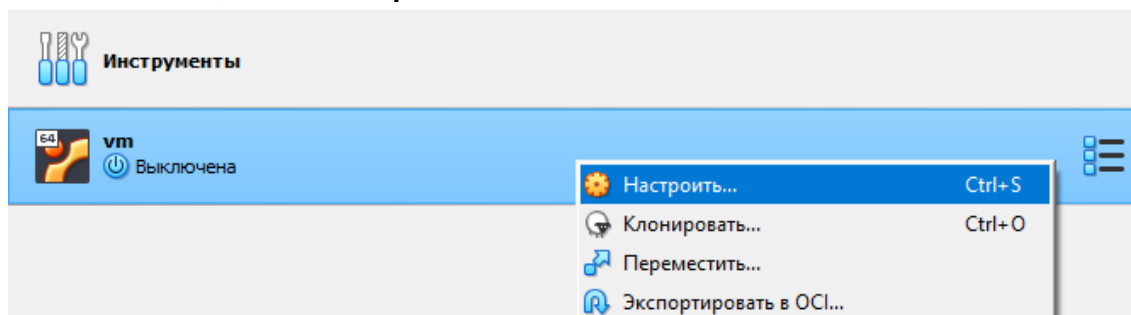


Рисунок 3-13. Переход к настройкам VM

- Перейдите во вкладку **Сеть > Дополнительно** в списке **Неразборчивый режим** выберите **Разрешить всё**

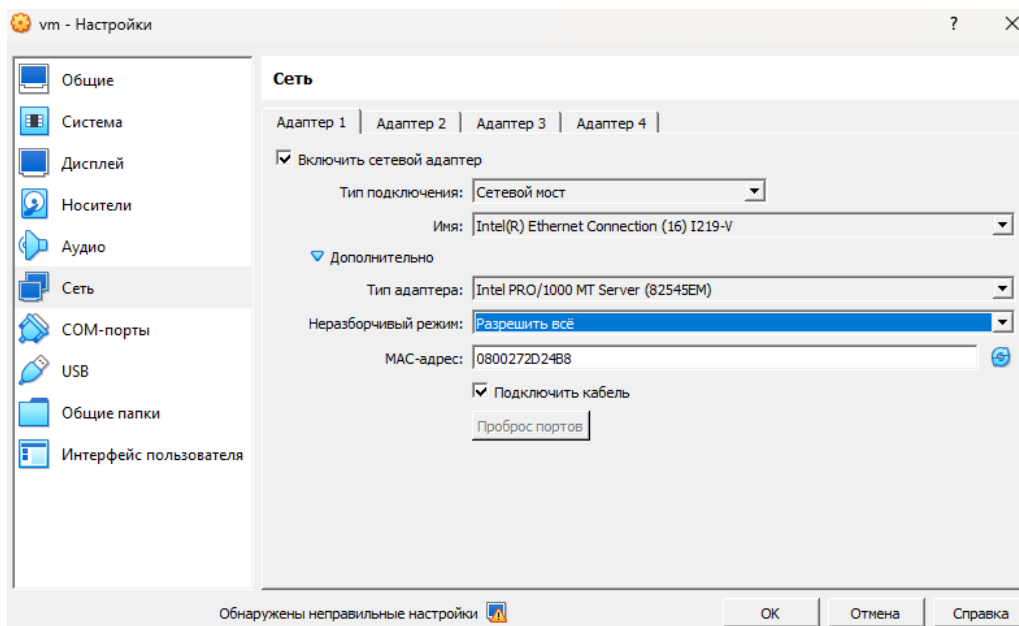


Рисунок 3-14. Настройка незборчивого режима

Устранение неполадок

При возникновении ошибок введите в терминале РЕД ОС команду:

```
sudo ip link set enp2s0 promisc on
```

enp2s0 – имя сетевого интерфейса

❗ После завершения установки выполните шаги, описанные в [разделе 5](#).

❗ **ВНИМАНИЕ!** В случае необходимости переноса ВМ с контроллером на другой сервер, ознакомьтесь с инструкцией в [разделе 6](#).

3.3. Установка контроллера на Hyper-V

3.3.1. Предварительные настройки

❗ **ВАЖНО!** После развертывания виртуальной машины контроллера, при первом запуске она должна получить IP-адрес по DHCP!

1. Перед импортом виртуальной машины необходимо настроить параметры сети. Для этого перейдите в раздел **Действие** и далее в **Диспетчер виртуальных коммутаторов**.
2. Далее выберите **Внешняя** и нажмите **Создать**.

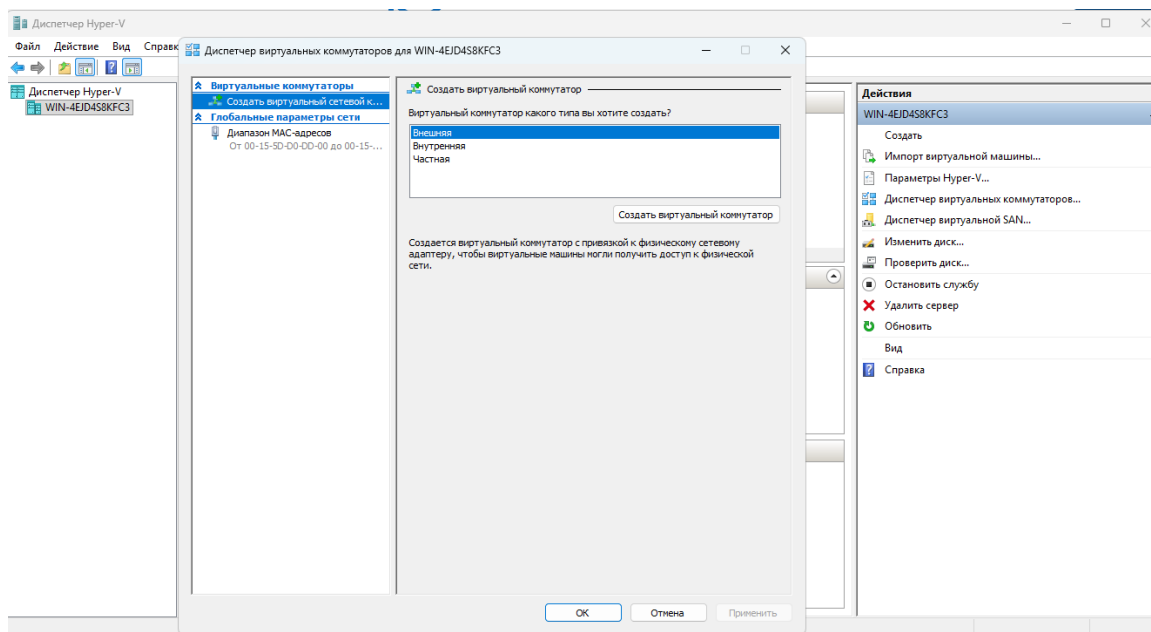


Рисунок 3-15. Настройка параметров сети

3. Настройте параметры по примеру ниже (рис. 3-16), затем нажмите **Ок**.

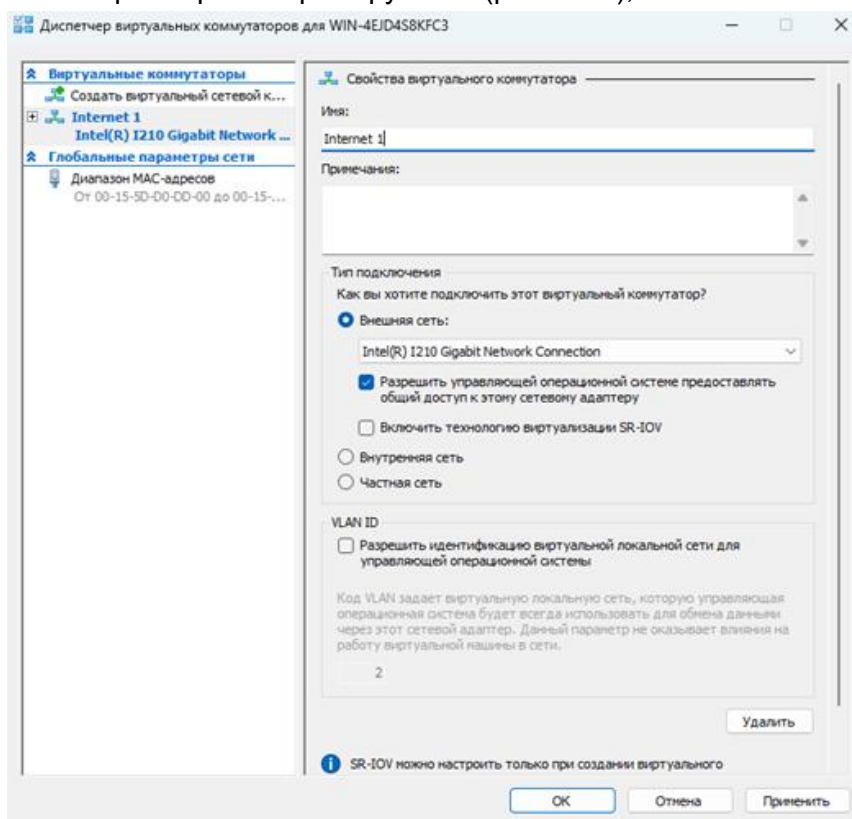


Рисунок 3-16. Настройка параметров сети

3.3.2. Установка контроллера

1. Перейдите в **Диспетчер Hurer-V** и нажмите на текущий сервер, затем **Импорт виртуальной машины**.

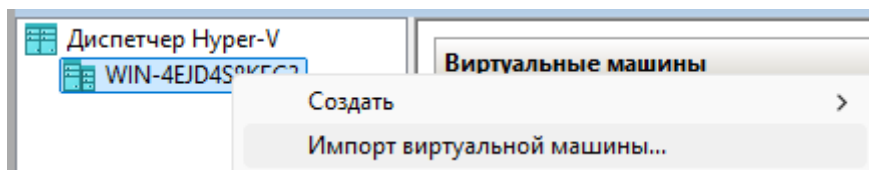


Рисунок 3-17. Импорт виртуальной машины

2. Выберите папку (распакованный архив) с образом виртуальной машины, затем нажмите **Далее**.
3. Нажмите **Далее**.

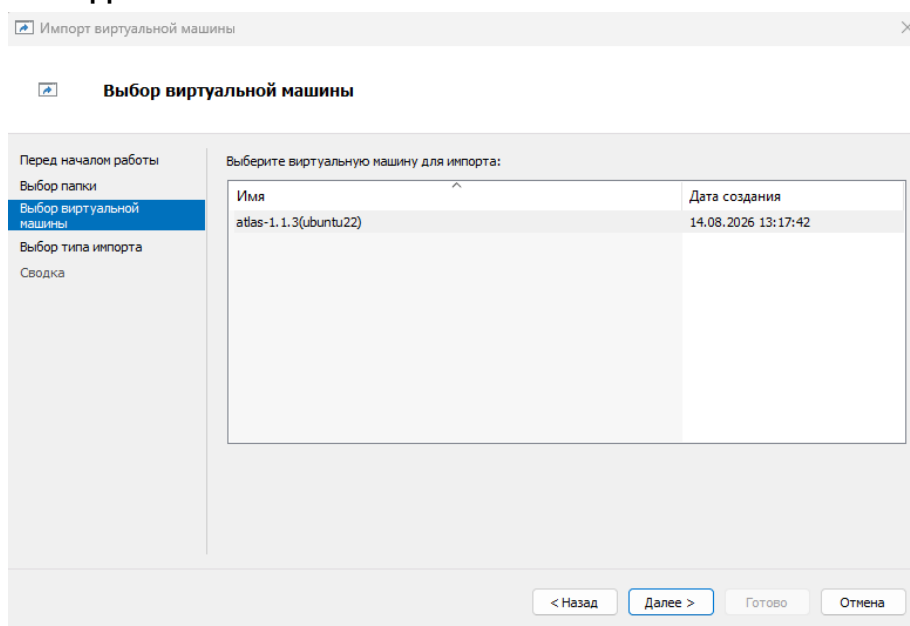


Рисунок 3-18. Импорт виртуальной машины

4. Выберите **Регистировать виртуальную машину по месту (использовать существующий уникальный идентификатор)**, затем нажмите **Далее**.

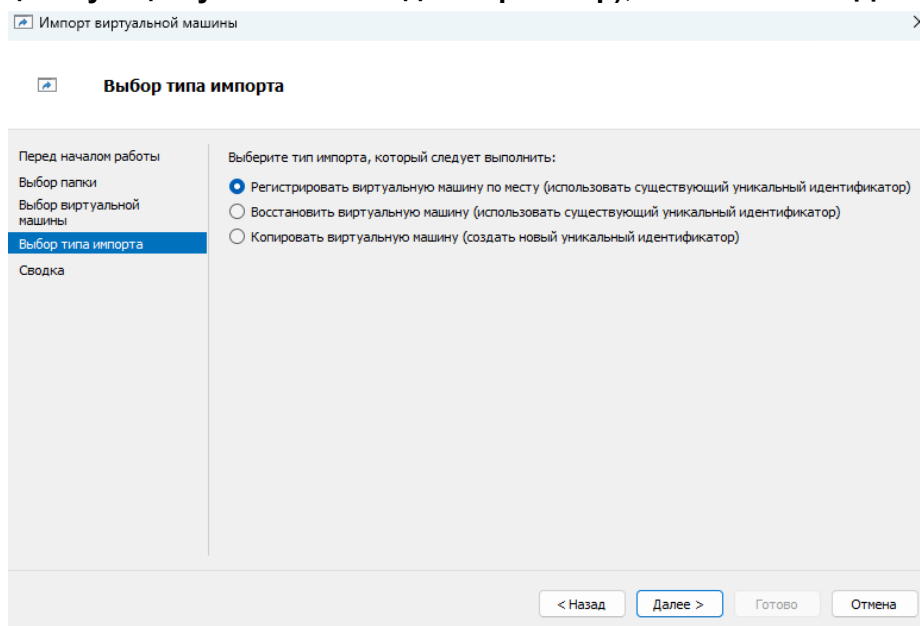


Рисунок 3-19. Импорт виртуальной машины



5. После завершения работы нажмите **Готово**.

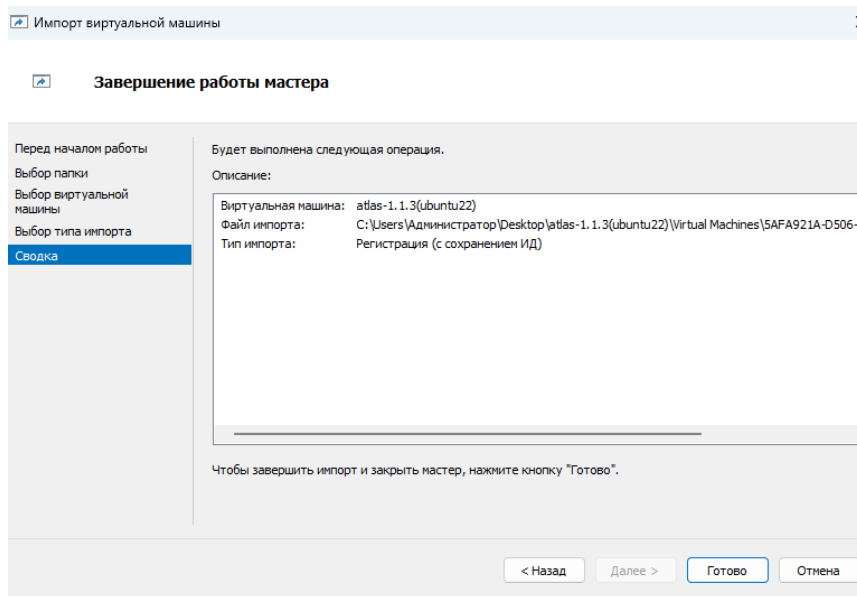


Рисунок 3-20. Завершение импорта

❗ После завершения установки выполните шаги, описанные в [разделе 5](#).

❗ **ВНИМАНИЕ!** В случае необходимости переноса ВМ с контроллером на другой сервер, ознакомьтесь с инструкцией в [разделе 6](#).



4. РАБОТА С ПРЕДУСТАНОВЛЕННЫМИ ПЛАТФОРМАМИ

4.1. Порядок работы

1. Извлеките сервер из упаковочной тары и установите в стойку.
2. Подключите сервер согласно схеме подключения из раздела [Сценарии развертывания](#) с учетом выбранного сценария.
3. Подключите ПК в одну подсеть с сервером и установите на нём следующие сетевые параметры:
 - IP-адрес: **192.168.1.2**;
 - Маска подсети: **255.255.255.0**;
 - Шлюз: **192.168.1.1**.
4. Откройте браузер и перейдите в веб-интерфейс контроллера.
 - IP-адрес по умолчанию: **192.168.1.200**
 - Логин / пароль: **admin / admin1234**



5. Перед началом работы с контроллером выполните шаги, описанные в [разделе](#)



5. НАЧАЛО РАБОТЫ С КОНТРОЛЛЕРОМ

⚠ ВНИМАНИЕ: для корректной работы контроллеры обязательно выполните шаги ниже:

1. Перейдите в браузере по IP-адресу ВМ.

Логин пароль: **admin / admin1234**

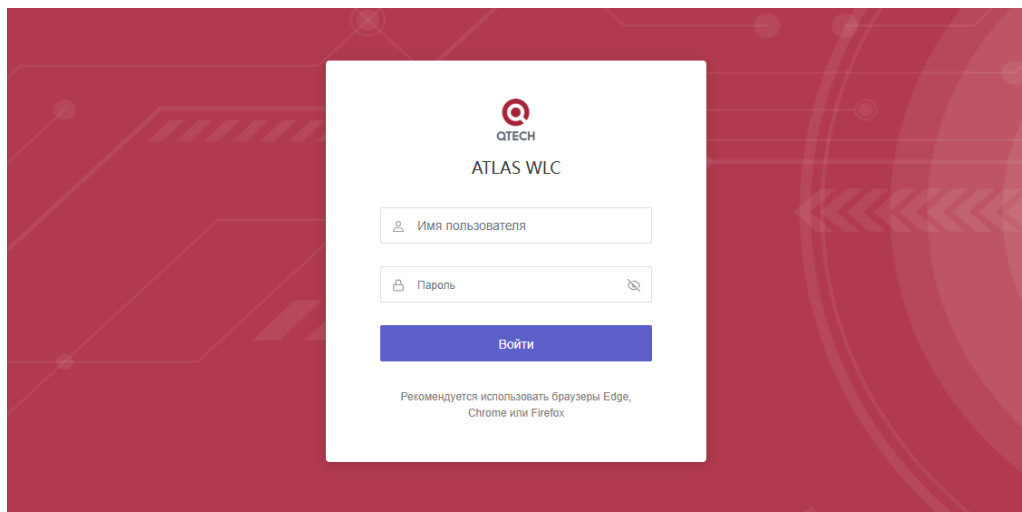


Рисунок 5-1. Вход в систему

2. Назначьте статический IP-адрес контроллеру (см. [раздел 9.2](#))
3. Примените ключи (см. [раздел 8](#))
4. Установите правильное системное время (см. [раздел 9.3](#))



6. ПЕРЕНОС ВИРТУАЛЬНОЙ МАШИНЫ С КОНТРОЛЛЕРОМ

В случае необходимости переноса VM с контроллером используйте следующую последовательность действий.

⚠ Прежде чем переносить виртуальную машину с контроллером QWC-ATLAS **внимательно ознакомьтесь** с инструкцией ниже!

Данная инструкция приведена для гипервизора VMWare ESXi 7. Перенос на всех прочих гипервизорах должен выполняться по аналогичному принципу.

⚠ **ВАЖНО! Неправильный перенос VM (путем экспорта и регистрации VM) повлечет за собой следующие последствия:**

- смена MAC-адреса VM;
- ключ активации становится недействительным.

6. Включите SSH на ESXi через Host → Actions → Services → Enable SSH

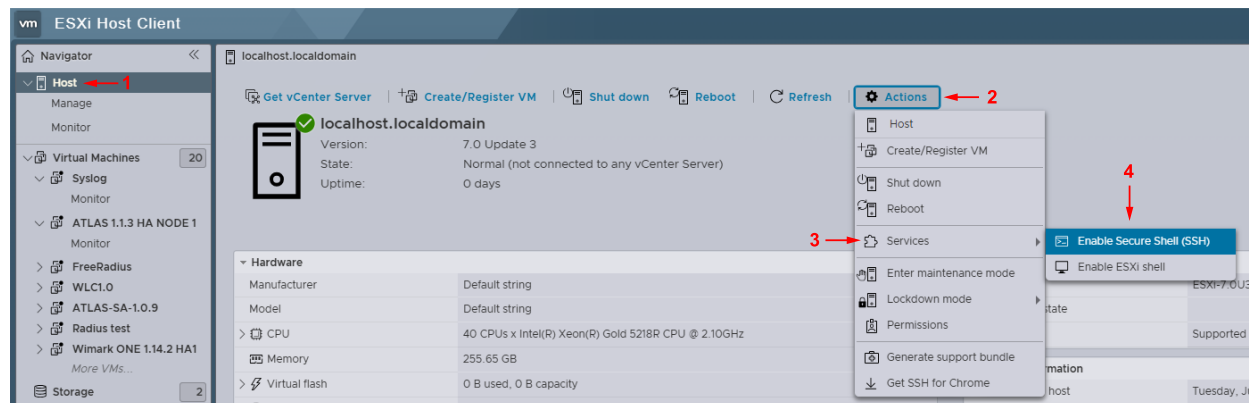


Рисунок 6-1. Включение SSH на ESXi

7. Выключите виртуальную машину
8. Подключитесь к ESXi по SSH
9. Перейдите в каталог виртуальных машин:

```
cd /vmfs/volumes
```

10. Скопируйте каталог виртуальной машины на свой сервер

```
scp -r root@IP_ESXi:/vmfs/volumes/datastore1/VM /путь/на/своем/сервере/VM
```

11. Дождитесь завершения копирования.

⚠ Файл -flat.vmdk может иметь значительный размер – процесс копирования может занять продолжительное время.

12. Перенесите каталог на новый ESXi

```
scp -r /путь/на/своем/сервере/OLD_VM root@IP_ESXi:/vmfs/volumes/datastore2/NEW_VM
```

13. Проверьте на новом ESXi наличие всех файлов:

- .vmx конфигурация;
- .vmdk и -flat.vmdk диски;
- .nvram;



- .vmxf;
 - .vmsd (если есть снапшоты).
14. Зарегистрируйте виртуальную машину через файл .vmx. Правой кнопкой мыши → Register VM

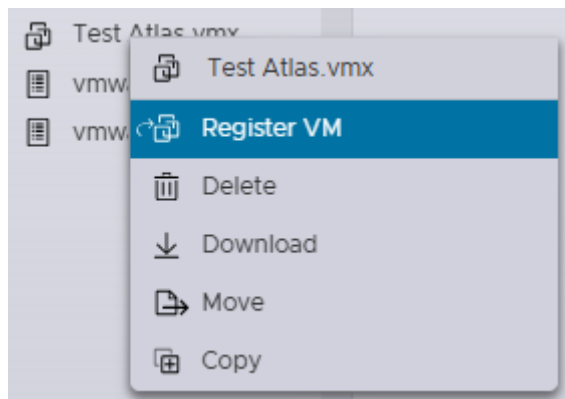


Рисунок 6-2. Регистрация виртуальной машины

15. При первом запуске выберите **I moved it**.



7. ИНТЕРФЕЙС ПЛАТФОРМЫ

7.1. Домашняя страница

После успешной авторизации вы увидите домашнюю страницу контроллера, содержащую главное меню. Разделы главного меню описаны в табл. 2.

Таблица 2 – Разделы главного меню контроллера

Раздел главного меню	Опции
 CLI	• переход в веб-консоль для конфигурирования контроллера
 Сеть	• настройки сети
 Обновление	• обновление ПО контроллера
 Сброс	• сброс до заводских настроек
 Активация	• применение активационных ключей
 Управление	• переход на основную страницу для управления ТД
 Время	• настройка часового пояса • настройка NTP
 Бэкап	• сохранение резервной копии конфигурации контроллера
 Восстановление	• восстановление конфигурации контроллера из резервной копии



Раздел главного меню	Опции
 О системе	• информация о версии ПО контроллера
 НА	• настройка резервированной пары (High Availability) • просмотр состояния резервированной пары
 Сертификат HTTPS	• добавление SSL-сертификата
 Нагрузка	• информация о состоянии и ресурсах системы
 Перезагрузка	• перезагрузка контроллера

7.2. Управление

Основные функции контроллера осуществляются на странице **Управление**. Страница **Управление** содержит навигационное меню с разделами, каждый из которых открывает окна для настройки соответствующих опций.

Таблица 3 – Меню страницы «Управление»

Раздел меню	Опции
 Организация	• создание, просмотр и редактирование организаций
 Пользователи	• просмотр списка подключенных КУ • создание и редактирование учетных записей для портала авторизации и MAC-авторизации; • создание группы локальных пользователей
 Точки доступа	• мониторинг статусов ТД; • управление ТД: перезагрузка, применение организации и др.
 	• конфигурация встроенного портала авторизации;



Раздел меню	Опции
Портал и AAA	- настройка внешнего RADIUS сервера; - настройка внешнего портала авторизации; - ограничение числа подключенных КУ для локального аккаунта пользователя
 Wi-Fi	создание, настройка, редактирование SSID
 Статистика	статистические данные о КУ, ТД, трафике, радио
 Журналы событий	- история подключения КУ; - состояние ТД; - история действий на контроллере.
 Обновить ТД	- загрузка ПО ТД на контроллер; - обновление ТД
 Настройки	- настройка регуляторного домена; - настройка SMTP; - настройка SNMP; - другие настройки.

Для удобства работы с контроллером в веб-интерфейсе используются графические элементы управления в виде иконок. Каждая иконка соответствует определённому действию или функции. Описание и назначение иконок приведены в таблице 4.

Таблица 4 – Элементы управления в веб-интерфейсе контроллера

Иконка	Действие
	Редактировать
	Удалить
	Обновить данные на странице
	Скрыть пароль
	Показать пароль



Иконка	Действие
	Добавить элемент
	Выбрать элемент из списка (чекбокс)
	Переход на домашнюю страницу



8. ПРИМЕНЕНИЕ АКТИВАЦИОННОГО КЛЮЧА

Для полноценной работы контроллера необходимо получить и применить активационные ключи.

8.1. Правила применения активационного ключа

1. **Файлы с активационными ключами.** Для работы контроллера необходимо иметь два файла:

- **MAC_vAC_sys.lic** – файл с активационным ключом системы, разблокирующий функционал контроллера;
- **MAC_vAC_quantity_No.lic** – файл с активационным ключом ТД, определяющий количество точек доступа, которыми может управлять контроллер.

MAC – MAC-адрес контроллера;

quantity – количество точек доступа;

No – номер файла с активационным ключом.

2. **Суммирование количества точек доступа.** Доступное количество точек доступа на контроллере суммируется после применения разных активационных ключей. Например, если на контроллере применен ключ для n точек доступа, то после применения дополнительного ключа для m точек доступа общее количество возможных ТД на контроллере будет равняться $n+m$.

3. **Перевыпуск активационных ключей.** Файлы с активационными ключами генерируются на основе сетевых параметров виртуальной машины. В связи с этим необходим перевыпуск активационных ключей в следующих случаях:

- перенос виртуальной машины с контроллером на другой сервер;
- замена сетевого адаптера.

❗ При замене Backup-ноды в НА-паре **файл с активационным ключом ТД** изменять не требуется. Для новой ноды необходимо заново получить и применить только **файл с активационным ключом системы**.

8.2. Применение активационных ключей в НА-паре.

1. Рекомендуется сначала применить активационные ключи: файл активационного ключа системы на обе ноды и файл активационного ключа ТД на одну из нод, и только после этого объединять их в НА-пару.
2. **Суммирование количества точек доступа.** Доступное количество точек доступа является суммой ТД с обеих нод.
3. Если файл с активационным ключом ТД был сгенерирован на основе аппаратной информации ноды и загружен на данную ноду, то такая нода считается **Primary AC**. В случае выхода из строя **Primary AC**, **Backup AC** продолжает работу, так как файл с активационным ключом ТД временно хранится в памяти резервной ноды. При этом нельзя допускать выключение или перезагрузку Backup-ноды, так как **файл с активационным ключом ТД** станет недействительным.
4. **Primary AC** нельзя заменить без перевыпуска активационных ключей.

8.3. Порядок применения активационного ключа

1. Перейдите в раздел **Лицензия**.



2. Скачайте файл для запроса активационного ключа, нажав кнопку **Скачать** (рис. 8-1). Начнется скачивание файла вида **ff-ff-ff-ff-ff-ff_lic.req**, содержащего в имени внутренний MAC-адрес контроллера. Обратите внимание: он не совпадает с MAC-адресом сетевого интерфейса (CPU-MAC).

Файл запроса лицензии (.req)

Скачать

Отправьте файл **license.req** в техническую поддержку для запроса лицензий.

Рисунок 8-1. Получение файла для запроса активационных ключей

3. Для получения активационных ключей создайте тикет в тех. поддержке.
 - 3.1. Перейдите по ссылке <https://qtech.intradesk.ru/task/list/create>
 - 3.2. Создайте заявку и обозначьте тему заявки «Активация ключей QTECH Atlas».
 - 3.3. В заявке прикрепите файл **ff-ff-ff-ff-ff-ff_lic.req**.
 - 3.4. В веб-интерфейсе контроллера перейдите в CLI и введите команду **show version**. Полученный вывод прикрепите к тикету.
 - 3.5. При отгрузке беспроводного решения **QTECH** передаётся сертификат. **ID сертификата** также нужно указать в тикете.

Пример ID сертификата:

СИ999-01042026

Пример вывода команды **show version**:

```
ATLAS WLC>en
ATLAS WLC#show version
  ATLAS WLC Device, Compiled on Dec 09 11:15:54 2025
  sysLocation
  CPU MAC          00-0c-29-5d-46-49
  VLAN MAC         af-88-26-5d-46-49
  SoftWare Version 1.0.10
  Serial No        af88265d4649

  All rights reserved
  Uptime is 0 weeks, 0 days, 0 hours, 16 minutes
```

Рисунок 8-2. Пример вывода команды **show version**

4. После этого вы получите два файла с активационными ключами.
- ❗ **Время ответа по запросу активационных ключей составляет 1-2 рабочих дня.**
5. Загрузите **Файл лицензии системы** (1) и **Файл лицензии на точки доступа** (2), нажав кнопку **Загрузить**.
- ❗ **ВНИМАНИЕ!** Перед тем как активировать ключи, откройте CLI контроллера и убедитесь, что в выводе команды **show version** в строках **CPU MAC** и **VLAN MAC** указаны корректные данные. В случае, если отображаются нули **00-00-00-00-00-00**, перезагрузите беспроводной контроллер, и проверьте вывод **show version** снова.

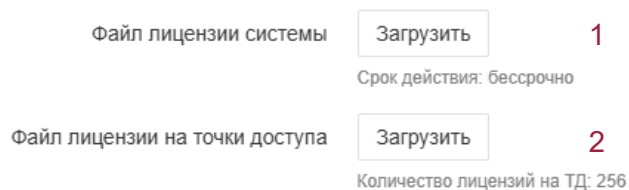


Рисунок 8-3. Загрузка файлов с активационными ключами

8.4. Проверка применения активационного ключа

Перейдите в CLI и проверьте применение активационных ключей (см. [раздел «Проверка применения активационных ключей»](#)).



9. СИСТЕМНЫЕ НАСТРОЙКИ КОНТРОЛЛЕРА

9.1. Переключение языка веб-интерфейса

Перейдите по IP-адресу контроллера. В правом верхнем углу страницы авторизации выберите нужный язык.



Рисунок 9-1. Переключение языка веб-интерфейса

9.2. Изменение IP-адреса контроллера

1. На главной странице контроллера перейдите в раздел **Сеть**. Установите переключатель **IP адрес по DHCP** влево, чтобы отключить получение IP адреса по DHCP. Впишите IP-адрес контроллера, маску сети, шлюз, а также основной и альтернативный DNS-сервера.

Рисунок 9-2. Пример настройки статического IP-адреса контроллера

2. Перейдите по новому IP-адресу в новой вкладке браузера.

9.3. Настройка времени и NTP-сервера

1. На главной странице контроллера перейдите в раздел **Время**.
2. Выберите часовой пояс в соответствующем выпадающем списке, а также настройте дату и время в поле **Установить время вручную**.



Рисунок 9-3. Настройка даты и времени на контроллере

3. Чтобы настроить синхронизацию через NTP-сервер, установите переключатель **Служба NTP** вправо и впишите адрес NTP-сервера в поле **NTP-сервер**.

При необходимости вы можете добавить несколько NTP-серверов. Для этого впишите их, разделив запятыми. Поле может содержать не более 60 символов!

Служба NTP

NTP-сервер

несколько серверов NTP, разделенных запятыми.

Рисунок 9-4. Настройка NTP-сервера на контроллере

(i) После изменения времени или часового пояса на контроллере время на точках доступа обновляется не сразу. Синхронизация выполняется автоматически - точка доступа периодически запрашивает текущее время у контроллера. После стабилизации времени интервал между запросами увеличивается для снижения сетевой нагрузки. Поэтому точка доступа может некоторое время использовать предыдущее значение времени. В зависимости от текущего интервала синхронизация может занять от нескольких минут до 1,5 часа.

Если необходимо применить изменения немедленно, перезагрузите точки доступа. После перезагрузки и восстановления связности с контроллером синхронизация времени выполняется сразу.



9.4. Обновление ПО контроллера

❗ ВАЖНО:

- перед обновлением контроллера ознакомьтесь с примечаниями к актуальной версии ПО на странице контроллера (вкладка «**Документация и ПО**») на сайте <https://www.qtech.ru/>;
- обновление возможно только на версию равную или выше текущей;
- файл обновления ПО контроллера имеет формат **.tar**;
- обновление ПО резервированной пары осуществляется на каждой ноде отдельно!

1. На домашней странице контроллера перейдите в **Обновление**. Нажмите **Загрузить** для загрузки файла с ПО.

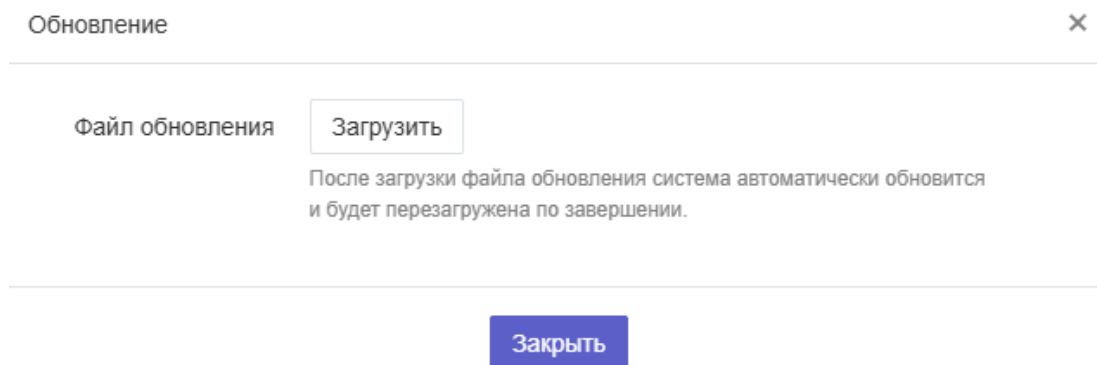


Рисунок 9-5. Обновление контроллера

2. Обновление начнется автоматически и займёт не более 5 минут. После успешного завершения обновления произойдет перенаправление на главную страницу обновленного контроллера. Если это не произошло, откройте веб-интерфейс контроллера в новой вкладке.
3. Проверьте, что обновление прошло успешно. Для этого откройте раздел **О системе** и убедитесь, что версия ПО соответствует установленной.

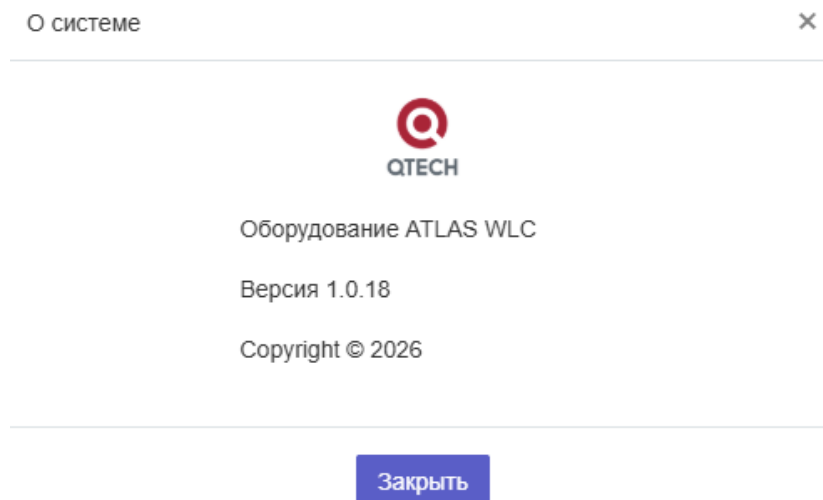


Рисунок 9-6. Информация о версии контроллера

9.5. Создание и восстановление резервной копии конфигурации через WEB-интерфейс

❗ ВАЖНО:

- файл резервной копии должен соответствовать текущей версии системы;
- при несовпадении версий восстановление может завершиться с ошибкой;
- в процессе восстановления контроллер автоматически перезагружается;
- при HA-конфигурации достаточно выполнить восстановление на master-ноде — после её перезагрузки конфигурация будет автоматически синхронизирована со всеми узлами кластера.
- файлы резервных копий SA- и HA-контроллеров несовместимы между собой

1. Получить файл резервной копии можно в разделе **Бэкап** на главной странице. В этом разделе можно скачать файл, созданный за последние 5 дней, либо создать новый с текущей конфигурацией, нажав кнопку **Создать бэкап**.

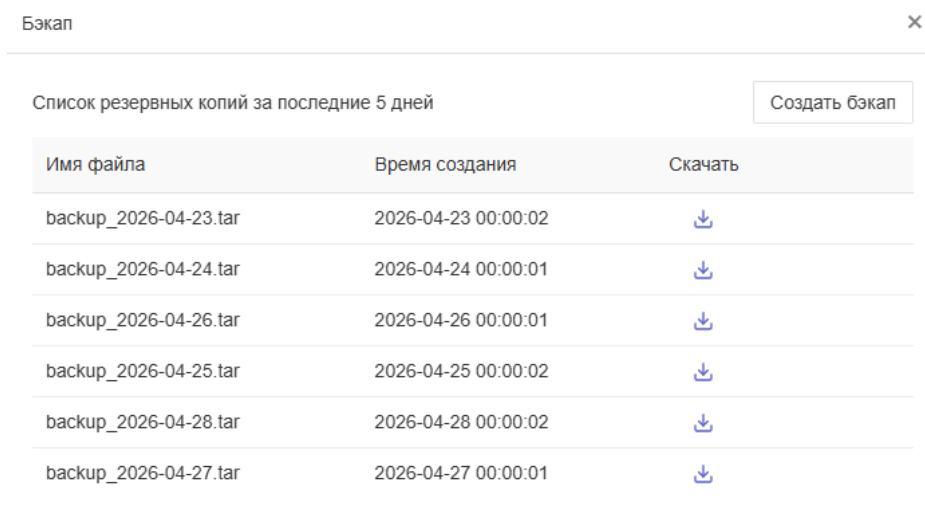


Рисунок 9-7. Раздел Backup



2. Чтобы выполнить восстановление из имеющейся резервной копии, необходимо перейти в раздел **Восстановление** и загрузить файл с помощью кнопки **Загрузить**.

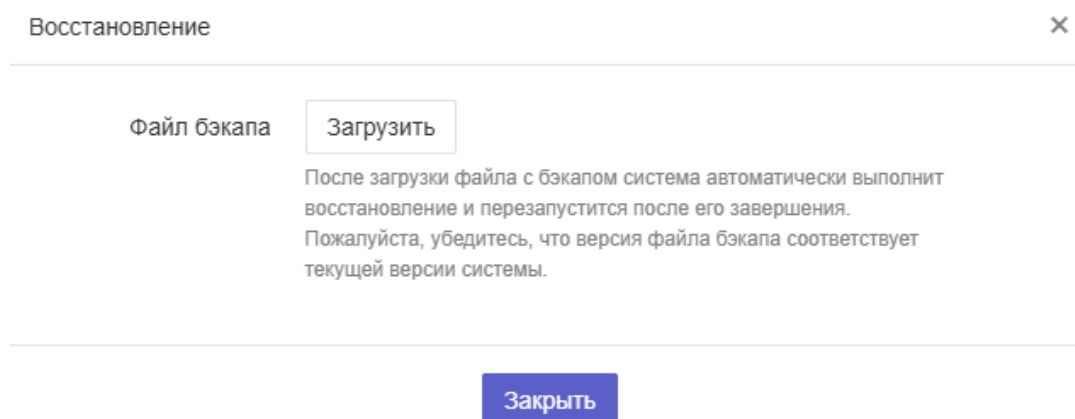


Рисунок 9-8. Раздел «Восстановление»

9.6. Сброс до заводских настроек

1. На домашней странице контроллера нажмите на **Сброс**, затем **Ок**

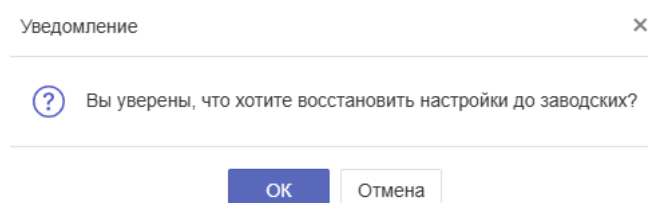


Рисунок 9-9. Сброс до заводских настроек

После этого все настройки на контроллере будут сброшены.



10. НАСТРОЙКА РЕЗЕРВИРОВАННОЙ ПАРЫ (HIGH AVAILABILITY)

10.1. Конфигурация резервированной пары

⚠ ВАЖНО: перед настройкой HA ознакомьтесь с [правилами применения активаций в HA-паре](#).

1. Создайте вторую виртуальную машину с контроллером аналогично [разделу 3](#).
2. Перейдите в веб-интерфейс по IP-адресу контроллера, являющегося **Primary AC**. На домашней странице контроллера перейдите в **HA**.
3. В поле **Резервный IP** впишите IP-адрес второго контроллера. В поле **Виртуальный IP** впишите виртуальный IP-адрес, который будет являться IP-адресом HA контроллера.
4. Если в подсети уже есть HA-пара, измените значение поля **ID кластера**, например, на 244. **ID кластера** каждой HA-пары в подсети должен быть уникальным. Если это единственная HA-пара в подсети, оставьте значение по умолчанию.

HA ×

Основной IP

10.78.64.38

Резервный IP

Виртуальный IP

ID кластера

Если в сети несколько HA-кластеров, укажите уникальный ID (1-255) для каждого.

Запустить

Закрыть

Рисунок 10-1. Настройка HA-пары

5. Нажмите **Запустить** для применения настроек.

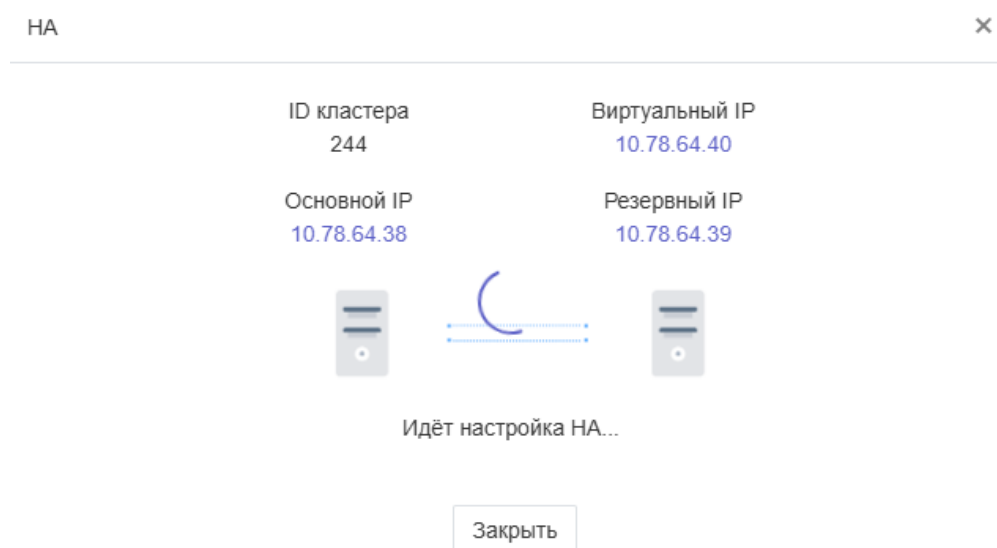


Рисунок 10-2. Настройка HA-пары

6. Через 1-2 минуты перейдите по виртуальному IP-адресу и убедитесь, что контроллер доступен по этому адресу.

10.2. Мониторинг состояния

Проверить состояние нод можно в разделе **НА**.

Статус «**Синхронизация в норме**» свидетельствует о корректной работе HA-пары (рис. 10-3).

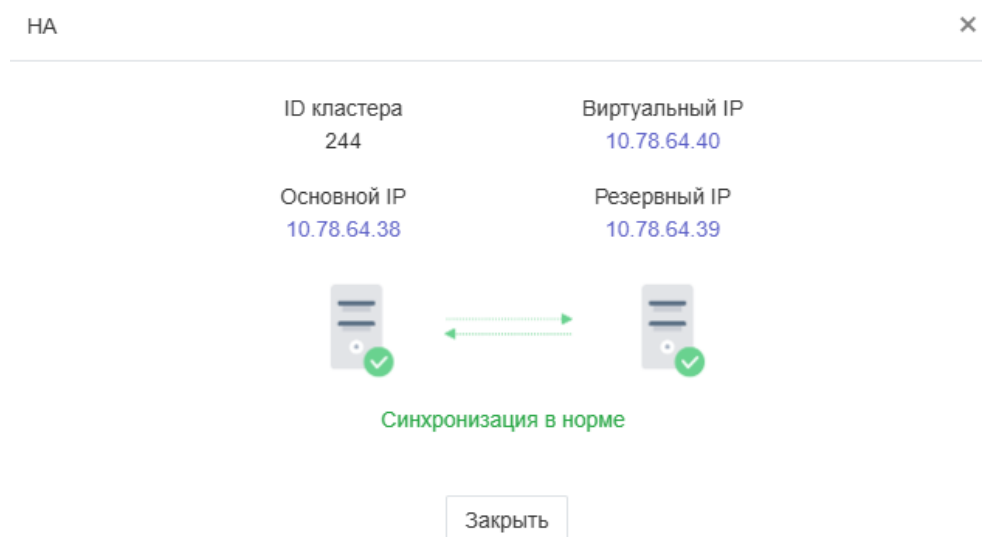


Рисунок 10-3. Корректная работа HA-пары

В случае недоступности одной из нод статус изменится на «**Резервный узел недоступен**» (рис. 10-4).

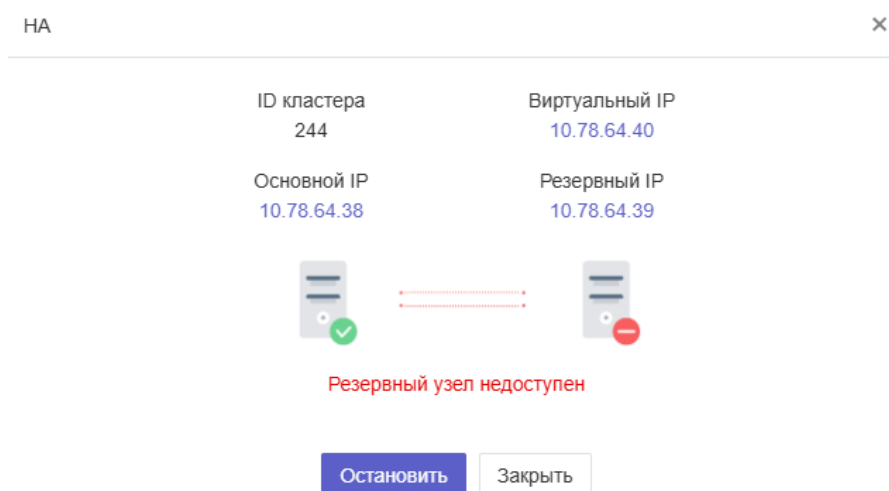


Рисунок 10-4. Недоступность Ваксир-ноды

При выходе из строя одной из нод вы получите оповещение о недоступности ноды с указанием IP-адреса этой ноды (рис. 10-5).

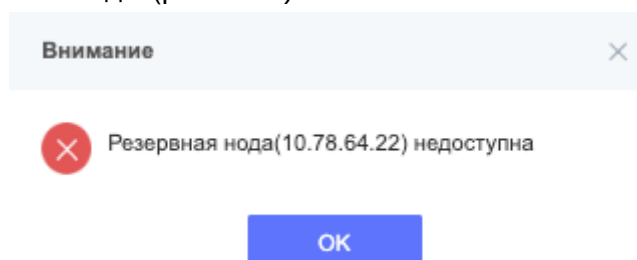


Рисунок 10-5. Оповещение о недоступности ноды

10.3. Логика использования IP-адресов

Для настройки резервной пары требуется три IP-адреса: IP-адрес первой ноды, IP-адрес второй ноды и виртуальный IP-адрес (VIP).

- Доступ к веб-интерфейсу контроллера возможен по любому из IP-адресов, однако при переходе в раздел **Управление** происходит автоматическое перенаправление на VIP-адрес контроллера.
- Подключение к контроллеру по SSH возможно только по IP-адресу мастер-ноды или по VIP-адресу контроллера.

10.4. Остановка HA

1. Определите, какая нода является мастером в разделе **HA**, и перейдите по её IP-адресу. На главной странице снова перейдите в **HA** и нажмите **Остановить**, затем **ОК**.

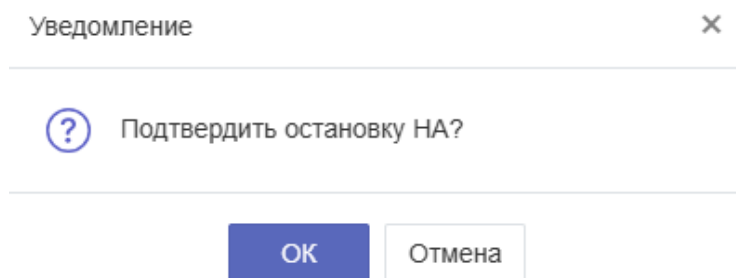


Рисунок 10-6. Остановка HA-пары

2. Через 1-2 минуты перейдите по IP-адресам каждой из нод, и убедитесь, что они теперь являются отдельными контроллерами.



11. ПОДКЛЮЧЕНИЕ ТД К КОНТРОЛЛЕРУ

Подключить точку доступа к контроллеру можно двумя способами:

- через опцию DHCP 43;
- статически через веб-интерфейс ТД.

Стоит учитывать, что приоритет адреса, по которому ТД подключается к контроллеру, следующий:

1. адрес, указанный в опции DHCP;
2. адрес, указанный статически на ТД.

В случае, если адрес, указанный в опции DHCP недоступен, ТД подключится к адресу, указанному на ТД статически.

11.1. Подключение точек доступа к контроллеру через опцию 43

На коммутаторах QTECH опция 43 задается в формате

`option 43 ZZXXYYYYYY`,

где **ZZ** — это префикс вендора в шестнадцатеричном формате (для ATLAS он равен 01);

XX — это количество адресов, умноженное на 4, в шестнадцатеричном формате (для одного адреса он равен 04);

YYYYYY — это IP-адрес контроллера в шестнадцатеричном формате.

1. Получите опцию 43 для вашего контроллера с помощью онлайн генератора:
<https://shimi.net/services/opt43/>

Для этого впишите IP-адрес контроллера в поле и нажмите **Give me my Option 43!**

Wireless Controllers Option 43 Generator

option 43 static prefix for vendor Cisco: f1 (hex)
IP count: 1
IP count * 4 bytes (hex): 04
IP 10.78.64.23 => 0a4e4017 (hex)

Resulting IOS command would therefore be:

option 43 hex f1040a4e4017

Wireless Controller Type:

Controller IP address(es): (separate by space, comma, colon, semicolon, or newline)

Рисунок 11-1. Получение опции 43

2. В полученной команде замените первый символ опции на 0 и задайте её в DHCP пуле для точек доступа.

Пример задания опции 43 на коммутаторе QTECH:

`option 43 hex 01040a4e4017`

Пример задания опции 43 на Mikrotik:

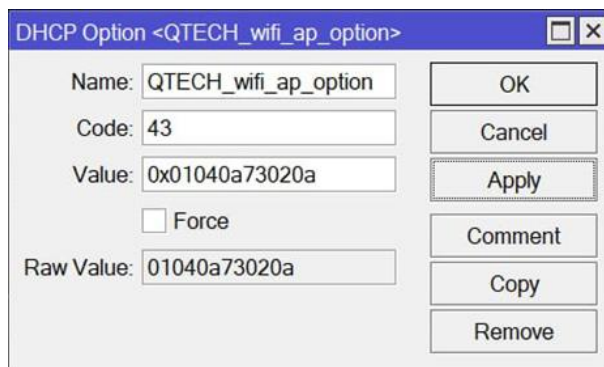


Рисунок 11-2. Пример задания опции 43 на Mikrotik

11.2. Подключение точек доступа через веб-интерфейс ТД

1. Перейдите в веб-интерфейс ТД по IP-адресу.

Логин / пароль: **admin /admin**

2. Перейдите в **System Settings > Manage AC Settings**, нажмите **Edit** и впишите IP-адрес контроллера в поле **AC IP Address 1** и нажмите **Save**, затем **OK**

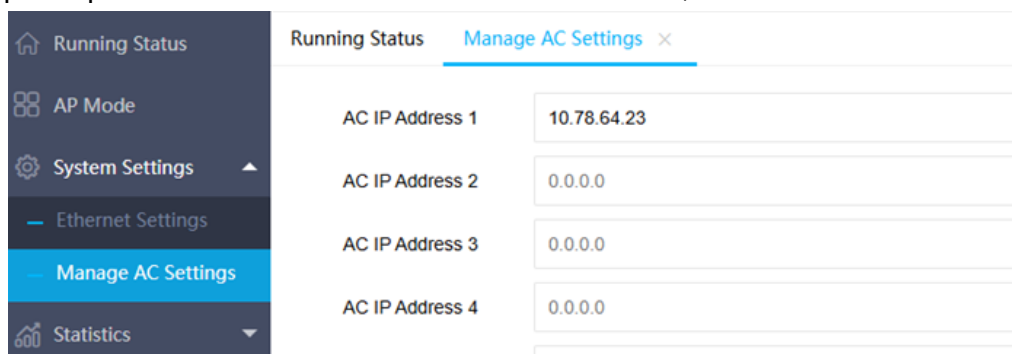


Рисунок 11-3. Пример задания адреса контроллера на ТД

3. Нажмите OK и убедитесь, что ТД подключилась к контроллеру (см. [раздел 11.4](#))

11.3. Подключение ТД к нескольким контроллерам

В веб-интерфейсе ТД в разделе **Manage AC Settings** возможна настройка приоритетного списка контроллеров. Вы можете указать до 4-х IP-адресов контроллеров в заданном порядке. Можно указывать как одиночные контроллеры, так и VIP-адреса HA-пар, к которым должны быть применены отдельные активационные ключи.

При запуске ТД подключается к контроллеру, адрес которого прописан в поле **AC IP Address 1**. В случае недоступности этого контроллера выполняется попытка подключения к следующему по приоритету контроллеру (**AC IP Address 2**). Если второй контроллер также недоступен, точка доступа последовательно переходит к следующему адресу в списке.

Running Status Manage AC Settings x

AC IP Address 1 10.78.64.37

AC IP Address 2 10.78.64.38

AC IP Address 3 10.78.64.39

AC IP Address 4 10.78.64.40

AC IPv6 Address 1 ::

AC IPv6 Address 2 ::

AC IPv6 Address 3 ::

AC IPv6 Address 4 ::

AC URL Address Please Input AC URL Address

Save Return

Рисунок 11-4. Подключение ТД к нескольким контроллерам

Данная конфигурация рекомендуется для архитектуры с географическим резервированием.

ПРИМЕЧАНИЯ:

- Контроллеры, указанные в списке, не синхронизируются между собой и работают независимо.
- После восстановления доступности контроллера с более высоким приоритетом точка доступа продолжает работать с тем контроллером, к которому она была подключена на момент отказа, вплоть до первой перезагрузки точки доступа. После перезагрузки точка доступа выполняет подключение к первому доступному контроллеру с наивысшим приоритетом из списка.

11.4. Проверка подключения ТД к контроллеру

1. ТД отразятся на контроллере в разделе **Точки доступа > Не назначено**, либо в уже созданной организации с автоматическим применением по IP-адресу. Все точки должны быть в статусе “онлайн”.

Назначить организацию

Не назначено: 2

☐ IP	MAC	SN	Модель	Версия	Статус	Действия
☐ 10.78.51.8	08-c6-b3-fd-76-10	QWP882500000059	QWP-88	V1.0.2	Онлайн	

Рисунок 11-5. Новые ТД на контроллере

2. Изначально точки доступа не привязаны к какой-либо организации. Для дальнейшей работы с ТД назначьте им организацию (Создание организации). Для этого перейдите в раздел **Точки доступа > Не назначено**, выберите ТД и нажмите **Назначить организацию** и выберите нужную организацию.



Назначить организацию

✕

Организация *

▼

Сохранить

Рисунок 11-6. Назначение организации



12. СЕТЕВАЯ БЕЗОПАСНОСТЬ

12.1. Требования к TCP/UDP портам

Для корректной работы контроллера должны быть открыты порты, указанные в таблице ниже.

Таблица 5 – Требуемые порты

Назначение	Порты
Данные FTP	TCP: 20
Управляющий канал FTP	TCP: 21
SSH	TCP: 22
Telnet	TCP: 23
HTTP / HTTPS (управление через веб-интерфейс)	TCP: 80 / 443
VRRP в HA конфигурации	TCP: 112 IP-адрес: 224.0.0.18
rsync в HA конфигурации	TCP: 873
mysqld	TCP: 3306
Получение статуса резервного хоста в HA конфигурации	TCP: 8082, 8083
HTTP-портал	TCP: 8987
Пассивный режим передачи данных FTP	TCP: 50000-52000
Перенаправление портала	TCP: 53725, 53726
Управление между контроллером и ТД	TCP: 57776, 57777
TFTP	UDP: 69
NTP	UDP: 123
SNMP	UDP: 161



Назначение	Порты
RADIUS	UDP: 1812, 12512–12543
radiusd	UDP: 1815, 1816, 1817, 1820
Портал	UDP: 2000, 7749, 57790
RADIUS CoA	UDP: 3799
dot11r	UDP: 58000

12.2. Доступ к управлению ТД

РЕКОМЕНДУЕТСЯ:

- отключить telnet на ТД;
- отключить web GUI на ТД;
- отключить SSH на ТД (при необходимости);
- сменить логин и пароль на ТД.

Настройка доступа к управлению ТД возможна для точек доступа, принадлежащих одной организации, и осуществляется в окне редактирования соответствующей организации. Для этого перейдите в раздел **Управление > Организация**. Нажмите **Добавить** или на иконку редактирования напротив нужной организации, затем перейдите во вкладку **Доступ к ТД**.

Рисунок 12-1. Настройка доступа к управлению ТД

Пароль может содержать:

- от 8 до 32 символов;
- латинские буквы, цифры, нижнее подчеркивание.

12.3. Доступ к управлению контроллером

РЕКОМЕНДУЕТСЯ:

- сменить пароль по умолчанию для доступа к управлению контроллером;



- менять пароль каждые 3 месяца.

1. В правом верхнем углу домашней страницы контроллера нажмите на **admin**, затем **Сменить пароль**.



Рисунок 12-2. Смена пароля

2. Впишите текущий пароль, новый пароль и подтверждение нового пароля. Пароль может содержать:

- от 8 до 20 символов;
- латинские буквы, цифры, специальные символы (кроме пробелов).

Смена пароля ×

* Текущий пароль

* Новый пароль

Слабый Средний Надежный

* Подтверждение пароля

Сохранить Отмена

Рисунок 12-3. Смена пароля

3. По истечении 3 месяцев система оповестит о необходимости снова изменить пароль.

❗ При необходимости сбросить пароль, обратитесь в службу технической поддержки.

12.4. Принудительное отключение клиента от SSID

1. Перейдите в **Управление > Пользователи**. Нажмите на **Отключить** напротив КУ, которое необходимо отключить (рис. 12-4), затем нажмите **ОК**.



Время в сети	IP контроллер	Длительность	Трафик (МБ)	Тип пользовате.	Действия
2026-05-04 08:43:19	10.78.64.11	1ч43мин31с	1.78М	WPA-Enterprise	Отключить b
2026-05-04 10:26:59	10.78.64.11	0с	0.00М	WPA-Enterprise	Отключить b

Рисунок 12-4. Принудительное отключение клиента от SSID

❗ ПРИМЕЧАНИЯ:

- Обратите внимание, что данные действия не запрещают повторную попытку подключения КУ к той же сети, и при наличии необходимости такая попытка должна быть заблокирована иными средствами (на RADIUS-сервере, путем создания черных списков и т. д.)
- Опция работает только для КУ, прошедших аутентификацию по учетным данным (через портал авторизации или WPA-EAP).

12.5. Загрузка SSL-сертификата

- Перейдите в **Сертификат HTTPS**
- Нажмите **Загрузить** и выберите .key файл. Аналогично загрузите .crt файл. Затем нажмите **Сохранить**.

После этого веб-служба перезапустится и откроется страница с установленным SSL-сертификатом.



13. УПРАВЛЕНИЕ ТД

13.1. Редактирование информации о ТД

Перейдите в **Точки доступа**. В столбце **Действия** нажмите на иконку редактирования напротив нужной точки доступа.

В окне редактирования можно изменить имя ТД, назначить организацию и вписать информацию о местоположении ТД.

Редактирование MAC-адреса и SN невозможно.

Рисунок 13-1. Редактирование информации о ТД

13.2. Перезагрузка ТД

Для перезагрузки ТД выберите нужные точки доступа с помощью чекбокса, затем нажмите **Перезагрузка > Перезагрузить сейчас**.

Обновление статусов ТД происходит с задержкой. После отправки команды перезагрузки статус ТД может некоторое время отображаться как Online. Аналогично, после полного включения ТД статус ТД изменяется на Online не сразу, а после установления связи с контроллером.

Имя	IP	MAC	SN	Модель	Версия	Канал	Мощность
☒ QWP-86	10.78.64.5	08-c6-b3-fc-7d-70	QWP862500000120	QWP-86	1.0.5	1/149	22/22

Рисунок 13-2. Перезагрузка ТД

13.3. Перезагрузка ТД по расписанию

1. При необходимости можно установить расписание перезагрузки точек доступа. Для этого нажмите **Перезагрузка > Запланированное время перезагрузки**, затем нажмите **Добавить**.
2. В открывшемся окне настройки расписания впишите наименование плана перезагрузки.
3. Выберите периодичность перезагрузки: ежедневная перезагрузка или еженедельная перезагрузка. Задайте время и, в случае еженедельной перезагрузки, день недели.
4. Выберите точки доступа, к которым будет применять план перезагрузки.



Добавить

×

Наименование плана *

Время перезагрузки

☒ Ежедневная перезагрузка

☐ Еженедельная перезагрузка

23:30

ТД * MAC

Выбрать ТД

Рисунок 13-3. Настройка параметров для перезагрузки по расписанию

5. Нажмите **Отправить** для сохранения настроек.

13.4. Обновление ПО на ТД

⚠ **Внимание пользователям контроллера QWC-VC!**

После установки контроллера QTECH Atlas необходимо обновить ПО имеющихся ТД: заменить прошивки, предназначенные для работы с **QWC-VC**, на ПО, совместимое с контроллером QTECH Atlas. Для этого необходимо обратиться в техподдержку: www.qtech.ru/support/.

За работоспособность точек доступа при самостоятельном обновлении QTECH ответственности не несет.

1. Перейдите в **Управление > Обновить ТД > Файлы обновлений**. Нажмите **Выбрать** и выберите архив с ПО. Затем нажмите **Отправить**.

ПО для точек доступа можно скачать на официальном сайте QTECH на страницах точек доступа в разделе **Беспроводные сети и решения**: <https://www.qtech.ru/catalog/wireless/>

Файл обновления ТД

Выберите файл обновления

Выбрать

Отправить

qtech-atlas-qwp-82_v1.0.2.tar

×

Рисунок 13-4. Загрузка ПО ТД на контроллер

2. В случае, если для определенной модели ТД загружено больше одной прошивки, нажмите иконку «Добавить элемент» напротив нужной прошивки.

QWP-86	1.0.0	2026-04-17 17:20:44	Отключен	🗑️ ➕
	1.0.5	2026-04-17 17:26:45	Включен	🗑️

Рисунок 13-5. Применение загруженного ПО

3. Перейдите во вкладку **Обновление ТД**.
4. Выберите тип обновления: по организации – обновление ТД, принадлежащие выбранной организации; или по модели – обновление ТД одной модели.



Обновление ТД

Обновление ТД

Тип обновления ☒ По организации ☐ По модели

Время обновления ☒ Немедленно ☐ Запланированное время

Рисунок 13-6. Обновление ПО ТД

- Выберите время обновления: немедленно или запланированное время. Чтобы задать время обновления, нажмите на пустое поле. В выпадающем меню **сначала** задайте время, **затем** выберите дату в календаре.

☐ Немедленно ☒ Запланированное время

2026-04-30 14:30:00

Апр 2026							
нед	Пн	Вт	Ср	Чт	Пт	Сб	Вс
14	30	31	1	2	3	4	5
15	6	7	8	9	10	11	12
16	13	14	15	16	17	18	19
17	20	21	22	23	24	25	26
18	27	28	29	30	1	2	3
19	4	5	6	7	8	9	10

Сегодня 14 30

Рисунок 13-7. Задание времени обновления

13.5. Настройка LAN порта точки доступа

- Перейдите в **Управление > Точки доступа**, нажмите на иконку редактирования напротив нужной ТД и впишите номер VLAN в поле **LAN порт1** (или оставьте значение 1, если необходимо, чтобы порт был привязан к VLAN управления).
- После сохранения конфигурации точка доступа будет находиться в статусе «Офлайн» в течение примерно одной минуты. По истечении этого времени настройки будут применены.

Редактирование ТД

Имя * QWP-88 Местоположение

Организация * QWP-88 SN QWP882500000043

MAC 00-1f-ce-07-66-0b

VLAN порт

LAN порт1: 149

Рисунок 13-8. Настройка LAN порта



14. СОЗДАНИЕ И НАЗНАЧЕНИЕ ОРГАНИЗАЦИИ

14.1. Основные параметры организации

1. Чтобы создать организацию перейдите в раздел **Организация** и нажмите кнопку **Добавить**.
2. Во вкладке **Основная информация** впишите название организации, номер телефона, адрес и диапазон IP-адресов для автоматического назначения организации точкам доступа, IP-адрес которых входит в этот диапазон.
При необходимости можно добавить несколько диапазонов нажмите на иконку добавления справа от диапазона.

The screenshot shows a web form titled 'Добавить' (Add) with a close button 'X'. It has three tabs: 'Основная информация' (Basic Information), 'Радиоинтерфейсы' (Radio Interfaces), and 'Доступ к ТД' (Access to TD). The 'Основная информация' tab is active. It contains the following fields:

- Название *** (Name): A text input field.
- Телефон** (Phone): A text input field with the placeholder 'Пр.: +7 900 000-00-00'.
- Адрес** (Address): A text input field.
- Диапазон IP** (IP Range): Two text input fields with placeholders 'Пр.: 192.168.1.1' and 'Пр.: 192.168.1.10', separated by a tilde '~'. To the right of the second field is a blue circular icon with a plus sign inside.

Рисунок 14-1. Создание организации

14.2. Дополнительные параметры организации

1. **Динамический канал** – автоматический выбор канала по расписанию. Автоматическая настройка каналов осуществляется 1 раз в день. Настроить время для автоматической настройки можно через CLI (см. [раздел 23.6](#))
2. **Индикатор ТД** – включение / выключение индикаторов на ТД, поддерживающих эту функцию.
3. **Эко-режим** – опция энергосбережения для ТД, поддерживающих 802.3bt.

The screenshot shows the same 'Добавить' form, but with the 'Радиоинтерфейсы' (Radio Interfaces) tab selected. It contains four radio button options:

- Динамический канал** (Dynamic channel): Radio buttons for 'Вкл' (On) and 'Выкл' (Off), with 'Выкл' selected.
- AirMatch**: Radio buttons for 'Вкл' (On) and 'Выкл' (Off), with 'Выкл' selected.
- Индикатор ТД** (TD Indicator): Radio buttons for 'Вкл' (On) and 'Выкл' (Off), with 'Вкл' selected.
- Эко-режим** (Eco-mode): Radio buttons for 'Вкл' (On) and 'Выкл' (Off), with 'Выкл' selected.

Рисунок 14-2. Дополнительные параметры организации

14.3. Настройка радиоинтерфейсов

Задайте настройки радио для организации: стандарт 802.11 и ширину канала.

- **Radio1** – настройка радиомодуля 2,4 ГГц



- **Radio2** – настройка радиомодуля 5 ГГц
- **Radio3** – настройка второго радиомодуля 5 ГГц (при наличии)

Рисунок 14-3. Настройки радио для организации

14.4. Удаленный доступ к ТД

Во вкладке **Доступ к ТД** настройте доступ к ТД через telnet, SSH и веб-интерфейс.

Рисунок 14-4. Настройка удалённого доступа к ТД

14.5. Смена организации на ТД

1. Если необходимо сменить организацию, к которой привязаны точки доступа, перейдите в **Управление > Точки доступа**.
2. С помощью чек-бокса выберите нужные ТД, затем нажмите **Назначить организацию**.

Назначено: 2 Не назначено: 0 ☒ Онлайн ☒ Офлайн

☐ Имя	IP	MAC	SN
☒ QWP-82	10.78.64.215	08-c6-b3-fd-af-b0	QWP8225

Рисунок 14-5. Выбор точек доступа

3. В открывшемся окне выберите организацию, затем нажмите **Сохранить**.

Назначить организацию ×

Организация *

Рисунок 14-6. Выбор организации



15. СОЗДАНИЕ БЕСПРОВОДНОЙ СЕТИ

15.1. Создание беспроводной сети. Основные параметры.

1. Перейдите в раздел **Wi-Fi** и нажмите кнопку **Добавить** Во вкладке **Основное** задайте имя беспроводной сети (SSID), клиентский VLAN, способ аутентификации и статус беспроводной сети.
2. Выберите организации, к которым будет привязан этот SSID.

The screenshot shows a dialog box titled 'Добавить' (Add) with a close button 'X'. It has two tabs: 'Основное' (Basic) and 'Дополнительно' (Advanced). The 'Основное' tab is active. It contains the following fields and controls:

- SSID**: A text input field with the placeholder 'Наименование SSID'.
- VLAN ID**: A text input field with the value '1'.
- Статус**: Radio buttons for 'Включен' (Enabled) and 'Отключен' (Disabled). 'Включен' is selected.
- Аутентификация**: A dropdown menu with the selected option 'Без аутентификации' (No authentication).

Below the tabs is a section titled 'Выберите организацию и группу пользователей' (Select organization and user group) with a search input 'Название организации' and a list of checkboxes:

- ☐ Root
 - ☐ Public Group
 - ☐ Default Group
- ☒ 88bugtest
 - ☐ Default Group

At the bottom are two buttons: 'Создать еще' (Create more) and 'Сохранить' (Save).

Рисунок 15-1. Создание SSID

15.2. Дополнительные настройки SSID

Во вкладке **Дополнительно** можно настроить частотный диапазон, режим безопасности. При необходимости включите L2-изоляцию, настройте ограничение пропускной способности, расписание вещания SSID, скрытый SSID и черный список MAC-адресов.

The screenshot shows the same 'Добавить' dialog box, but with the 'Дополнительно' (Advanced) tab active. It contains the following fields and controls:

- Диапазон**: A dropdown menu with the selected option '2.4 ГГц+5 ГГц'.
- L2 изоляция K/V**: Radio buttons for 'Вкл' (On) and 'Выкл' (Off). 'Выкл' is selected.
- Режим безопасности**: A dropdown menu with the selected option 'Открытый' (Open).
- Восходящая пропускная способность (Кбит/с)**: A text input field with the value '8-4194303'.
- Нисходящая пропускная способность (Кбит/с)**: A text input field with the value '8-4194303'.
- Расписание (Выключение SSID)**: Two time input fields with placeholders 'Пример: 08:30' and 'Пример: 09:30', separated by a tilde '~' and a plus icon.
- Скрыть SSID**: Radio buttons for 'Да' (Yes) and 'Нет' (No). 'Нет' is selected.
- Чёрный список MAC**: A text input field with the placeholder 'MAC' and a plus icon.

At the bottom are two buttons: 'Создать еще' (Create more) and 'Сохранить' (Save).

Рисунок 15-2. Настройка SSID



Подробное описание настройки этих параметров ниже.

15.2.1. Настройка изоляции клиентов

Чтобы включить изоляцию клиентов (в пределах BSSID) установите переключатель на **Вкл.**

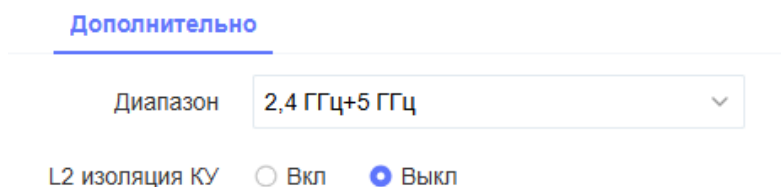


Рисунок 15-3. Включение изоляции клиентов

15.2.2. Настройка режима безопасности

Доступны следующие режимы безопасности:

- Открытый
- WPA/WPA2-Personal;
- OWE-Transition;
- WPA2/WPA3-Personal.

Ниже пример настройки WPA2/WPA3-PSK.

1. Выберите соответствующий тип шифрования.
2. Задайте пароль (минимум 8 символов).

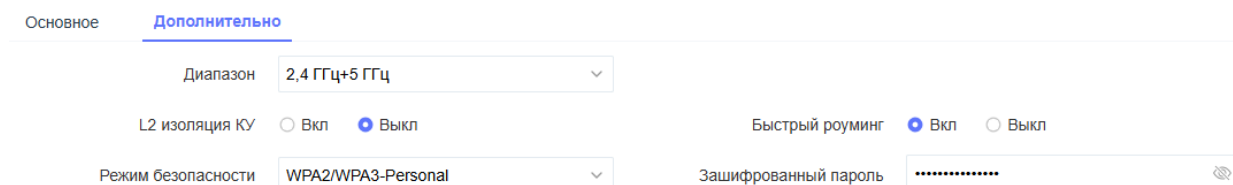


Рисунок 15-4. Настройка режима безопасности

i Настройка режима безопасности WPA3-SAE (only) осуществляется только через CLI (см. [раздел 23.9](#))

15.2.3. Настройка 802.11r (fast transition)

Для настройки хэндовера установите переключатель **Быстрый роуминг** на **Вкл.**



Рисунок 15-5. Настройка хэндовера

15.2.4. Ограничение пропускной способности

Впишите нужные значения пропускной способности клиента в кбит/с.

i Указанные значения применяются к каждому КУ.

Восходящая пропускная
способность (Кбит/с)

8-4194303

Нисходящая пропускная
способность (Кбит/с)

8-4194303

Рисунок 15-6. Настройка ограничения пропускной способности

15.2.5. Настройка расписания вещания SSID

Задайте интервал времени, в течение которого SSID будет отключен.

Максимальное количество интервалов – 3.

Расписание (Выключение SSID)	00:00	~	8:00	+
	12:00	~	13:00	-
	20:00	~	0:00	-

Рисунок 15-7. Настройка расписания вещания SSID

15.2.6. Настройка черного списка MAC-адресов

1. Чтобы добавить MAC-адрес клиентского устройства, впишите его в формате **ff-ff-ff-ff-ff-ff**.
2. Чтобы очистить список MAC-адресов, нажмите **Очистить**

Чёрный список MAC	02-40-a2-5f-b1-d6	+	Очистить
	02-68-48-c8-2d-99	-	
	6c-48-3f-a8-91-03	-	

Рисунок 15-8. Настройка чёрного списка MAC-адресов



16. БЕЗОПАСНОСТЬ И АУТЕНТИФИКАЦИЯ

i Беспроводной контроллер выполняет **функции аутентификатора** в сценариях с использованием следующих способов аутентификации:

- MAC-аутентификация;
- внутренний портал авторизации.

16.1. Настройка WPA-EAP

1. Перейдите в раздел **Портал и AAA > Внешний AAA**. Заполните поля (IP-адрес RADIUS-сервера, порт авторизации, порт аккаунтинга, ключ).

Внешний AAA

IP-адрес, порты авторизации и секретный ключ должны быть заполнены вместе либо не заполнены вовсе. Если указан порт аккаунтинга, порт авторизации тоже обязателен.

IP	
Порт авторизации	
Порт аккаунтинга	
Секретный ключ	
nas-id	
Сохранить	

Рисунок 16-1. Настройка RADIUS-сервера

2. Перейдите в раздел **Wi-Fi**. Нажмите кнопку **Добавить** или на кнопку редактирования напротив уже созданной сети.
3. В **Аутентификация** выберите WPA2/WPA3 Enterprise, в **AAA** – Внешний AAA.

Основное	Дополнительно
Наименование SSID	
SSID *	
VLAN ID *	1
Статус *	☒ Включен ☐ Отключен
Аутентификация *	WPA2/WPA3 Enterprise
AAA	Внешний AAA

Рисунок 16-2. Настройка WPA-EAP

16.2. Динамическое назначение VLAN (DVA)

Dynamic VLAN Assignment (DVA) позволяет автоматически назначать клиенту VLAN после успешной аутентификации по 802.1X. Номер VLAN передается RADIUS-сервером в ответе Access-Accept, после чего контроллер помещает КУ в соответствующий VLAN.

В данном разделе приведен пример настройки DVA (dynamic vlan assignment) с использованием FreeRADIUS.



Настройка со стороны контроллера: создайте SSID с режимом безопасности WPA-EAP (см. [раздел 16.1](#)). В поле **VLAN ID** оставьте значение по умолчанию.

Настройка со стороны FreeRADIUS

1. Настройте **clients.conf**

Откройте файл

```
sudo nano /etc/freeradius/3.0/clients.conf
```

Добавьте клиента:

```
client private-network-1 {  
    ipaddr      = 10.78.64.0/24  
    secret      = testing123-3  
}
```

2. Настройте пользователей с VLAN в users

Откройте файл

```
sudo nano /etc/freeradius/3.0/users
```

Добавьте пользователей согласно примеру ниже:

```
test149 Cleartext-Password := "test149"  
    Tunnel-Type = VLAN,  
    Tunnel-Medium-Type = IEEE-802,  
    Tunnel-Private-Group-Id = 149,  
    Reply-Message := "Hello, %{User-Name}"
```

```
test150 Cleartext-Password := "test150"  
    Tunnel-Type = VLAN,  
    Tunnel-Medium-Type = IEEE-802,  
    Tunnel-Private-Group-Id = 150,  
    Reply-Message := "Hello, %{User-Name}"
```

3. Настройте файл **/etc/freeradius/3.0/sites-enabled/default**

Откройте файл

```
sudo nano /etc/freeradius/3.0/sites-enabled/default
```

В блоке **authorize** добавьте:

```
if (User-Name == "test149") {  
    update reply {  
        Tunnel-Private-Group-Id := "149"  
    }  
}  
if (User-Name == "test150") {  
    update reply {  
        Tunnel-Private-Group-Id := "150"
```



```
}
}
```

В блоке **post-auth** добавьте:

```
update reply {
  Tunnel-Type := VLAN
  Tunnel-Medium-Type := IEEE-802
  Tunnel-Private-Group-Id:= "%{reply:Tunnel-Private-Group-ID}"
}
```

Проверка на FreeRADIUS

Для проверки ответа сервера выполните команду:

echo -e "User-Name = test149\nUser-Password = test149" | radclient -x 10.78.64.14 auth testing123-3

```
root@radius:/tmp# echo -e "User-Name = test149\nUser-Password = test149" | radclient -x
10.78.64.14 auth testing123-3
Sent Access-Request Id 32 from 0.0.0.0:51609 to 10.78.64.14:1812 length 65
  User-Name = "test149"
  User-Password = "test149"
  Cleartext-Password = "test149"
Received Access-Accept Id 32 from 10.78.64.14:1812 to 10.78.64.14:51609 length 71
  Message-Authenticator = 0x2dbe980fdada4258dac1affa1c27171
  Tunnel-Private-Group-Id:0 = "149"
  Tunnel-Type:0 = VLAN
  Tunnel-Medium-Type:0 = IEEE-802
  Reply-Message = "Hello, test149"
```

Рисунок 16-3. Вывод при корректной работе DVA

При корректной работе DVA в Access-Accept должен присутствовать атрибут Tunnel-Private-Group-Id:0 = "**<номер VLAN>**".

16.3. Настройка RADIUS-атрибутов для ограничения и приоритезации трафика

Этот раздел описывает процесс настройки политик доступа, ограничения скорости и приоритезации трафика для беспроводных клиентов на базе контроллера ATLAS.

Функционал поддерживается на следующих версиях оборудования:

- QWP-88 – 1.0.4 и выше
- QWP-82 – 1.0.4 и выше
- QWP-86 – 1.0.6 и выше

i Настройка на стороне контроллера ATLAS осуществляется через CLI (см. [раздел 23.1](#))

Пример настройки FreeRADIUS

1. На стороне FreeRADIUS создайте файл: **/etc/freeradius/3.0/dictionary.atlas** со следующим содержимым:

VENDOR

ATLAS

27514



```

BEGIN-VENDOR      ATLAS

ATTRIBUTE          ATLAS-Bandwidth-Max-Down 144 integer
ATTRIBUTE          ATLAS-Bandwidth-Max-Up   145  integer
ATTRIBUTE          ATLAS-ACL-Down           146 string
ATTRIBUTE          ATLAS-ACL-Up              147 string
ATTRIBUTE          ATLAS-DS-POLICY-Down     148  string
ATTRIBUTE          ATLAS-DS-POLICY-Up       149  string

END-VENDOR      ATLAS

```

2. Подключите созданный словарь в систему, отредактировав файл **/etc/freeradius/3.0/dictionary** и добавив в его конец строку:

```
$INCLUDE dictionary.atlas
```

3. Настройка пользователя в файле **/etc/freeradius/3.0/users**:

```

test149  Cleartext-Password := "test149"
         ATLAS-ACL-Down = "IPV4:ipdown",
         ATLAS-ACL-Up = "IPV4:ipup",
         Reply-Message := "Hello, %{User-Name}"

```

При необходимости для ограничения полосы пропускания используйте:

```

ATLAS-Bandwidth-Max-Down = 10240,
ATLAS-Bandwidth-Max-Up = 5120,

```

Для QoS:

```

ATLAS-DS-POLICY-Down = "QoS_Down",
ATLAS-DS-POLICY-Up = "QoS_Up",

```

16.4. MAC-аутентификация

16.4.1. Настройка белого списка MAC-адресов

1. Перейдите в раздел **Wi-Fi**. Нажмите кнопку **Добавить** или на кнопку редактирования напротив уже созданной сети.
2. В **Аутентификация** выберите Аутентификация по MAC.

Аутентификация *

Примечание: Для работы аутентификации по MAC необходимо либо добавить MAC-адрес КУ в белый список, либо создать локальную учетную запись с MAC-адресом пользователя.

Рисунок 16-4. Настройка MAC-аутентификации

Для работы аутентификации по MAC-адресу необходимо либо добавить MAC-адрес КУ в белый список, либо создать локальную учетную запись с MAC-адресом пользователя. Первый вариант подойдет, если достаточно создать общий белый список для всех SSID.

3. Добавьте MAC-адреса КУ в белый список. Для этого перейдите в **Wi-Fi > Белый список MAC**, нажмите кнопку **Добавить**.

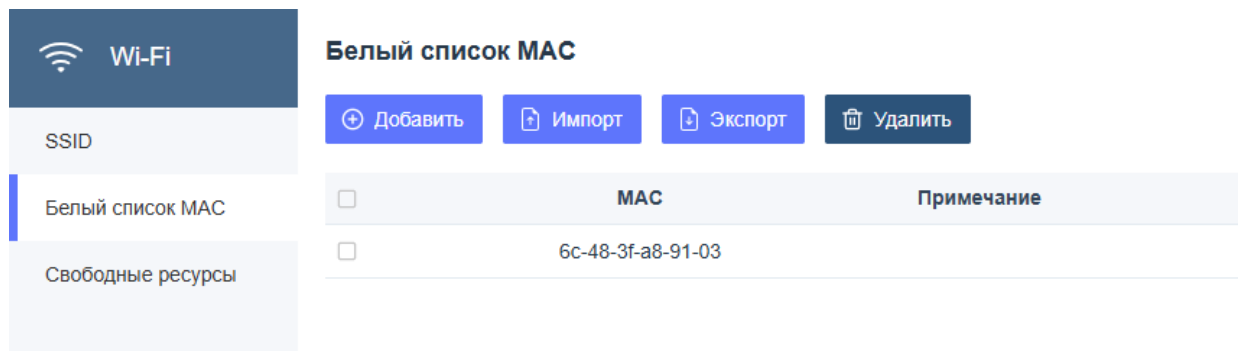


Рисунок 16-5. Добавление КУ в белый список

4. Впишите MAC-адрес клиентского устройства в формате ff-ff-ff-ff-ff-ff.

Рисунок 16-6. Добавление КУ в белый список

❗ «Белый список MAC» является общим для всех SSID, на которых включена аутентификация по MAC. Если для разных SSID необходимо использовать отдельные белые списки, их можно настроить, используя [локальные учетные записи](#) и [группы пользователей](#).

16.4.2. Создание локальной учетной записи для MAC-аутентификации

1. Перейдите в **Пользователи > Локальная учетная запись**, нажмите **Добавить**.
2. Добавьте пользователя. Заполни необходимые поля:
 - **Логин** - MAC-адрес устройства (в формате **xx-xx-xx-xx-xx-xx**);
 - **Имя** - произвольное имя (например, user1);
 - **Пароль** – любое текстовое значение (*поле является обязательным для заполнения, но при MAC-аутентификации этот пароль не заполняется на клиентском устройстве*);
 - **Организация** – выберите нужную организацию;
 - **Группа пользователей** – выберите нужную группу пользователей (подробнее см. [раздел 16.5](#))



Добавить

Логин * 6c-48-3f-a8-91-03 Имя * user1

Пароль * Телефон +7

Организация * ORG Группа пользователей * GROUP_1

Email Должность

Статус
☒ Включен ☐ Отключен

Создать еще Сохранить

Рисунок 16-7. Создание учетной записи

Чтобы настроить отдельные белые списки для разных SSID, воспользуйтесь инструкцией из следующего раздела.

16.5. Группы пользователей

Группы пользователей позволяют настроить разные локальные учетные записи для разных SSID внутри одной организации. Таким образом можно создать отдельные белые списки MAC-адресов для разных SSID, а также отдельные учетные записи для аутентификации через внутренний портал.

Создайте группы пользователей по примеру ниже.

1. Создайте организацию (например, **ORG**).
2. Перейдите в **Пользователи > Группа пользователей**. Нажмите на созданную организацию, затем нажмите «Добавить», чтобы добавить группу пользователей внутри этой организации.

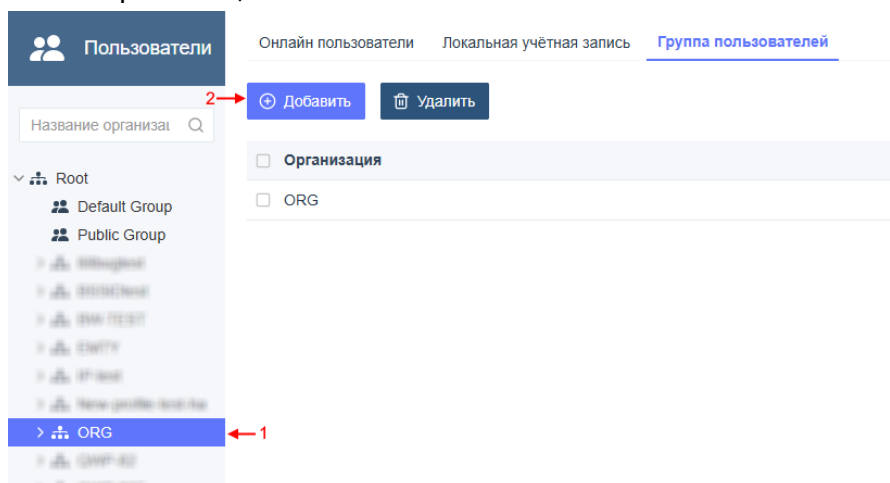


Рисунок 16-8. Создание группы пользователей

3. Впишите название группы пользователей. Аналогично создайте необходимое количество групп пользователей.



Рисунок 16-9. Создание группы пользователей

4. Создайте SSID (например, **SSID_1**). Выберите созданную для этого SSID группу пользователей (в примере – **GROUP_1**) и **группу по умолчанию**. Аналогично создайте SSID, привязанные к другим группам пользователей.

Рисунок 16-10. Настройка SSID

В примере **SSID_1** привязан к **GROUP_1** и к **группе по умолчанию**, **SSID_2** – к **GROUP_2** и **группе по умолчанию**.

5. Создайте локальную учетную запись.

Пример создания учетной записи для MAC-аутентификации см. в [разделе 16.4.2](#).

Пример создания учетной записи для внутреннего портала см. в [разделе 16.6](#).

Выберите созданную организацию (в примере – **ORG**).

Выберите группу пользователей, в зависимости от того, к какому SSID устройство должно иметь доступ.

- Выберите **GROUP_1**, если устройству разрешен доступ только к **SSID-1**;
- Выберите **GROUP_2**, если устройству разрешен доступ только к **SSID-2**;
- Выберите «**Группа по умолчанию**», если устройству разрешен доступ ко всем сетям внутри организации.



Добавить

Логин *

Имя *

Пароль *

Телефон

Организация *

Группа пользователей *

Email

Должность

Статус
☒ Включен ☐ Отключен

Рисунок 16-11. Создание локальной учетной записи

16.6. Создание локальных учетных записей для пользователей Wi-Fi

В этом разделе описано создание локальных учетных записей для авторизации пользователей на странице внутреннего портала. Создать учетные записи можно двумя способами:

- с помощью веб-интерфейса;
- с помощью импорта **.xls файла** с данными УЗ.

Создание УЗ с помощью веб-интерфейса

1. Перейдите в **Пользователи > Локальная учетная запись**, нажмите **Добавить**.
2. Заполните поля Логин, Имя, Пароль, выберите организацию и группу пользователей.

Добавить

Логин *

Имя *

Пароль *

Телефон

Организация *

Группа пользователей *

Email

Должность

Статус
☒ Включен ☐ Отключен

Рисунок 16-12. Создание локальной учетной записи



Создание УЗ с помощью импорта таблицы

1. Нажмите на **Импорт**, скачайте шаблон. Откройте скачанный .xls файл.

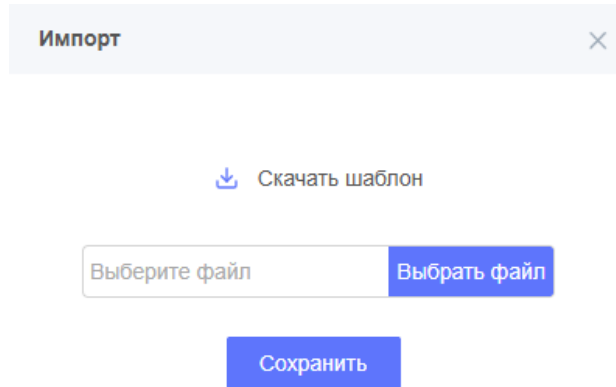


Рисунок 16-13. Создание локальной учетной записи

2. Впишите данные УЗ, которые необходимо создать, сохраните файл.

	A	B	C	D	E	F	G	H
1	#Название организации, имя и логин являются обязательными полями; остальные - необязательные.							
2	#Телефон должен содержать полные 11 цифр. Логин - от 4 до 20 символов.							
3	#Ошибочные данные при импорте не будут приняты. Пожалуйста, исправьте ошибки и импортируйте снова.							
4	Название организации	Имя	Группа пользователей	Логин	Телефон	Пароль в открытом	Email	Должность
5	Root	username1	Default Group	username1		password1		
6	Root	username2	Default Group	username2		password2		
7	Root	username3	Default Group	username3		password3		
8	Root	username4	Default Group	username4		password4		
9	Root	username5	Default Group	username5		password5		
10	Root	username6	Default Group	username6		password6		
11	Root	username7	Default Group	username7		password7		
12	Root	username8	Default Group	username8		password8		
13	Root	username9	Default Group	username9		password9		
14	Root	username10	Default Group	username10		password10		

Рисунок 16-14. Создание локальной учетной записи

3. В меню Импорт выберите отредактированный файл и нажмите **Сохранить**. Убедитесь, что УЗ из таблицы отобразились в списке.

☐	Логин	Имя	Телефон	Email	Организация	Группа пользователей	Должность	Статус	Действия
☐	username	username			Root	Default Group		Включен	✎ ✖
☐	username1	username1			Root	Default Group		Включен	✎ ✖
☐	username10	username10			Root	Default Group		Включен	✎ ✖
☐	username2	username2			Root	Default Group		Включен	✎ ✖
☐	username3	username3			Root	Default Group		Включен	✎ ✖
☐	username4	username4			Root	Default Group		Включен	✎ ✖
☐	username5	username5			Root	Default Group		Включен	✎ ✖
☐	username6	username6			Root	Default Group		Включен	✎ ✖
☐	username7	username7			Root	Default Group		Включен	✎ ✖
☐	username8	username8			Root	Default Group		Включен	✎ ✖
☐	username9	username9			Root	Default Group		Включен	✎ ✖

Рисунок 16-15. Создание локальной учетной записи

16.7. Настройка внутреннего портала авторизации.

1. Создайте локальную учетную запись (см. [раздел 17.5](#)).
2. Перейдите в раздел **Портал** и **AAA**. Настройте внешний вид страницы авторизации.

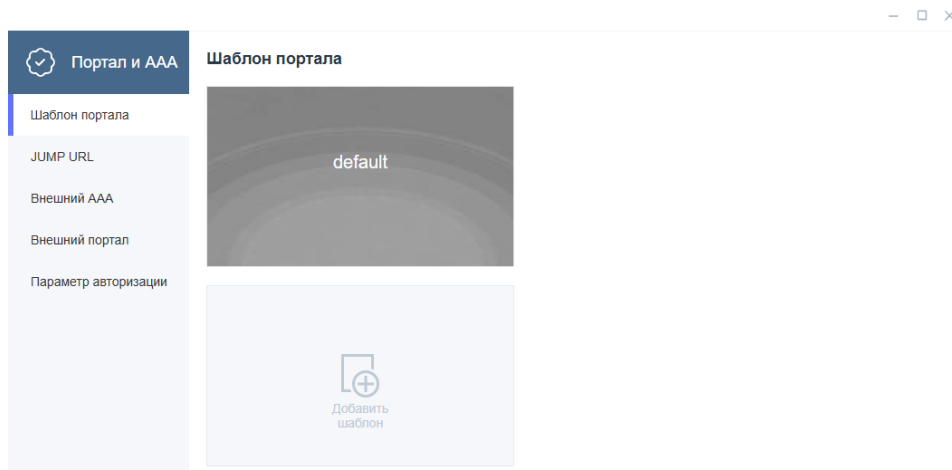


Рисунок 16-16. Настройка внутреннего портала авторизации

3. Создайте беспроводную сеть (см. [раздел 15.1](#)). Выберите способ аутентификации **Учетная запись**, шаблон порта – default или созданный шаблон, портал и AAA – **По умолчанию**.

Рисунок 16-17. Настройка внутреннего портала авторизации

4. При первом подключении необходимо сменить пароль. Для этого нажмите на кнопку **Изменить пароль**.

Рисунок 16-18. Страница портала авторизации

5. Заполните поля, нажмите **Сохранить**.



Изменить пароль

Имя пользователя / Телефон

Старый пароль

Новый пароль

Подтвердите пароль

Назад Сохранить

Рисунок 16-19. Смена пароля пользователя

6. Авторизуйтесь с новым паролем.



17. НАСТРОЙКА ВНЕШНЕГО ПОРТАЛА АВТОРИЗАЦИИ

17.1. Интеграция с системой WNAM

В данном разделе описывается настройка взаимодействия контроллера с системой управления сетевым доступом WNAM версий 1.6 и 2 для гостевой авторизации клиентских устройств.

Убедитесь, что сервер авторизации доступен с контроллера, точек доступа и клиентских устройств, а также отсутствуют блокировки трафика между контроллером и сервером WNAM на промежуточном сетевом оборудовании.

Используемые протоколы:

- RADIUS (UDP 1812 и 1813);
- Portal Protocol v2.0 (UDP 2000).

Для настройки внешнего портала в разделе контроллера **Управление > Портал и AAA**, откройте вкладку **Внешний портал**

Рисунок 17-1. Настройка внешнего портала

Заполните следующие поля:

- **IP RADIUS-сервера** – IP-адрес системы WNAM;
- **Порт авторизации** – порт (по умолчанию 1812);
- **Порт аккаунтинга** – порт (по умолчанию 1813);
- **Ключ RADIUS-сервера** – общий секрет, также настроенный на стороне WNAM;
- **URL портала** – форма адреса внешнего портала авторизации:

для WNAM 1.6:

https://<FQDN_или_IP_WNAM>/cp/qtechatlas

**для WNAM 2:**

https://<FQDN_или_IP_WNAM>/portal

После настройки портала необходимо создать и настроить беспроводную сеть. В разделе **Управление > Wi-Fi** создайте беспроводную сеть со следующими параметрами:

- **SSID** – имя беспроводной сети;
- **VLAN ID** – номер VLAN для клиентских устройств;
- **Аутентификация** – выберите значение **Учетная запись**;
- **Портал** – выберите ранее настроенный **внешний портал**;
- Выберите организацию, к которой относятся точки доступа, транслирующие данный SSID.

Рисунок 17-2. Настройка беспроводной сети

На этом конфигурация на стороне контроллера закончена.

Ниже приведен пример фрагмента **show running-config** после конфигурации. Он представлен в справочных целях, поскольку начиная с версии 1.0.18 настройка рекомендуется через веб-интерфейс контроллера.

```
ATLAS WLC#show running-config
```

```
...
```

```
radius source-ipv4 <IP_Контроллера>
```

```
radius-server authentication host <IP_WNAM> key 0 wnam_radius
```

```
radius-server accounting host <IP_WNAM> key 0 wnam_radius
```

```
aaa-accounting enable
```

```
aaa enable
```

```
radius nas-ipv4 <IP_Контроллера>
```

```
!
```



...

```
aaa group server radius external_portal_radius
```

```
server <IP_WNAM>
```

```
!
```

```
no login
```

```
ucs enable
```

```
url-filter permit 4 <FQDN_WNAM>
```

...

```
network 41
```

```
ssid TEST_WNAM
```

```
vlan 149
```

```
device-finger enable
```

```
update-time 2026-05-12 17:49:56
```

```
!
```

```
ap profile 16
```

```
name Default
```

```
ap escape
```

```
ap escape client-persist
```

```
quick-ip-report
```

```
update-time 2026-04-22 15:12:31
```

```
radio 1
```

```
mode axg
```

```
schedule-mode fair
```

```
vap 0
```

```
!
```

```
vap 2
```

```
enable
```

```
network 41
```

```
!
```

```
!
```

```
radio 2
```

```
mode axa
```

```
schedule-mode fair
```

```
vap 0
```

```
!
```

```
vap 2
```

```
enable
```

```
network 41
```

```
!
```

```
!
```

```
radio 3
```

```
mode axa
```

```
schedule-mode fair
```

```
vap 0
```

```
!
```

```
vap 2
```

```
enable
```

```
network 41
```

```
!
```

```
!
```



```
!  
ap database 08-c6-b3-fd-76-10  
profile 16  
!  
...  
!  
captive-portal  
enable  
authentication-mode pap  
portal version 2  
nas-ipv4 <IP_Контроллера>  
external portal-server server-name manageserver_portal ipv4 <IP_Контроллера>  
external portal-server server-name external_portal ipv4 <IP_WNAM>  
free-resource 1 destination ipv4 <IP_Контроллера>/32 source any  
extern-portal enable  
extern-aaa enable  
...  
configuration 4  
enable  
redirect mode ap  
radius accounting  
no radius-accounting update disable  
radius-acct-server external_portal_radius  
radius-auth-server external_portal_radius  
mac-portal authentication  
fast-mac-auth  
redirect attribute url-after-login enable  
redirect attribute url-after-login encode base64  
redirect attribute url-after-login name url  
redirect attribute ssid enable  
redirect attribute nas-ip enable  
redirect attribute apmac enable  
redirect attribute usermac enable  
ac-name ATLAS  
redirect url-head https://<FQDN_WNAM>/cp/qtechatlas  
portal-server ipv4 external_portal  
url-filter permit 4  
interface ws-network 41  
...  
  
end
```

Алгоритм работы

1. Клиентское устройство проходит процедуру ассоциации с точкой доступа: клиент отправляет 802.11 Association Request, точка доступа отвечает 802.11 Association Response. После успешного подключения клиент получает IP-адрес от DHCP-сервера.
2. Контроллер отправляет на RADIUS-сервер запрос Access-Request, используя MAC-адрес клиентского устройства в качестве параметра User-Name.
3. RADIUS-сервер возвращает Access-Reject, так как устройство еще не авторизовано в системе или его предыдущая сессия истекла.

4. Операционная система КУ выполняет проверку сетевой доступности, отправляя HTTP-запрос на тестовый ресурс (например, www.msftconnecttest.com/connecttest.txt для Windows).
5. Контроллер перехватывает HTTP-запрос клиента и выполняет перенаправление на URL внешнего портала авторизации, добавляя в URL параметры клиентской сессии.
6. Клиентское устройство открывает страницу портала, после чего пользователь вводит учетные данные, например, номер телефона и код подтверждения из SMS.
7. После успешной проверки данных портал WNAM отправляет на контроллер сообщение REQ_AUTH (UDP 2000), сигнализируя о готовности клиента к получению доступа.
8. Контроллер инициирует повторный запрос RADIUS Access-Request для подтверждения прав доступа.
9. RADIUS-сервер выполняет проверку учетных данных и при успешной аутентификации возвращает сообщение Access-Accept.
10. После получения Access-Accept контроллер открывает клиенту сетевой доступ и отправляет на WNAM сообщение ACK_AUTH, подтверждающее успешное завершение процедуры.
11. После успешной авторизации контроллер инициирует учет пользовательской сессии посредством отправки сообщения RADIUS Accounting-Request на RADIUS-сервер.

Ниже представлен фрагмент дампа трафика, иллюстрирующий взаимодействие (пункты 2, 3, 7-11) между контроллером и системой авторизации.

No.	Time	Time Delta	Source	Destination	Protocol	Length	Info
1	0.000000	0.000000	ATLAS	WNAM	RADIUS	238	Access-Request id=105
2	0.065003	0.065003	WNAM	ATLAS	RADIUS	82	Access-Reject id=105
3	0.101831	0.036828	ATLAS	WNAM	RADIUS	238	Access-Request id=106
4	0.168629	0.066798	WNAM	ATLAS	RADIUS	82	Access-Reject id=106
5	15.343818	15.175189	ATLAS	WNAM	RADIUS	238	Access-Request id=107
6	15.405337	0.061519	WNAM	ATLAS	RADIUS	82	Access-Reject id=107
7	29.028155	13.622818	WNAM	ATLAS	UDP	105	54583 → 2000 Len=61
8	29.084295	0.056140	ATLAS	WNAM	RADIUS	222	Access-Request id=108
9	29.148622	0.064327	WNAM	ATLAS	RADIUS	95	Access-Accept id=108
10	29.191035	0.042413	ATLAS	WNAM	UDP	88	2000 → 54583 Len=44
11	29.191060	0.000025	ATLAS	WNAM	RADIUS	209	Accounting-Request id=109
12	29.259033	0.067973	WNAM	ATLAS	RADIUS	64	Accounting-Response id=109

Рисунок 17-3. Пример дампа трафика взаимодействия контроллера с WNAM

В зависимости от версии WNAM, ссылка при перенаправлении клиента на портал будет иметь следующий формат:

- При WNAM 1.6:



https://<FQDN_WNAM>/cp/qtechatlas?wlanacip=<IP_Контроллера>&apmac=<MAC_ТД>&wlanuserip=<IP_КУ>&usermac=<MAC_КУ>&ssid=<Имя_SSID>&wlanacname=<ИМЯ_Контроллера>&url=<BASE64_URL_Редиректа>&redirect_mode=AP

- **При WNAM 2:**

https://<FQDN_WNAM>/portal?wlanacip=<IP_Контроллера>&apmac=<MAC_ТД>&wlanuserip=<IP_КУ>&usermac=<MAC_КУ>&ssid=<Имя_SSID>&wlanacname=<ИМЯ_Контроллера>&url=<BASE64_URL_Редиректа>&redirect_mode=AP

17.2. Диагностика взаимодействия с внешним порталом

 Для выявления ошибок взаимодействия с внешним порталом на стороне контроллера используется режим отладки и логирования событий **через CLI** (см. [раздел 24.2.2](#)).



18. НАСТРОЙКИ РАДИО

18.1. Настройка регуляторного домена (при необходимости)

Осуществляется глобально на контроллере. Перейдите в **Настройки > Код страны**. Выберите соответствующий регуляторный домен.

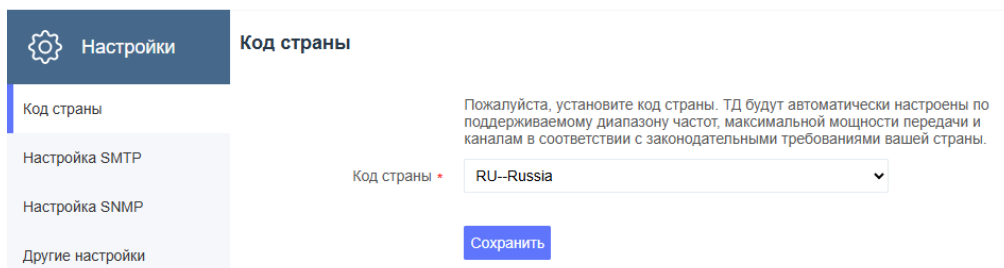


Рисунок 18-1. Настройка регуляторного домена

18.2. Изменение номера и ширины канала и мощности

1. Перейдите в **Управление > Точки доступа**. Выберите нужные ТД с помощью чекбокса и нажмите на **Массово > Настройка конфигурации** на верхней панели.

Чтобы изменить номер канала, выберите нужный номер из выпадающего списка напротив нужного радиомодуля. Аналогично измените мощность.

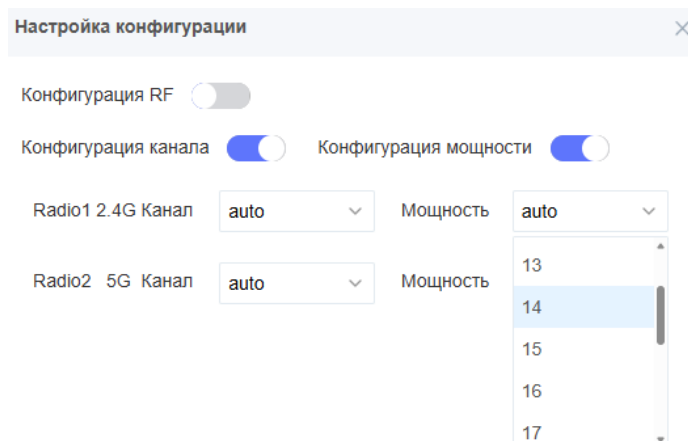


Рисунок 18-2. Настройки радио на ТД

i *Мощность передачи настраивается с шагом 1 дБ*

2. **Изменение ширины канала.** Изменить ширину канала можно в настройках организации (см. [раздела 14.3](#)).

18.3. Включение/выключение радиомодулей

1. Перейдите в **Управление > Точки доступа**. Выберите нужные ТД с помощью чекбокса и нажмите на **Массово > Настройка конфигурации** на верхней панели. Включите настройки **Конфигурация RF** с помощью переключателя, затем включите или отключите нужные радиомодули.

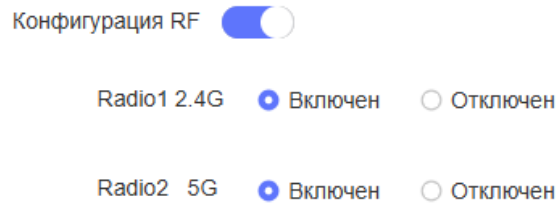


Рисунок 18-3. Включение/выключение радиомодулей

18.4. Настройка частотного плана

При необходимости ограничить использование отдельных радиоканалов точками доступа, настройте частотный план.

 *Настройка осуществляется **только через CLI** (см. [раздел 23.2](#)).*

 При задании каналов в channel-block ручная конфигурация каналов не из списка разрешенных применяться не будет!

 Категорически не рекомендуем использовать каналы, отличные от 1,6,11 в диапазоне 2,4 ГГц!

 В случае, если необходимо отключить все работающие каналы, отключите радиомодуль (см. [раздел 18.3](#))

18.5. Настройка Band Steering

 *Настройка осуществляется **только через CLI** (см. [раздел 23.8](#)).*



19. МОНИТОРИНГ

19.1. Мониторинг системных ресурсов

В разделе **Нагрузка** содержится информация о CPU, памяти, дисковом пространстве и TCP-соединениях.

- **CPU** – информация о текущей загрузке процессора в %;
- **Время работы** – время непрерывной работы системы с момента включения;
- **Память** – текущая загрузка оперативной памяти в процентах;
- **TCP Count** – количество активных TCP-соединений;

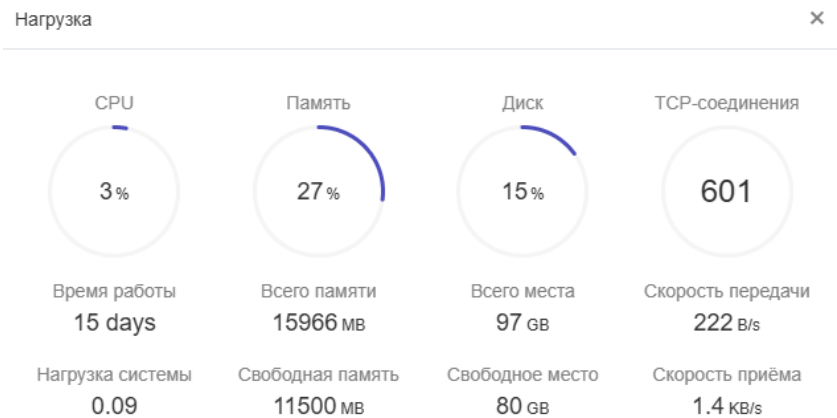


Рисунок 19-1. Информация о системных ресурсах

19.2. Просмотр информации о ТД

В разделе **Точки доступа** содержится список точек доступа со следующей информацией: имя ТД, IP-адрес, MAC-адрес, серийный номер, модель ТД, версия ПО и др.

ТД

Имя/IP/MAC/SN

Q

Добавить ТД

Назначить организацию

Импорт

Экспорт

Массово

Перезагрузка

Удалить

Назначено: 6

Не назначено: 3

☒ Онлайн

☒ Офлайн

Поля

☐	Имя	IP	MAC	SN	Модель	Версия	Канал	Мощность	Организация	Местоположение	Клиенты	Время в сети	Статус
☐	QWP-86	10.78.64.4	08-c6-b3-fc-7d-50	QWP862500000119	QWP-86	1.0.5	1/157	22/22	TEST-S		1	31мин14с	Онлайн
☐	QWP-86	10.78.64.5	08-c6-b3-fc-7d-70	QWP862500000120	QWP-86	1.0.5	1/149	22/22	TEST-S		0	23x21мин33с	Онлайн

Рисунок 19-2. Просмотр информации о состоянии ТД

19.3. Просмотр информации о клиентских устройствах

В разделе **Пользователи > Онлайн пользователи** содержится информация о клиентских устройствах: организация, назначенная точке доступа, к которой подключилось КУ, учетная запись, MAC-адрес КУ, IP-адрес КУ, время в сети и прочее.

Онлайн пользователи

Локальная учётная запись

Группа пользователей

Условия поиска

Поля

Все пользователи

Организация	Учётная запись	Имя пользо	MAC КУ	IP КУ	IPv6 КУ	Тип КУ	Имя SSID	Сигнал	MAC ТД	Имя ТД	Время в сети	IP контроллер	Длительность	Трафик (МБ)	Тип пользовате	Действия
OfficeNetwork			1e-57-cc-f9-d6-98	10.10.31.64		iPhone/iPad/iPod	ParentOffice Network	-40	08-c6-b3-fc-7a-b0	RY02-QT-A PT-701	2026-04-30 15:11:51	10.10.203.122	53мин54с	9.54M	WPA-Enterprise	Отключить
OfficeNetwork			02-bb-4f-6c-ff-9e	10.10.31.20		HUAWEI-NAMINAM-LX9	ParentOffice Network	-61	08-c6-b3-fc-7a-f0	RY02-QT-A PT-706	2026-04-30 15:34:16	10.10.203.122	49с	20.92M	WPA-Enterprise	Отключить

Рисунок 19-3. Просмотр информации о клиентских устройствах



19.4. Включение LLDP на точках доступа

ⓘ Включение LLDP осуществляется только **через CLI контроллера** (см. [раздел 22.6](#))

19.5. Настройка работы с syslog

ⓘ Настройка передачи логов на syslog-сервер осуществляется **только через CLI контроллера** (см. [раздел 23.4](#))

20. ЖУРНАЛ СОБЫТИЙ

В разделе **Журналы событий** отображается история событий, регистрируемых беспроводным контроллером.

20.1. Информация о клиентских устройствах

Раздел **Журналы событий > Пользователи** содержит историю подключения клиентских устройств, включая информацию об учетных записях, IP-адресах и MAC-адресах КУ, SSID, время подключения и отключения КУ и др.

В этом разделе отображаются данные за последние **30 дней**.



Учетная запись	Организация	Имя	IP КУ	IPv6 КУ	MAC КУ	Тип КУ	SSID	MAC ТД	Имя ТД	Время входа в сеть	Время выхода из сети	Использован
☐	OfficeNetwork		10.10.31.85		6e-b0-1f-17-27-43	POCO-F6	ParentOfficeNetwork	08-c6-b3-fc-7a-10	QWP-86	2026-05-04 11:19:14	2026-05-04 11:19:42	0
☐	OfficeNetwork		10.10.31.85		6e-b0-1f-17-27-43	Other	ParentOfficeNetwork	08-c6-b3-fc-7a-10	QWP-86	2026-05-04 10:19:11	2026-05-04 11:19:11	4.56
☐	OfficeNetwork		10.10.31.203		ae-51-94-20-a9-18	other	ParentOfficeNetwork	08-c6-b3-fc-7a-b0	QWP-86	2026-05-04 11:07:24	2026-05-04 11:14:04	0.03
☐	OfficeNetwork		10.10.31.20		02-bb-4f-6c-ff-9e	HUAWEI-NAMNAM-LX9	ParentOfficeNetwork	08-c6-b3-fc-7a-10	QWP-86	2026-05-04 10:51:46	2026-05-04 11:12:25	37.18

Рисунок 20-1. Информация о клиентских устройствах

20.2. Информация о состоянии ТД

В **Журналы событий > Устройства** отображена история изменения статусов точек доступа, включая информацию о серийных номерах, MAC-адресах и IP-адресах ТД, назначенных организациях и времени изменения статуса ТД.

В этом разделе отображаются данные за последние **30 дней**.

Пользователи

Устройства

Система

Условия поиска

Экспорт

Удалить

Удаление по условию

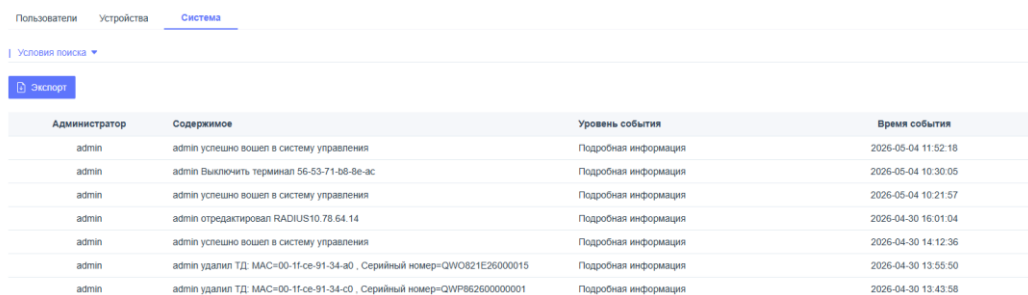
Поля

☐	Тип	SN	MAC	IP	Организация	Статус	Время обновления статуса
☐	AP	QWP882500000047	08-c6-b3-fc-7a-90	10.10.203.134	OfficeNetwork	Онлайн	2026-05-04 13:03:43
☐	AP	QWP882500000046	08-c6-b3-fc-7a-70	10.10.203.133	OfficeNetwork	Онлайн	2026-05-04 13:03:20
☐	AP	QWP882500000050	08-c6-b3-fc-7a-10	10.10.203.139	OfficeNetwork	Онлайн	2026-05-04 13:02:05
☐	AP	QWP882500000042	08-c6-b3-fc-79-10	10.10.203.142	OfficeNetwork	Офлайн	2026-05-04 13:00:03
☐	AP	QWP822500000019	00-1f-ce-07-65-06	10.200.203.12	OfficeNetwork	Офлайн	2026-05-04 13:00:01

Рисунок 20-2. Информация о состоянии ТД

20.3. История действий пользователя

Журналы событий > Система содержит историю действий пользователя, включая информацию об имени администратора, описании действия, уровне события и времени события.



Администратор	Содержимое	Уровень события	Время события
admin	admin успешно вошел в систему управления	Подробная информация	2026-05-04 11:52:18
admin	admin Выключить терминал 56-53-71-b8-8e-ac	Подробная информация	2026-05-04 10:30:05
admin	admin успешно вошел в систему управления	Подробная информация	2026-05-04 10:21:57
admin	admin отредактировал RADIUS10.78.64.14	Подробная информация	2026-04-30 16:01:04
admin	admin успешно вошел в систему управления	Подробная информация	2026-04-30 14:12:36
admin	admin удалил ТД: MAC=00-1f-ce-91-34-a0, Серийный номер=QW0821E26000015	Подробная информация	2026-04-30 13:55:50
admin	admin удалил ТД: MAC=00-1f-ce-91-34-c0, Серийный номер=QWP862600000001	Подробная информация	2026-04-30 13:43:58

Рисунок 20-3. История действий пользователя



21. НАСТРОЙКА SNMP

21.1. Включение SNMP

1. Перейдите в **Настройки > Настройка SNMP**.
2. Выберите версию SNMP и нажмите на **Вкл.**
3. Для отправки SNMP-трапов в разделе **Трап хост** нажмите на **Вкл.**, впишите IP-адрес сервера, на который контроллер должен отправлять трапы, затем выберите версию SNMP.
4. Впишите IP-адреса серверов, которым разрешено получать данные о контроллере, в поле «Ограничение IP-адреса».

Настройка SNMP

The screenshot displays the 'Настройка SNMP' (SNMP Configuration) interface. It is divided into several sections:

- SNMPV1,SNMPV2C:** Includes a toggle for 'SNMPV1,SNMPV2C' (set to 'Вкл' / On), a text field for 'Имя сообщества чтения' (Reading community) with the value 'public', and a 'Скачать MIB' (Download MIB) link.
- SNMPV3:** Includes a toggle for 'SNMPV3' (set to 'Выкл' / Off).
- Трап хост (Trap host):** Includes a toggle for 'SNMP Трап' (set to 'Вкл' / On), a text field for 'Трап хост' (Trap host) with the value '10.78.32.234', and a dropdown for 'Тип протокола' (Protocol type) set to 'V2C'.
- Безопасный IP-адрес (Secure IP address):** Includes a text field for 'Ограничение IP-адреса' (IP address restriction) with the value '10.78.32.234' and an 'Отправить' (Send) button.

Рисунок 21-1. Настройка SNMP

21.2. Настройка SNMP трапов

 *Настройка SNMP трапов осуществляется **только** через **CLI** контроллера (см. [раздел 23.7](#))*



22. НАЧАЛО РАБОТЫ С CLI

⚠ ВНИМАНИЕ! Руководство по CLI в данный момент находится в разработке. Любые действия в CLI, кроме описанных в данном руководстве, могут привести к **ошибкам** в работе контроллера.

22.1. Основные режимы CLI

Для выполнения настройки через CLI, откройте вкладку CLI на главной странице контроллера.

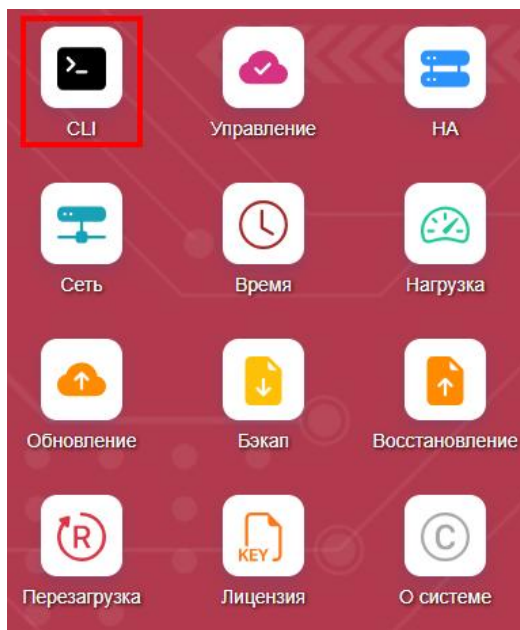


Рисунок 22-1. Переход на страницу CLI

При работе с CLI контроллера используются следующие режимы (соответствуют стилю Cisco CLI):

- пользовательский режим;
- привилегированный режим;
- режим конфигурации.

ATLAS WLC>
ATLAS WLC>en

*приглашение пользовательского режима
вход в привилегированный режим*

ATLAS WLC#
ATLAS WLC#conf t

*приглашение привилегированного режима
вход в режим конфигурации*

ATLAS WLC(config)#

приглашение режима конфигурации

Основные настройки беспроводной сети осуществляются в режиме конфигурации беспроводного контроллера:

ATLAS WLC(config)#wireless

вход в режим конфигурации беспроводного контроллера

ATLAS WLC(config-wireless)#

*приглашение режима конфигурации беспроводного
контроллера*



Настройка профиля выполняется в режиме конфигурации профиля:

ATLAS WLC(config-wireless)# ap profile **<номер профиля>** *вход в режим конфигурации профиля*

ATLAS WLC(config-ap-profile)# *приглашение режима конфигурации профиля*

22.2. Организация и ap profile

Каждой созданной в веб-интерфейсе организации соответствует профиль в CLI:

ap profile **<номер профиля>**

Чтобы узнать номер профиля, соответствующего конкретной организации, введите в привилегированном режиме CLI команду:

show wireless ap database **<MAC-адрес ТД, которой назначена организация>**

```
ATLAS WLC#show wireless ap database 08-c6-b3-fe-0e-30
AP MAC Address..... 08-c6-b3-fe-0e-30
AP Name..... -----
Location.....
AP Mode..... ws-managed
Password Configured..... No
Profile..... 15 - Default
Radio 1 Status..... Enabled
Radio 1 Channel..... Auto
Radio 1 Power..... Auto
Radio 1 Antenna Gain..... 0
Radio 2 Status..... Enabled
Radio 2 Channel..... Auto
Radio 2 Power..... Auto
Radio 2 Antenna Gain..... 0
Radio 3 Status..... Enabled
Radio 3 Channel..... Auto
Radio 3 Power..... Auto
Radio 3 Antenna Gain..... 0
Ethernet Rate Limit Enabled..... Yes
Ethernet Rate Limit Timer Granularity (msec)... 100
Ethernet Rate Limit ARP Requests..... 500
Ethernet Rate Limit Broadcast..... 1000
Ethernet Rate Limit Multicast..... 10000
Ethernet Rate Limit Unicast..... 60000
Ethernet Rate Limit Unicast Promiscuous..... 60000
Management ip address..... -----
Management ipv6 address..... -----
Net-ID.....
```

Рисунок 22-2. Номер профиля

В строке **Profile** найдите номер профиля нужной организации.

22.3. SSID и network

Проверьте номер network, присвоенный данному SSID, с помощью команды:

ATLAS WLC#show wireless network



```
ATLAS WLC>enable
ATLAS WLC#sh wireless network

Network  SSID                                Hide SSID  Security Mode
-----  -
1        Guest Network                          Enable     WPA Personal
2        Managed SSID 2                        Disable    None
3        Managed SSID 3                        Disable    None
4        Managed SSID 4                        Disable    None
5        Managed SSID 5                        Disable    None
6        Managed SSID 6                        Disable    None
7        Managed SSID 7                        Disable    None
8        Managed SSID 8                        Disable    None
9        Managed SSID 9                        Disable    None
10       Managed SSID 10                     Disable    None
11       Managed SSID 11                     Disable    None
12       Managed SSID 12                     Disable    None
13       Managed SSID 13                     Disable    None
14       Managed SSID 14                     Disable    None
15       Managed SSID 15                     Disable    None
16       Managed SSID 16                     Disable    None
17       testik 82E                          Disable    WPA Personal
18       test1                              Disable    WPA Personal
19       test2                              Disable    WPA Personal
20       test3                              Disable    WPA Personal
21       test4                              Disable    WPA Personal
22       test5                              Disable    WPA Personal
23       test6                              Disable    WPA Personal
24       test7                              Disable    WPA Personal
25       test8                              Disable    WPA Personal
26       test9                              Disable    WPA Personal
27       test10                             Disable    WPA Personal
28       test11                             Disable    WPA Personal
29       test12                             Disable    WPA Personal
30       test13                             Disable    WPA Personal
31       test14                             Disable    WPA Personal
32       test15                             Disable    WPA Personal
33       test radius                         Disable    WPA Enterprise
35       TEST                              Disable    WPA Enterprise
ATLAS WLC#
```

Рисунок 22-3. Вывод команды show wireless network



23. НАСТРОЙКА ЧЕРЕЗ CLI

23.1. Настройка RADIUS-атрибутов для ограничения и приоритезации трафика

1. Перейдите в режим конфигурации беспроводного контроллера.

```
ATLAS WLC>en
```

```
ATLAS WLC#conf t
```

```
ATLAS WLC(config)#wireless
```

2. Включите обработку QoS на точках доступа:

```
ATLAS WLC(config-wireless)# ap client-qos
```

```
ATLAS WLC(config-wireless)# exit
```

3. Создайте QoS политики, пример конфигурации:

```
ATLAS WLC(config)# class-map DEFAULT
```

```
ATLAS WLC(config-classmap-default)#exit
```

```
ATLAS WLC(config)# policy-map QoS_Down
```

```
ATLAS WLC(config-policymap-qos_down)# class DEFAULT
```

```
ATLAS WLC(config-policymap-qos_down-class-default)# set ip dscp 46
```

```
ATLAS WLC(config-policymap-qos_down-class-default)#exit
```

```
ATLAS WLC(config-policymap-qos_down)#exit
```

```
ATLAS WLC(config)# policy-map QoS_Up
```

```
ATLAS WLC(config-policymap-qos_up)# class DEFAULT
```

```
ATLAS WLC(config-policymap-qos_up-class-default)# set ip dscp 46
```

```
ATLAS WLC(config-policymap-qos_up-class-default)# exit
```

```
ATLAS WLC(config-policymap-qos_up)# exit
```

4. Настройте ACL, пример конфигурации:

```
ATLAS WLC(config)#ip access-list extended ipdown
```

```
ATLAS WLC(config-ip-ext-nacl-ipdown)# deny ip any-source any-destination
```

```
ATLAS WLC(config-ip-ext-nacl-ipdown)# exit
```

```
ATLAS WLC(config)#ip access-list extended ipup
```

```
ATLAS WLC(config-ip-ext-nacl-ipup)# permit ip any-source any-destination
```

```
ATLAS WLC(config-ip-ext-nacl-ipup)# exit
```

5. Сохраните конфигурацию:

```
ATLAS WLC#write
```

```
Confirm to overwrite current startup-config configuration [Y/N]:y
```



Политики будут применяться после успешной аутентификации на основе атрибутов, передаваемых RADIUS-сервером в Access-Accept.

23.2. Настройка частотного плана

6. Перейдите в режим конфигурации беспроводного контроллера.

```
ATLAS WLC#en
```

```
ATLAS WLC#conf t
```

```
ATLAS WLC(config)#wireless
```

7. Перейдите в режим настройки профиля точки доступа (организации)

```
ATLAS WLC(config-wireless)#ap profile 15
```

8. Впишите список запрещенных каналов для каждого радиомодуля: **radio 1** – 2,4 ГГц, **radio 2** – 5 ГГц

```
ATLAS WLC(config-ap-profile)#radio 1
```

```
ATLAS WLC(config-ap-profile-radio)#channel block 2;3;4;5;7;8;9;10
```

```
ATLAS WLC(config-ap-profile-radio)#exit
```

```
ATLAS WLC(config-ap-profile)#radio 2
```

```
ATLAS WLC(config-ap-profile-radio)#channel block  
132;136;140;144;149;153;157;161;165
```

```
ATLAS WLC(config-ap-profile-radio)#end
```

9. Примените изменения профиля

```
ATLAS WLC#wireless ap profile apply 15
```

10. Для подтверждения применения настроек впишите Y

```
All configurations will be send to the aps associated to this profile and associated  
clients on these aps will be disconnected. Because of work mode configurations,  
some aps associated to this profile will disconnect. Are you sure you want to apply  
the profile configuration? [Y/N] Y
```

```
AP Profile apply is in progress.
```

11. Сохраните конфигурацию контроллера и подтвердите сохранение

```
ATLAS WLC#wr
```

```
Confirm to overwrite current startup-config configuration [Y/N]:Y
```

23.3. Включение LLDP на точках доступа

1. Перейдите в режим конфигурации беспроводного контроллера.

```
ATLAS WLC>en
```

```
ATLAS WLC#conf t
```

```
ATLAS WLC(config)#wireless
```

2. В открывшейся консоли введите следующие команды:

```
ATLAS WLC(config-wireless)#ap profile 8
```

```
ATLAS WLC(config-ap-profile)#lldp enable
```

```
ATLAS WLC(config-ap-profile)#lldp message-transmission enable
```

```
ATLAS WLC(config-ap-profile)#exit
```



```
ATLAS WLC(config-wireless)#end
```

```
ATLAS WLC#wireless ap profile apply 8
```

All configurations will be send to the aps associated to this profile and associated clients on these aps will be disconnected. Because of work mode configurations, some aps associated to this profile will disconnect. Are you sure you want to apply the profile configuration? [Y/N] y

AP Profile apply is in progress.

```
ATLAS WLC#write
```

Confirm to overwrite current startup-config configuration [Y/N]:y

23.4. Настройка работы с syslog

23.4.1. Отправка логов контроллера

1. Перейдите в режим конфигурации

```
ATLAS WLC>en
```

```
ATLAS WLC#conf t
```

2. Включите отправку логов на внешний syslog-сервер:

```
ATLAS WLC(config)#logging 10.78.64.15 level informational
```

В примере:

- 10.78.64.15 – IP-адрес syslog-сервера;
- level – уровень логирования.

Всего доступно **4 уровня логирования** (соответствуют SNMP)

- critical
- warnings
- informational
- debugging

3. Включите события, которые необходимо передать на syslog-сервер:

```
ATLAS WLC(config)#wireless
```

```
ATLAS WLC(config-wireless)#syslogflags ap-failure
```

Всего доступно **6 типов событий**:

- ap-failure – сообщения об ошибках подключения и аутентификации ТД;
- ap-state – сообщения об изменениях состояния ТД;
- attack-event – сообщения об обнаружении атак;
- client-failure – сообщения об ошибках подключения и аутентификации КУ;
- client-state – сообщения об изменениях состояния КУ;
- ws-status – сообщения о состоянии беспроводной сети.

23.4.2. Отправка логов точек доступа

1. Перейдите в режим конфигурации профиля

2. Включите отправку логов точек доступа, которым назначен этот профиль



ATLAS WLC(config-ap-profile)#ap syslog **10.78.64.15**

10.78.64.15 – IP-адрес syslog-сервера;

23.5. Добавление дополнительных AAA-серверов через CLI

1. Сначала создайте SSID с типом WPA Enterprise через веб-интерфейс.

Рисунок 23-1. Настройка SSID

2. Далее добавьте RADIUS-сервер через CLI:

ATLAS WLC(config)#radius-server authentication host **<IP_адрес_RADIUS_сервера>** key 0 **<Общий_ключ>**

ATLAS WLC(config)#radius-server accounting host **<IP_адрес_RADIUS_сервера>** key 0 **<Общий_ключ>**

3. Создайте AAA-группу и добавьте в неё RADIUS-сервер:

ATLAS WLC(config)#aaa group server radius **<Имя_AAA_группы>**

ATLAS WLC(config-gs-radius)#server **<IP_адрес_RADIUS_сервера>**

4. После этого привяжите созданную AAA-группу к нужному SSID:

ATLAS WLC(config)#wireless

ATLAS WLC(config-wireless)#network **<ID_сети>**

ATLAS WLC(config-network)#radius server-name auth **<Имя_AAA_группы>**

ATLAS WLC(config-network)#radius server-name acct **<Имя_AAA_группы>**

5. После завершения настройки сохраните конфигурацию

ATLAS WLC#write

Confirm to overwrite current startup-config configuration [Y/N]:y

ID_сети – см. [раздел 22.3](#)

Пример настройки:



```
ATLAS WLC>
ATLAS WLC>enable
ATLAS WLC#conf t
ATLAS WLC(config)#radius-server authentication host 10.78.64.17 key 0 testing123-3
ATLAS WLC(config)#radius-server accounting host 10.78.64.17 key 0 testing123-3
ATLAS WLC(config)#aaa group server radius freeradius2
ATLAS WLC(config-gs-radius)#server 10.78.64.17
ATLAS WLC(config-gs-radius)#exit
ATLAS WLC(config)#wireless
ATLAS WLC(config-wireless)#network 35
ATLAS WLC(config-network)#radius server-name auth freeradius2
ATLAS WLC(config-network)#radius server-name acct freeradius2
ATLAS WLC(config-network)#end
ATLAS WLC#write
Confirm to overwrite current startup-config configuration [Y/N]:y
```

Рисунок 23-2. Пример настройки

23.6. Изменение времени автоматической настройки каналов

Для 2,4 ГГц:

ATLAS WLC(config-ap-profile)#channel-plan bgn time **ЧЧ:ММ**

Для 5 ГГц:

ATLAS WLC(config-ap-profile)#channel-plan an time **ЧЧ:ММ**

ЧЧ:ММ – часы:минуты

23.7. Настройка SNMP трапов

1. Чтобы посмотреть, какие трапы отправляет контроллер, выполните команду:

ATLAS WLC#show wireless trapflags

Пример вывода:

```
AP Failure Traps..... Enable
AP State Change Traps..... Enable
Client Failure Traps..... Enable
Client State Change Traps..... Enable
Peer Switch Traps..... Enable
RF Scan Traps..... Disable
Rogue AP Traps..... Enable
WIDS Status Traps..... Enable
Wireless Status Traps..... Enable
Wireless Attack Traps..... Enable
```

Рисунок 23-3. Пример вывода команды

2. Чтобы включить отправку конкретного события, выполните команду

ATLAS WLC(config-wireless)#trapflags **<тип события>**

- **ap-failure** – сообщения об ошибках подключения и аутентификации ТД;
- **ap-state** – сообщения об изменениях состояния ТД;
- **attack-event** – сообщения об обнаружении атак;



- **client-failure** – сообщения об ошибках подключения и аутентификации КУ;
- **client-state** – сообщения об изменениях состояния КУ;
- **rf-scan** – сообщения о новых обнаруженных SSID
- **rogue-ap** – сообщения об обнаруженных Rogue AP
- **ws-status** – сообщения о состоянии беспроводной сети.

3. Чтобы отключить отправку конкретного события, выполните команду
ATLAS WLC(config-wireless)#no trapflags <тип события>

23.8. Настройка Band Steering

Чтобы включить опцию Band Steering выполните команду ниже в режиме конфигурирования профиля.

```
ATLAS WLC(config-ap-profile)#band-select enable
```

```
ATLAS WLC(config-ap-profile)#band-select download
```

Чтобы отключить опцию Band Steering выполните команду ниже в режиме конфигурирования профиля.

```
ATLAS WLC(config-ap-profile)#no band-select enable
```

23.9. Настройка режима WPA3-SAE (only)

1. Включите WPA3-SAE (only) для нужной сети.

```
ATLAS WLC(config-wireless)# network <ID_сети>
```

```
ATLAS WLC(config-network)# wpa versions wpa3
```

ID_сети – см. [раздел 22.3](#)

2. Сохраните конфигурацию.

```
ATLAS WLC#write
```

```
Confirm to overwrite current startup-config configuration [Y/N]: y
```

3. Примените профиль.

```
ATLAS WLC#wireless ap profile apply <номер профиля>
```

All configurations will be send to the aps associated to this profile and associated clients on these aps will be disconnected. Because of work mode configurations, some aps associated to this profile will disconnect. Are you sure you want to apply the profile configuration? [Y/N] y

номер профиля – см. [раздел 22.2](#)



24. ДИАГНОСТИКА ЧЕРЕЗ CLI

24.1. Процедура диагностики в CLI

1. Отключите тайм-аут сессии, чтобы сессия не завершалась автоматически из-за отсутствия активности:
ATLAS WLC(config)#exec-timeout 0
2. Включите вывод отладочной информации в текущую CLI-сессию
ATLAS WLC#terminal monitor
3. Включите необходимые отладочные сообщения (debug)

Пример команды

ATLAS WLC#debug wireless discovery packet all

4. После завершения диагностики отключите все активные отладочные сообщения (debug)
ATLAS WLC#no debug all
5. Отключите вывод отладочной информации в текущую CLI-сессию
ATLAS WLC#terminal no monitor
6. Сбросьте настройки тайм-аута сессии
ATLAS WLC(config)#no exec-timeout

24.2. Вывод отладочной информации (debug)

Все команды выполняются в привилегированном режиме.

24.2.1. Диагностика проблем с подключением ТД к контроллеру

Отладка процесса обнаружения точек доступа контроллером:

debug wireless discovery packet all

Вывод информации об ошибках при подключении ТД к контроллеру

debug wireless ap authentication error

24.2.2. Диагностика проблем с конфигурацией ТД

Отладка обмена сообщениями между контроллером и точкой доступа

debug wireless ap-config packet send

debug wireless ap-config packet receive

debug wireless ap-config packet dump

24.2.3. Диагностика проблем с подключением КУ к SSID

Отладка процесса подключения КУ к конкретной ТД

debug wireless client-association internal info <MAC-адрес ТД>

Отладка событий AAA

debug aaa detail event

debug aaa detail request

debug aaa detail connection



Отладка взаимодействия контроллера с внешним порталом

```
debug captive-portal trace
debug captive-portal detail event
debug captive-portal packet all
debug captive-portal error
```

24.2.4. Диагностика работы опции «Динамический канал»

```
debug wireless channel event
```

Пример вывода:

```
%Sep 24 13:51:40 2026 filename:channel_power.c, lineno:161, Time 5G channel-plan action
process start on profiles : 9
%Sep 24 13:51:40 2026 filename:channel_adjustment.c, lineno:2749, ACS is needed to be
performed this turn.
%Sep 24 13:51:40 2026 filename:channel_adjustment.c, lineno:2760, ACS start for AP:08-
c6-b3-fd-af-b0/Radio:2 with sumRSSI: 0.
%Sep 24 13:51:40 2026 filename:channel_adjustment.c, lineno:2012, ACS complete for
AP:08-c6-b3-fd-af-b0/Radio:2. newChannel is 60, oldChannel is 140.
%Sep 24 13:51:40 2026 filename:channel_power.c, lineno:504, Time 5G channel-plan
action calculating done.
Wireless channel algorithm complete
%Sep 24 13:51:40 2026 filename:channel_power.c, lineno:521, Time 5G channel-plan
action applying done.
%Sep 24 13:51:40 2026 filename:channel_power.c, lineno:549, Time 5G channel-plan
action process done.
```

24.3. Команды show

Все команды выполняются в привилегированном режиме.

24.3.1. Просмотр информации о подключенных точках доступа

```
show wireless ap summary
```

Пример вывода:

MAC Address (*) Peer Managed	IP Address	Location	Reboot Mode	System Up Time	Online Time
08-c6-b3-fd-76-10	10.78.64.10		Warm Start	0d:00:20:25	0d:00:00:00
08-c6-b3-fe-0e-30	10.78.64.5		Warm Start	0d:00:22:18	0d:00:20:02

Рисунок 24-1. Пример вывода команды

```
show wireless ap status
```

Пример вывода:



MAC Address (*) Peer Managed	IP Address	Profile	Status	Configuration Status	Age
08-c6-b3-fd-76-10	10.78.64.10	16	Failed	Not Config	2d:18:07:46
08-c6-b3-fe-0e-30	10.78.64.5	19	Managed	Success	0d:00:00:04

Рисунок 24-2. Пример вывода команды

24.3.2. Просмотр информации о радиоинтерфейсах ТД

show wireless ap radio status

Пример вывода:

```
ATLAS WLC#show wireless ap radio status
```

MAC Address (*) Peer Managed	Location	Radio	Channel	Transmit Power (%)	WLAN Util (%)	Auth. Clients
08-c6-b3-fd-76-10		1	11	100	10	1
08-c6-b3-fd-76-10		2	161	100	1	3
08-c6-b3-fe-0e-30		1	11	100	23	0
08-c6-b3-fe-0e-30		2	149	100	5	1

2.4G Clients:1 5G Clients:4

Рисунок 24-3. Пример вывода команды

24.3.3. Проверка применения активационных ключей

show wireless switch local status

Убедитесь, что в выводе команды show wireless switch local status значение в строке **Maximum Managed Access Points** соответствует количеству точек доступа в ключе.

Пример вывода:

```
ATLAS WLC#show wireless switch local status
Switch IP Address..... 10.78.64.37
Cluster Priority..... 1
AP Image Download Mode..... Integrated, Independent
Total Access Points..... 12
Managed Access Points..... 2
Connection Failed Access Points..... 10
Discovered Access Points..... 0
Maximum Managed Access Points..... 256
Total Clients..... 5
Authenticated Clients..... 5
Distributed Tunnel Clients..... 0
WLAN Utilization..... 25
```

Рисунок 24-4. Пример вывода команды

show license

Вывод команды show license должен содержать наименование файла лицензии ТД в строке **License name** и количество точек доступа в ключе в строке **License ap-count**.

Пример вывода:

```
ATLAS WLC#show license
License name: 08-c6-b3-fd-76-10_vAC_256_1.lic
License ap-count: 256
License module: none
License total period: forever
```

Рисунок 24-5. Пример вывода команды



24.3.4. Просмотр информации о подключении пользователей

show wireless client terminal status

Пример вывода:

```
ATLAS WLC#show wireless client terminal status
```

MAC Address (*) Peer Managed	Channel	Physical Mode	802.11n Capable	802.11ac Capable	802.11ax Capable	802.11be Capable	Transmit Data Rate	RSSI	Power Save Mode
88:8e:6d:88:8e:6d	6	802.11b/g/n	Yes	No	No	No	86 Mbps	44	None
88:8e:6d:88:8e:6d	1	802.11b/g/n	Yes	No	No	No	28 Mbps	50	None
88:8e:6d:88:8e:6d	6	802.11b/g/n	Yes	No	No	No	86 Mbps	42	None

Рисунок 24-6. Пример вывода команды

❗ ПРИМЕЧАНИЕ: Стоит учитывать, что если capabilities не зафиксированы или устройство ушло в энергосберегающий режим, параметры скорости и режима могут отображаться как 0 Mbps и None.



25. СКАНИРОВАНИЕ РАДИОЭФИРА

❗ На данный момент функция поддерживается только ТД QWP-88. Поддержка остальных ТД находится в разработке.

25.1. Настройка сканирования

1. Задайте длительность сканирования радиоэфира.

ℹ Увеличение длительности сканирования позволяет ТД собрать больше информации об окружающих SSID, однако стоит учитывать, что это может негативно повлиять на качество обслуживания беспроводных клиентов. **Значение по умолчанию** – 10 мс.

Команда выполняется в режиме конфигурации профиля.

Для настройки 2,4 ГГц выполните:

```
ATLAS WLC(config-ap-profile)#radio 1
```

Для настройки 5 ГГц выполните:

```
ATLAS WLC(config-ap-profile)#radio 2
```

Затем задайте длительность сканирования для нужного радиомодуля:

```
ATLAS WLC(config-ap-profile-radio)#rf-scan duration 100
```

100 – длительность сканирования в мс

2. Задайте интервал формирования отчета об обнаруженных SSID

```
ATLAS WLC(config-wireless)#rfscan-report-interval 180
```

180 – интервал между формированием отчета в секундах

25.2. Просмотр информации об обнаруженных SSID

1. Для просмотра списка обнаруженных SSID выполните команду ниже.

```
ATLAS WLC(config-wireless)#show wireless ap rf-scan status
```

Пример вывода:

```
ATLAS WLC#show wireless ap rf-scan status
```

MAC Address	SSID	Physical Mode	Chan	Status	Age
802.11b/g		802.11b/g	11	Unknown	0d:01:28:16
802.11b/g		802.11b/g	11	Unknown	0d:01:28:16
802.11a		802.11a	132	Unknown	0d:01:27:54
802.11a		802.11a	132	Unknown	0d:01:27:54
802.11b/g		802.11b/g	6	Unknown	0d:01:28:16
802.11b/g		802.11b/g	6	Unknown	0d:01:28:16
802.11a		802.11a	132	Unknown	0d:01:27:54
802.11a		802.11a	132	Unknown	0d:01:27:54
802.11a		802.11a	52	Unknown	0d:01:27:54
802.11b/g		802.11b/g	6	Unknown	0d:01:28:16
802.11b/g		802.11b/g	1	Unknown	0d:01:28:16
802.11b/g		802.11b/g	1	Unknown	0d:01:28:16
802.11a		802.11a	165	Unknown	0d:01:27:54
802.11b/g		802.11b/g	11	Unknown	0d:01:28:16
802.11a		802.11a	144	Unknown	0d:01:27:54
802.11b/g		802.11b/g	1	Unknown	0d:01:28:16
802.11a		802.11a	157	Unknown	0d:01:27:54
802.11b/g		802.11b/g	1	Unknown	0d:01:28:16
802.11a		802.11a	60	Unknown	0d:01:27:54
802.11b/g		802.11b/g	1	Unknown	0d:01:28:16
802.11b/g		802.11b/g	11	Unknown	0d:01:28:16
802.11a		802.11a	36	Unknown	0d:01:27:54
802.11b/g		802.11b/g	1	Unknown	0d:01:28:16
802.11b/g		802.11b/g	1	Unknown	0d:01:28:16
802.11b/g		802.11b/g	11	Unknown	0d:01:28:16
802.11b/g		802.11b/g	11	Unknown	0d:01:28:16

Рисунок 25-1. Пример вывода команды

2. Для просмотра списка обнаруженных SSID на конкретной ТД выполните команду ниже:

Для 2,4 ГГц

ATLAS WLC#show wireless ap <MAC-адрес ТД> radio 1 neighbor ap status

Для 5 ГГц

ATLAS WLC#show wireless ap <MAC-адрес ТД> radio 2 neighbor ap status

Пример вывода:

```
MAC address..... 08-c6-b3-fd-76-10
Location.....
Radio..... 1 - Sentry
Neighbor AP MAC SSID Channel RSSI Status Count Age clients wlanUtil dataRate
```

6	-70	Unknown	1	0d:00:31:47			
6	-32	Unknown	7	0d:00:00:18			
11	-39	Managed	15	0d:00:06:48	0/0	77/10	0
6	-51	Unknown	19	0d:00:00:18			
6	-51	Unknown	18	0d:00:00:18			
11	-44	Unknown	21	0d:00:00:18			
11	-82	Unknown	1	0d:00:12:18			
11	-78	Unknown	21	0d:00:00:18			
11	-81	Unknown	3	0d:00:00:18			
11	-80	Unknown	12	0d:00:06:18			
6	-78	Unknown	10	0d:00:01:48			
10	-82	Unknown	3	0d:00:12:18			
11	-78	Unknown	21	0d:00:00:18			
9	-81	Unknown	1	0d:00:18:18			
9	-81	Unknown	3	0d:00:16:48			
1	-66	Unknown	11	0d:00:00:18			
11	-79	Unknown	6	0d:00:06:48			
11	-81	Unknown	1	0d:00:16:48			
11	-70	Unknown	5	0d:00:01:48			
11	-73	Unknown	20	0d:00:00:18			
6	-76	Unknown	1	0d:00:21:18			
12	-84	Unknown	1	0d:00:36:18			
11	-69	Unknown	20	0d:00:00:18			
4	-84	Unknown	1	0d:00:01:48			
4	-83	Unknown	1	0d:00:30:18			
11	-75	Unknown	6	0d:00:21:18			
11	-83	Unknown	1	0d:00:06:48			
1	-83	Unknown	8	0d:00:00:18			
4	-69	Unknown	4	0d:00:15:18			
11	-83	Unknown	2	0d:00:11:47			
13	-86	Unknown	3	0d:00:27:18			
6	-71	Unknown	17	0d:00:00:18			
1	-77	Unknown	2	0d:00:18:18			
11	-32	Managed	21	0d:00:00:18	0/0	27/15	0
11	-13	Unknown	21	0d:00:00:18			
1	-26	Managed	20	0d:00:00:18	0/0	70/12	0
1	-16	Managed	21	0d:00:00:18	0/0	70/12	0
9	-80	Unknown	3	0d:00:21:48			
11	-54	Unknown	21	0d:00:00:18			
4	-64	Unknown	9	0d:00:01:48			
1	-81	Unknown	1	0d:00:06:18			
3	-85	Unknown	1	0d:00:36:18			
11	-84	Unknown	3	0d:00:03:18			
11	-78	Unknown	14	0d:00:01:48			
11	-81	Unknown	1	0d:00:27:18			
11	-70	Unknown	21	0d:00:00:18			
8	-81	Unknown	9	0d:00:00:18			
2	-71	Unknown	1	0d:00:18:18			
7	-81	Unknown	5	0d:00:11:47			
7	-84	Unknown	6	0d:00:12:18			

Рисунок 25-2. Пример вывода команды

3. Чтобы очистить список SSID выполните команды ниже. После выполнения этих команд ТД выполняют новое сканирование и формируют список обнаруженных SSID заново.

ATLAS WLC#clear wireless ap neighbors

ATLAS WLC#clear wireless ap rf-scan list



26. ROGUE AP DETECTION

⚠ На данный момент функция поддерживается только ТД QWP-88. Поддержка остальных ТД находится в разработке.

Функция Rogue AP detection предназначена для обнаружения точек доступа, которые не являются разрешенными и могут представлять угрозу безопасности.

Контроллер анализирует обнаруженные SSID, и в зависимости от настроек WIDS, может определить точку доступа как Rogue (несанкционированную).

WIDS (Wireless Intrusion Detection System) – система обнаружения угроз в беспроводной сети. В CLI можно настроить обнаружение различных типов угроз:

ATLAS WLC(config-wireless)#wids-security <тип угрозы>

1. **wids-security fakeman-ap-chan-invalid** – обнаружение поддельных точек доступа, которые используют MAC-адрес управляемой ТД, но вещают на канале, отличном от назначенного контроллером для этой ТД.
2. **wids-security fakeman-ap-no-ssid** – обнаружение ТД со скрытым SSID
3. **wids-security managed-ap-ssid-invalid** – обнаружение управляемых ТД, которые транслируют SSID, не соответствующий настроенным SSID на этих ТД
4. **wids-security unknown-ap-managed-ssid** – обнаружение неизвестных точек доступа, которые вещают SSID, настроенный на контроллере

ⓘ Функционал WIDS на данный момент находится в разработке. В CLI доступны команды для настройки других типов угроз, однако в текущей версии поддерживаются только функции, описанные в данном разделе.

26.1. Обнаружение Rogue AP

1. В списке обнаруженных SSID найдите SSID со статусом Rogue (см. [раздел 25.2](#))

802.11b/g	1	Unknown	0d:00:09:24
802.11b/g	1	Unknown	0d:00:29:13
802.11b/g	11	Unknown	0d:01:56:13
802.11a	132	Rogue	0d:00:00:02
802.11b/g	7	Unknown	0d:00:05:12

Рисунок 26-1. Обнаружение Rogue AP

2. Чтобы узнать тип угрозы, на основании которого обнаруженная ТД была отмечена как Rogue, выполните команду:

ATLAS WLC#show wireless ap <BSSID> rf-scan rogue-classification

BSSID – скопируйте BSSID из столбца MAC Address вывода команды «show wireless ap rf-scan status»

Пример вывода:

Test ID	Cond Detect	MAC Addr (radio)	Test Config	Test Result	Time Since 1st Report	Time Since Last Report
WIDSAPROGUE01	False	00-00-00-00-00-00(0)	Disable		0d:00:00:00	0d:00:00:00
WIDSAPROGUE02	True	08-c6-b3-fd-92-f0(2)	Enable	Rogue	0d:00:01:27	0d:00:00:22
WIDSAPROGUE03	False	00-00-00-00-00-00(0)	Disable		0d:00:00:00	0d:00:00:00
WIDSAPROGUE04	False	00-00-00-00-00-00(0)	Disable		0d:00:00:00	0d:00:00:00
WIDSAPROGUE05	False	00-00-00-00-00-00(0)	Disable		0d:00:00:00	0d:00:00:00
WIDSAPROGUE06	False	00-00-00-00-00-00(0)	Disable		0d:00:00:00	0d:00:00:00
WIDSAPROGUE07	False	00-00-00-00-00-00(0)	Disable		0d:00:00:00	0d:00:00:00
WIDSAPROGUE08	False	00-00-00-00-00-00(0)	Enable		0d:00:00:00	0d:00:00:00
WIDSAPROGUE09	False	00-00-00-00-00-00(0)	Disable		0d:00:00:00	0d:00:00:00
WIDSAPROGUE10	False	00-00-00-00-00-00(0)	Disable		0d:00:00:00	0d:00:00:00
WIDSAPROGUE11	False	00-00-00-00-00-00(0)	Disable		0d:00:00:00	0d:00:00:00
WIDSAPROGUE12	False	00-00-00-00-00-00(0)	Disable		0d:00:00:00	0d:00:00:00
WIDSAPROGUE01.....	Administrator configured rogue AP					
WIDSAPROGUE02.....	Managed SSID from an unknown AP					
WIDSAPROGUE03.....	Managed SSID from a fake managed AP					
WIDSAPROGUE04.....	AP without an SSID					
WIDSAPROGUE05.....	Fake managed AP on an invalid channel					
WIDSAPROGUE06.....	Managed SSID detected with incorrect security					
WIDSAPROGUE07.....	Invalid SSID from a managed AP					
WIDSAPROGUE08.....	AP is operating on an illegal channel					
WIDSAPROGUE09.....	Standalone AP with unexpected configuration					
WIDSAPROGUE10.....	Unexpected WDS device detected on network					
WIDSAPROGUE11.....	Unmanaged AP detected on wired network					
WIDSAPROGUE12.....	Administrator configured rogue SSID					

Рисунок 26-2. Пример вывода команды

В данном примере обнаружена неизвестная ТД, которая вещала SSID, идентичный настроенному на контроллере.

- Чтобы вручную снять с ТД отметку Rogue выполните команду ниже:

ATLAS WLC#wireless acknowledge-rogue <BSSID>

26.2. Настройка SNMP трапов для Rogue AP

Настройка SNMP трапов описана в [разделе 23.7](#).



27. MULTICAST TO UNICAST (M2U)

❗ На данный момент функция полноценно поддерживается только ТД QWP-88. Поддержка остальных ТД находится в разработке.

Функция M2U преобразует multicast-пакет в unicast перед отправкой клиенту: при получении multicast-трафика драйвер беспроводного интерфейса ищет клиентов, подписанных на данную группу (по таблице IGMP Snooping), и отправляет каждому из них отдельный unicast-кадр вместо общей multicast-рассылки.

IGMP Snooping – механизм, за счет которого ТД узнает, какие клиенты подписаны на какую multicast-группу.

Для трансляции multicast-трафика (видео, аудио, IPTV и т.п.) через Wi-Fi рекомендуется использовать точки доступа QWP-88 с включенным m2u - это даст наиболее стабильную доставку.

Настройка

1. Включите IGMP Snooping глобально
ATLAS WLC(config-wireless)#igmp snooping
2. Включите M2U на конкретной сети
ATLAS WLC(config-wireless)#network <ID_сети>

ID_сети – см. [раздел 22.3](#)

ATLAS WLC(config-network)#igmp snooping m2u

3. Настройте порог отключения M2U по числу членов группы
ATLAS WLC(config-network)#m2u threshold <2-256>

Значением по умолчанию является 6. Если число клиентов в multicast-группе превышает порог, m2u для этой группы автоматически отключается.



28. СЦЕНАРИИ РАЗВЕРТЫВАНИЯ

28.1. Общие настройки для всех сценариев

В данном разделе рассмотрены примеры БЛВС с использованием контроллера QTECH Atlas и точек доступа QWP/QWO. Точки доступа и беспроводной контроллер подключены к коммутатору линейки QSW. Питание точек доступа осуществляется по технологии PoE. Коммутатор подключен к маршрутизатору линейки QSR.

На коммутаторе настроены следующие VLAN:

- 132, 164, 100 – VLAN управления для ТД и контроллера;
- 150 и 151 – клиентские VLAN, которые будут привязаны к SSID.

Маршрутизатор является шлюзом (L3) для всех рассматриваемых VLAN.

Подключение точек доступа к контроллеру реализовано через опцию 43 DHCP.

Примеры конфигурации коммутатора и маршрутизатора приведены в табл. 6-7.

Таблица 6 – Настройка коммутатора на примере **QSW-4530-30TX-POE**

Порты в сторону точек доступа	Interface Ethernet1/0/11 switchport mode trunk switchport trunk allowed vlan 150 switchport trunk native vlan 132 Interface Ethernet1/0/21 switchport mode trunk switchport trunk allowed vlan 151 switchport trunk native vlan 132
Порт в сторону платформы с контроллером	Interface Ethernet1/0/2 switchport mode access switchport access vlan 132
Порт в сторону маршрутизатора	Interface Ethernet1/0/1 switchport mode trunk switchport trunk allowed vlan 150-151,132
DHCP пул для VLAN управления	ip dhcp pool MGMT network-address 10.78.32.0 255.255.255.0 default-router 10.78.32.1 dns-server 8.8.8.8 option 43 hex f1040a4e2032
DHCP пул для клиентских VLAN (на примере VLAN 150)	ip dhcp pool SSID-1 network-address 10.78.50.0 255.255.255.0 default-router 10.78.50.1 dns-server 8.8.8.8
VLAN-интерфейсы (на примере VLAN 132)	interface Vlan132 ip address 10.78.32.2 255.255.255.0



Таблица 7 – Настройка маршрутизатора на примере QSR-1920-22-AC

Порт в сторону коммутатора	switchport mode trunk switchport trunk allowed vlan 150-151,132
VLAN-интерфейсы (на примере VLAN 132)	interface vlan132 ip address 10.78.32.1 255.255.255.0 ip nat inside ip helper-address 10.78.32.2 exit

28.2. Сценарий 1. Отдельно стоящая инфраструктура

Рассмотрим пример БЛВС с использованием standalone контроллера QTECH Atlas и точек доступа QWP/QWO. В данной сценарии используется контроллер Standalone (SA), т. е. контроллер представлен в одном экземпляре. Такой вариант приемлем в небольших или средних сетях, не требующих высокую степень отказоустойчивости.

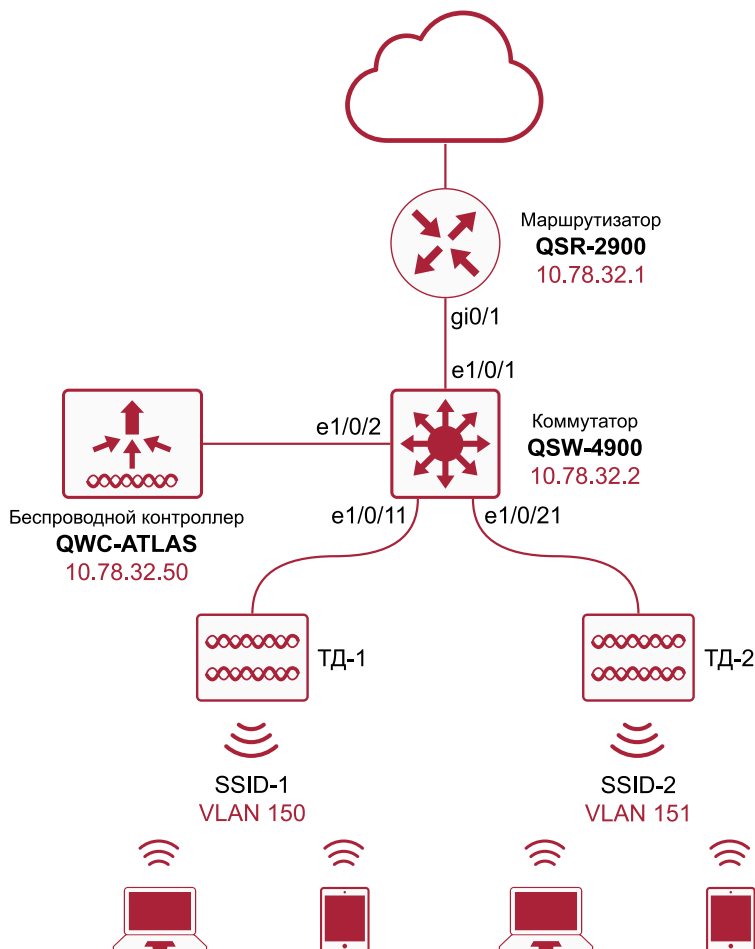


Рисунок 27-1. Отдельно стоящая инфраструктура



28.3. Сценарий 2. High Availability

Для повышения надежности и непрерывности функционирования БЛВС возможен такой вариант развертывания контроллера, как High Availability (HA), т. е. резервированная пара. Контроллеры работают по схеме Active-Standby.

Для примера рассмотрим схему на рис. 27-2. Предположим, что нода 1 является активным контроллером, выполняющим все функции, т. е. Master. В этот момент нода 2 является резервным компонентом и находится в состоянии готовности, постоянно синхронизируясь с нодой 1, чтобы иметь актуальное состояние системы. При отказе ноды 1, нода 2 оперативно берет на себя выполнение всех функций, обеспечивая бесперебойную работу БЛВС.

В данном случае контроллеры имеют общий виртуальный IP (VIP). Именно его следует указать в опции 43 DHCP для точек доступа (см. табл. 10). Остальные настройки портов остаются аналогичными табл. 8-9 ([раздел 26.1](#)).

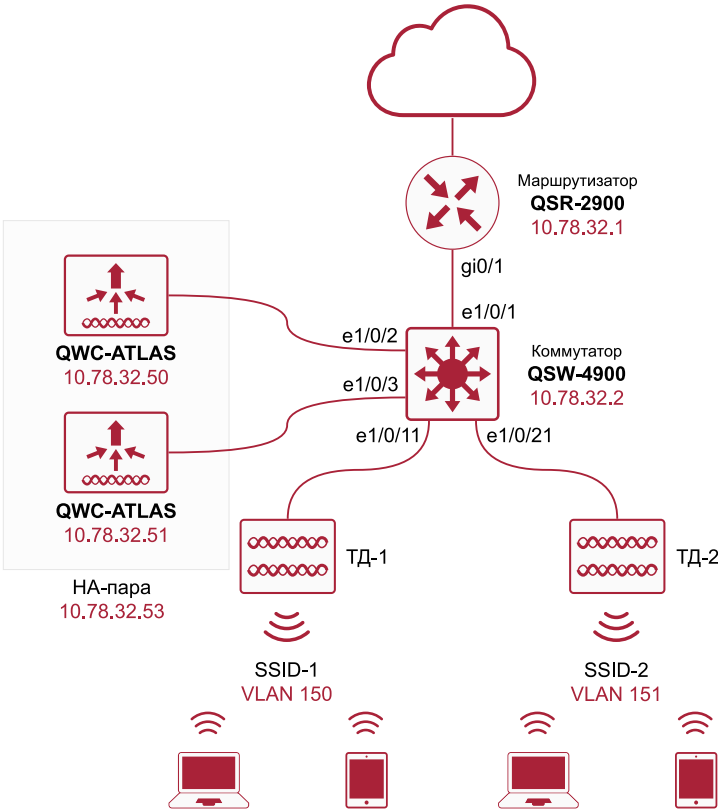


Рисунок 27-2. High Availability

Таблица 8 – Настройка DHCP для VLAN управления (HA)

DHCP пул для VLAN управления	<pre>ip dhcp pool MGMT network-address 10.78.32.0 255.255.255.0 default-router 10.78.32.1 dns-server 8.8.8.8 option 43 hex f1040a4e2035</pre>
------------------------------	---



28.4. Сценарий 3. Распределенная сеть с филиалами

При необходимости организовать централизованное управление точками доступа, расположенными в разных зданиях, можно развернуть сеть с филиальной инфраструктурой.

Настройки коммутаторов и маршрутизаторов в локальной сети остаются прежними ([разделы 27.1-27.3](#)), однако, чтобы обеспечить L3 связность между беспроводным контроллером и удаленными точками доступа, необходимо организовать защищенный туннель.

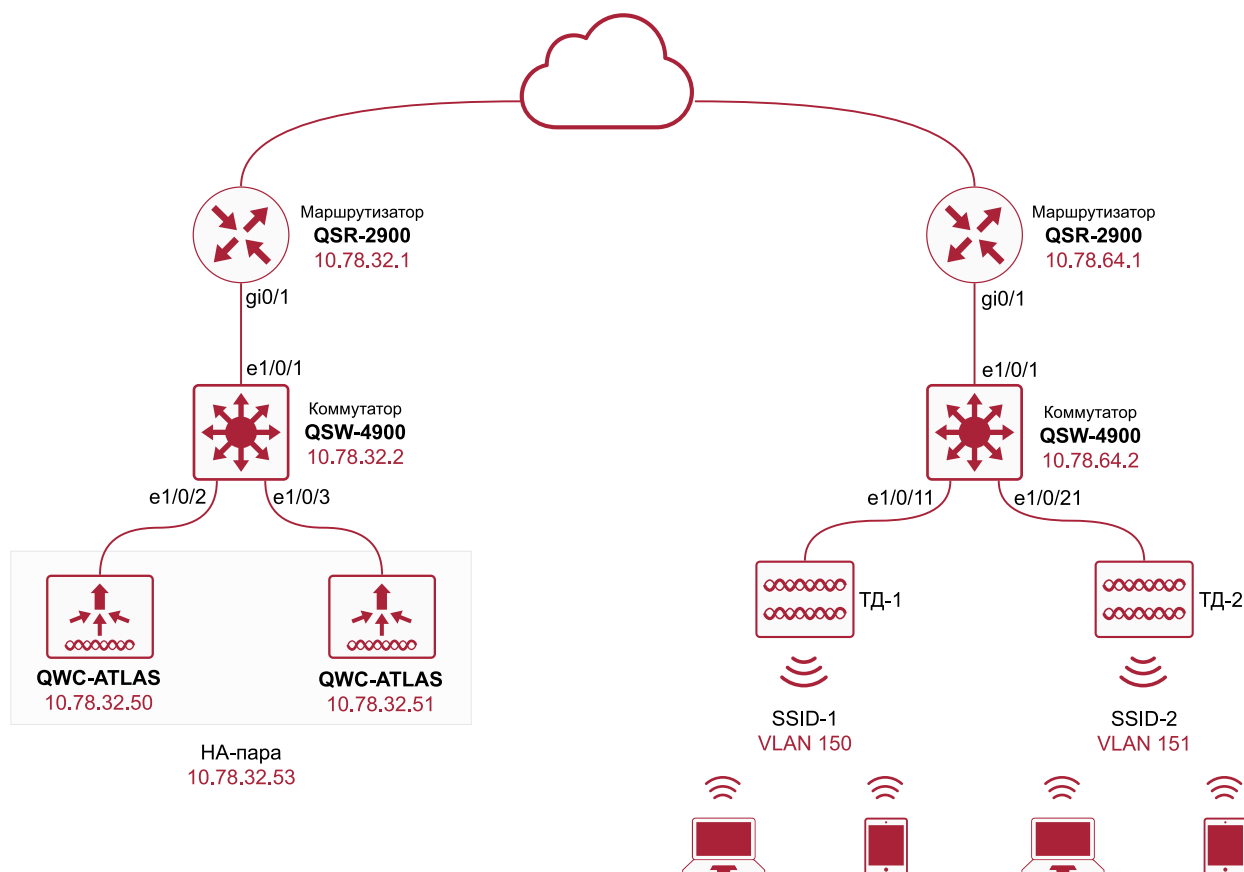


Рисунок 27-3. Филиальная инфраструктура

28.5. Сценарий 4. Георезервирование

В данном сценарии контроллеры QTECH Atlas размещены в двух географически разнесённых ЦОДах. В каждом ЦОД развернута отдельная HA-пара. Точки доступа при этом в самих ЦОДах отсутствуют и находятся в филиалах, которые также территориально разнесены.

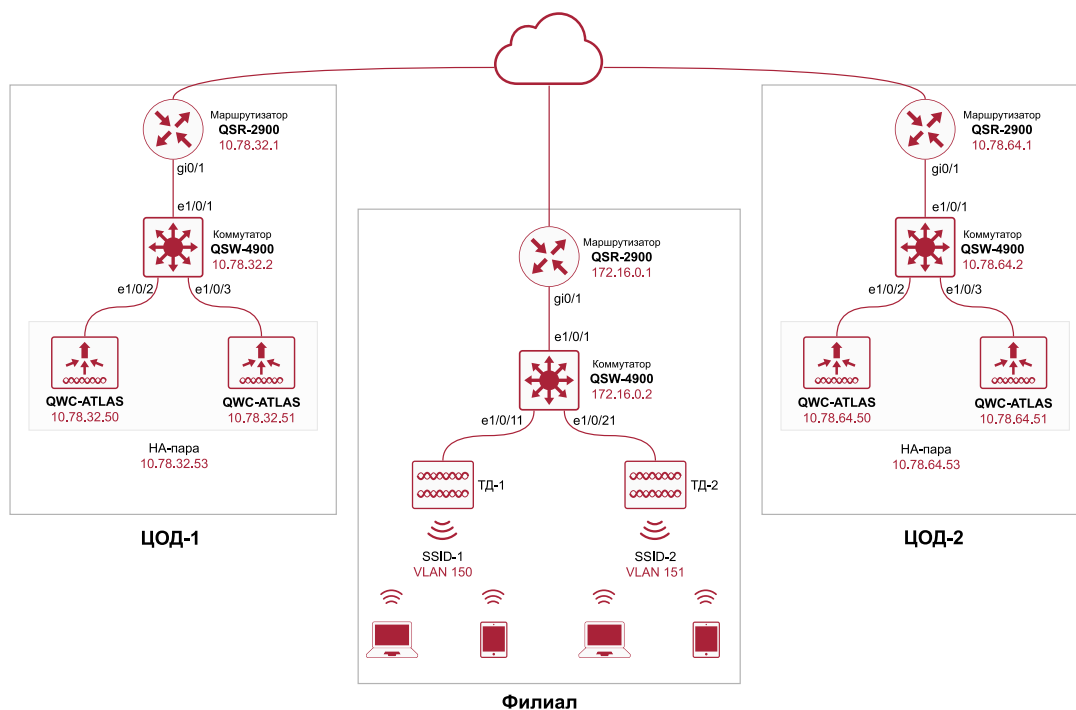


Рисунок 27-4. Филиальная инфраструктура

Настройки коммутаторов и маршрутизаторов в локальной сети остаются прежними ([разделы 27.1-27.3](#)), однако, чтобы обеспечить L3 связность между каждой HA-парой и удаленными точками доступа, необходимо организовать защищенный туннель.

Назначить точке доступа IP-адреса HA-пар можно в веб-интерфейсе ТД (см. [раздел 11.3](#)).



29. ОБЩАЯ ИНФОРМАЦИЯ

29.1. 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.

29.2. Техническая поддержка

Если вам необходимо содействие в вопросах, касающихся нашего оборудования, то можете воспользоваться разделом технической поддержки пользователей QTECH на нашем сайте www.qtech.ru/support/.

Телефон Технической поддержки +7 (495) 269-08-81

Центральный офис +7 (495) 477-81-18

29.3. Электронная версия документа

Дата публикации 01.10.2026