Контроллеры беспроводного доступа
WLC-15, WLC-30, WLC-3200, WLC-3250, WLC-3350, vWLC

Troubleshooting guide
Версия ПО 1.39.2

Содержание

⚠ Чтобы повысить точность диагностики, рекомендуется временно отключать firewall на всех интерфейсах. Для этого используйте команду **ip firewall disable** на каждом интерфейсе. Траблшутинг правил firewall не будет описываться в рамках данного раздела.
Начиная с версии 1.36.1 firewall можно отключить глобально:

```
wlc(config)# ip firewall disable
```

1 Сбор диагностической информации на контроллере WLC

1.1 Как собрать show tech-support в CLI контроллера

Для сбора диагностической информации через интерфейс командной строки (CLI) воспользуйтесь командой **show tech-support**. Контроллер сформирует единый архив, содержащий системные и сервисные журналы (логи), конфигурационные файлы и информацию о системе.

Имя файла генерируется автоматически по шаблону: YYYYMMDD-HHMMSS_show_tech-support_SN.tar.gz.

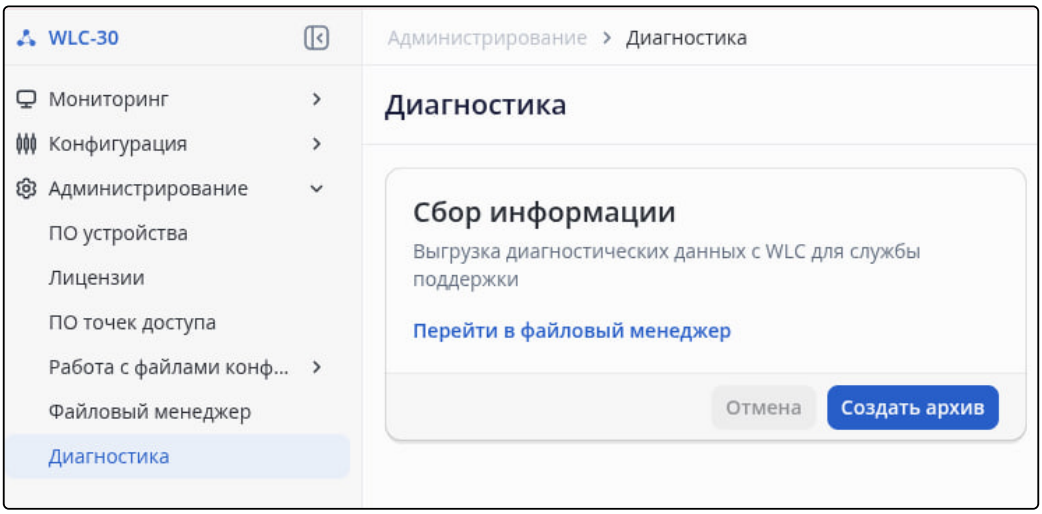
```
wlc# show tech-support
|****************************************| 100% Success.
Show tech-support output available at: flash:data/20260902_103154_show_tech-
support_NP1F000668.tar.gz
```

Скопировать созданный архив с контроллера можно с помощью любого удобного протокола.

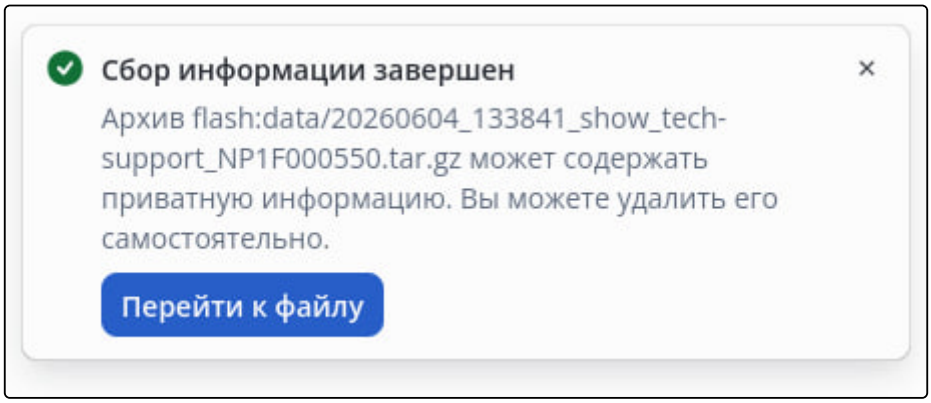
> ⚠ Начиная с версии 1.39.1 сбор диагностической информации можно запускать и скачивать в WEB-интерфейсе контроллера.

1.2 Как собрать show tech-support в WEB-интерфейсе контроллера

Для сбора диагностической информации с контроллера в WEB-интерфейсе перейдите во вкладку «Администрирование» → «Диагностика» → «Сбор информации». Для запуска сбора данных используйте кнопку «Создать архив».



Все необходимые файлы будут объединены в архив. О завершении формирования архива сообщит всплывающее уведомление.



Чтобы сразу перейти к созданному архиву, нажмите кнопку «Перейти к файлу». Собранные данные можно найти на странице «Файловый менеджер» в подменю «Flash».

1.3 Как собрать troubleshooting-file точки доступа в CLI контроллера

Для сбора комплексной системной информации с одной точки доступа или всех точек доступа в заданной локации используется команда **show tech-support wlc**. При выполнении команды создается задание на формирование и скачивание с точки доступа tech-support архива, который необходим для анализа службой технической поддержки в случае возникновения неполадок.

```
wlc# show tech-support wlc ap 68:13:e2:1f:7f:e0
2026-06-22T17:08:13+07:00 %WLC-W-WARN: BTE:tech-support archive from AP "68:13:e2:1f:7f:e0":
task started
wlc# 2026-06-22T17:08:15+07:00 %WLC-W-WARN: BTE:tech-support archive from AP
"68:13:e2:1f:7f:e0": FINISHED (1/1)
2026-06-22T17:08:15+07:00 %WLC-W-WARN: BTE:show tech-support wlc output available at:
flash:data/06-22_17:08_techsupp_68:13:e2:1f:7f:e0_WEP-3ax.tar.gz

wlc# show tech-support wlc ap-location default-location
2026-06-22T17:10:49+07:00 %WLC-W-WARN: BTE:tech-support archive from location "default-
location": task started
2026-06-22T17:10:55+07:00 %WLC-W-WARN: BTE:tech-support archive from location "default-
location": FINISHED (43/43)
2026-06-22T17:10:55+07:00 %WLC-W-WARN: BTE:show tech-support wlc output available at:
flash:data/06-22_17:10_techsupp_default-location.tar
```

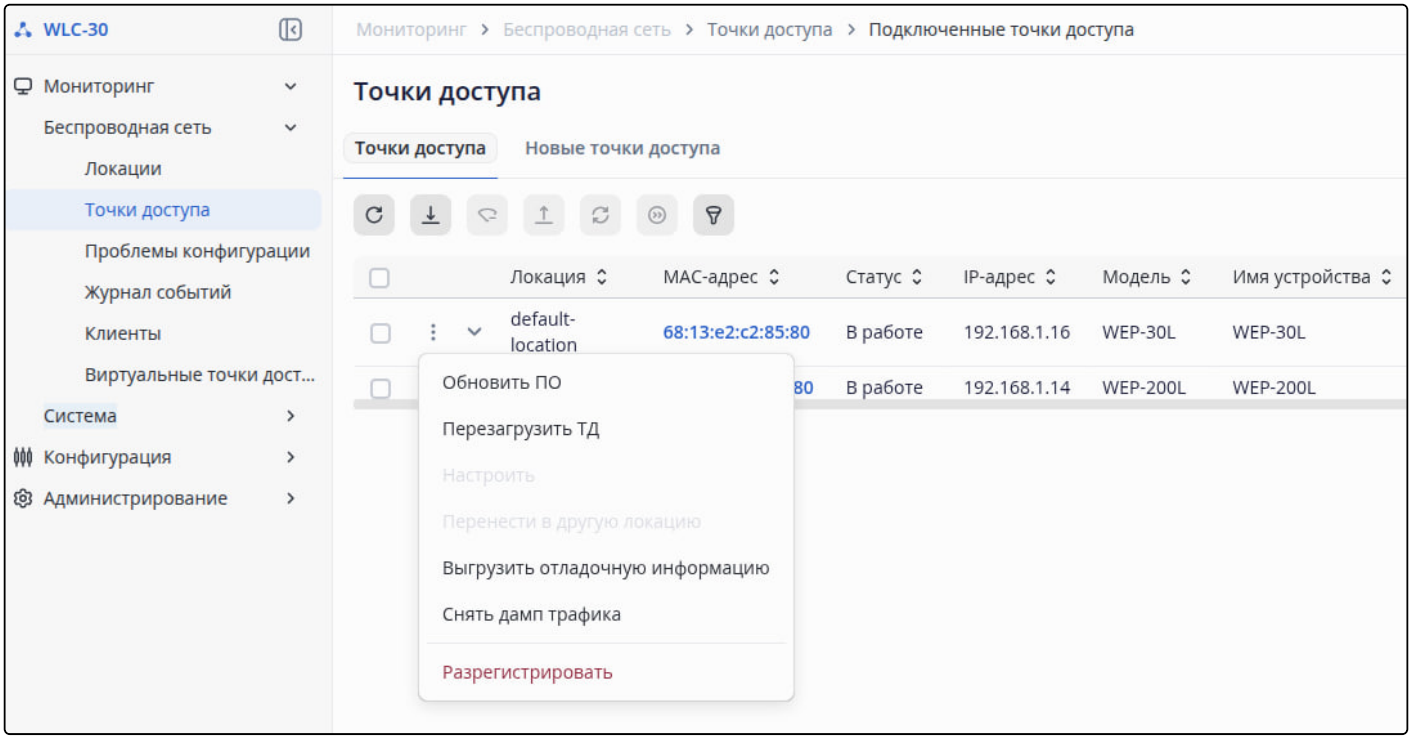
Задание работает в фоновом режиме. По завершению появляется архив в локальной директории контроллера: flash:data/. Статус и история заданий доступна в выводе команды **show wlc background download**.

```
wlc# show wlc background download
Time                  Status      Type           Object
Done/Total   Storage
-------------------   ---------   ------------   ------------------------------------------
----------   --------------------
2026-09-03 05:42:03   Finished    Tech-support   MAC AP: 68:13:e2:c2:85:80
1/1          flash:data/
2026-09-03 05:45:42   Finished    Tech-support   MAC AP: 68:13:e2:c2:85:80
1/1          flash:data/
2026-09-03 06:51:40   Finished    Tech-support   MAC AP: 68:13:e2:c2:85:80
1/1          flash:data/
```

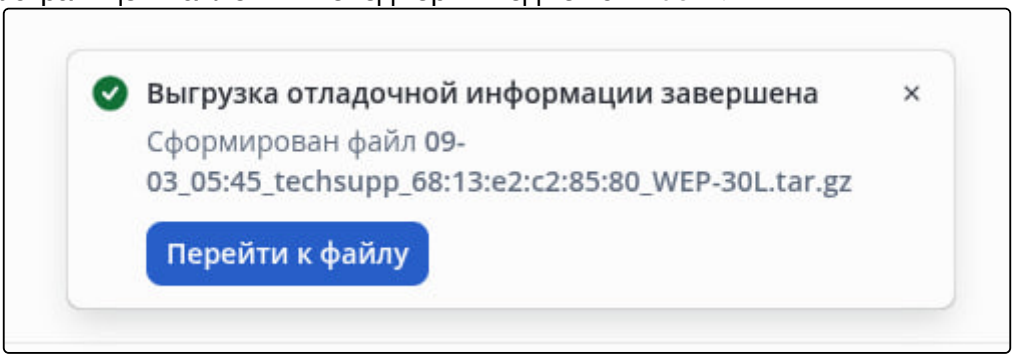
- Сбор комплексной системной информации с ТД **возможен**, если они находятся с статусе:
  - Active
  - Sandboxed
  - Cfg_Failed
  - Failed
  - Lost (при условии, что соединение с ТД существует, а переход в статус Lost вызван непредвиденной ошибкой)
- Сбор комплексной системной информации **невозможен** для моделей ТД: WEP-2ac, WEP-2ac Smart, WOP-2ac, WOP-2ac:rev.B, WOP-2ac:rev.C.

1.4 Как собрать troubleshooting-file точки доступа в WEB-интерфейсе контроллера

Для сбора комплексной системной информации точки доступа в WEB-интерфейсе контроллера перейдите во вкладку «Мониторинг» → «Беспроводная сеть» → «Точки доступа». Для запуска сбора данных используйте кнопку «Выгрузить отладочную информацию» в контекстном меню конкретной точки доступа.

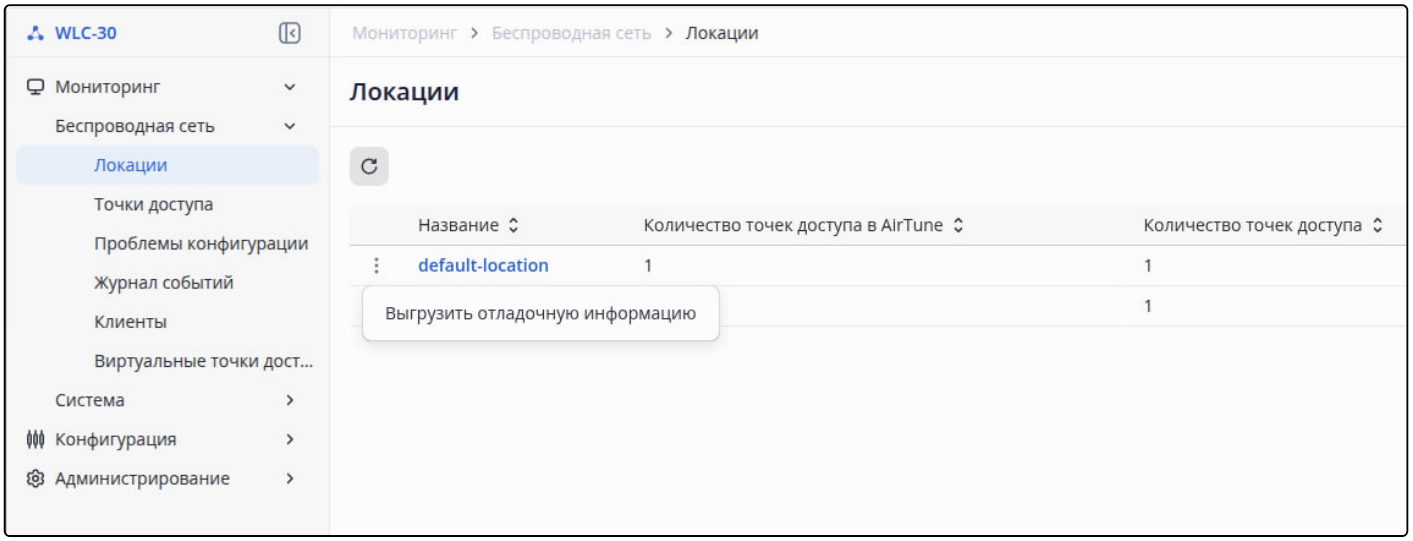


Чтобы сразу перейти к созданному архиву, нажмите кнопку «Перейти к файлу». Собранные данные можно найти на странице «Файловый менеджер» в подменю «Flash».

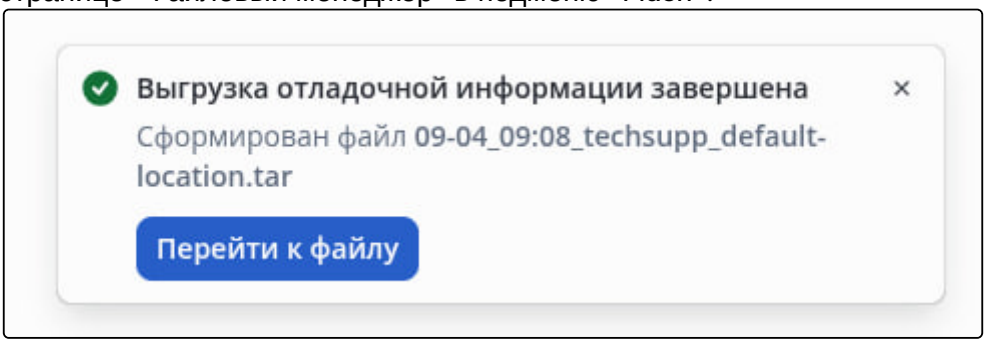


Для сбора комплексной системной информации со всех точек доступа в рамках локации в WEB-интерфейсе контроллера перейдите во вкладку «Мониторинг» → «Беспроводная сеть» → «Локации».

Для запуска сбора данных используйте кнопку «Выгрузить отладочную информацию» в контекстном меню конкретной локации.



Чтобы сразу перейти к созданному архиву, нажмите кнопку «Перейти к файлу». Собранные данные можно найти на странице «Файловый менеджер» в подменю «Flash».



1.5 Как собрать дамп трафика с интерфейсов контроллера в CLI

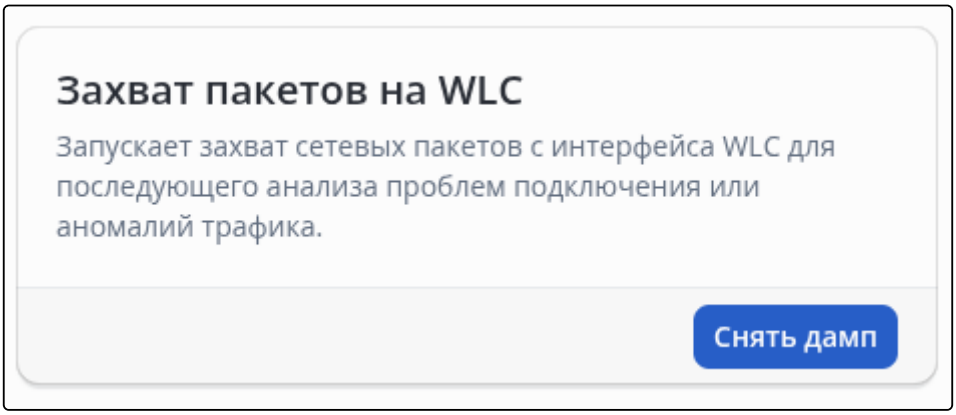
Для снятия дампа трафика на сетевом интерфейсе в режиме реального времени попакетно используйте команду **monitor**. Для записи дампа в файл необходимо указать параметр **file** и путь для сохранения файла. Число захваченных пакетов по умолчанию 1000, для захвата большего чиста пакетов необходимо использовать параметр **packets.**

Пример для снятия дампа трафика с интерфейса gigabitethernet 1/0/2 с протокола UDP по порту 67 и записью в файл *dhcp_dump.pcap*. Более подробно параметры для сбора дампа описаны в Справочнике команд.

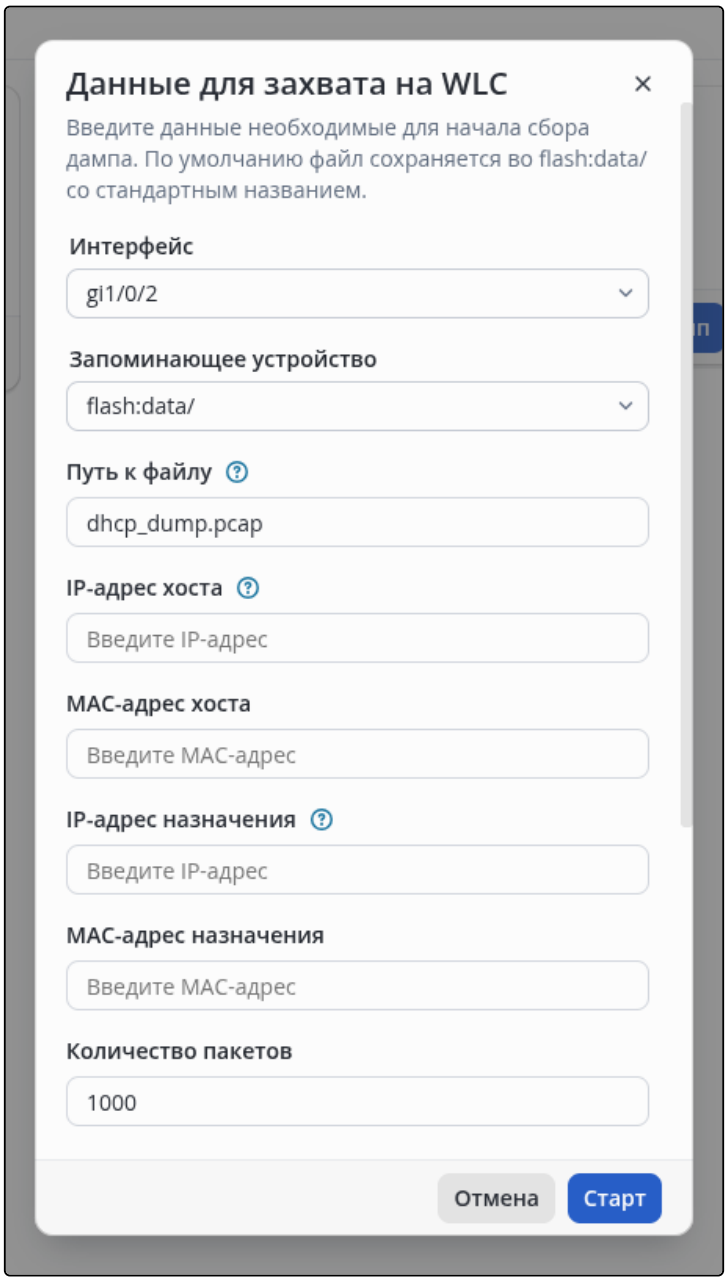
```
wlc# monitor gigabitethernet 1/0/2 protocol udp port 67 file flash:data/dhcp_dump.pcap packets
1500
```

1.6 Как собрать дамп трафика с интерфейсов контроллера в WEB-интерфейсе

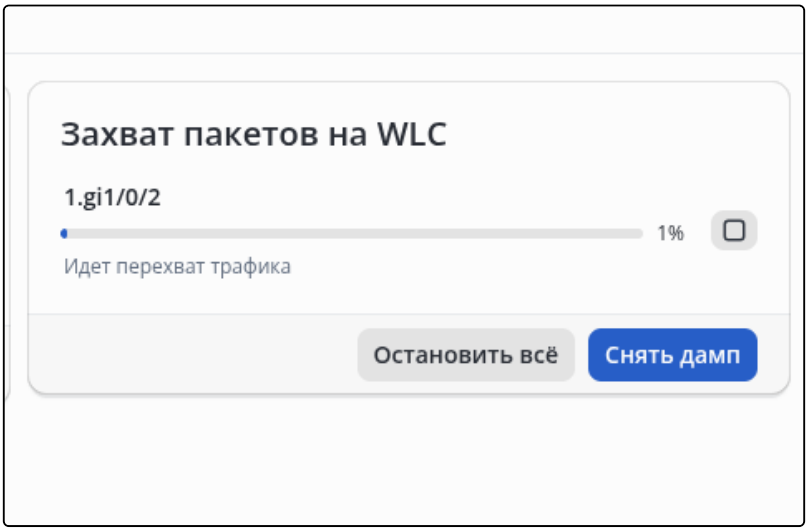
Для снятия дампа с интерфейсов контроллера в WEB-интерфейсе перейдите во вкладку «Администрирование» → «Диагностика» → «Захват пакетов на WLC». Для запуска сбора данных используйте кнопку «Снять дамп».



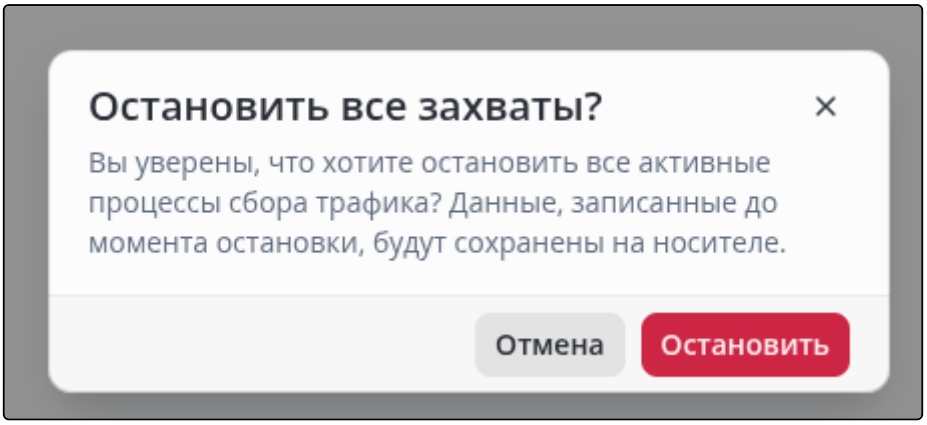
Для продолжения на всплывающей странице требуется настроить параметры для сбора дампа. Более подробно эти параметры описаны в Руководстве по эксплуатации.



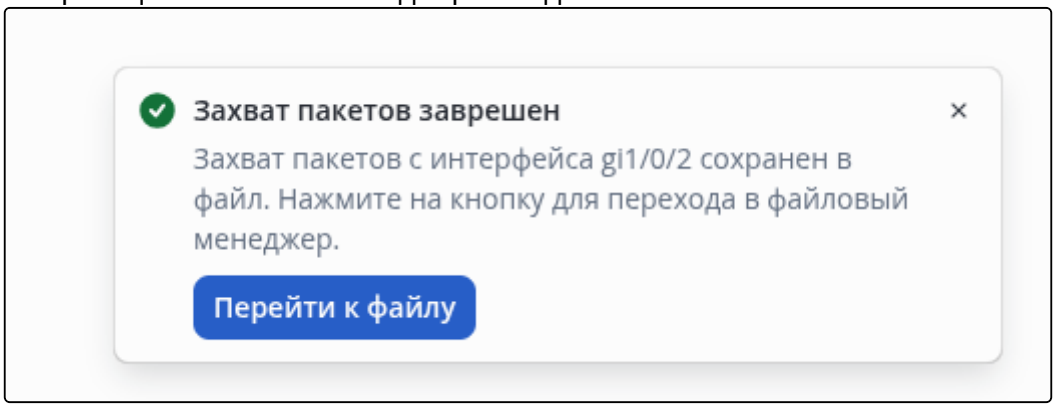
Запуск сбора трафика производится кнопкой «Старт».



После запуска трафика будет отображаться процесс захвата установленного числа пакетов визуально и в процентах. Одновременно можно запустить до 10 сборов дампа. В случае необходимости остановки одного из захвата пакетов нажмите кнопку  . Выбранный поток остановит запись в файл. Файл будет доступен для скачивания. Для остановки всех потоков нажмите «Остановить всё».



Чтобы сразу перейти к созданному файлу, нажмите кнопку «Перейти к файлу». Собранные данные можно найти на странице «Файловый менеджер» в подменю «Flash».



1.7 Как собрать дамп трафика с точки доступа в CLI контроллера

Для захвата трафика (дамп трафика, собранный через tcpdump) с точки доступа необходимо использовать команду **monitor wlc ap.** При выполнении команды создается задание на сбор дампа, которое работает в фоновом режиме и по завершению формируется файл в формате .pcap в локальной директории контроллера: *flash:data/* с последующей возможностью копирования на *usb/mmc/flash:data/ tftp-server*. Если в команде не будут заданы время сбора или размер файла, захват трафика

прекратится через 24 часа после начала выполнения. Статус и история заданий доступны в выводе команды show wlc background download.

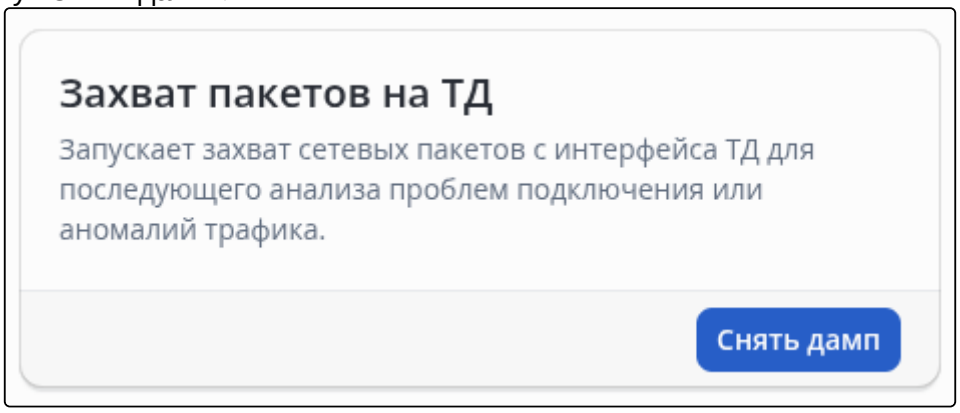
Пример для снятия дампа трафика с точки доступа с MAC-адресом a8:f9:4c:1f:f0:04 с интерфейса radio0 с временем захвата 30 секунд и записью в файл *radiodump2.pcap*. Более подробно параметры для сбора дампа описаны в Справочнике команд.

```
wlc# monitor wlc ap a8:f9:4c:1f:f0:04 radio0 timeout 30 file flash:data/radiodump2.pcap
```

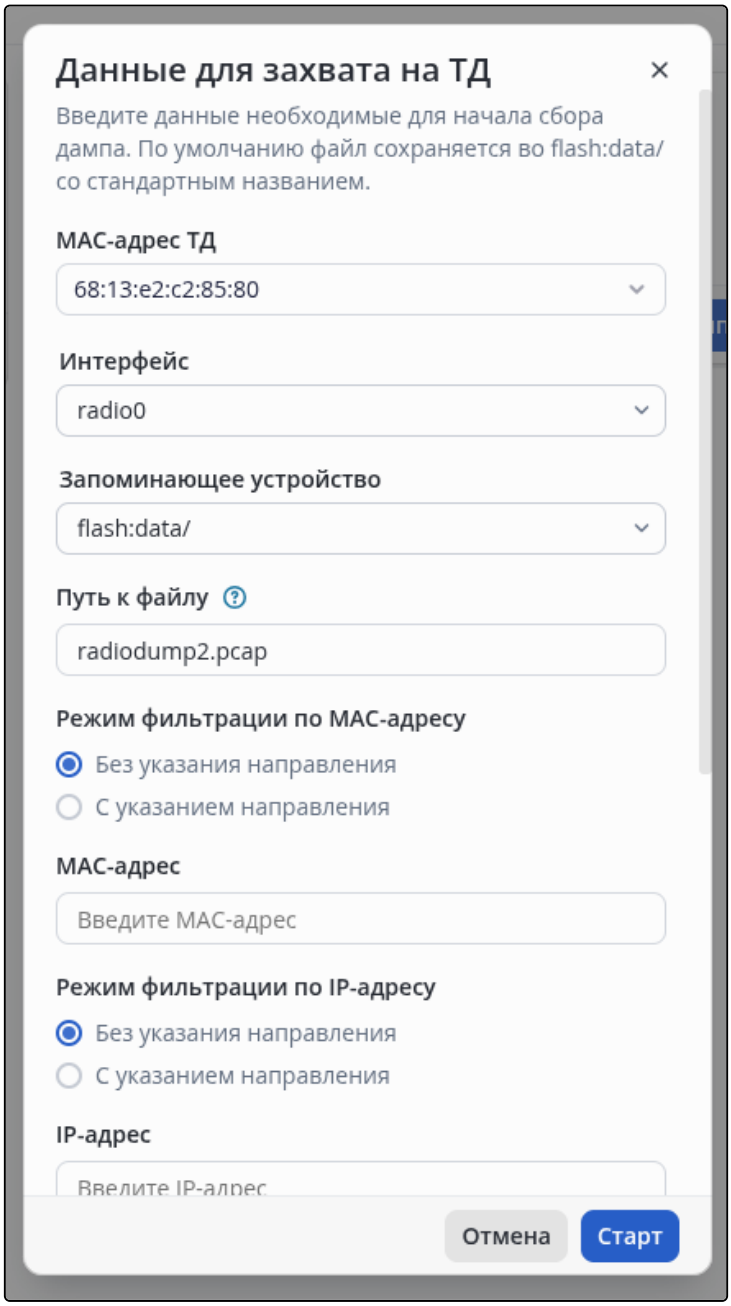
⚠
- Сбор дампа трафика с ТД **возможен**, если они находятся с статусе:
  - Active
  - Sandboxed
  - Cfg_Failed
  - Failed
  - Lost (при условии, что соединение с ТД существует, а переход в статус Lost вызван непредвиденной ошибкой)
- Сбор дампа трафика **невозможен** для моделей ТД: WEP-2ac, WEP-2ac Smart, WOP-2ac, WOP-2ac:rev.B, WOP-2ac:rev.C.

1.8 Как собрать дамп трафика с точки доступа в WEB-интерфейсе контроллера

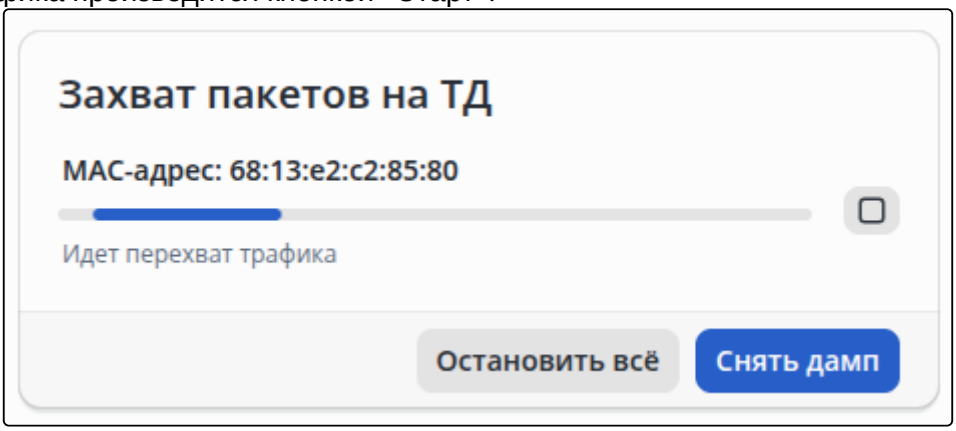
Для захвата трафика с точки доступа в WEB-интерфейсе контроллера перейдите во вкладку «Администрирование» → «Диагностика» → «Захват пакетов на ТД». Для запуска сбора данных используйте кнопку «Снять дамп».



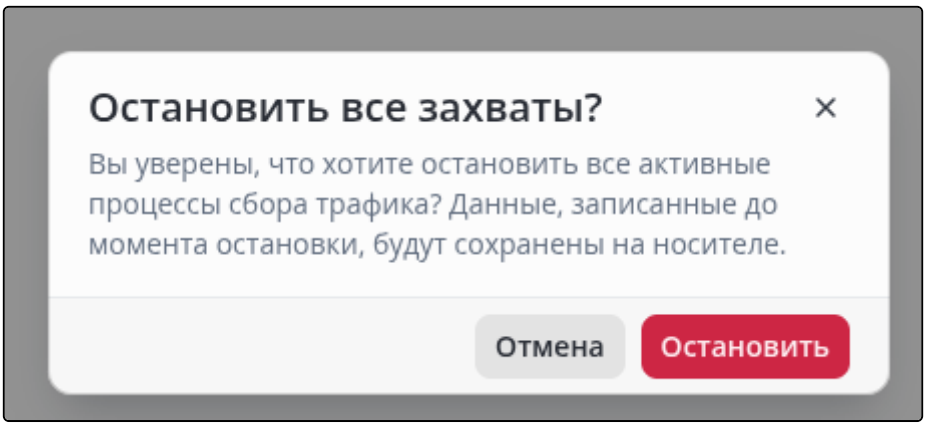
Задайте параметры захвата во всплывающем окне. Более подробно эти параметры описаны в Руководстве по эксплуатации



Запуск сбора трафика производится кнопкой «Старт».



После запуска трафика будет отображаться процесс захвата установленного числа пакетов визуально и в процентах. Одновременно можно запустить до 10 сборов дампа. В случае необходимости остановки одного из захвата пакетов нажмите кнопку  . Выбранный поток остановит запись в файл. Файл будет доступен для скачивания. Для остановки всех потоков нажмите «Остановить всё».



Чтобы сразу перейти к созданному файлу, нажмите кнопку «Перейти к файлу». Собранные данные можно найти на странице «Файловый менеджер» в подменю «Flash».

2 Точка доступа не регистрируется на контроллере

Посмотреть статус и другую информацию о всех точках доступа, обслуживаемых контроллером, можно с помощью команды **show wlc ap all.**

```
wlc# show wlc ap all

MAC address         Status              IP address        SW version         Hostname
Ap-location                       Uptime              Clients

(2g/5g/6g/all)
-----------------   ----------------   ---------------   ----------------
------------------------------   -------------------------------   ----------------
-------------------
68:13:e2:35:e9:d0   Active              192.168.1.2       2.9.0 build 842    WEP-30L
default-location                  02,22:53:42         0/0/-/0
cc:9d:a2:c2:96:c0   Active              192.168.1.5       1.15.0 build 42    WEP-3ax
default-location                  00,18:53:00         0/0/-/0
```

Описание статусов:

- Active – точка доступа подключена, сконфигурирована и находится в работе;
- Failed – в процессе работы точки доступа что-то пошло не так, NETCONF-соединение при этом может присутствовать;
- Lost – точка доступа отключена или до нее потерян доступ, NETCONF-соединение отсутствует;
- Pre-configured – для точки доступа в конфигурации настроен индивидуальный профиль по MAC-адресу и при этом она еще не подключалась к контроллеру;
- Applying cfg – NETCONF-соединение установлено и точка в данный момент применяет конфигурацию, сгенерированную контроллером;
- Cfg Failed – конфигурация для точки предоставлена с ошибками. Подробнее можно посмотреть командой show wlc configuration warnings;
- Ready – точка доступа содержит актуальную версию программного обеспечения, установила пароль из конфигурации и готова к установлению NETCONF-соединения, ожидает подключения со стороны контроллера;
- Rebooting – точка доступа перезагружается по запросу администратора;
- Reconnecting – точка доступа прекратила NETCONF-соединение и пытается снова подключиться;
- Registering – точка доступа прошла регистрацию и получила сертификат;
- Sandboxed – NETCONF-соединение установлено, но на контроллере нет конфигурации для данной точки;
- Updating creds – точка доступа обновляет пароль, NETCONF-соединение разорвано;
- Upgrading FW – точка доступа обновляет программное обеспечение.

⚠ Необходимо обязательно синхронизировать время на контроллере и точках доступа, т. к. корректное время позволяет пройти проверку валидности сертификатов.

Для корректной регистрации точек доступа на контроллере требуется синхронизация времени. Настройте NTP-сервер, чтобы контроллер получил актуальное время от вышестоящего сервера (пример настройки представлен в разделе Настройка NTP-сервера). Затем укажите адрес контроллера в качестве NTP-сервера для точек доступа в 42 опции DHCP (пример настройки представлен в разделе Настройка DHCP-сервера), чтобы точки доступа также смогли получить актуальное время.

2.1 Точка доступа не регистрируется на контроллере с ошибкой: AP enter to Failed state, desc: 'data-tunnel:status=can-not-create-tunnel'

1. Проверьте, что **radius-server local** включен.

```
wlc# show running-config radius-server local

radius-server local
  virtual-server default
    enable
  exit
  enable
exit
```

2. Ключ в host должен совпадать с ключом, указанным для **nas local** в **radius-server local.** Эта связка обязательна для поднятия туннелей.

```
wlc# show running-config aaa

radius-server local
  nas local
    key ascii-text encrypted 8CB5107EA7005AFF
    network 127.0.0.1/32
  exit
  enable
exit
radius-server host 127.0.0.1
  key ascii-text encrypted 8CB5107EA7005AFF
exit
```

3. После устранения проблем перерегистрируйте ТД на контроллере:

```
wlc# renew wlc ap failed
```

2.2 Точка доступа не регистрируется на контроллере с ошибкой: no firmware image for upgrade

Версия ТД не совместима с версией контроллера, поэтому ТД не может пройти регистрацию. Необходимо загрузить ПО точек доступа на контроллер для их обновления (команды для обновления точек доступа представлены в разделе Обновление точек доступа. Просмотреть информацию о минимальной поддерживаемой версии ПО для каждой модели точки доступа, а также о загруженных на контроллере актуальных файлах ПО ТД можно командой:

```
wlc# show wlc ap firmware
```

2.3 Точка доступа не регистрируются на контроллере с ошибкой: authentication error: failed to connect AP

1. Проверьте, получила ли точка доступа адрес.
2. Проверьте корректное написание 43 опции 15 подопции в конфигурации DHCP-сервера, необходимой для того, чтобы точка доступа автоматически пришла на контроллер и включилась в работу под его управлением. Опция содержит HTTPS URL контроллера, имеет вид https://192.168.1.1:8043/ и не должна

содержать пробелы или другие лишние символы.

```
wlc# show running-config dhcp server pool ap-pool

 vendor-specific
suboption 15 ascii-text "https://192.168.1.1:8043"
exit
```

3. Если в блоке ip-pool настроена подсеть, отличная от дефолтного значения 0.0.0.0/0, убедитесь, что ТД входят в список разрешенных IP-адресов.

```
wlc# show running-config wlc ip-pool default-ip-pool

ip-pool default-ip-pool
  description "default-ip-pool"
  ap-location default-location
  network 0.0.0.0/0
```

2.4 Точка доступа не регистрируется на контроллере с ошибкой: AP enter to Failed state, desc: 'CoA timeout expired

1. Убедитесь, что точки доступа получают 42 опцию DHCP с адресом NTP-сервера и на них актуальное время.

```
WEP-200L(root):/# date
Mon Aug 11 14:35:31 WIT 2025
```

2. Проверьте, что в softgre-controller в качестве nas-ip-address указано 127.0.0.1.

```
wlc# show running-config softgre-controller

softgre-controller
  nas-ip-address 127.0.0.1
  data-tunnel configuration wlc
  aaa radius-profile default_radius
  keepalive-disable
  service-vlan add 3
  enable
exit
```

3. Для организации туннеля точка доступа–контроллер, требуется RADIUS-авторизация на контроллере. Она не проксируется на внешний RADIUS, поэтому в блоке профиля «aaa radius-profile default_radius» параметр «radius-server host» должен быть «127.0.0.1». Убедитесь, что данный блок настроен верно.

```
wlc# show running-config aaa

radius-server host 127.0.0.1
  key ascii-text encrypted 8CB5107EA7005AFF
exit
aaa radius-profile default_radius
radius-server host 127.0.0.1
exit
```

2.5 Точка доступа не регистрируется на контроллере с цикличной сменой статусов в service-activator

1. Для диагностирования проблемы проверьте журнал точек доступа на контроллере WLC: циклическая смена статусов в `service-activator` указывает на проблему подключения.

```
2026-04-10T10:55:18+07:00 AP 0c:ee:20:00:10:40 status awaited, AP model: WEP-550K, SW version:
1.3.0 build 99, IP address: 192.168.1.2, description: 'SA_FREE: start tracking AP with path [/
wait/ap]'
2026-04-10T10:55:18+07:00 AP 0c:ee:20:00:10:40 status awaited, AP model: WEP-550K, SW version:
1.3.0 build 99, IP address: 192.168.1.2, description: 'SA_FREE: connection path /register/ap,
valid AP json'
2026-04-10T10:55:18+07:00 AP 0c:ee:20:00:10:40 status awaited, AP model: WEP-550K, SW version:
1.3.0 build 99, IP address: 192.168.1.2, description: 'SA_FREE: authenticating'
2026-04-10T10:55:18+07:00 AP 0c:ee:20:00:10:40 status join-auto, AP model: WEP-550K, SW
version: 1.3.0 build 99, IP address: 192.168.1.2, description: 'SA_FREE: auto authenticate
enabled'
2026-04-10T10:55:18+07:00 AP 0c:ee:20:00:10:40 status join-auto, AP model: WEP-550K, SW
version: 1.3.0 build 99, IP address: 192.168.1.2, description: 'SA_FREE: AP removed from
unauthorized'
2026-04-10T10:55:18+07:00 AP 0c:ee:20:00:10:40 status join-auto, AP model: WEP-550K, SW
version: 1.3.0 build 99, IP address: 192.168.1.2, description: 'SA_FREE: remove from tracking'
2026-04-10T10:55:19+07:00 AP 0c:ee:20:00:10:40 status registering, AP model: WEP-550K, SW
version: 1.3.0 build 99, IP address: 192.168.1.2, description: 'SA_FREE: connection path /
register/ap, valid AP json'
2026-04-10T10:55:19+07:00 AP 0c:ee:20:00:10:40 status awaited, AP model: WEP-550K, SW version:
1.3.0 build 99, IP address: 192.168.1.2, description: 'SA_FREE: start tracking AP with path [/
wait/ap]'
```

Проверьте `syslog.log` на точках доступа. Для этого можно подключиться к ней по ssh и проверить наличие ошибок SSL-соединения, свидетельствующих о сбое при установлении соединения с контроллером.

2. Узнайте выданный точке доступа IP-адрес с помощью команды **show wlc service-activator aps**.

```
wlc# show wlc service-activator aps
MAC address         Status          IP address        Board type         SW version         HW
version    Serial number
-----------------   -------------   ---------------   ----------------   ----------------
-----------   --------------
0c:ee:20:00:10:40   Join-auto       192.168.1.2       WEP-550K           1.3.0 build 99     1v2
WP61000031
```

3. Перейдите по ssh на точку доступа (пароль по умолчанию – admin/password) и воспользуйтесь командой **monitoring events.**

```
wlc# ssh admin 192.168.1.2
admin@192.168.1.2's password:
WEP-550K(root):/# monitoring events
Apr 10 03:43:41 WEP-550K daemon.info WLC-SA[10709]: Successfully connected to https://
192.168.1.1:8043/ott/register/ap
Apr 10 03:43:41 WEP-550K daemon.info WLC-SA[10709]: Received SA_SERVER_CODE_AUTH_REQUIRED from
https://192.168.1.1:8043
Apr 10 03:43:42 WEP-550K daemon.info WLC-SA[10720]: Successfully connected to https://
192.168.1.1:8043/ott/wait/ap
Apr 10 03:43:42 WEP-550K daemon.info SA_SERVER[10719]: 192.168.1.1 successfully connected to
the SA Server
Apr 10 03:43:42 WEP-550K daemon.info SA_SERVER[10719]: Received a certificate from 192.168.1.1
Apr 10 03:43:43 WEP-550K daemon.err WLC-SA[10739]: Connection to https://192.168.1.1:8044/ott/
register/ap failed SSL connect error: error:1416F086:SSL
routines:tls_process_server_certificate:certificate verify failed, reason: Hostname mismatch
```

⚠ Наличие ошибки
`failed SSL connect error: error:1416F086:SSL routines:tls_process_server_certificate:certificate verify failed, reason: Hostname mismatch`

сигнализирует о несовпадении адресов в 43 опции 15 подопции DHCP-сервера и outside-address в блоке конфигурации wlc.

4. Проверьте корректное написание 43 опции 15 подопции в конфигурации DHCP-сервера, необходимой для того, чтобы точка доступа автоматически пришла на контроллер и включилась в работу под его управлением. Опция содержит HTTPS URL контроллера, имеет вид https://192.168.1.1:8043/ и не должна содержать пробелы или другие лишние символы.

```
wlc# show running-config dhcp server pool ap-pool

ip dhcp-server pool ap-pool
  network 192.168.1.0/24
  address-range 192.168.1.2-192.168.1.254
  default-router 192.168.1.1
  dns-server 192.168.1.1
  option 42 ip-address 192.168.1.1
  vendor-specific
    suboption 12 ascii-text "192.168.1.1"
    suboption 15 ascii-text "https://192.168.1.1:8043" <------------------------
  exit
exit
```

5. Убедитесь, что параметр `outside-address` в конфигурации WLC совпадает с адресом, указанным в 43 опции 15 подопции DHCP-сервера. Только при этом условии точка доступа сможет корректно зарегистрироваться на контроллере.

```
wlc# sh running-config wlc
wlc
  outside-address 192.168.1.1
```

3 Клиент не получает адрес при подключении к точке доступа

3.1 Клиент не получает адрес при подключении к точке доступа – схема с SoftGRE-туннелями

1. Проверьте, что локация работает в режиме туннелирования. Должен быть включен режим **mode tunnel**:

```
wlc# show running-config wlc ap-location default-location

ap-location default-location
    description "default-location"
    mode tunnel
    ap-profile default-ap
    airtune-profile default_airtune
    ssid-profile default-ssid
  exit
```

2. Проверьте блок настроек ssid-profile. В нем должен быть клиентский VLAN в команде **vlan-id.**

```
wlc# show running-config wlc ssid-profile

ssid-profile default-ssid
  description "default-ssid"
  ssid "default-ssid"
  radius-profile default-radius
  vlan-id 3
  security-mode WPA2_1X
  802.11kv
  band 2g
  band 5g
  enable
exit
```

3. Проверьте блок настроек softgre-controller. В нем должен быть клиентский VLAN в команде **service-vlan.**

```
wlc# show running-config softgre-controller

softgre-controller
  nas-ip-address 127.0.0.1
  data-tunnel configuration wlc
  aaa radius-profile default_radius
  keepalive-disable
  service-vlan add 3
  enable
exit
```

4. Проверьте, включен ли функционал автоматического поднятия SoftGRE-туннелей:

```
wlc# show running-config tunnels

tunnel softgre 1
  mode data
  local address 192.168.1.1
  default-profile
  enable
exit
```

5. Проверьте, что 12 подопция 43 опции, необходимая для построения SoftGRE data-туннелей, задана корректно: не должно быть пробелов, точек и других символов.

```
wlc# show running-config dhcp server pool ap-pool

ip dhcp-server pool ap-pool
  network 192.168.1.0/24
  address-range 192.168.1.2-192.168.1.254
  default-router 192.168.1.1
  dns-server 192.168.1.1
  option 42 ip-address 192.168.1.1
  vendor-specific
    suboption 12 ascii-text "192.168.1.1"              <------------------------
    suboption 15 ascii-text "https://192.168.1.1:8043"
  exit
exit
```

6. Убедитесь, что создан бридж для терминации клиентского трафика и указан пользовательский VLAN.

```
wlc# show running-config bridges

 bridge 3
  vlan 3
  mtu 1458
  security-zone users
  ip address 192.168.2.1/24
  no spanning-tree
  enable
exit
```

7. Проверьте, что параметр force-up, назначен для vlan с пользовательским трафиком.

```
wlc# show running-config vlans
vlan 3
  force-up   <--------------------------
exit
vlan 2
exit
```

8. Убедитесь, что бридж для терминации клиентского трафика в состоянии up.

```
wlc# show interfaces status
Interface               Admin        Link    MTU     MAC address         Last change     Mode
                        State        State                               (d,h:m:s)
--------------------    ----------   -----   -----   -----------------   -------------
------------
gi1/0/1                 Up           Up      1500    90:54:b7:3a:35:21   00,03:47:21
switchport
gi1/0/2                 Up           Down    1500    90:54:b7:3a:35:22   03,17:28:58
routerport
gi1/0/3                 Up           Up      1500    90:54:b7:3a:35:23   00,01:29:28
switchport
gi1/0/4                 Up           Down    1500    90:54:b7:3a:35:24   03,17:28:58
routerport
gi1/0/5                 Up           Down    1500    90:54:b7:3a:35:25   03,17:28:58
routerport
gi1/0/6                 Up           Down    1500    90:54:b7:3a:35:26   03,17:28:58
routerport
br1                     Up           Up      1500    90:54:b7:3a:35:20   00,03:47:18
routerport
br2                     Up           Up      1500    90:54:b7:3a:35:20   00,03:47:18
routerport
br3                     Up           Up      1458    90:54:b7:3a:35:20   03,17:28:48
routerport   <---------------------------
```

3.2 Клиент не получает адрес при подключении к точке доступа – схема Local switching

⚠ **Local switching** – режим VAP для точек доступа Eltex, который работает только в схеме с GRE-туннелированием и позволяет выпускать трафик клиентов отдельного SSID с точки доступа во VLAN без туннеля.

Ниже приведен пример настройки для выпуска клиентского трафика с точки доступа по L2 с терминации на WLC.

1. Убедитесь, что в настройках SSID включен режим local-switching и указан номер VLAN для передачи пользовательского трафика.

```
wlc# show running-config wlc ssid-profile default-ssid

ssid ssid-profile default-ssid
    description "default-ssid"
    ssid "default-ssid"
    radius-profile default-radius
    vlan-id 3
    security-mode WPA2_1X
    local-switching
    802.11kv
    band 2g
    band 5g
    enable
exit
```

2. Проверьте, что на интерфейсе в сторону точек доступа настроен прием пользовательского трафика VLAN, заданный в SSID.

```
wlc# show running-config interfaces

interface gigabitethernet 1/0/3
  mode switchport
  switchport mode trunk
  switchport trunk allowed vlan add 3
exit
```

3. Проверьте, что создан бридж для клиентского трафика и указан пользовательский VLAN.

```
wlc# show running-config bridges

 bridge 3
  vlan 3
  security-zone users
  ip address 192.168.2.1/24
  no spanning-tree
  enable
exit
```

4. Проверьте, что на коммутаторе настроен VLAN для передачи пользовательского трафика. Например:

```
Настройка порта в сторону точек доступа:
MES2324P#configure
MES2324P(config)#interface GigabitEthernet 1/0/3
MES2324P(config-if)#switchport mode trunk
MES2324P(config-if)#switchport trunk allowed vlan add 3     # VLAN 3 – для передачи
пользовательского трафика
MES2324P(config-if)#switchport trunk native vlan 5          # VLAN 5 – VLAN управления точкой
доступа
MES2324P(config-if)#exit


Настройка порта в сторону WLC:
MES2324P(config)#interface GigabitEthernet 1/0/5
MES2324P(config-if)# switchport mode trunk
MES2324P(config-if)#switchport trunk allowed vlan add 3,5
MES2324P(config-if)#exit
```

3.3 Клиент не получает адрес при подключении к точке доступа – схема без GRE-туннелирования

⚠ Если не используется схема с туннелированием (точкам доступа не выдается 12 подопция DHCP), то не требуется указывать local-switching в настройках ssid.

1. Убедитесь, что точкам доступа не выдается 12 подопция 43 опции, необходимая для построения SoftGRE data-туннелей. После удаления опции необходимо перезагрузить точку доступа.

```
wlc# show running-config dhcp server pool ap-pool

ip dhcp-server pool ap-pool
    vendor-specific
     suboption 15 ascii-text "https://192.168.1.1:8043"
    exit
```

2. Проверьте, что в локации **отключен** режим **mode tunnel**:

```
wlc# show running-config wlc ap-location default-location

ap-location default-location
  description default-location
  radio-2g-profile default_2g
  radio-5g-profile default_5g
  ap-profile default-ap
  ssid-profile default-ssid
  exit
```

3. Убедитесь, что в настройках SSID **отключен** режим local-switching и указан номер VLAN для передачи пользовательского трафика.

```
wlc# show running-config interfaces

ssid ssid-profile default-ssid
    description "default-ssid"
    ssid "default-ssid"
    radius-profile default-radius
    vlan-id 3
    security-mode WPA2_1X
    802.11kv
    band 2g
    band 5g
    enable
exit
```

4. Проверьте, что на интерфейсе для подключения точек доступа настроен вывод пользовательского трафика с тегом.

```
wlc# show running-config interfaces

interface gigabitethernet 1/0/3
  mode switchport
  switchport mode trunk
  switchport trunk allowed vlan add 3
exit
```

5. Проверьте, что создан бридж для терминации клиентского трафика и указан пользовательский VLAN.

```
wlc# show running-config bridges

 bridge 3
  vlan 3
  mtu 1458
  security-zone users
  ip address 192.168.2.1/24
  no spanning-tree
  enable
exit
```

6. Также рекомендуется удалить настройки для конфигурации SoftGRE-туннелей.

```
wlc(config)# no tunnel softgre 1
wlc(config)# no softgre-controller
```

7. Проверьте, что на коммутаторе настроен VLAN для передачи пользовательского трафика. Например:

```
Настройка порта в сторону точек доступа:
MES2324P#configure
MES2324P(config)#interface GigabitEthernet 1/0/3
MES2324P(config-if)#switchport mode trunk
MES2324P(config-if)#switchport trunk allowed vlan add 3     # VLAN 3 – для передачи
пользовательского трафика
MES2324P(config-if)#switchport trunk native vlan 5          # VLAN 5 – VLAN управления точкой
доступа
MES2324P(config-if)#exit


Настройка порту в сторону WLC:
MES2324P(config)#interface GigabitEthernet 1/0/5
MES2324P(config-if)# switchport mode trunk
MES2324P(config-if)#switchport trunk allowed vlan add 3,5
MES2324P(config-if)#exit
```

4 Ошибка сертификатов: error – certificate is not yet valid

```
wlc(change-expired-password)# commit
error - certificate is not yet valid
check radius: got 1 errors during validation
check cert and ca in radius local: certificate does not match ca
error - can't commit configuration.
```

Если дата и время установлены некорректно, при commit может появиться ошибка **"error – certificate is not yet valid".** Для решения этой проблемы необходимо установить дату и время через u-boot.

Зайдите в загрузчик через консольный интерфейс. В процессе загрузки устройства после появления сообщения:

```
Autobooting in 5 seconds, enter to command line available now
u-boot>
```

Введите слово **stop**.

⚠ Актуально только для устройств WLC-30 на версии 1.26 и выше, для остальных устройств WLC команда доступна с версии 1.30.

Введите команды **date reset** для сброса даты и **reset** для перезагрузки устройства.

```
u-boot> date reset
u-boot> reset
```

Для всех остальных устройств введите команды для очистки раздела data **clear_mtd_data** и **reset** для перезагрузки устройства, если версия ПО 1.26 или ниже.

```
u-boot> clear_mtd_data
u-boot> reset
```

5 Не работают физические интерфейсы

Проблема 1: После применения конфигурации агрегированного интерфейса нет прохождения трафика.

```
wlc# configure
wlc(config)# interface port-channel 1
wlc(config-port-channel)# ip firewall disable
wlc(config-port-channel)# ip address 192.0.2.1/24
wlc(config-port-channel)# exit
wlc(config)# interface tengigabitethernet 1/0/1
wlc(config-if-te)# mode switchport
wlc(config-if-te)# channel-group 1 mode auto
wlc(config-if-te)# exit
wlc(config)# interface tengigabitethernet 1/0/2
wlc(config-if-te)# mode switchport
wlc(config-if-te)# channel-group 1 mode auto
wlc(config-if-te)# do commit
wlc(config-if-te)# do confirm
```

В выводе статуса физические интерфейсы и агрегированный в статусе down.

```
wlc# show interfaces status
Interface              Admin        Link    MTU     MAC address         Last change     Mode
                       State        State                               (d,h:m:s)
--------------------   ----------   -----   -----   -----------------   -------------
------------
te1/0/1                Up           Down    1500    a8:f9:4b:ab:0e:39   00,00:00:26
switchport
te1/0/2                Up           Down    1500    a8:f9:4b:ab:0e:39   00,00:00:27
switchport
po1                    Up           Down    1500    a8:f9:4b:ab:0e:39   00,00:00:23
routerport
```

Решение: По умолчанию интерфейс port-channel поднимается со значением скорости, равной 1G. Для того чтобы на интерфейсах, отличных от gigabitethernet, поднялись линки, необходимо вручную прописать идентичную скорость для агрегированного интерфейса:

```
wlc(config-if-port-channel)# speed 10G
```

Проблема 2: Физический интерфейс не добавляется в port-channel.

```
wlc(config)# interface port-channel 3
wlc(config-if-port-channel)# mode routerport
wlc(config-if-port-channel)# exit
wlc(config)# interface gigabitethernet 1/0/5
wlc(config-if-gi)# channel-group 3 mode auto
error - Can not set channel-group on interface gigabitethernet 1/0/5, set mode switchport or
hybrid first
```

Ошибка заложена в понимании конфигурации. Режим routerport можно выбрать только для port-channel, но не для физического интерфейса. При добавлении в агрегированный интерфейс физический интерфейс всегда должен быть в режиме switchport.

Проблема 3: Не работают интерфейсы XG (10G) на скорости 1G. Применимо к моделям WLC-3200/3250/3350.

Для работы interface tengigabitethernet на скорости 1G необходимо перевести диапазон необходимых интерфейсов на скорость 1G и перезагрузить контроллер.

```
wlc# configure
wlc(config)# interface tengigabitethernet 1/0/1-4
wlc(config-if-te)# speed 1000M
wlc(config-if-te)# do commit
wlc(config-if-te)# do confirm
wlc(config-if-gi)# end
wlc# reload system
Do you really want to reload system now? (y/N): y
```

Проблема 4: После применения скорости все равно не поднимаются интерфейсы.

Одна из возможных причин – кабель/sfp-трансивер. Помимо физической исправности необходимо перепроверить, на какую скорость он рассчитан.

```
2026-01-22T04:00:21+00:00 %LINK-I-UP: twentyfivegigabitethernet 1/0/1 changed state to up,
speed 1000M full-duplex
```

Решение: Поменять кабель или применить именно эту скорость к port-channel.

6 Не работает Enterprise-авторизация в схеме с проксированием на внешний RADIUS-сервер

Проблема 1: Некорректный адрес контроллера в radius-profile.

В журнале событий авторизации клиентов фиксируются ошибки 802.1x auth fail и Unspecified:

```
wlc# show wlc journal clients
2026-06-16T08:17:59+00:00 Client 22:ec:85:1e:08:60 RADIUS authentication failed on AP 68:13:e2:3
5:e9:d0, SSID: !TEST_A_F, RSSI: -34, interface: wlan1-va0, band: 5 GHz, AP location: default-
location, reason: 23, description: '802.1x auth fail'
2026-06-16T08:18:08+00:00 Client 22:ec:85:1e:08:60 username: 'test' RADIUS authentication
failed on AP 68:13:e2:35:e9:d0, SSID: !TEST_A_F, RSSI: -26, interface: wlan1-va0, band: 5 GHz,
AP location: default-location, domain: 'default', reason: 1, description: 'Unspecified
```

При просмотре логов RADIUS в режиме отладки вывод полностью отсутствует, так как запросы от ТД не доходят до сервера:

```
wlc# debug
wlc(debug)# show radius-debug
wlc(debug)#
```

Решение: Точки доступа не знают, на какой адрес отправлять RADIUS-запросы. Необходимо явно указать IP-адрес контроллера в используемом radius-profile.

> ⚠ Если на сети развернута схема с резервированием контроллеров, в профиле необходимо указывать виртуальный IP-адрес (VIP) кластера.

```
wlc# show running-config wlc radius-profile default-radius

radius-profile default-radius
description "default-radius"
auth-address 192.168.1.11 # Указывается IP-адрес (или VIP) контроллера
auth-password ascii-text encrypted 8CB5107EA7005AFF
domain default
exit
```

Проблема 2: Несовпадение общего ключа.

Пароли, настроенные в radius-profile и в параметрах nas ap локального RADIUS-сервера, не совпадают.

Клиенты получают отказ в авторизации с кодами ошибок 802.1x auth fail или Unspecified:

```
wlc# show wlc journal clients
2026-06-16T08:40:35+00:00 Client 22:ec:85:1e:08:60 RADIUS authentication failed on AP 68:13:e2:3
5:e9:d0, SSID: !TEST_A_F, RSSI: -32, interface: wlan1-va0, band: 5 GHz, AP location: default-
location, reason: 23, description: '802.1x auth fail'
2026-06-16T08:40:44+00:00 Client 22:ec:85:1e:08:60 RADIUS authentication failed on AP 68:13:e2:3
5:e9:d0, SSID: !TEST_A_F, RSSI: -28, interface: wlan1-va0, band: 5 GHz, AP location: default-
location, reason: 1, description: 'Unspecified'
```

При несовпадении общего ключа RADIUS-сервер отбрасывает некорректно подписанные пакеты, игнорируя запросы ТД. В логах **show radius-debug** фиксируется циклическое получение пакетов Access-

Request и их мгновенное удаление по таймауту/завершению без отправки ответа (Cleaning up request packet due to done):

```
wlc# debug
wlc(debug)# show radius-debug

(23) Tue Jun 16 08:40:57 2026: Debug: Received Access-Request Id 5 from 192.168.1.2:59262 to
192.168.1.11:1812 length 271
(23) Tue Jun 16 08:40:58 2026: Debug: Cleaning up request packet ID 5 with timestamp +1469 due
to done
(24) Tue Jun 16 08:40:59 2026: Debug: Received Access-Request Id 5 from 192.168.1.2:59262 to
192.168.1.11:1812 length 271
(24) Tue Jun 16 08:41:00 2026: Debug: Cleaning up request packet ID 5 with timestamp +1471 due
to done
(25) Tue Jun 16 08:41:01 2026: Debug: Received Access-Request Id 5 from 192.168.1.2:59262 to
192.168.1.11:1812 length 271
(25) Tue Jun 16 08:41:02 2026: Debug: Cleaning up request packet ID 5 with timestamp +1473 due
to done
```

Решение: Убедитесь, что ключ шифрования (пароль), используемый точкой доступа в radius-profile, строго совпадает с ключом, настроенным для сетевого устройства (NAS) на RADIUS-сервере. Установите идентичные пароли в конфигурации radius-profile и radius-server local nas ap.

```
wlc# show running-config radius-server local

radius-server local  nas ap
key ascii-text encrypted 8CB5107EA7005AFF # Ключ должен быть идентичным
network 192.168.1.0/24
exit

wlc# show running-config wlc radius-profile default-radius

radius-profile default-radius
description "default-radius"
auth-address 192.168.1.11
auth-password ascii-text encrypted 8CB5107EA7005AFF # Ключ должен быть идентичным
domain default
exit
```

Проблема 3: Блокировка портов RADIUS межсетевым экраном на контроллере

Логи отладки RADIUS **show radius-debug** остаются пустыми, так как межсетевой экран блокирует трафик до того, как он будет передан службе RADIUS.

```
wlc# debug
wlc(debug)# show radius-debug
wlc(debug)#
```

Клиенты не могут пройти авторизацию, фиксируются типовые ошибки 802.1x auth fail и Unspecified:

```
2026-08-05T09:18:51+00:00 Client d6:64:6e:70:59:80 RADIUS authentication failed on AP 68:13:e2:
c2:85:80, SSID: !TEST_A_F, RSSI: -34, interface: wlan1-va0, band: 5 GHz, AP location: default-
location, auth step: eap, reason: 23, description: '802.1x auth fail'
2026-08-05T09:19:00+00:00 Client d6:64:6e:70:59:80 RADIUS authentication failed on AP 68:13:e2:
c2:85:80, SSID: !TEST_A_F, RSSI: -35, interface: wlan1-va0, band: 5 GHz, AP location: default-
location, auth step: eap, reason: 1, description: 'Unspecified'
```

Решение: Добавьте разрешающие правила для UDP-портов RADIUS (1812 — авторизация, 1813 — учет трафика) в конфигурацию межсетевого экрана или временно отключите его для локализации проблемы.

```
object-group service radius_auth
  port-range 1812
  port-range 1813
exit
```

```
wlc(config)# ip firewall disable
```

Проблема 4: Некорректные учетные данные пользователя

Наиболее распространенная причина отказа (Access-Reject) — ввод пользователем неверного логина/пароля или отсутствие учетной записи в базе данных авторизации.

В журнале событий отображается ошибка авторизации на шаге обмена TLS-сертификатами/данными пользователя (параметр auth step: tls и описание Auth no longer valid):

```
2026-08-05T10:14:01+00:00 Client d6:64:6e:70:59:80 username: 'test' RADIUS authentication
failed on AP 68:13:e2:c2:85:80, SSID: !TEST_A_F, RSSI: -40, interface: wlan1-va0, band: 5 GHz,
AP location: default-location, domain: 'default', auth step: tls, reason: 2, description: 'Auth
no longer valid'
```

Поскольку локальный RADIUS-сервер контроллера работает как прокси-сервер, он перенаправляет запрос на внешний RADIUS-сервер и получает от него явный ответ Access-Reject (отказ в доступе). После этого локальный сервер обрабатывает отказ и отправляет итоговый Access-Reject на точку доступа для отключения клиента:

```
wlc# debug
wlc(debug)# show radius-debug
(38) Wed Aug 5 10:14:01 2026: Debug: Received Access-Reject Id 170 from 100.127.1.3:1812 to
100.127.2.47:52906 length 49 # Получен отказ от вышестоящего сервера (100.127.1.3)
(38) Wed Aug 5 10:14:01 2026: Debug: Using Post-Auth-Type Reject
(38) Wed Aug 5 10:14:01 2026: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(38) Wed Aug 5 10:14:01 2026: Debug: Sent Access-Reject Id 135 from 192.168.1.11:1812 to
192.168.1.15:37061 length 44 # Отправлен итоговый отказ на ТД (192.168.1.15)
```

Если включить запись на локальный syslog-сервер сообщений локального RADIUS-сервера, можно увидеть в логах, причину отказа авторизации "Login incorrect":

```
wlc# show running-config syslog

syslog file flash:syslog/radius_test
  severity debug
  match process-name radius-server
exit

logging radius

wlc-30# show syslog flash:syslog/radius_test2

2026-09-09T10:03:38+00:00 %RADIUS-D-DEBUG: notice: (23) Login incorrect (Home Server says so):
[testuser/<no User-Password attribute>] (from client ap port 1 cli F6-22-49-51-F1-AC)
2026-09-09T10:03:38+00:00 %RADIUS-D-DEBUG: notice: (23) Login incorrect: [testuser/<no User-
Password attribute>] (from client ap port 1 cli F6-22-49-51-F1-AC)
```

Решение:

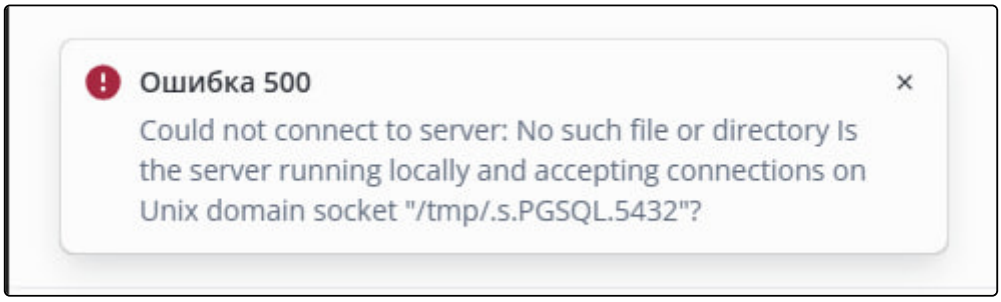
1. Проверьте правильность ввода учетных данных (логина и пароля) на клиентском устройстве.
2. Проверьте наличие и статус учетной записи в базе данных внешнего RADIUS-сервера (Active Directory, LDAP или локальная база внешнего сервера).

7 Ошибка «DMGR:failed to open transaction» и переполнение памяти Flash на контроллерах WLC

При переполнении дискового пространства базы данных в системных журналах (логах) контроллера WLC циклически фиксируются следующие предупреждения:

```
2026-06-02T11:42:11+03:00 %WLC-W-WARN: DMGR:failed to open transaction
2026-06-02T11:42:21+03:00 %WLC-W-WARN: DMGR:failed to open transaction
2026-06-02T11:42:31+03:00 %WLC-W-WARN: DMGR:failed to open transaction
```

На контроллере полностью перестает отображаться актуальный журнал событий.



Причина: Проблема вызвана переполнением базы данных журналов, расположенной во внутренней Flash-памяти устройства. В текущих версиях ПО контроллера поддерживается ограничение только по сроку хранения записей, но не по их физическому объему на диске. При высокой активности беспроводного трафика и большом количестве событий Flash-память заполняется раньше, чем срабатывает ротация по времени.

7.1 Решение

Для восстановления работоспособности необходимо полностью удалить поврежденную базу данных.

7.1.1 Версия ПО 1.39.1 или выше

Выполните команду:

```
wlc# clear wlc database
```

В схема с резервированием команду удаления нужно выполнить на контроллера в статусе Active. После выполнения команды создастся новая база данных и пройдет синхронизация с резервными контроллерами.

Если на резервном контроллере синхронизация не восстановилась в течение 20 минут после удаления базы данных на контроллера в статусе Standby, необходимо выполнить команду для удаления. Просмотра статуса синхронизации доступен в выводе команды *show high-availability state*.

⚠ Команда **clear wlc database** доступна начиная с версии 1.39.1

7.1.2 Версия ПО ниже 1.39.1

Если версия ПО ниже 1.39.1, авторизуйтесь на контроллере под учетной записью с правами **techsupport**. Выполните команду для удаления директории с базой данных:

```
techsupport@wlc:~$ sudo rm -rf /mnt/data/pgsql/
```

Выполните перезагрузку устройства для инициализации новой чистой базы данных:

```
techsupport@wlc:~$ reload-system
```

⚠ База данных PostgreSQL пересоздается непосредственно в процессе загрузки ПО WLC, поэтому перезагрузка контроллера после удаления файлов является обязательным шагом. Обратите внимание, что после выполнения процедуры все старые журналы событий будут безвозвратно удалены с контроллера.

В схема с резервированием используйте следующий пошаговый алгоритм для очистки БД без прерывания обслуживания клиентов:

1. **Очистка базы на резервном контроллере в статусе Standby:**
   - Авторизуйтесь под учетной записью techsupport на резервной ноде.
   - Выполните команду полного удаления директории базы данных.
   - Перезагрузите резервную ноду.
   - При старте устройства пустая база данных будет создана автоматически.

   ```
   techsupport@wlc-2:~$ sudo rm -rf /mnt/data/pgsql/
   techsupport@wlc-2:~$ reload-system
   ```

2. **Переключение ролей (Миграция активности):**
   Переключите мастерство на очищенную резервную ноду. Новые системные события начнут записываться в чистую, только что созданную базу данных.
3. **Очистка базы на бывшем основном контроллере:**
   Авторизуйтесь на устройстве, которое теперь перешло в статус резервного (бывший VRRP Master со сломанной базой данных). Выполните действия из п.1.

   ```
   techsupport@wlc-1:~$ sudo rm -rf /mnt/data/pgsql/
   techsupport@wlc-1:~$ reload-system
   ```

4. **Синхронизация и возврат к штатному режиму:**
   После включения резервный контроллер автоматически синхронизирует базу данных с активного мастера и продолжит работу в штатном режиме.
   После завершения процесса синхронизации данных (при необходимости) переключите мастерство обратно на исходный контроллер.

7.2 Настройка защиты от повторного переполнения

После удаления базы данных необходимо настроить превентивные меры, выбрав один из следующих вариантов:

- **Вариант 1** (Рекомендуемый при интенсивном логировании): Перенос хранения системных журналов на внешний накопитель (процесс настройки подробно описан в разделе Изменение пути хранения журналов WLC.
- **Вариант 2** (Ограничение срока хранения данных): Настройка автоматического удаления старых записей через 10–30 дней. Ограничение настраивается в режиме конфигурирования для всех типов журналов:

```
wlc(config)# wlc-journal wids
wlc(config-wlc-journal-wids)# limit days 30
wlc(config-wlc-journal-wids)# exit

wlc(config)# wlc-journal clients
wlc(config-wlc-journal-clients)# limit days 30
wlc(config-wlc-journal-clients)# exit

wlc(config)# wlc-journal ap
wlc(config-wlc-journal-ap)# limit days 30
wlc(config-wlc-journal-ap)# exit

wlc(config)# wlc-journal all
wlc(config-wlc-journal-all)# limit days 30
wlc(config-wlc-journal-all)# end
```

⚠ В схемах с резервированием происходит автоматическая синхронизация конфигурационных файлов между нодами. Настройки обоих контроллеров WLC должны быть строго идентичными. Если вы настраиваете лимиты хранения журналов, это необходимо делать на активном устройстве (Master).

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Для получения технической консультации по вопросам эксплуатации оборудования ООО «Предприятие «ЭЛТЕКС» Вы можете обратиться в Сервисный центр компании:

Форма обратной связи на сайте: https://eltex.ru/support/

Servicedesk: https://servicedesk.eltex-co.ru

На официальном сайте компании Вы можете найти техническую документацию и программное обеспечение для продукции ООО «Предприятие «ЭЛТЕКС», обратиться к базе знаний, оставить интерактивную заявку или проконсультироваться у инженеров Сервисного центра:

Официальный сайт компании: https://eltex.ru

База знаний: https://docs.eltex-co.ru/display/EKB/Eltex+Knowledge+Base

Центр загрузок: https://eltex.ru/downloads