

# Интеграция AxeINAC с контроллерами беспроводного доступа Ubiquiti Unifi

В данной статье рассматривается процесс интеграции AxeINAC 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 AxeINAC необходимо обеспечить правильное сетевое взаимодействие на всем пути сетевого оборудования. На рис. 1 представлена гибкая схема подключения сетевого оборудования, позволяющая реализовать весь функционал WLC:

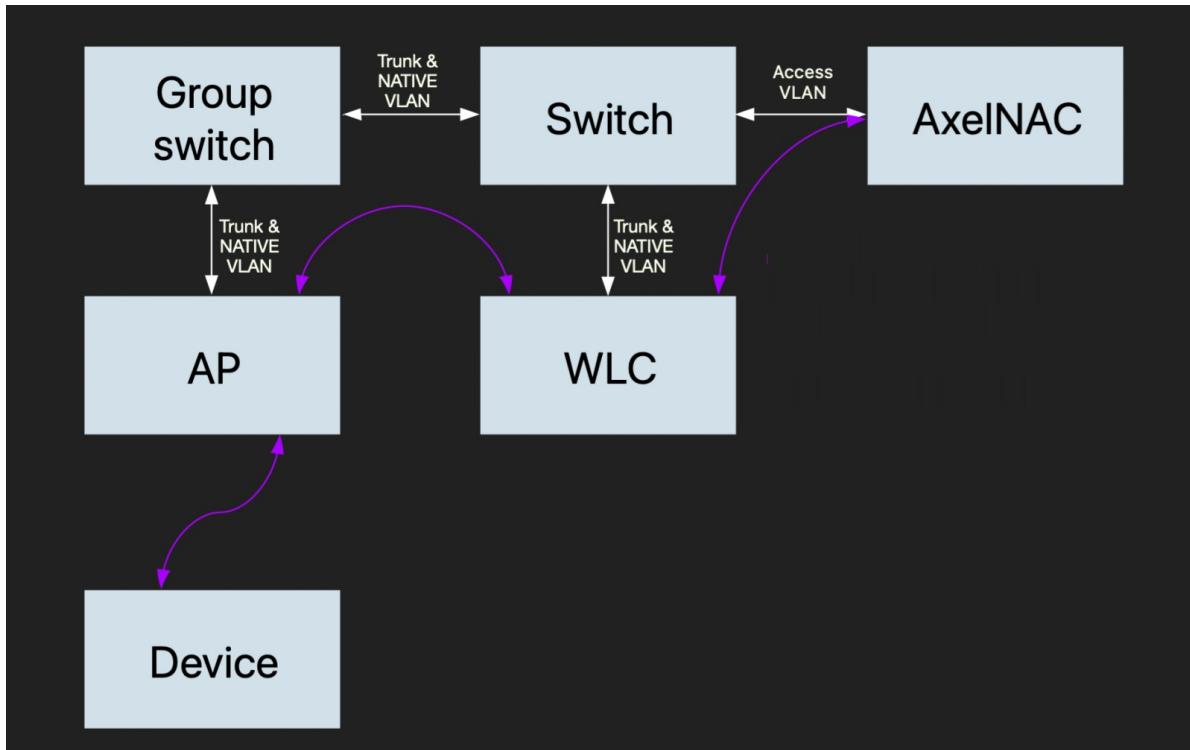


Рисунок 1 — Концептуальная схема соединения сетевого оборудования

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

- **AxeINAC** — виртуальный или физический сервер AxeINAC;
- **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 AxeINAC, 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**. Пролистайте страницу вниз и в блоке **Device authentication** установите флагок 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.

**DEVICE AUTHENTICATION**

Authentication between devices and the Network application.

**SSH Authentication**

Enable SSH authentication

Username  Password

SSH Credentials can be seen and changed by all of Site Admins.

**SSH Keys**

i No SSH keys have been defined.

+ ADD NEW SSH KEY

APPLY CHANGES RESET EXPORT SITE

**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 (данний 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 (данний параметр включает аккаунтинг);
- **Interim Update** — установите флажок для параметра Enable Interim Update (данний 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.

**EDIT RADIUS PROFILE - AXELNAC**

Profile Name

VLAN Support

Enable RADIUS assigned VLAN for wired network

Enable RADIUS assigned VLAN for wireless network

RADIUS Auth Server

IP Address  Port  Password/Shared Secret  i X

+ ADD AUTH SERVER

Accounting

Enable accounting

Enable Interim Update

Interim Update i

i

RADIUS Accounting Server

IP Address  Port  Password/Shared Secret  i X

+ ADD ACCOUNTING SERVER

SAVE CANCEL

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** — установить 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	AxelNAC-EAP				
Enabled	<input checked="" type="checkbox"/> Enable this wireless network				
Security	<input type="radio"/> Open <input type="radio"/> WEP <input type="radio"/> WPA Personal <input checked="" type="radio"/> WPA Enterprise <input type="radio"/> Hotspot 2 OSSEN				
WPA3	<input type="checkbox"/> Support WPA3 connections				
RADIUS Profile	AxelNAC <input type="button" value="Create new RADIUS profile"/>				
Hotspot 2.0	<input type="checkbox"/> Enable Hotspot 2.0				
Guest Policy	<input type="checkbox"/> Apply guest policies (captive portal, guest authentication, access)				
Network	<input checked="" type="checkbox"/> RADIUS assigned VLAN				
<b>ADVANCED OPTIONS ▾</b>					
WiFi Band	<input type="radio"/> 2.4 Ghz <input type="radio"/> 5 Ghz <input checked="" type="radio"/> Both				
Broadcasting APs	<table border="1"><thead><tr><th>AP GROUP NAME ↑</th><th>APS</th></tr></thead><tbody><tr><td>All APs</td><td>1 <input type="button" value="VIEW"/></td></tr></tbody></table>	AP GROUP NAME ↑	APS	All APs	1 <input type="button" value="VIEW"/>
AP GROUP NAME ↑	APS				
All APs	1 <input type="button" value="VIEW"/>				
Multicast and Broadcast Filtering	<input type="checkbox"/> Block LAN to WLAN Multicast and Broadcast Data				
Fast Roaming	<input type="checkbox"/> Enable fast roaming				
Hide SSID	<input type="checkbox"/> Prevent this SSID from being broadcast				
Group Rekey Interval	<input checked="" type="checkbox"/> Enable GTK rekeying every <input type="text" value="3600"/> seconds				
User Group	<input type="button" value="Default"/>				

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**.

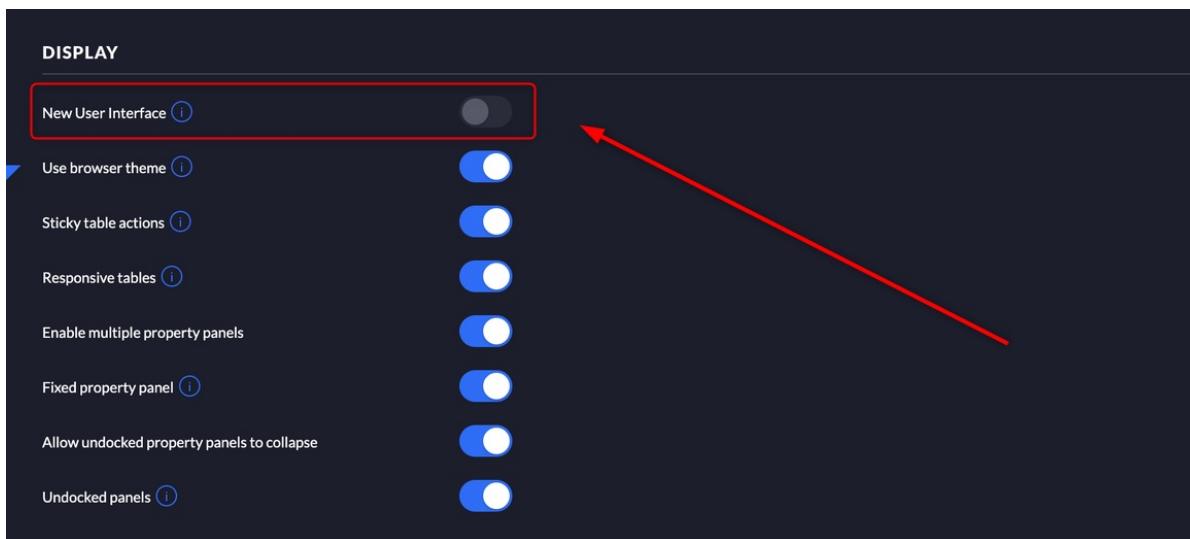
**Шаг 2.** Выполните настройку следующим образом:

- **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.

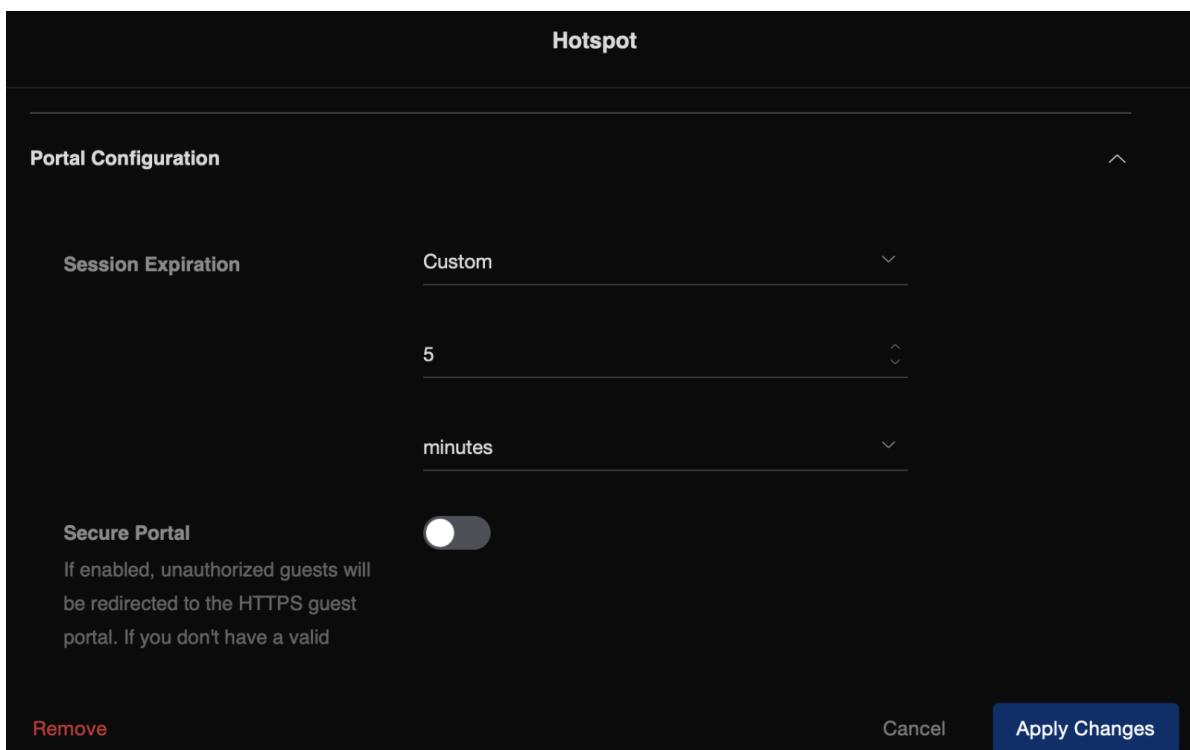
Guest Control	
<b>GUEST POLICIES</b>	
Guest Portal	<input checked="" type="checkbox"/> Enable Guest Portal <small>NETWORK APPLICATION MUST BE ONLINE.</small>
Authentication	<input type="radio"/> No authentication <input type="radio"/> Hotspot <input type="radio"/> Facebook WiFi <input checked="" type="radio"/> External portal server
Custom Portal	IPv4 Address <input type="text" value="172.16.190.7"/>
Redirection	<input type="checkbox"/> Use Secure Portal <input type="checkbox"/> Redirect using hostname <input type="text" value="http://"/> <input type="checkbox"/> Enable HTTPS Redirection
<b>ACCESS CONTROL</b>	
Pre-Authorization Access	<input type="text" value="172.16.190.7/32"/> <input type="button" value="X"/> <input type="button" value="ADD IPV4 HOSTNAME OR SUBNET"/>
Post-Authorization Restrictions	<input type="button" value="ADD IPV4 HOSTNAME OR SUBNET"/>
<input type="button" value="APPLY CHANGES"/> <input type="button" value="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 флагок для параметра **Enable this wireless network**, для того , чтобы профиль стал активным;
- **Security** — выберите значение Open;
- **Guest Policy** — установите флагок 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 флагок для параметра **RADIUS DAC/DAC (CoA)**, чтобы активировать поддержку СоA.

## Wireless Networks

### EDIT WIRELESS NETWORK - AXEL-PORTAL

Name/SSID	Axel-portal				
Enabled	<input checked="" type="checkbox"/> Enable this wireless network				
Security	<input checked="" type="radio"/> Open <input type="radio"/> WEP <input type="radio"/> WPA Personal <input type="radio"/> WPA Enterprise <input type="radio"/> Hotspot 2 OSEN				
Guest Policy	<input checked="" type="checkbox"/> Apply guest policies (captive portal, guest authentication, access)				
Network	<input checked="" type="checkbox"/> RADIUS assigned VLAN <a href="#">i</a>				
<b>ADVANCED OPTIONS ▾</b>					
WiFi Band	<input type="radio"/> 2.4 Ghz <input type="radio"/> 5 Ghz <input checked="" type="radio"/> Both				
Broadcasting APs	<table border="1"><thead><tr><th>AP GROUP NAME ↑</th><th>APS</th></tr></thead><tbody><tr><td>All APs</td><td>1 <a href="#">VIEW</a></td></tr></tbody></table> <a href="#">Create New AP Group</a>	AP GROUP NAME ↑	APS	All APs	1 <a href="#">VIEW</a>
AP GROUP NAME ↑	APS				
All APs	1 <a href="#">VIEW</a>				
Multicast and Broadcast Filtering	<input type="checkbox"/> Block LAN to WLAN Multicast and Broadcast Data <a href="#">i</a>				
Hide SSID	<input type="checkbox"/> Prevent this SSID from being broadcast				
User Group	Default <a href="#">▼</a>				

**Шаг 7.** Пролистайте 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*.

<b>RADIUS MAC AUTHENTICATION ▾</b>	
Enabled	<input checked="" type="checkbox"/> Enable RADIUS MAC authentication
RADIUS Profile	AxeINAC <a href="#">▼</a> <a href="#">Create new RADIUS profile</a>
MAC Address Format <a href="#">i</a>	aa:bb:cc:dd:ee:ff <a href="#">▼</a>
Empty Password	<input type="checkbox"/> Allow empty password
<b>SAVE</b> CANCEL	

Нажмите **SAVE**, чтобы применить изменения.

## Интеграция WLC с AxeINAC

### Описание взаимодействия AxeINAC с сетевым оборудованием Ubiquiti-Unifi.

AxeINAC 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 AxeINAC.
2. AxeINAC отправляет ответ на контроллер.
3. Контроллер передает ответ на точку доступа.

## Настройка профиля WLC в AxeINAC

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

**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;
- **СоA-порт** — укажите порт 8443 (в качестве протокола обмена данными Unifi используют протокол **STUN**, который использует порт 8443).

Новое сетевое устройство **default**

**RADIUS**

Секретная фраза

Использовать СоA  По умолчанию (Да)  
Использовать СоA, 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 AxelNAC для выполнения реаутентификации RADIUS. По умолчанию на этом сервере размещен локальный коннектор.

IP-адрес контроллера **10.197.10.11**  
Данный IP-адрес будет использоваться для запросов на реаутентификацию. Обычно применяется только для Wi-Fi.

Disconnect-порт  
Укажите порт для переадресации Disconnect-запроса.

СоA-порт **8443**  
Укажите порт для переадресации СоA-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**

**Веб-службы**

Транспортный протокол **HTTPS**

Имя пользователя **admin**

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/МАС-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.

Определение	Роли	Режим Inline	RADIUS	SNMP	CLI	Веб-службы	Базовый режим
IP-адрес/МАС-адрес/диапазон (CIDR)	10.197.10.12						<input checked="" type="checkbox"/>
Описание	AP1						
Тип	Unifi Controller						
Режим	Продуктивный						
Группа сетевых устройств	default - (Switches Default Values)						
Метод реаутентификации	<input type="button" value="Выберите опцию"/>						
Реаутентификация на предыдущем сетевом устройстве	<input checked="" type="checkbox"/> Да	Данный параметр позволяет выполнять реаутентификацию/CoA на предыдущем коммутаторе, к которому было ранее подключено устройство.					
Обеспечение работы внешнего портала	<input checked="" type="checkbox"/> Да	Принудительно использовать внешний портал, если это поддерживается сетевым оборудованием.					
VoIP	<input type="checkbox"/> По умолчанию (Нет)						
Обнаружение VoIP DHCP	<input checked="" type="checkbox"/> По умолчанию (Да)	Определить VoIP по отпечатку DHCP.					

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

**Создать** **Сбросить** **Отмена**

**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);
- **СоA-порт** — укажите порт 3799.

Новое сетевое устройство **default**

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

Секретная фраза **\*\*\*\*\*** 

Использовать СоA  По умолчанию (Да)  
Использовать СоA, 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 AxeINAC для выполнения реаутентификации RADIUS. По умолчанию на этом сервере размещен локальный коннектор.

IP-адрес контроллера **10.197.10.11**  
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 **3799**  
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 AxeINAC 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 **HTTPS** 

Имя пользователя **admin**

Пароль **\*\*\*\*\*** 

**Создать** **Сбросить** **Отмена**

После создания профиля запросы с первого созданного SSID будут определяться и AxeINAC будет отвечать на них. Для того, чтобы добавить остальные SSID, необходимо добавить их профили в AxeINAC 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.

The screenshot shows the UniFi Network interface. On the left, there's a sidebar with various icons. The main area displays a table of UniFi devices. One row is selected for 'AXEL-AP-TEST', which is listed as 'Online' with IP address 10.197.10.12, connected via 'Wired' to the 'LAN' network. To the right of the device table is a detailed view for 'AXEL-AP-TEST'. This view includes tabs for 'Overview', 'Insights', and 'Settings'. The 'Overview' tab is active, showing sections for 'Uplink (Wired)', 'Air Stats', 'Downlinks', 'AP Group', 'Clients / Guests', and 'WLAN'. Under 'WLAN', a table lists four wireless interfaces (ath6, ath5, ath1, ath0) with their respective MAC addresses (82:a7:41:04:3b:f2, 72:a7:41:04:3b:f2, 72:a7:41:03:3b:f2, 70:a7:41:03:3b:f2), ESSIDs (Axel-portal, AxelNAC..., Axel-portal, AxelNAC...), and channels (149, 149, 11, 11). At the bottom of the overview panel are 'Apply Update' and 'Compliance' buttons.

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

The screenshot shows the 'Новое сетевое устройство' (New Network Device) configuration dialog. The top navigation bar includes tabs for 'Определение' (1), 'Роли', 'Режим Inline', 'RADIUS', 'SNMP', 'CLI', 'Веб-службы', and 'Базовый режим' (switched off). The main configuration area has the following fields:

- IP-адрес/МАС-адрес/диапазон (CIDR):** 72:a7:41:04:3b:f2
- Описание:** AP1
- Тип:** Unifi Controller
- Режим:** Продуктивный
- Группа сетевых устройств:** default - (Switches Default Values)
- Метод реаутентификации:** Выберите опцию (button)
- Реаутентификация на предыдущем сетевом устройстве:** Да (switched on)
 

Данный параметр позволяет выполнять реаутентификацию/CoA на предыдущем коммутаторе, к которому было ранее подключено устройство.
- Обеспечение работы внешнего портала:** Да (switched on)
 

Принудительно использовать внешний портал, если это поддерживается сетевым оборудованием.
- VoIP:** По умолчанию (Нет) (switched off)
- Обнаружение VoIP DHCP:** По умолчанию (Да) (switched on)
 

Определить VoIP по отпечатку DHCP.

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

At the bottom are buttons for 'Создать' (Create), 'Сбросить' (Reset), and 'Отмена' (Cancel).

## 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: 14

Последнее обновление: 1 июл., 2025

Обновлено от: Егоров В.

Ревизия: 4

База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 1.2.0 -> AxelNAC. Руководство по интеграции с сетевым оборудованием -> Интеграция AxelNAC с контроллерами беспроводного доступа Ubiquiti UniFi <https://docs.axel.pro/entry/14/>