

Интеграция AxelNAC с контроллерами беспроводного доступа Ubiquiti Unifi

В данной статье рассматривается процесс интеграции AxelNAC с контроллером беспроводного доступа Ubiquiti Unifi версии 6.5.55.

Веб-интерфейс других версий Ubiquiti Unifi 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:

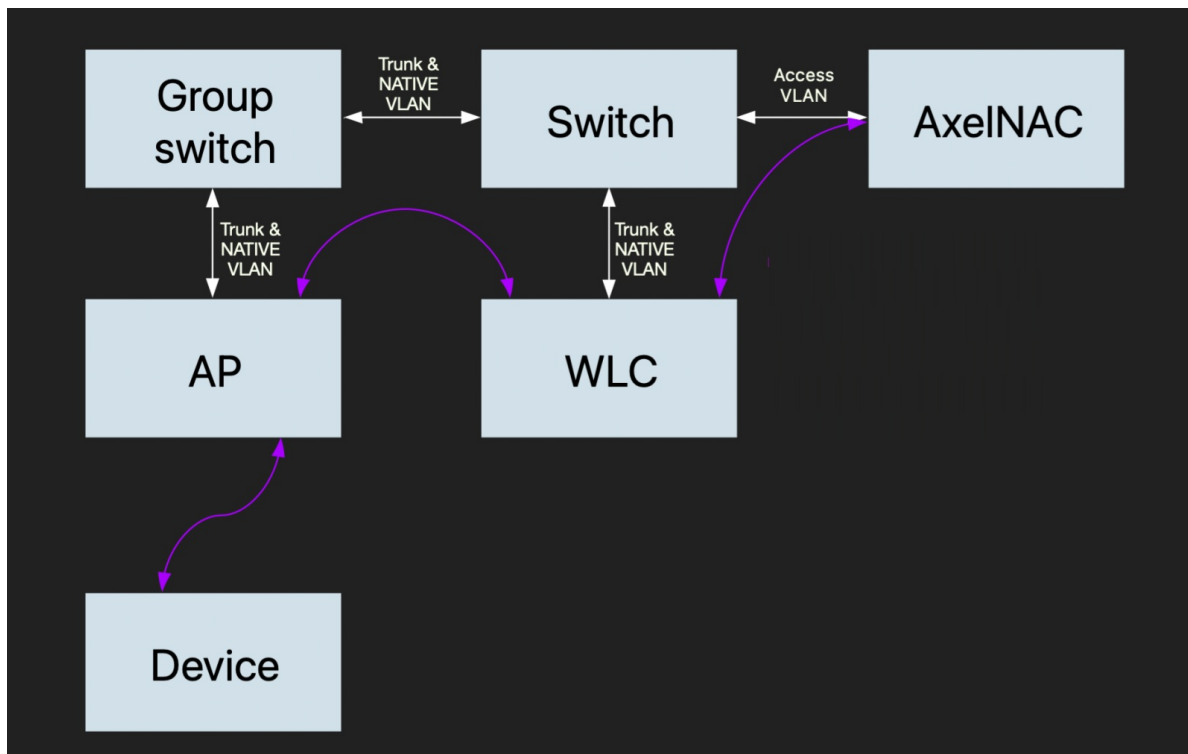


Рисунок 1 — Концептуальная схема соединения сетевого оборудования

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, APM с беспроводным интерфейсом.

При интеграции WLC с AxelNAC, точка доступа может работать в одном из двух режимов:

- **Local Mode** — в таком режиме точка доступа строит CAPWAP-туннель до контроллера, весь трафик пользователей передается на контроллер;
- **Flex Mode** — в таком режиме точка доступа отдает весь клиентский трафик коммутатору, к которому она подключена.

При использовании функционала Captive-портал, точка доступа перенаправляет запросы на контроллер, т.е. работает в режиме Local Mode. В остальных случаях точка доступа будет работать в режиме FlexConnect.

Настройка Ubiquiti Unifi

Настройка управляющего интерфейса

Для первичной настройки контроллера необходимо выполнить следующие шаги:

Шаг 1. Установите программное обеспечение **Unifi Controller Software**, настройте его через мастер настройки, после чего подключитесь к WEB-интерфейсу на порт 8443.

Шаг 2. Перейдите в раздел **Settings** → **Site**. Прокрутите страницу вниз и в блоке **Device authentication** установите флажок для параметра **Enable SSH authentication**.

Шаг 3. В полях **Username** и **Password** укажите учетные данные для подключения к точкам доступа по протоколу SSH. После этого нажмите **APPLY CHANGES** для сохранения настроек.

Шаг 4. Перейдите в раздел **Settings → Profiles** и создайте новый профиль RADIUS, нажав **CREATE NEW RADIUS PROFILE**, либо отредактируйте существующий профиль, нажав **EDIT**.

Шаг 5. Выполните настройку следующим образом:

- **Profile Name** — укажите имя профиля (например, AxelNAC);
- **VLAN Support** — установите флажок для параметра Enable RADIUS assigned VLAN for wireless network (данный параметр разрешает работу RADIUS-сервера для беспроводных соединений);
- **RADIUS Auth Server** — укажите IP-адрес, порт и секретный ключ для RADIUS-сервера аутентификации;
- **Accounting** — установите флажок для параметра Enable accounting (данный параметр включает аккаунтинг);
- **Interim Update** — установите флажок для параметра Enable Interim Update (данный параметр отвечает за необходимость клиента переавторизовываться после определенного интервала времени);
- **Interim Update Interval** — укажите интервал времени для реавторизации клиента;
- **RADIUS Accounting Server** — укажите IP-адрес, порт и секретный ключ для RADIUS-сервера аккаунтинга.

Нажмите **SAVE**, чтобы применить изменения.

Настройка защищенного SSID

Для того чтобы настроить защищенный SSID, выполните следующие шаги:

Шаг 1. Перейдите в раздел **Settings → Wireless Networks** и создайте новый профиль беспроводного соединения, нажав **CREATE NEW WIRELESS NETWORK**, либо отредактируйте существующий профиль, нажав **EDIT**.

Шаг 2. Выполните настройку следующим образом:

- **Name/SSID** — Укажите имя профиля беспроводного соединения (например, AxelNAC-EAP);
- **Enabled** — установите флажок для параметра **Enable this wireless network** для того, чтобы профиль стал активным;
- **Security** — выберите значение WPA Enterprise;
- **RADIUS Profile** — укажите профиль RADIUS, который вы создали в предыдущем разделе;
- **WiFi Band** — выберите частоту работы Wi-Fi;
- **Broadcasting APs** — укажите группу точек доступа, для которых будет работать данный профиль;
- **Group Rekey Interval** — установите флажок для параметра **Enable GTK rekeying every**, чтобы активировать автоматическое обновление ключа шифрования данных на точках доступа. В поле справа укажите интервал обновления в секундах;
- **User Group** — укажите группу пользователей, для которых будет работать данный профиль;
- **RADIUS DAC/DAC (CoA)** — установите флажок для параметра **RADIUS DAC/DAC (CoA)**, чтобы активировать поддержку CoA.

Wireless Networks

EDIT WIRELESS NETWORK - AXELNAC-EAP

Name/SSID:

Enabled: Enable this wireless network

Security: Open WEP WPA Personal WPA Enterprise
 Hotspot 2 OSEN

WPA3: Support WPA3 connections

RADIUS Profile: [Create new RADIUS profile](#)

Hotspot 2.0: Enable Hotspot 2.0

Guest Policy: Apply guest policies (captive portal, guest authentication, access)

Network: RADIUS assigned VLAN

ADVANCED OPTIONS

WiFi Band: 2.4 Ghz 5 Ghz Both

Broadcasting APs

AP GROUP NAME	APS	
<input checked="" type="checkbox"/> All APs	1	VIEW

[Create New AP Group](#)

Multicast and Broadcast Filtering: Block LAN to WLAN Multicast and Broadcast Data

Fast Roaming: Enable fast roaming

Hide SSID: Prevent this SSID from being broadcast

Group Rekey Interval: Enable GTK rekeying every seconds

User Group:

Нажмите **SAVE**, чтобы применить изменения.

Настройка открытого SSID с поддержкой WEB-аутентификации

Для того чтобы настроить открытый SSID с поддержкой WEB-аутентификации, выполните следующие шаги:

Шаг 1. Перейдите в раздел **Settings** → **Guest Control**.

Шаг 2. Выполните настройку следующим образом:

- **Guest Portal** — установите флажок для параметра **Enable Guest Portal**, для того чтобы активировать поддержку гостевого портала;
- **Authentication** — выберите параметр External portal server, для перенаправления пользователей на гостевой портал AxelNAC;
- **Custom Portal** — кажите IP-адрес гостевого портала, на который будет происходить переадресация;
- **Pre-authorization Access** — укажите VIP адрес AxelNAC.

Guest Control

GUEST POLICIES

Guest Portal: Enable Guest Portal NETWORK APPLICATION MUST BE ONLINE.

Authentication: No authentication Hotspot Facebook WiFi External portal server

Custom Portal: IPv4 Address:

Redirection: Use Secure Portal
 Redirect using hostname:
 Enable HTTPS Redirection

ACCESS CONTROL

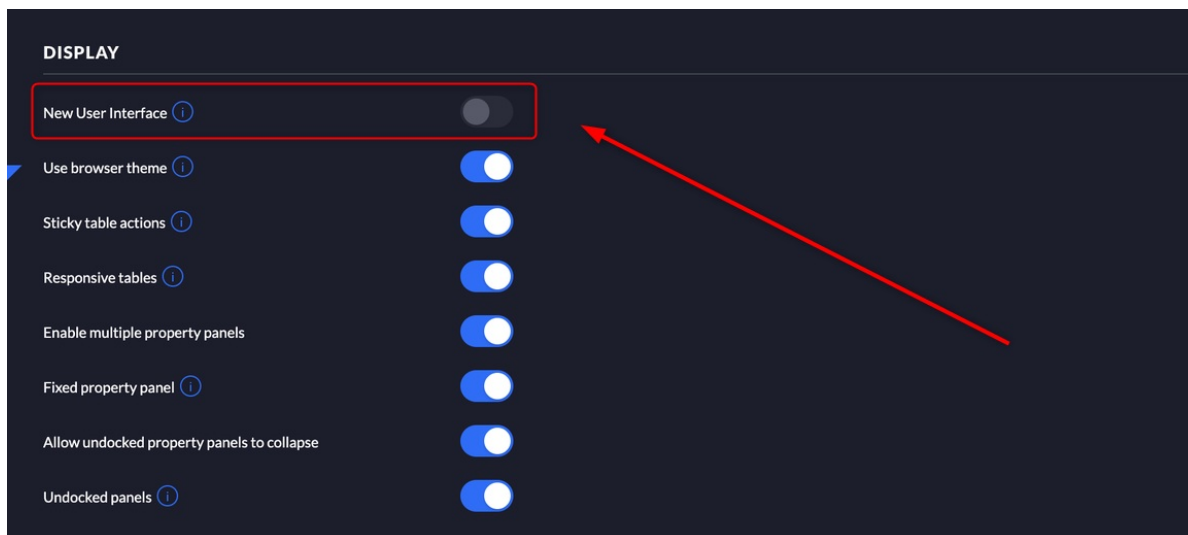
Pre-authorization Access: [+](#) ADD IPV4 HOSTNAME OR SUBNET

Post-authorization Restrictions: [+](#) ADD IPV4 HOSTNAME OR SUBNET

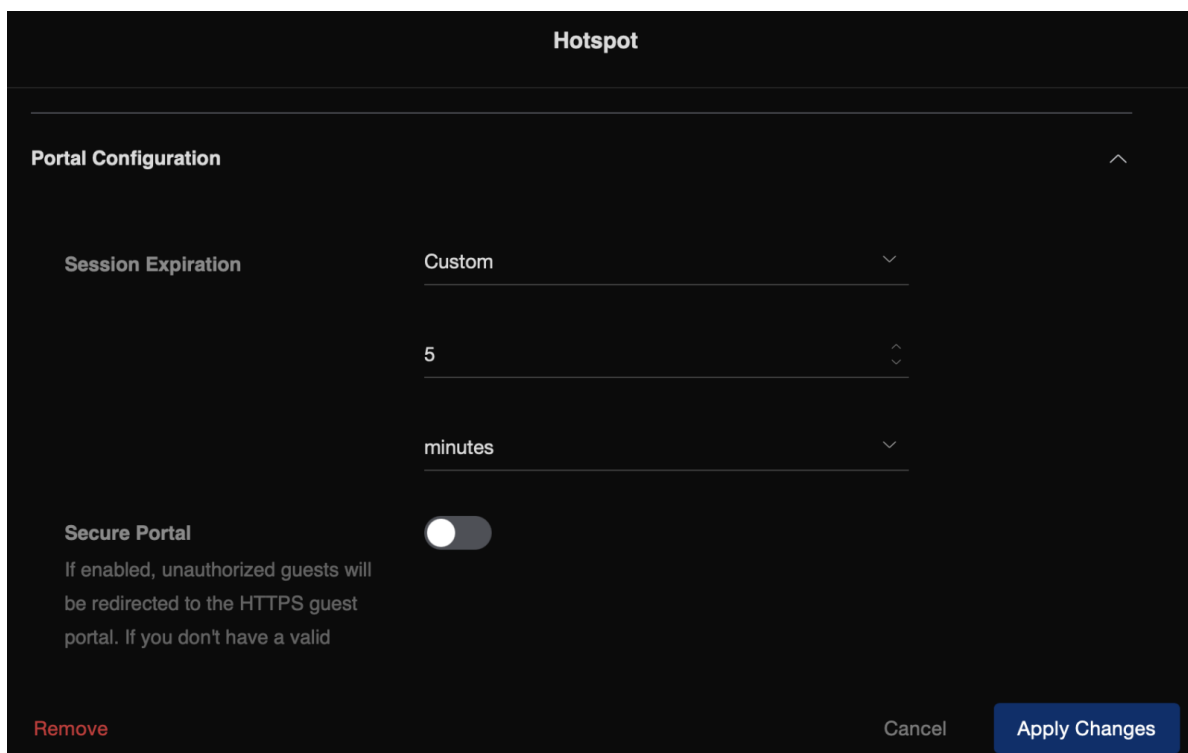
[APPLY CHANGES](#) [RESET](#)

Нажмите **APPLY CHANGES**, чтобы применить настройки.

Шаг 3. Перейдите в раздел **Settings → User Interface** и переключитесь на новый пользовательский интерфейс, активировав параметр **New User Interface**. После этого нажмите **APPLY CHANGES**, чтобы применить настройки.



Шаг 4. Перейдите в раздел **Guest Hotspot → Portal configuration** установите время истечения пользовательской сессии. После этого нажмите **APPLY CHANGES**, чтобы применить настройки.



Шаг 5. Вернитесь в старый пользовательский интерфейс и перейдите в раздел **Settings → Wireless Networks**, затем создайте новый профиль беспроводного соединения, нажав **CREATE NEW WIRELESS NETWORK**, либо отредактируйте существующий профиль, нажав **EDIT**.

Шаг 6. Выполните настройку следующим образом:

- **Name/SSID** — Укажите имя профиля беспроводного соединения (например, Axel-portal);
- **Enabled** — установите флажок для параметра **Enable this wireless network** для того, чтобы профиль стал активным;
- **Security** — выберите значение Open;
- **Guest Policy** — установите флажок для параметра **Apply guest policies (Captive-портал, guest authentication, access)**, чтобы активировать поддержку гостевого доступа;
- **WiFi Band** — выберите частоту работы Wi-Fi;
- **Broadcasting APs** — укажите группу точек доступа, для которых будет работать данный профиль;
- **User Group** — укажите группу пользователей, для которых будет работать данный профиль;
- **RADIUS DAC/DAC (CoA)** — установите флажок для параметра **RADIUS DAC/DAC (CoA)**, чтобы активировать поддержку CoA.

Wireless Networks

EDIT WIRELESS NETWORK - AXEL-PORTAL

Name/SSID: Axel-portal

Enabled: Enable this wireless network

Security: Open WEP WPA Personal WPA Enterprise
 Hotspot 2 OSEN

Guest Policy: Apply guest policies (captive portal, guest authentication, access)

Network: RADIUS assigned VLAN ⓘ

ADVANCED OPTIONS ▾

WiFi Band: 2.4 Ghz 5 Ghz Both

Broadcasting APs

AP GROUP NAME ↑	APS	
<input checked="" type="checkbox"/> All APs	1	VIEW

[Create New AP Group](#)

Multicast and Broadcast Filtering: Block LAN to WLAN Multicast and Broadcast Data ⓘ

Hide SSID: Prevent this SSID from being broadcast

User Group: Default

Шаг 7. Прокрутите страницу вниз до раздела **RADIUS MAC AUTHENTICATION** и выполните следующие настройки:

- **Enable** — установите флажок для параметра **Enable RADIUS MAC authentication**, чтобы включить поддержку аутентификации по RADIUS;
- **RADIUS Profile** — Укажите профиль RADIUS, который вы предварительно настроили;
- **MAC Address Format** — укажите формат представления MAC адреса — *aa:bb:cc:dd:ee:ff*.

RADIUS MAC AUTHENTICATION ▾

Enabled: Enable RADIUS MAC authentication

RADIUS Profile: AxelINAC [Create new RADIUS profile](#)

MAC Address Format ⓘ: aa:bb:cc:dd:ee:ff

Empty Password: Allow empty password

[SAVE](#) [CANCEL](#)

Нажмите **SAVE**, чтобы применить изменения.

Интеграция WLC с AxelINAC

Описание взаимодействия AxelINAC с сетевым оборудованием Ubiquiti-Unifi.

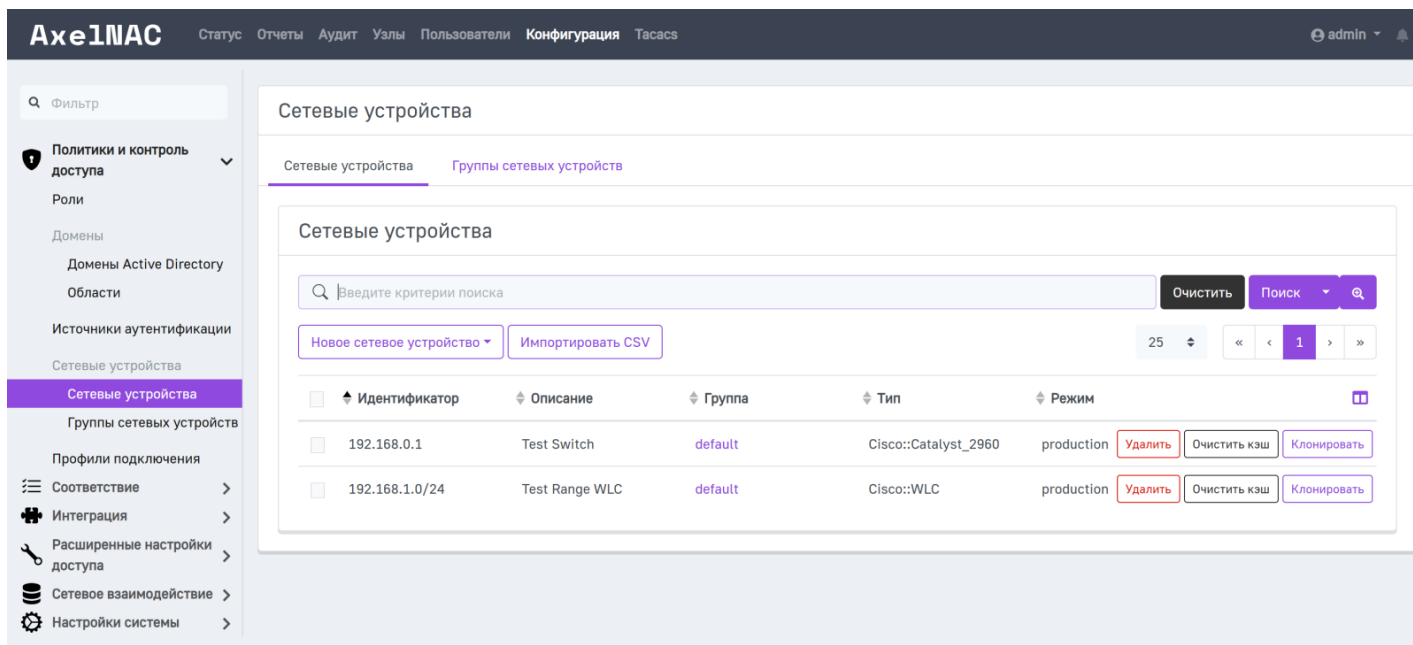
AxelINAC обменивается данными с WLC, но данные авторизованных пользователей приходят напрямую с точек доступа. То есть, точки доступа работают в режиме FlexConnect:

1. Трафик приходит с точки доступа на AxelINAC.
2. AxelINAC отправляет ответ на контроллер.
3. Контроллер передает ответ на точку доступа.

Настройка профиля WLC в AxelINAC

После того как контроллер настроен, необходимо настроить его профиль для AxelINAC.

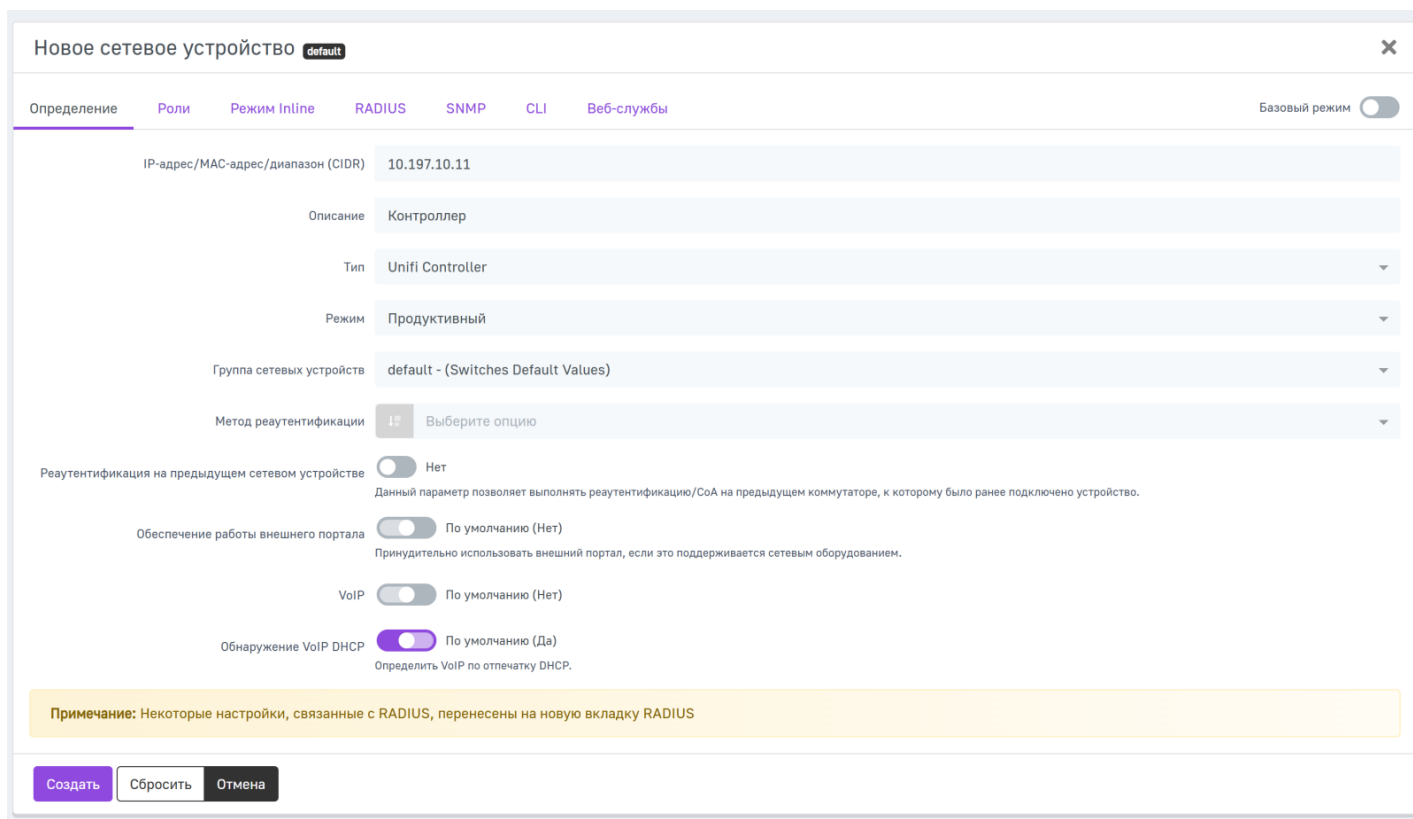
Шаг 1. Перейдите во вкладку **Конфигурация** → **Политика и контроль доступа** → **Сетевые устройства**, нажмите на кнопку **Новое сетевое устройство** и в выпадающем списке выберите к какой группе должно принадлежать устройство (по умолчанию создана группа **default**).



Также, вы можете указать диапазон адресов сетевого оборудования в рамках 1 профиля.

Шаг 2. На открывшейся странице выполните настройку следующим образом:

- **IP-адрес/MAC-адрес/диапазон (CIDR)** — укажите адрес управляющего интерфейса (данное значение будет отображаться в списке профилей коммутаторов);
- **Описание** — укажите описание профиля (данное значение будет отображаться в списке профилей коммутаторов);
- **Тип** — выберите из выпадающего списка тип контроллера (в нашем примере — Unifi Controller);
- **Режим** — Продуктивный.



Шаг 3. Переключитесь на вкладку **RADIUS** и выполните следующие настройки:

- **Секретная фраза** — укажите секретный ключ контроллера;
- **IP-адрес контроллера** — укажите IP-адрес контроллера;
- **CoA-порт** — укажите порт 8443 (в качестве протокола обмена данными Unifi используют протокол **STUN**, который использует порт 8443).

Новое сетевое устройство default
✕

[Определение](#)
[Роли](#)
[Режим Inline](#)
[RADIUS](#)
[SNMP](#)
[CLI](#)
[Веб-службы](#)
Базовый режим

Секретная фраза

Использовать CoA По умолчанию (Да)
Использовать CoA, если он доступен, для реавтентификации пользователя. Если данный параметр отключен, вместо него будет использоваться RADIUS Disconnect, если он доступен.

Использовать коннектор для реавтентификации По умолчанию (Да)
Использовать доступные коннекторы AxelNAC для выполнения реавтентификации RADIUS. По умолчанию на этом сервере размещен локальный коннектор.

IP-адрес контроллера
Данный IP-адрес будет использоваться для запросов на реавтентификацию. Обычно применяется только для Wi-Fi.

Disconnect-порт
Укажите порт для переадресации Disconnect-запроса.

CoA-порт
Укажите порт для переадресации CoA-запроса.

Валидация после MFA По умолчанию (Нет)
Добавить дополнительную проверку в поток RADIUS, чтобы определить, успешно ли пользователь подтвердил MFA.

Доступ к CLI/VPN разрешен По умолчанию (Нет)
Разрешить данному сетевому оборудованию использовать AxelNAC в качестве RADIUS-сервера для доступа к CLI или VPN.

Создать
Сбросить
Отмена

Шаг 4. Переключитесь на вкладку **Веб-службы** и установите значение **HTTPS** в поле **Транспортный протокол**, затем введите логин и пароль от учетной записи администратора контроллера.

Новое сетевое устройство default
✕

[Определение](#)
[Роли](#)
[Режим Inline](#)
[RADIUS](#)
[SNMP](#)
[CLI](#)
[Веб-службы](#)
Базовый режим

Транспортный протокол

Имя пользователя

Пароль

Создать
Сбросить
Отмена

Нажмите **Создать**, чтобы сохранить профиль контроллера.

Шаг 5. Пропишите MAC-адреса интерфейсов точек доступа в кэше AxelNAC с помощью следующей команды (это необходимо, чтобы связать MAC-адреса интерфейсов точек доступа с контроллером внутри AxelNAC):

```
/usr/local/pf/bin/pfcmd pfcron ubiquiti_ap_mac_to_ip
```

Шаг 6. Просмотрите кэш, и убедитесь, что в нем появились записи формата Ubiquiti-aa:bb:cc:dd:ee:ff, используя следующую команду:

```
/usr/local/pf/bin/pfcmd cache switch_distributed list
```

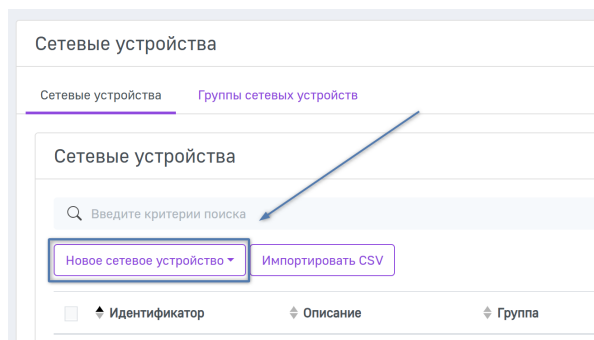
После этого контроллер считается добавленным в AxelNAC.

Настройка точек доступа Unifi

Так как данные пользователя приходит в AxelNAC с точки доступа, нам нужно добавить MAC-адрес/IP-адрес точки доступа в AxelNAC, иначе данный трафик будет игнорироваться.

Добавление точки доступа по IP-адресу

Шаг 1. Добавьте точку доступа в AxelNAC в качестве коммутатора. Для этого 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. На открывшейся странице выполните настройку следующим образом:

- **IP-адрес/MAC-адрес/диапазон (CIDR)** — укажите адрес управляющего интерфейса точки доступа (данное значение будет отображаться в списке профилей коммутаторов);
- **Описание** — укажите описание профиля (данное значение будет отображаться в списке профилей коммутаторов);
- **Тип** — выберите из выпадающего списка тип контроллера (в нашем примере — Unifi Controller);
- **Режим** — продуктивный;
- **Метод реаутентификации** — RADIUS;
- **Реаутентификация на предыдущем сетевом устройстве** — активируйте данный параметр для корректной работы CoA;
- **Обеспечение работы внешнего портала** — активируйте данный параметр для работы Captive-портал из AxelNAC.

Шаг 3. Переключитесь на вкладку **RADIUS** и выполните следующие настройки:

- **Секретная фраза** — укажите секретный ключ контроллера;
- **IP-адрес контроллера** — укажите IP-адрес контроллера, который вы настроили в предыдущем разделе (это необходимо для связи точки доступа с контроллером);
- **CoA-порт** — укажите порт 3799.

Новое сетевое устройство default ✕

Определение Роли Режим Inline **RADIUS** SNMP CLI Веб-службы Базовый режим

Секретная фраза

Использовать CoA По умолчанию (Да)
Использовать CoA, если он доступен, для реаутентификации пользователя. Если данный параметр отключен, вместо него будет использоваться RADIUS Disconnect, если он доступен.

Использовать коннектор для реаутентификации По умолчанию (Да)
Использовать доступные коннекторы AxelINAC для выполнения реаутентификации RADIUS. По умолчанию на этом сервере размещен локальный коннектор.

IP-адрес контроллера
Данный IP-адрес будет использоваться для запросов на реаутентификацию. Обычно применяется только для Wi-Fi.

Disconnect-порт
Укажите порт для переадресации Disconnect-запроса.

CoA-порт
Укажите порт для переадресации CoA-запроса.

Валидация после MFA По умолчанию (Нет)
Добавить дополнительную проверку в поток RADIUS, чтобы определить, успешно ли пользователь подтвердил MFA.

Доступ к CLI/VPN разрешен По умолчанию (Нет)
Разрешить данному сетевому оборудованию использовать AxelINAC в качестве RADIUS-сервера для доступа к CLI или VPN.

Создать & Закрыть Сбросить Отмена

Шаг 4. Переключитесь на вкладку **Веб-службы** и установите значение **HTTPS** в поле **Транспортный протокол**, затем введите логин и пароль от учетной записи администратора контроллера.

Новое сетевое устройство default ✕

Определение Роли Режим Inline RADIUS SNMP CLI **Веб-службы** Базовый режим

Транспортный протокол

Имя пользователя

Пароль

Создать Сбросить Отмена

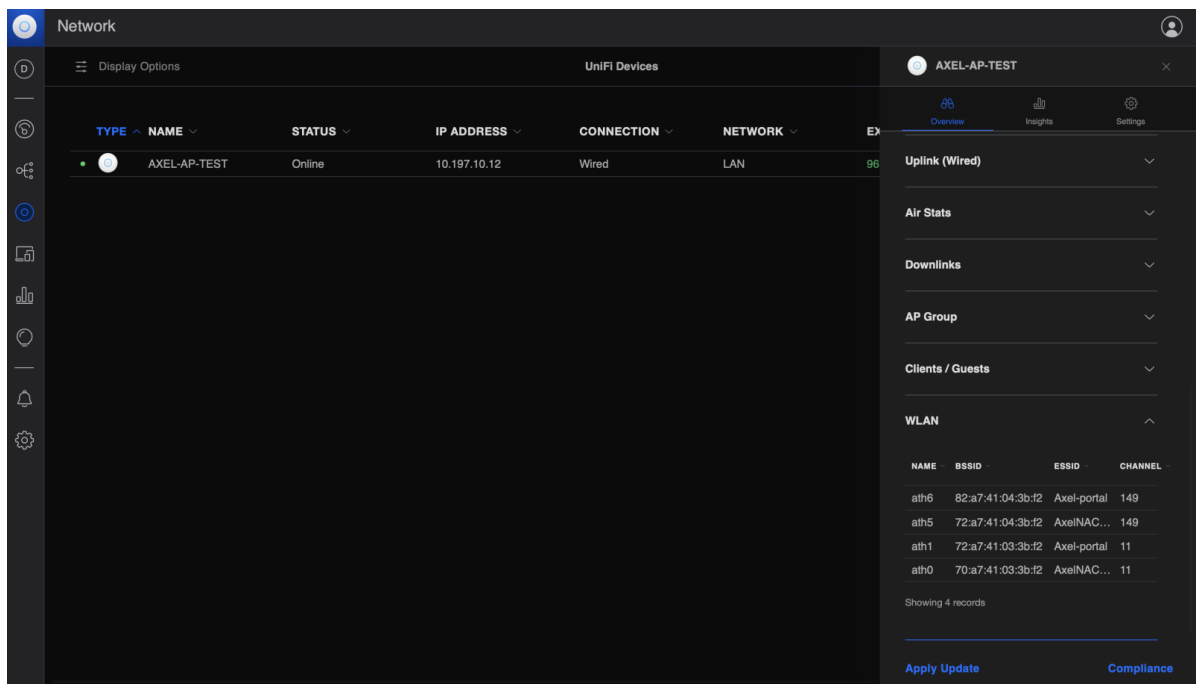
После создания профиля запросы с первого созданного SSID будут определяться и AxelINAC будет отвечать на них. Для того чтобы добавить остальные SSID, необходимо добавить их профили в AxelINAC в качестве новых точек доступа, используя их MAC-адрес.

Добавление отдельных SSID точек доступа

Чтобы добавить определенный SSID точки доступа и его MAC адрес, выполните следующие шаги:

Шаг 1. В WEB-интерфейсе контроллера перейдите во вкладку **Network** и выберите точку доступа.

Шаг 2. Внутри точки доступа откройте раздел **WLAN**, где вы сможете просмотреть MAC-адреса каждого SSID этой точки доступа.



Шаг 3. Выполните аналогичные настройки как при добавлении точки доступа по IP-адресу, но используйте MAC-адрес в качестве идентификатора.

Новое сетевое устройство default

Определение ¹ Роли Режим Inline RADIUS SNMP CLI Веб-службы Базовый режим

IP-адрес/MAC-адрес/диапазон (CIDR)

Описание

Тип

Режим

Группа сетевых устройств

Метод реавтентификации

Реавтентификация на предыдущем сетевом устройстве Да
Данный параметр позволяет выполнять реавтентификацию/CoA на предыдущем коммутаторе, к которому было ранее подключено устройство.

Обеспечение работы внешнего портала Да
Принудительно использовать внешний портал, если это поддерживается сетевым оборудованием.

VoIP По умолчанию (Нет)

Обнаружение VoIP DHCP По умолчанию (Да)
Определить VoIP по отпечатку DHCP.

Примечание: Некоторые настройки, связанные с RADIUS, перенесены на новую вкладку RADIUS

Настройка ролей для пользователей

Для каждого профиля точки доступа можно настроить свои роли с выдачей определенных VLAN. Для этого в профиле устройства переключитесь на вкладку **Роли**.

Настройка ролей осуществляется в профиле устройства, не на WLC.

ID статьи: 1044

Последнее обновление: 22 сент., 2025

Обновлено от: Михалева А.

Ревизия: 5

База знаний AxelINAC -> Документация -> Система контроля доступа к сети «AxelINAC». Версия 2.1.0 -> AxelINAC. Руководство по интеграции с сетевым оборудованием -> Интеграция AxelINAC с контроллерами беспроводного доступа Ubiquiti Unifi <https://docs.axel.pro/entry/1044/>