Интеграция AxelNAC с контроллерами беспроводного доступа Cisco WLC 5500

В данной статье рассматривается процесс интеграции AxelNAC с контроллером беспроводного доступа Cisco WLC 5500 версии 8.5.171.0.

Веб-интерфейс других версий Cisco WLC может незначительно отличаться.

Введение

Для корректной работы всего функционала контроллера беспроводного доступа (WLC) с AxelNAC необходимо обеспечить правильное сетевое взаимодействие на всем пути сетевого оборудования. На рис. 1 представлена гибкая схема подключения сетевого оборудования, позволяющая реализовать весь функционал WLC:

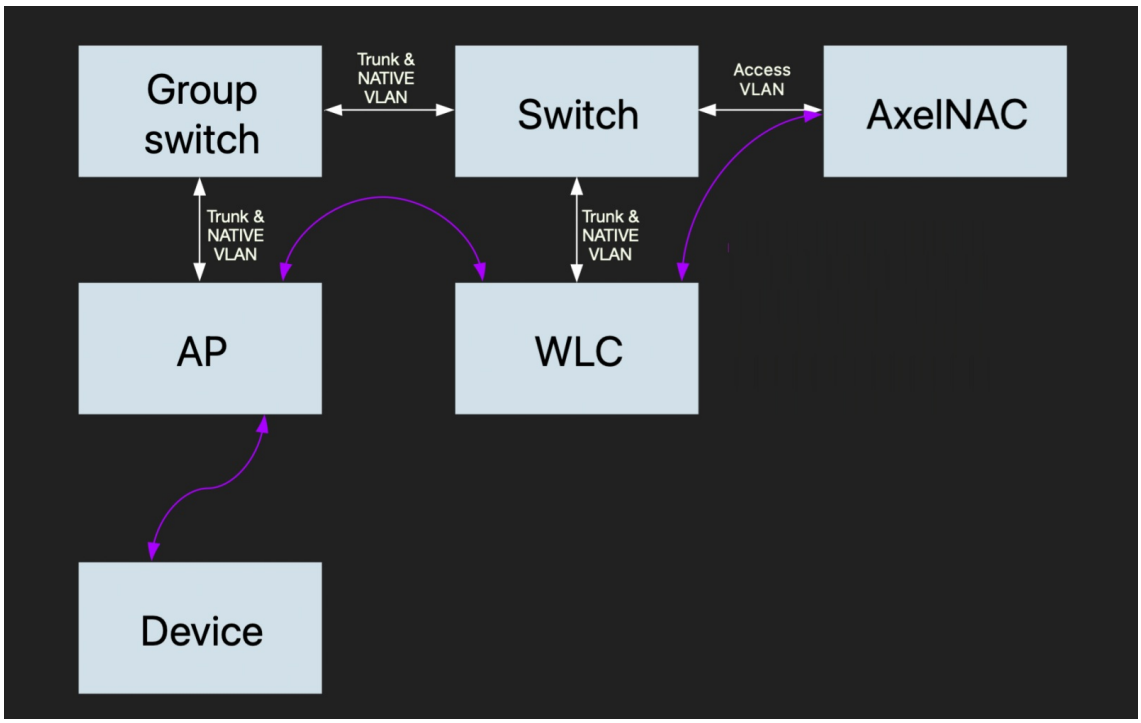


Рисунок 1 — Концептуальная схема соединения сетевого оборудования

Белые стрелки отображают физическое соединение устройств. Фиолетовыми стрелками показаны концептуальные соединения. Схема содержит следующие элементы:

- **AxelNAC** — виртуальный или физический сервер AxelNAC.
- **Switch** — физический коммутатор, на котором созданы все необходимые виртуальные локальные сети (VLAN);
- **Group switch** — физические коммутаторы, на которых созданы все необходимые VLAN;
- **WLC** — контроллер беспроводных сетей;
- **AP** — точка доступа;
- **Device** — конечное устройство, АРМ с беспроводным интерфейсом.

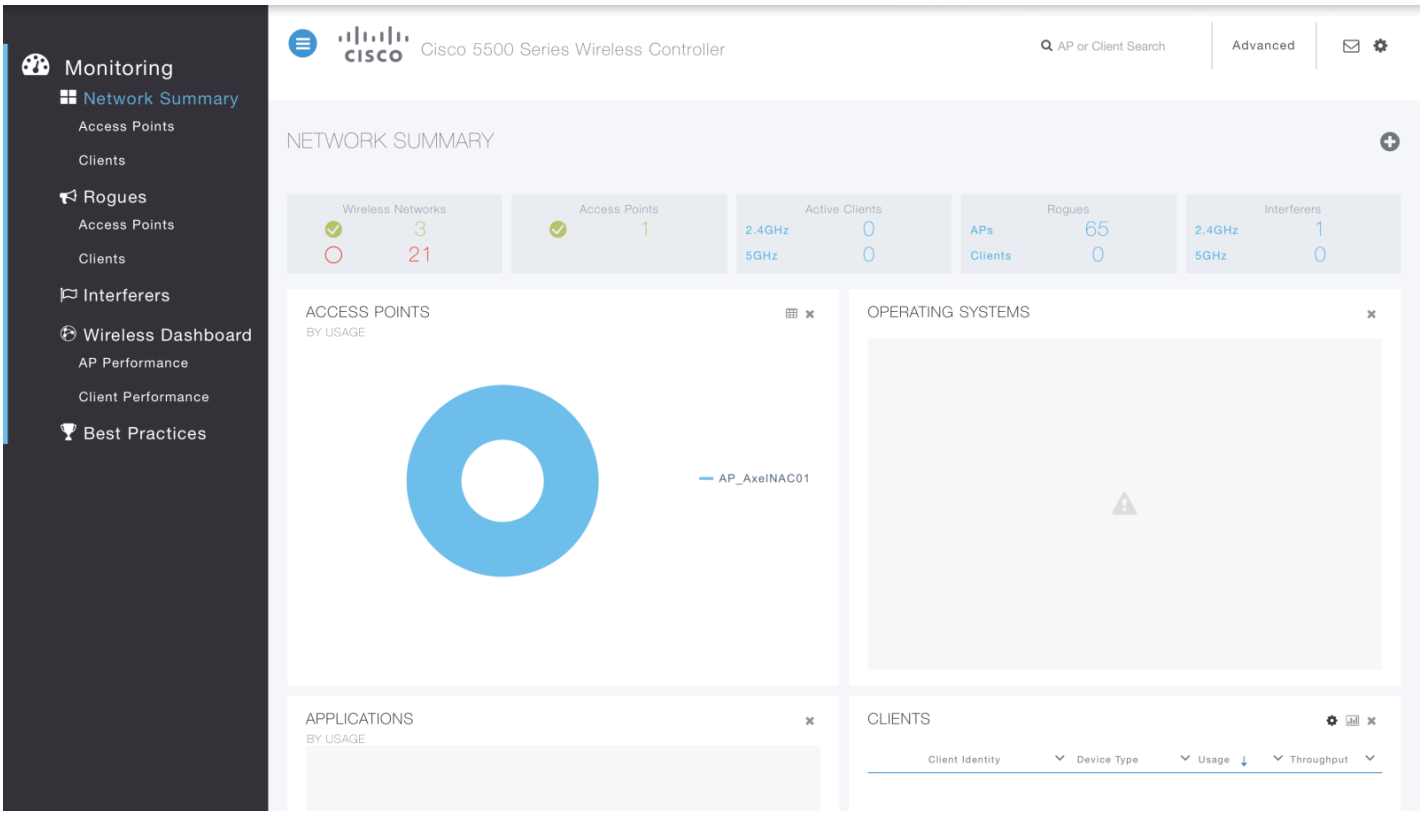
При интеграции WLC с AxelNAC, точку доступа можно настроить в одном из двух режимов:

- **Local Mode** — в таком режиме точка доступа строит CAPWAP-туннель до контроллера. В рамках этого режима весь трафик пользователей передается на контроллер, соответственно, интерфейс передачи необходимо настроить в режиме trunk со всеми пользовательскими VLAN (данный режим не поддерживается виртуальными WLC);
- **Flex Mode** — в таком режиме точка доступа отдает весь клиентский трафик коммутатору, к которому она подключена. Соответственно, интерфейс приема необходимо настроить в режиме trunk со всеми пользовательскими VLAN (данный режим поддерживается всеми типами контроллеров Cisco).

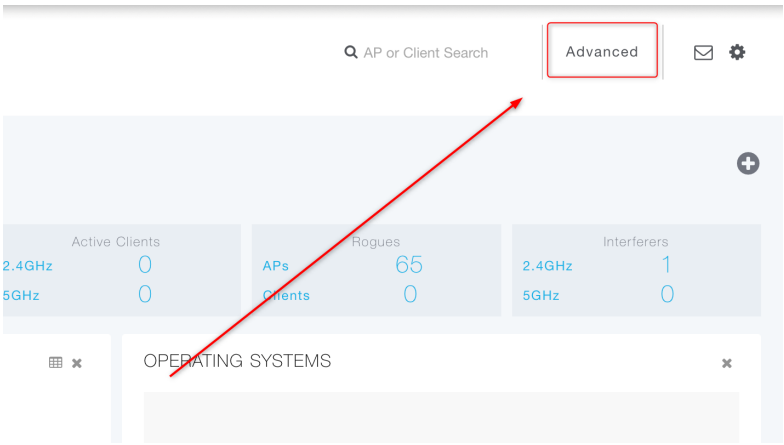
Настройка Cisco WLC

Настройка управляющего интерфейса

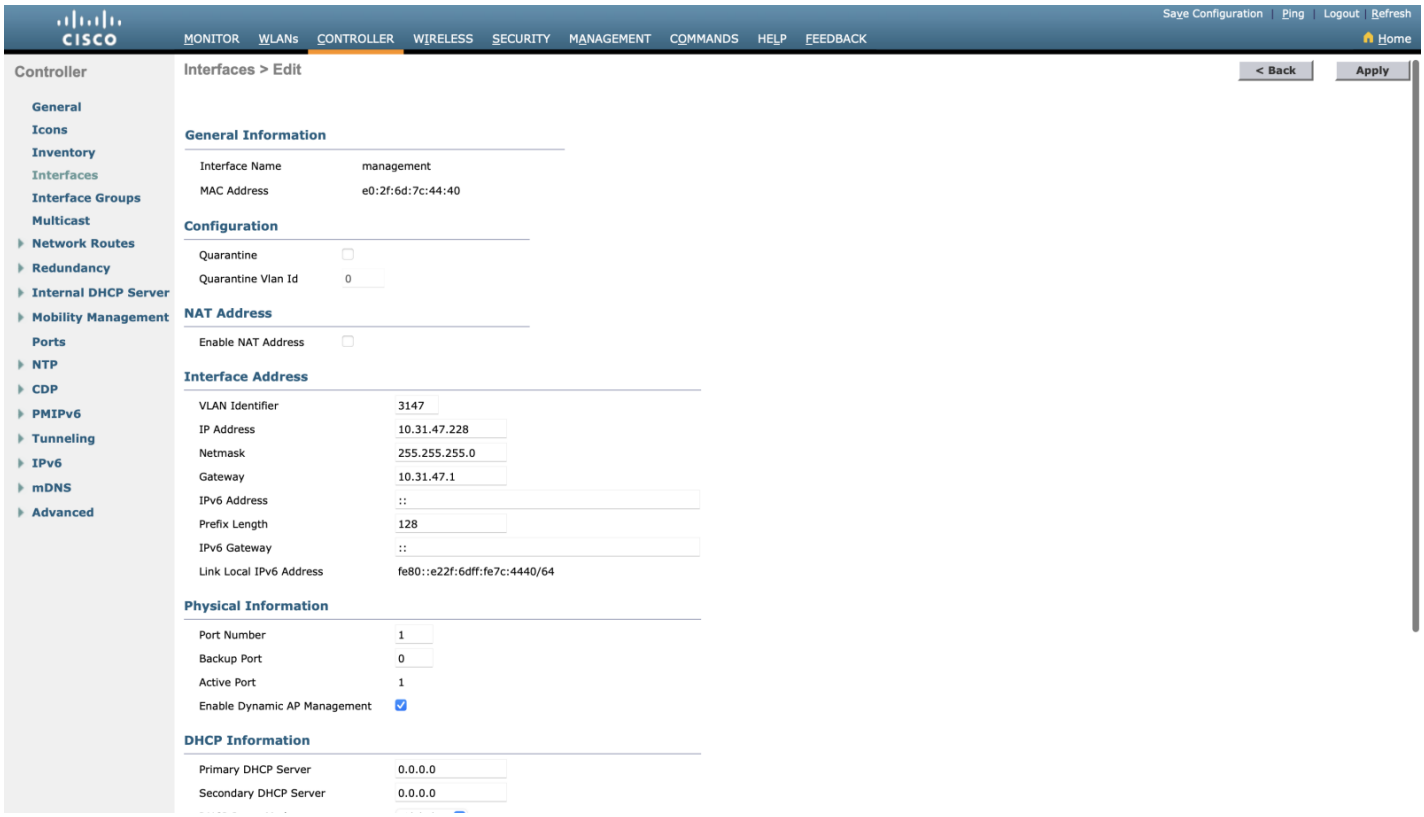
При первом подключении к контроллеру откроется страница с общей информацией и мониторингом:



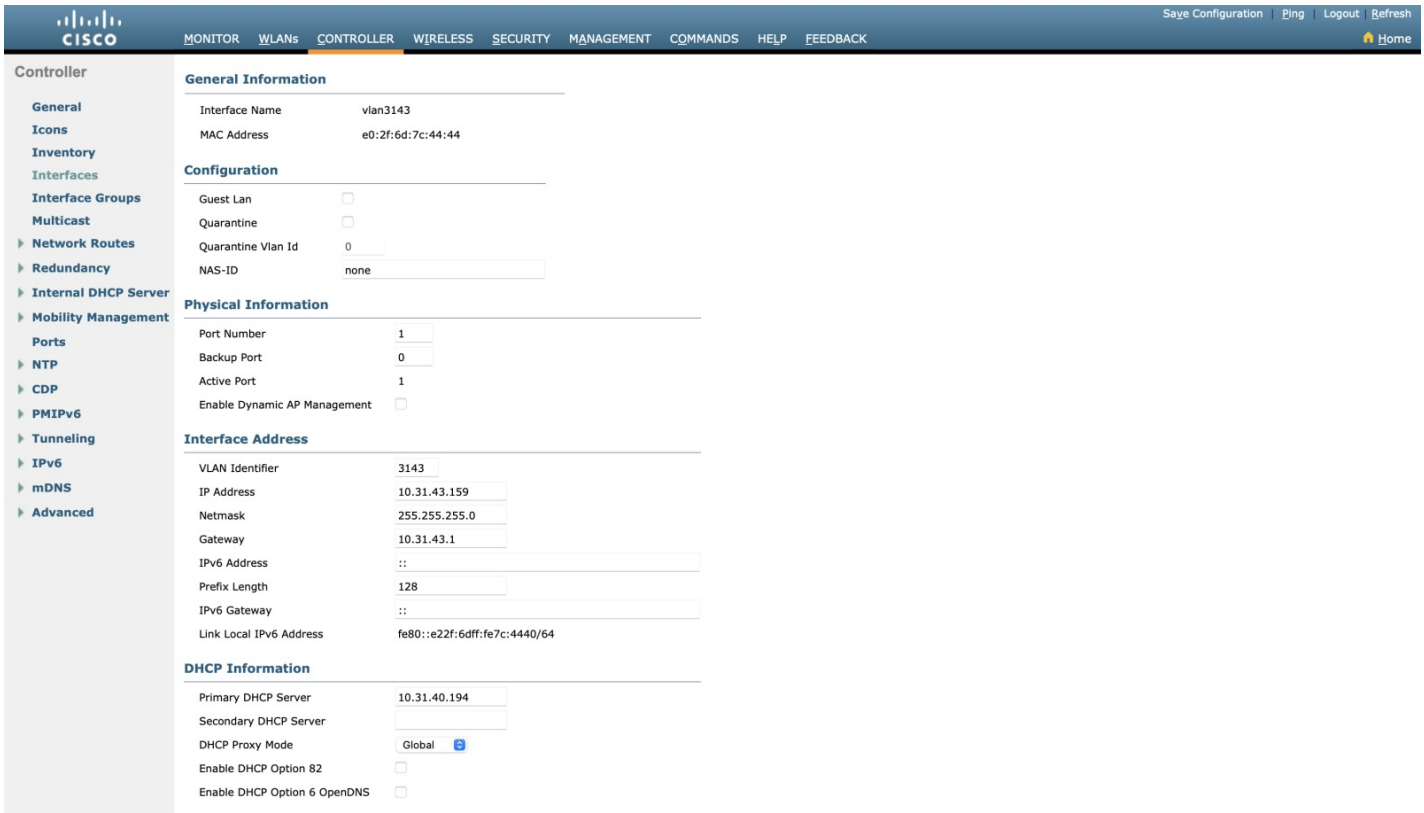
Шаг 1. Нажмите на кнопку **«Advanced»** в правом верхнем углу окна, чтобы перейти в режим **«Advanced»**.



Шаг 2. Перейдите в раздел **Controller → Interfaces** и настройте управляющий интерфейс как показано на скриншоте:



Шаг 3. В случае, если точки доступа планируется настраивать в **Local mode**, настройте виртуальный интерфейс с VLAN, в котором будут находиться конечные пользователи.

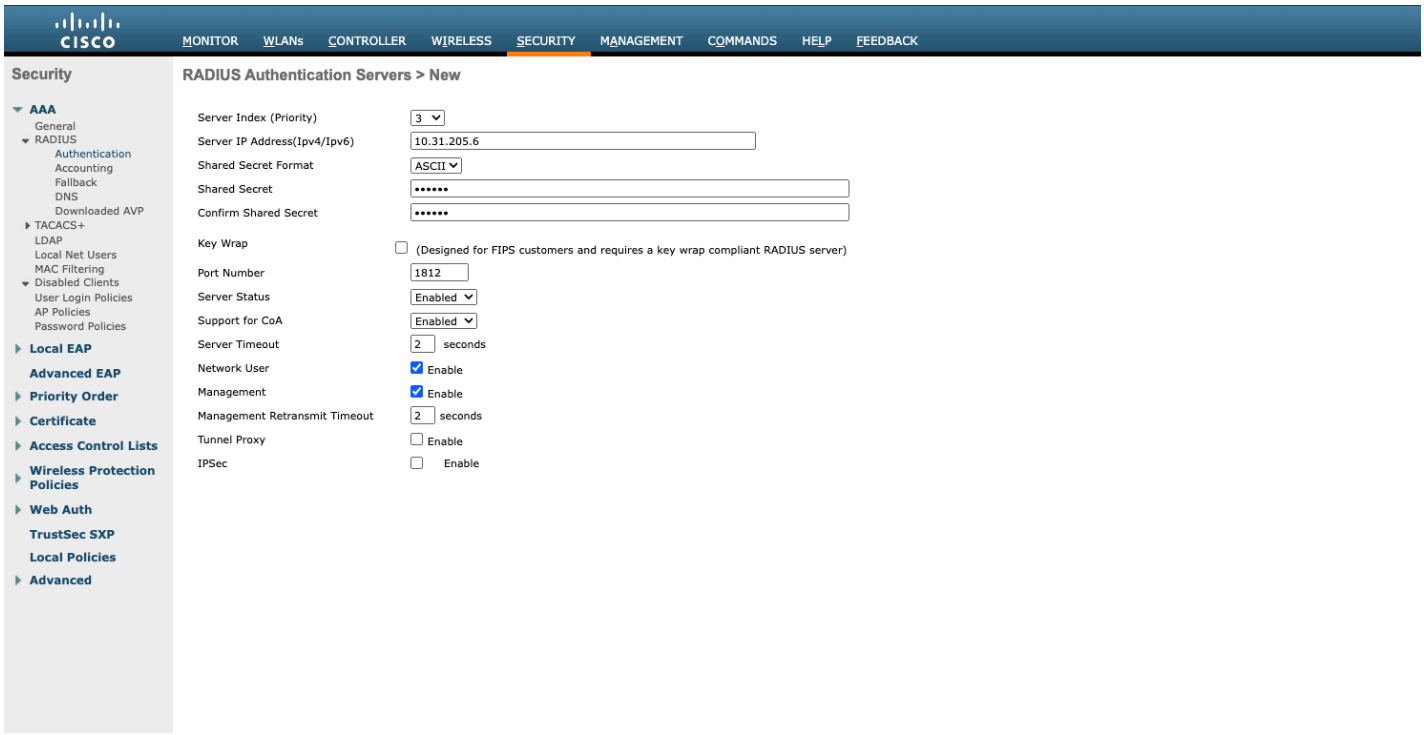


Для отправки IP helper в сторону AxelNAC на интерфейсе необходимо выделить один IP-адрес из подсети.

Настройка WLAN для аутентификации 802.1x.

Для работы аутентификаии 802.1x необходимо указать AxelNAC в качестве RADIUS-сервера для аутентификации и аудита:

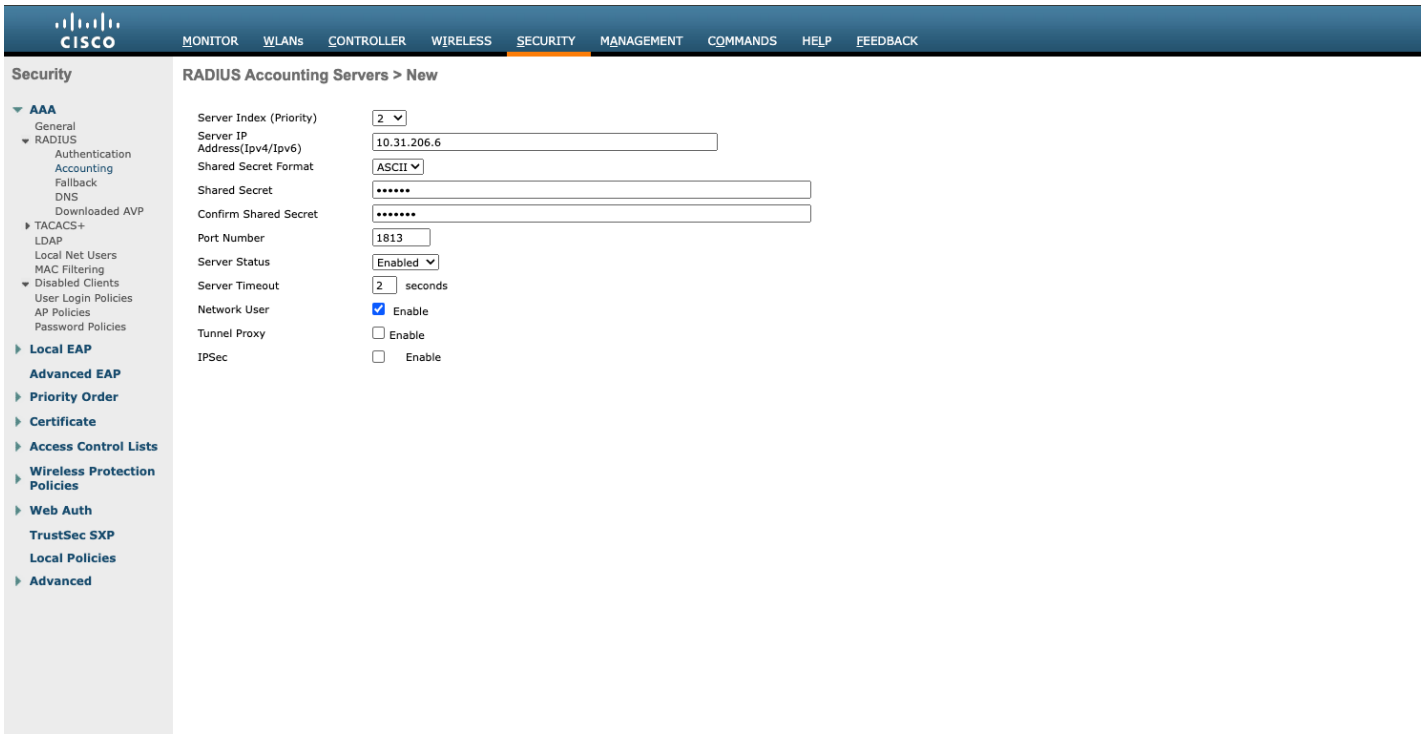
Шаг 1. Перейдите в раздел **Security → AAA → RADIUS → Authentication** и нажмите **New**.



Шаг 2. Укажите AxelNAC в качестве RADIUS-сервера (если вы используете кластер AxelNAC добавьте VIP).

Шаг 3. Укажите ключ доступа в поле **Shared Secret**, а также установите флажок для параметра Support for CoA.

Шаг 4. Перейдите в раздел **Security → AAA → RADIUS → Accounting** и нажмите **New**.



Шаг 5. Укажите AxelNAC в качестве RADIUS-сервера (если вы используете кластер AxelNAC добавьте VIP).

Шаг 6. Укажите ключ доступа в поле **Shared Secret**.

Добавление точек доступа

После настройки сетевых интерфейсов можно приступать к добавлению точек доступа к контроллеру. В нашем примере будет настроена точка доступа AIR-CAP2602I-R-K9. Для этого необходимо подключиться к точке доступа через консольный порт RJ-45 и выполнить следующие команды.

Если в вашей сети настроен DHCP — точка доступа запросит IP-адрес, станет видимой в сети и сможет получить настройки с WLC.

en
capwap ap controller <controller-management-ip-address>

Если в вашей сети не настроен или отсутствует DHCP, необходимо выполнить следующие команды:

capwap ap ip address «ip-address-AP/mask»

capwap ap ip default-gateway «ip-address»

capwap ap controller <controller-management-ip-address>

После этого, точка доступа станет видимой в сети и сможет получить настройки с WLC. Если этого не произошло, посмотрите отладочные логи на точке доступа. Проблема с DTLS решается выполнением на контроллере команд:

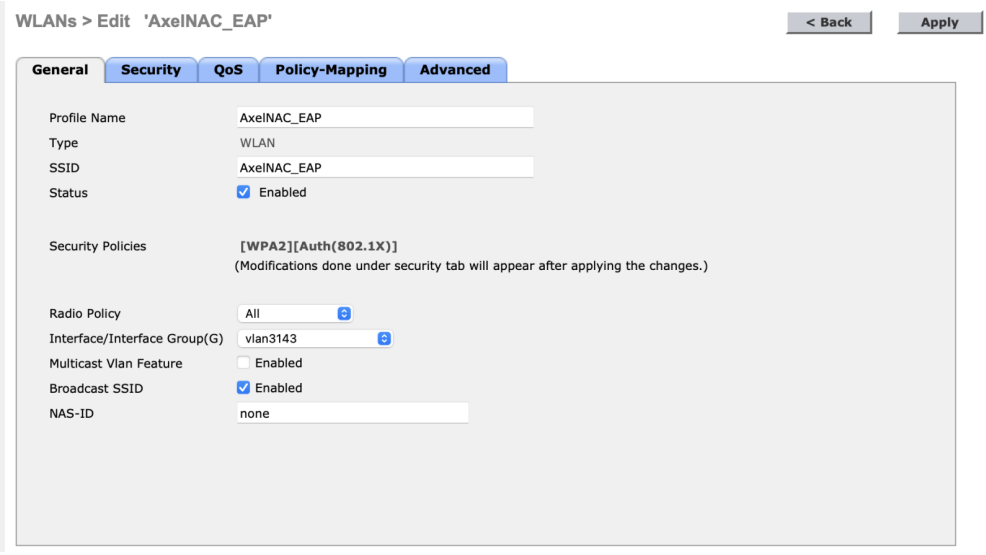
config ap cert-expiry-ignore mic enable
config ap cert-expiry-ignore ssc enable

Настройка WLAN 802.1x

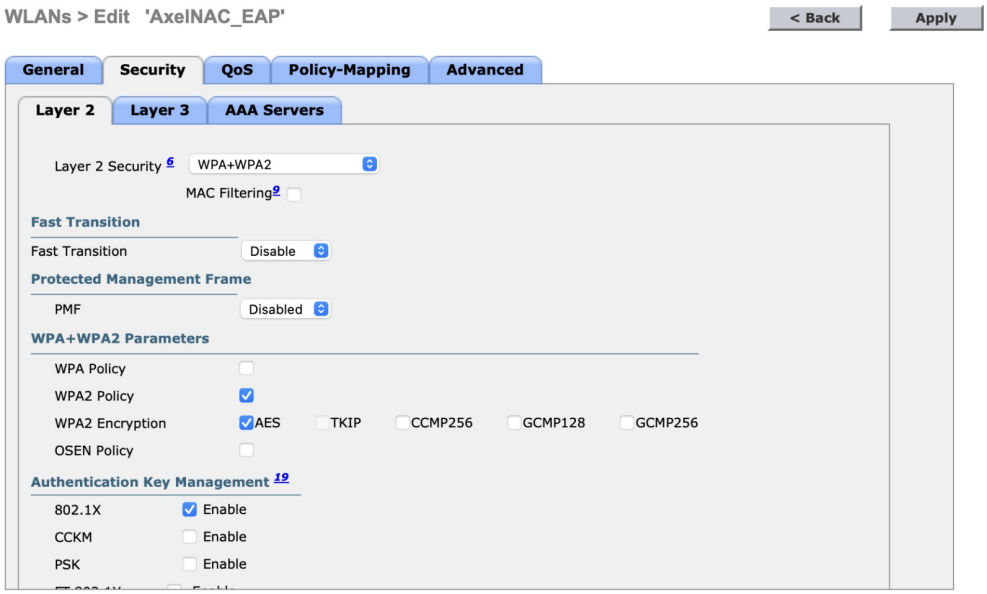
Для настройки WLAN 802.1x выполните следующие действия:

Шаг 1. Перейдите в раздел **WLANs** и создайте новый профиль, нажав **New**, либо отредактируйте существующий профиль, нажав **Edit**.

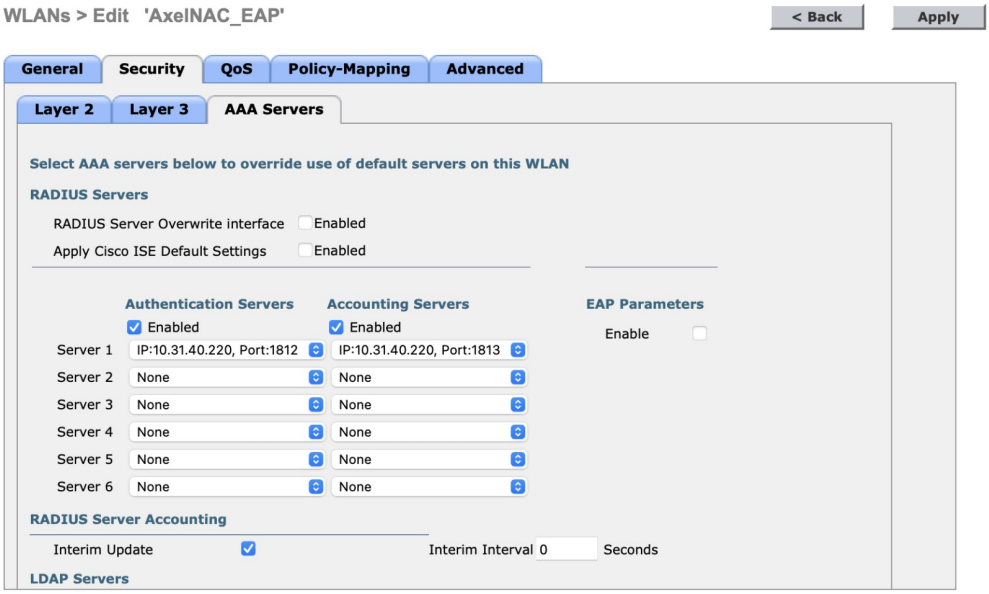
Шаг 2. Выполните основные настройки профиля беспроводного подключения на вкладке **General**, как показано на скриншоте:



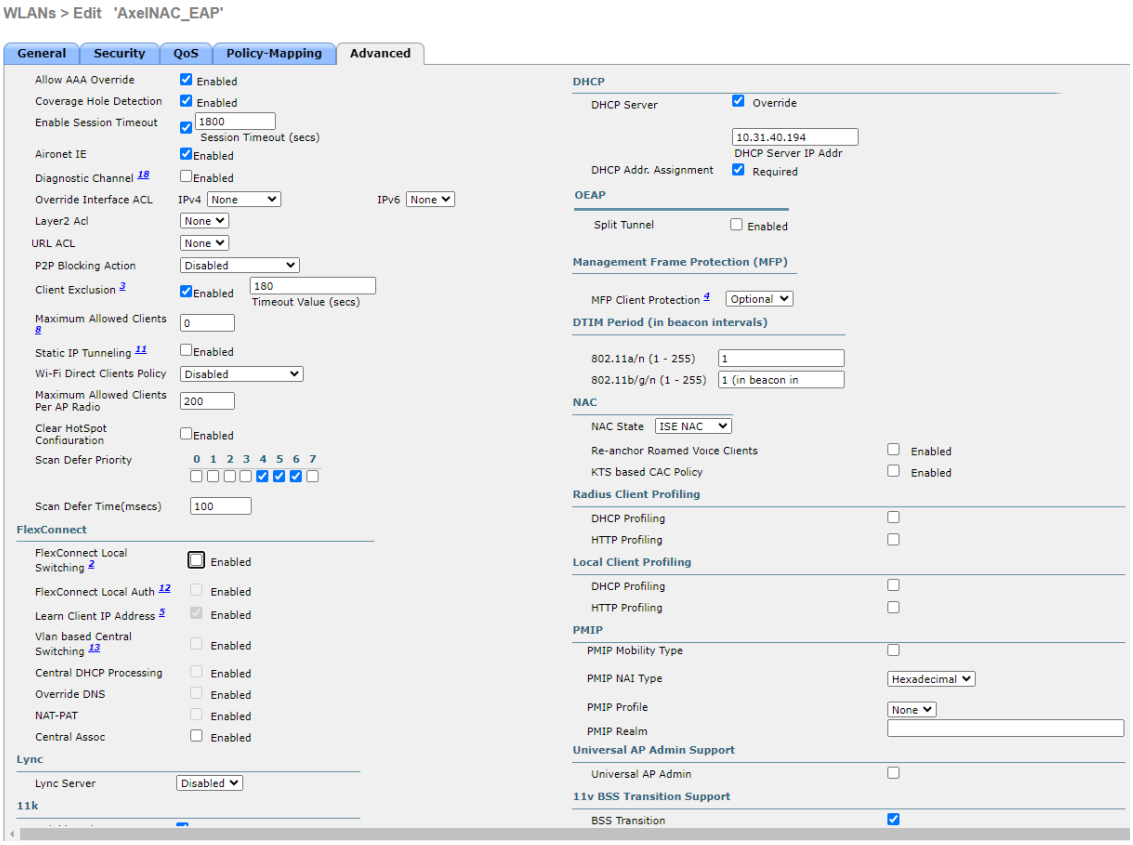
Шаг 3. Перейдите на вкладку **Security → Layer 2** и выполните настройку, как показано на скриншоте:



Шаг 4. На вкладке **Security → AAA Servers** укажите адреса аутентификации и аккаунтинга:



Шаг 5. Перейдите на вкладку **Advanced** и выполните настройку как показано на скриншоте:



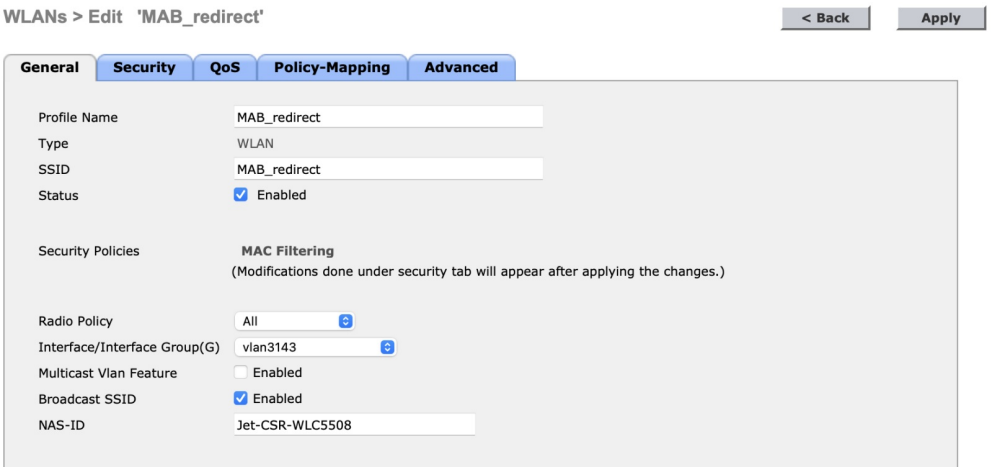
При настройке точек доступа в режиме **Flex Mode**, необходимо также задать значение в поле **FlexConnect Local Switching**.

Настройка Captive-портала

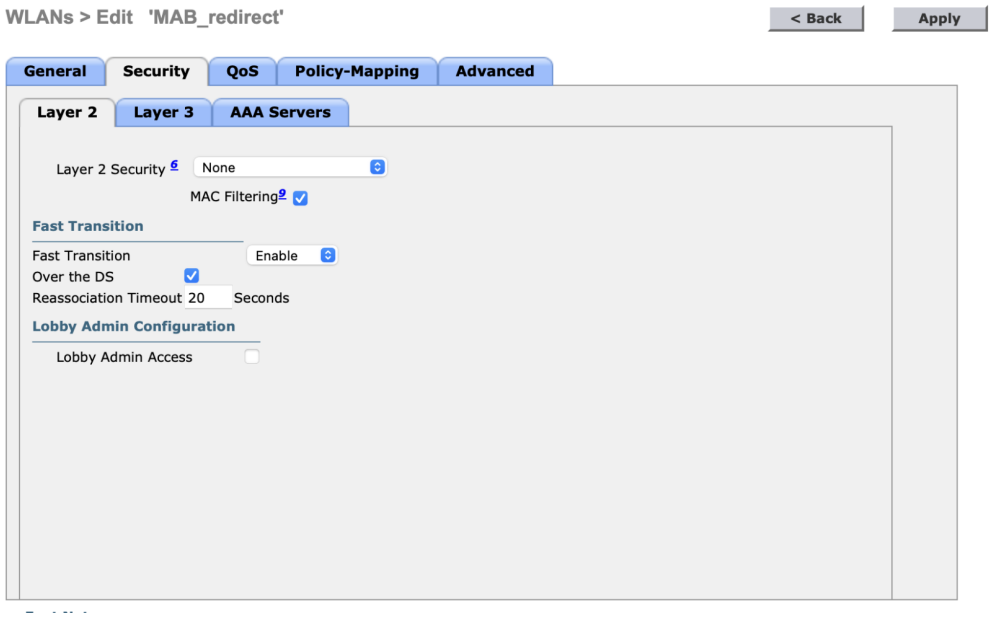
Для настройки Captive-портала выполните следующие действия:

Шаг 1. Перейдите в раздел **WLANs** и создайте новый профиль, нажав **New**, либо отредактируйте существующий профиль, нажав **Edit**.

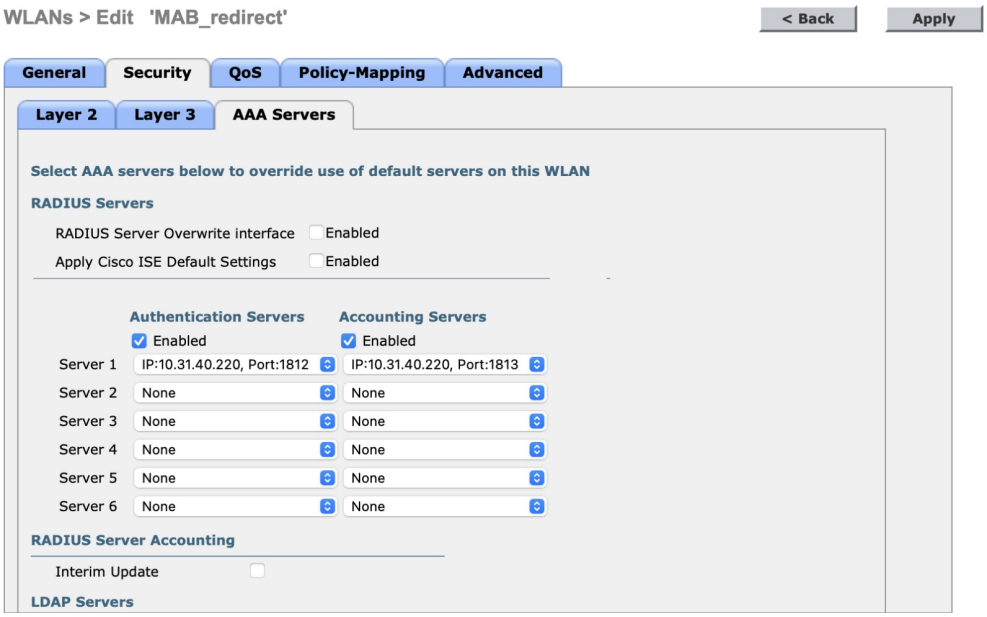
Шаг 2. Выполните основные настройки профиля беспроводного подключения на вкладке **General**, как показано на скриншоте:



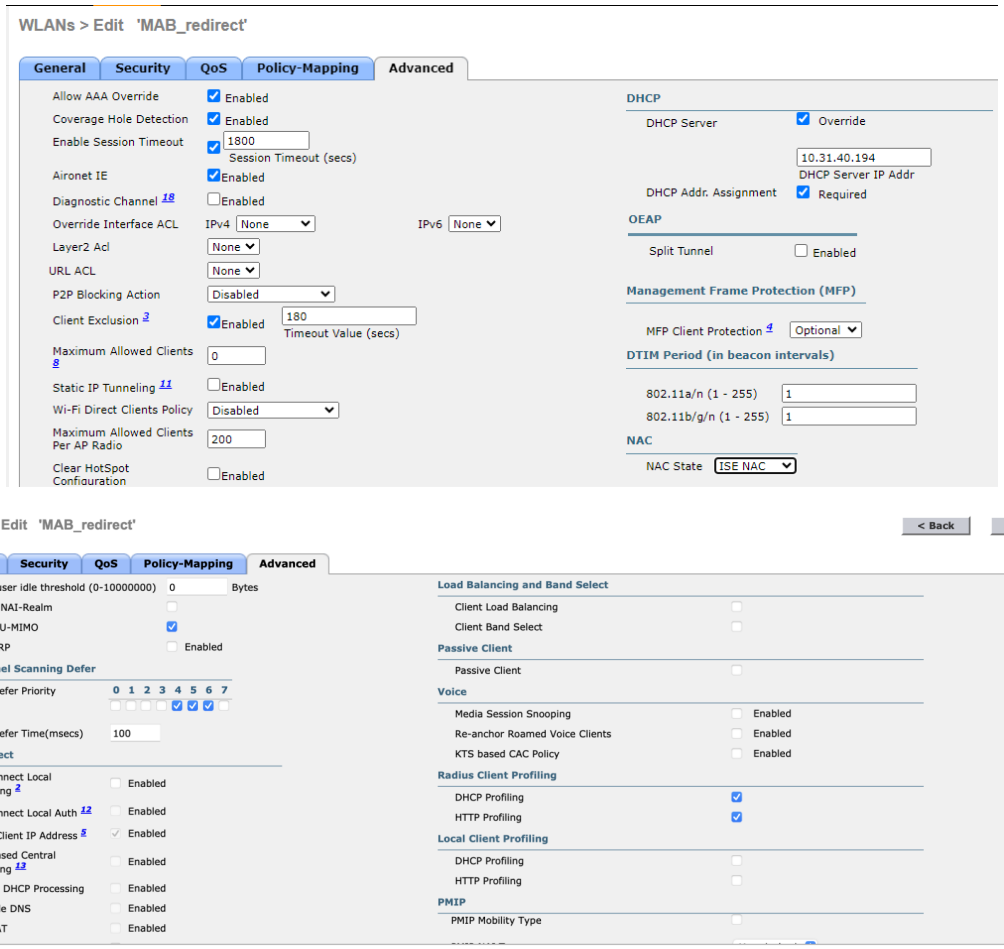
Шаг 3. Перейдите на вкладку **Security → Layer 2** и выполните настройку, как показано на скриншоте:



Шаг 4. На вкладке **Security → AAA Servers** укажите адреса аутентификации и аккаунтинга:



Шаг 5. Перейдите на вкладку **Advanced** и выполните настройку как показано на скриншотах ниже:



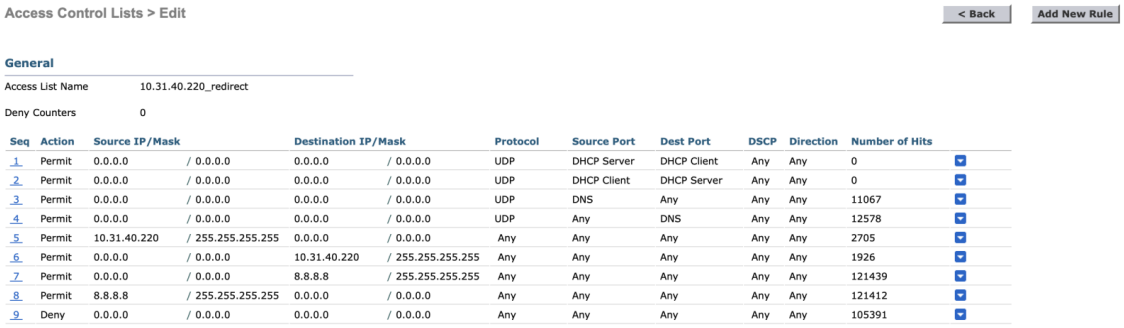
При настройке точек доступа в режиме **Flex Mode**, необходимо также задать значение в поле **FlexConnect Local Switching**.

Создание ACL-redirect для режима Local Mode

Для создания ACL-redirect для режима Local Mode выполните следующие действия:

Шаг 1. Перейдите в раздел **Security → Access Control Lists** и нажмите **Add New Rule**.

Шаг 2. Создайте правила, как показано на скриншоте ниже (в примере IP-адрес AxelNAC — 10.31.40.220):



Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	UDP	DHCP Server	DHCP Client	Any	Any	0
2	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	UDP	DHCP Client	DHCP Server	Any	Any	0
3	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	UDP	DNS	Any	Any	Any	11067
4	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	UDP	Any	DNS	Any	Any	12578
5	Permit	10.31.40.220	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any	Any	Any	2705
6	Permit	0.0.0.0	/ 0.0.0.0	10.31.40.220	/ 255.255.255.255	Any	Any	Any	Any	Any	1926
7	Permit	0.0.0.0	/ 0.0.0.0	8.8.8.8	/ 255.255.255.255	Any	Any	Any	Any	Any	121439
8	Permit	8.8.8.8	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any	Any	Any	121412
9	Deny	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any	Any	Any	105391

Создание ACL-redirect для режима Flex Mode

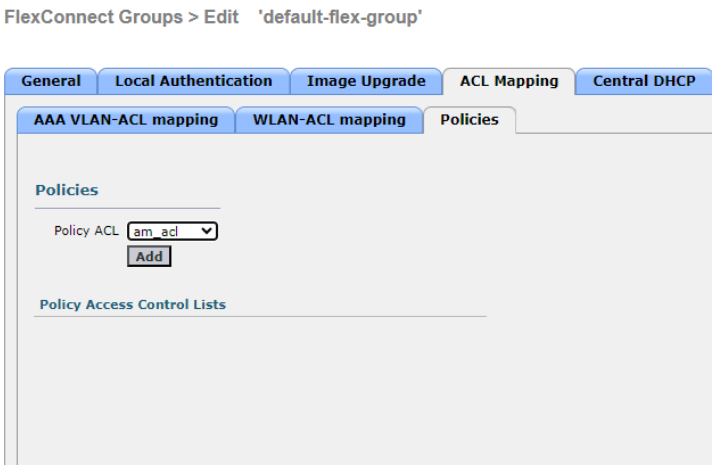
Для создания ACL-redirect для режима Flex Mode выполните следующие действия:

Шаг 1. Перейдите в раздел **Wireless → FlexConnect Groups → FlexConnect ACLs** и нажмите **Add New Rule**.

Шаг 2. Создайте правила аналогично режиму Local Mode.

Шаг 3. Перейдите в раздел **Wireless → FlexConnect Groups** и нажмите **Edit**, чтобы попасть в окно редактирования группы.

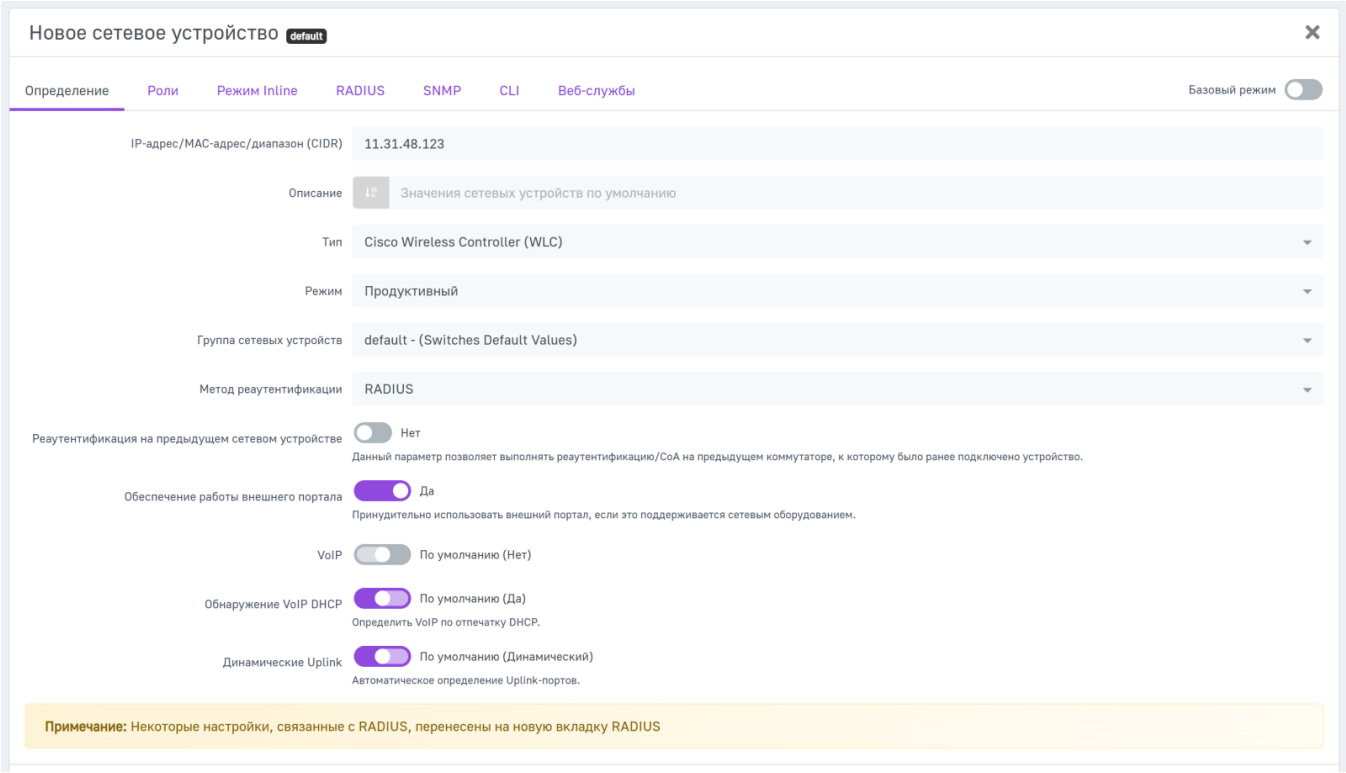
Шаг 4. На вкладке **ACL Mapping → Policies** назначьте ACL группе точек доступа.



Интеграция WLC с AxelNAC

После того как Cisco WLC настроен, необходимо настроить его профиль для AxelNAC.

Шаг 1. Перейдите во вкладку **Конфигурация → Политика и контроль доступа → Сетевые устройства** , нажмите на кнопку **Новое сетевое устройство** и в выпадающем списке выберите к какой группе должно принадлежать устройство (по умолчанию создана группа **default**).



Шаг 2. Укажите IP-адрес контролера (вы можете указать IP-адрес/MAC-адрес/IP-netmask).

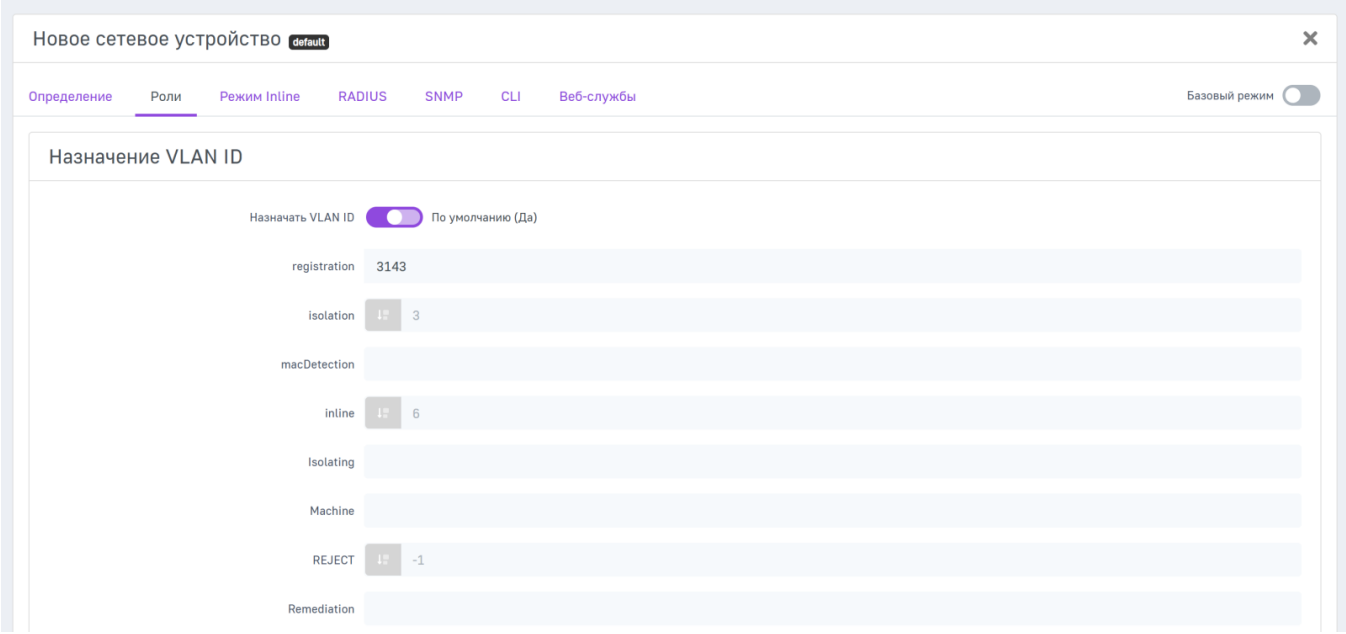
Шаг 3. Укажите тип устройства — в данном примере **Cisco Wireless Controller (WLC)**.

Шаг 4. В поле **Метод реаутентификации** из выпадающего списка выберите значение **RADIUS**.

Шаг 5. Активируйте переключатель **Обеспечение работы внешнего портала**.

Шаг 6. Переключитесь на вкладку **Роли**.

Шаг 7. Настройте VLAN который был создан и добавлен как VLAN для пользователей в WLAN WLC. В примере будет использоваться роль **registration**.



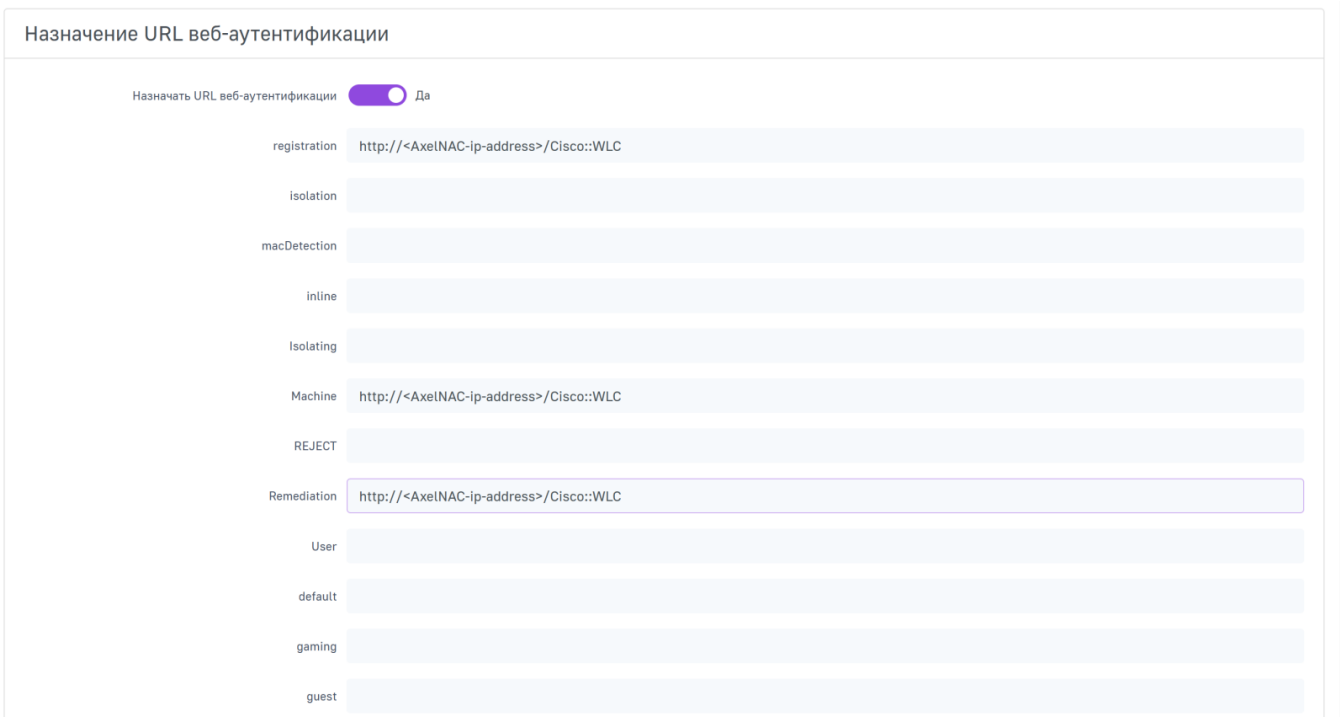
Теперь при подключении пользователя в Роли **registration** через этот контроллер поместит его в VLAN 3143.

Шаг 8. Активируйте переключатель **Назначать Local ACL** — данный функционал отвечает за отправку ACL или redirect-ACL.

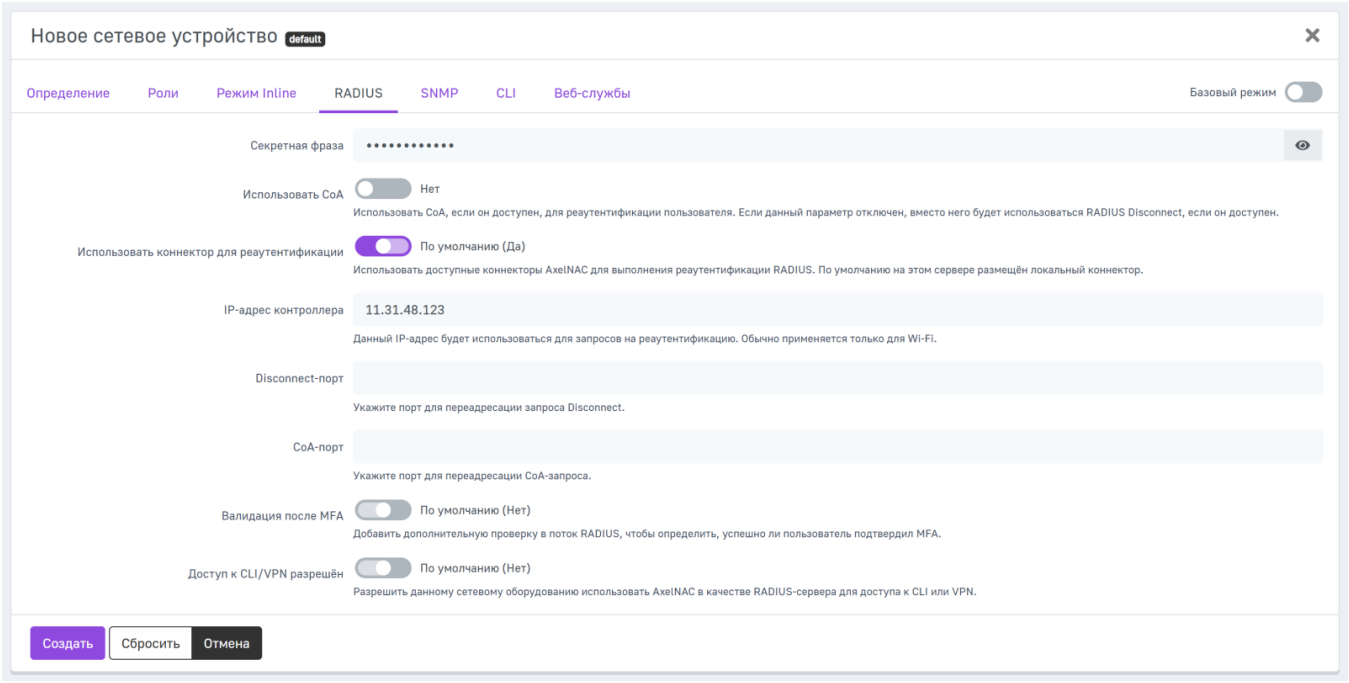
Шаг 9. Укажите для роли **registration** созданный ранее на контроллере ACL — "10.31.40.220_redirect". Теперь при подключении пользователя в роли **registration** через этот контроллер на него применится ACL "10.31.40.220_redirect".

Шаг 10. Активируйте переключатель **Назначать URL веб-аутентификации**. Это необходимо для того, чтобы ACL применялся как redirect-ACL.

Шаг 11. Укажите для роли **registration** значение "http://<AxelNAC-ip-address>/Cisco::WLC", уникальная ссылка будет генерироваться автоматически. Если вы хотите перенаправлять пользователей на HTTPS-портал, просто укажите значение "https://<AxelNAC-ip-address>/Cisco::WLC".



Шаг 12. Перейдите на вкладку **RADIUS**.



Шаг 13. Укажите секретную фразу, которую вы создали на контроллере.

Шаг 14. Установите переключатель **Использовать CoA** в положение **Нет**.

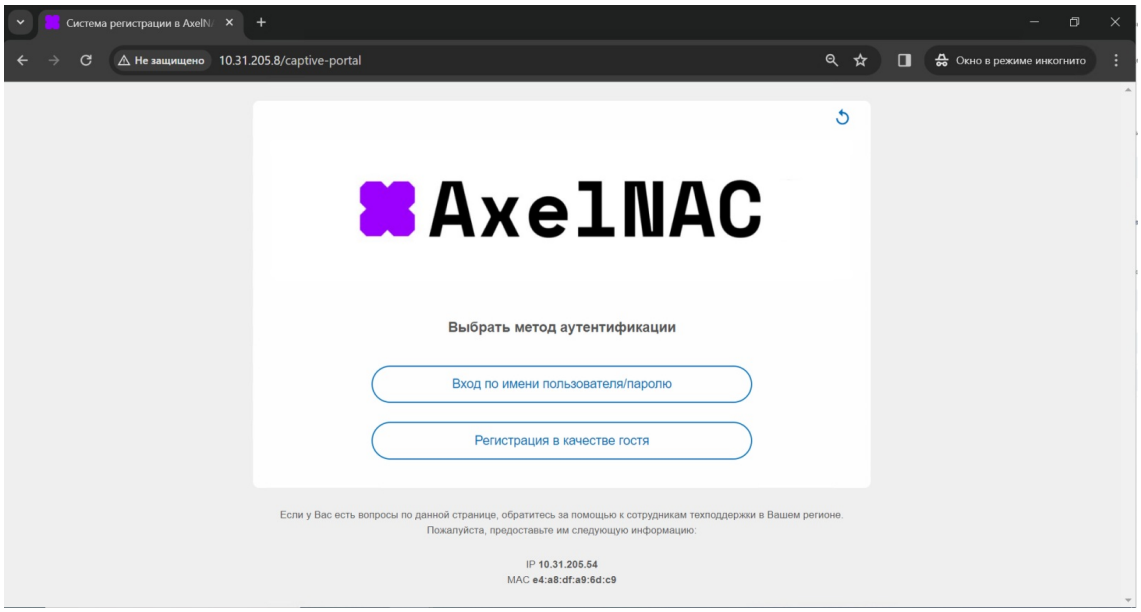
Шаг 15. Активируйте переключатель **Использовать коннектор для реаутентификации**.

Шаг 16. Укажите IP-адрес контроллера в поле **IP-адрес контроллера** как на примере.

Шаг 17. В поле **Disconnect-порт** укажите значение **1700**, и нажмите **Создать** в левом нижнем углу окна.

После этого профиль для сетевого оборудования считается настроенным. Теперь при подключении пользователя через контроллер, если он будет попадать в роль **registration**, пользователь будет попадать в **VLAN 3143**, ему будет отправлен **redirect-ACL** и ссылка на **redirect**.

Настройка Captive-портал в AxelNAC



Для того чтобы настроить работу Captive-портал в AxelNAC, выполните следующие шаги:

Шаг 1. Перейдите в раздел **Конфигурация → Сетевое взаимодействие → Интерфейсы** и выберите интерфейс на котором необходимо включить функционал Captive-портал.

Шаг 2. В строке **Дополнительный демон (демоны) прослушивания** добавьте значение **портал** из выпадающего списка, затем нажмите **Сохранить**.

Шаг 3. Перейдите в раздел **Статус → Службы** и перезапустите следующие службы:

- haproxy-portal;
- httpd.portal;
- iptables.

Последнее обновление: 28 окт., 2025
Обновлено от: Ильина В.
Ревизия: 7

https://docs.axel.pro/entry/649/