

# 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:

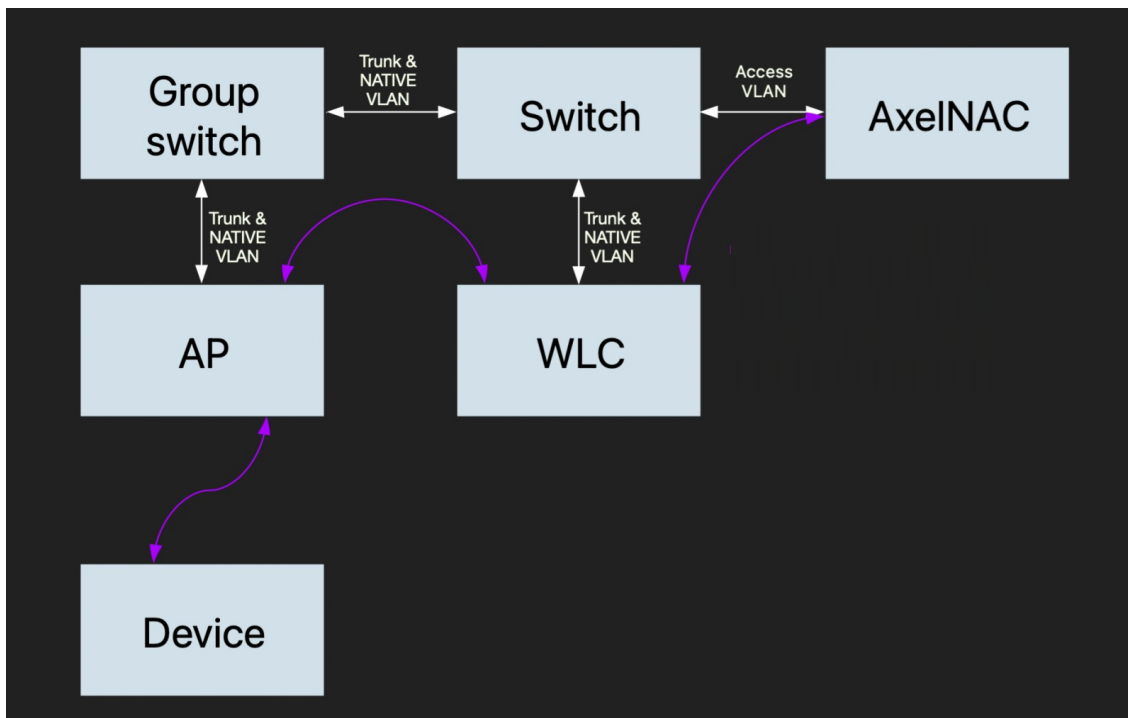


Рисунок 1 — Концептуальная схема соединения сетевого оборудования

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, APM с беспроводным интерфейсом.

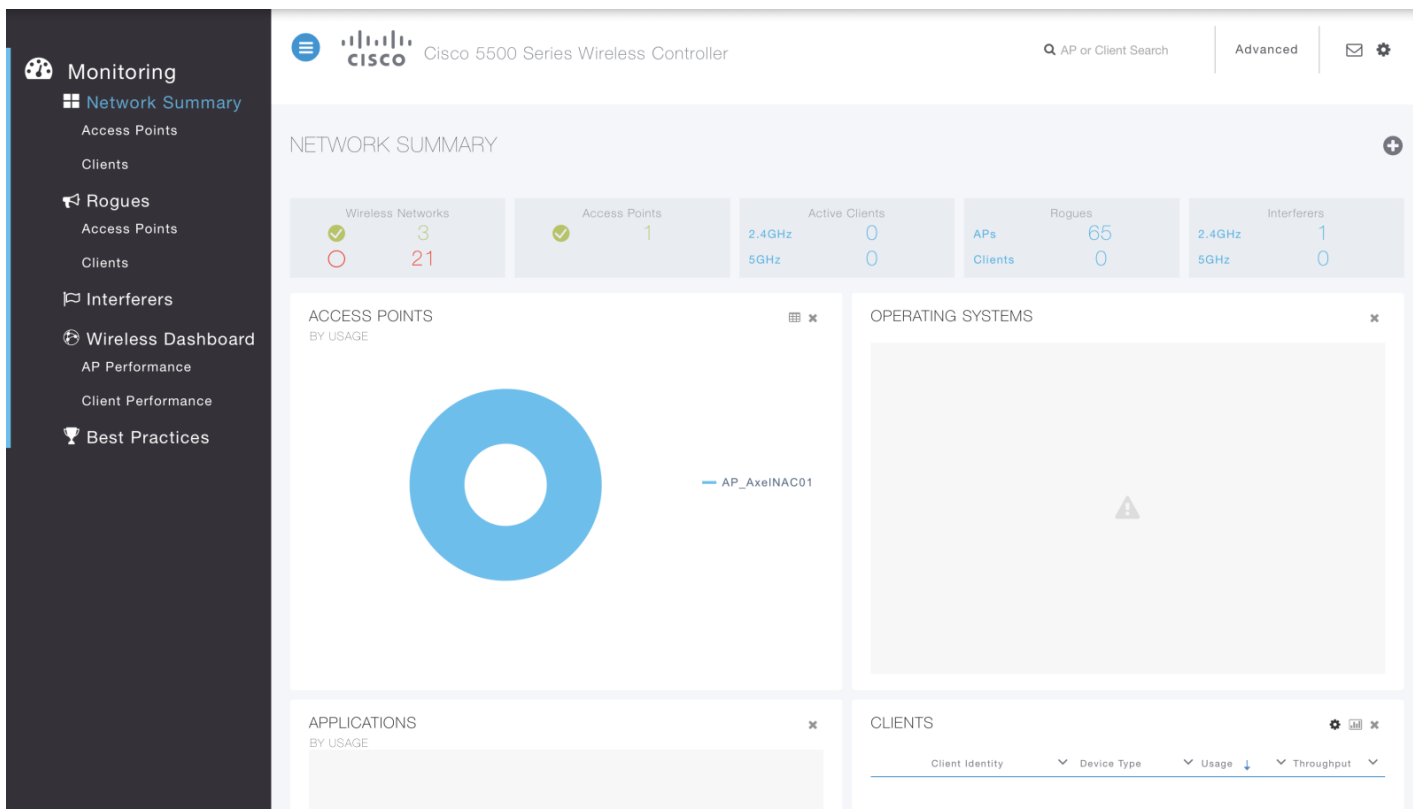
При интеграции WLC с AxelNAC, точку доступа можно настроить в одном из двух режимов:

- **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).

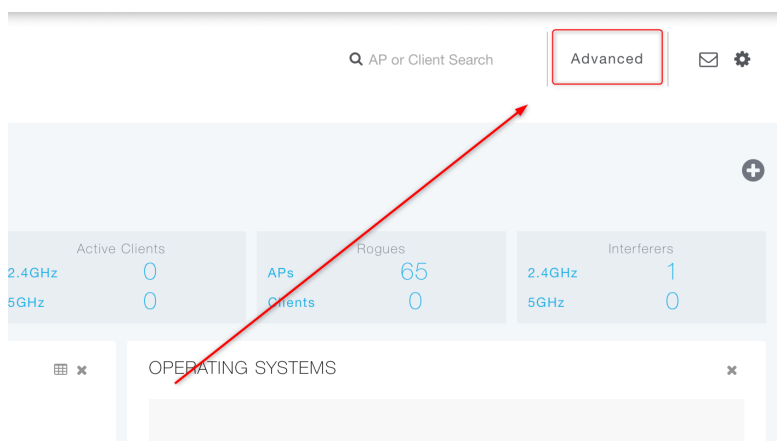
## Настройка Cisco WLC

### 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:

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Save Configuration Ping Logout Refresh Home

Controller Interfaces > Edit < Back Apply

**General Information**

Interface Name	management
MAC Address	e0:2f:6d:7c:44:40

**Configuration**

Quarantine

Quarantine Vlan Id

**NAT Address**

Enable NAT Address

**Interface Address**

VLAN Identifier	3147
IP Address	10.31.47.228
Netmask	255.255.255.0
Gateway	10.31.47.1
IPv6 Address	::
Prefix Length	128
IPv6 Gateway	::
Link Local IPv6 Address	fe80::e22f:6dff:fe7c:4440/64

**Physical Information**

Port Number	1
Backup Port	0
Active Port	1
Enable Dynamic AP Management	<input checked="" type="checkbox"/>

**DHCP Information**

Primary DHCP Server	0.0.0.0
Secondary DHCP Server	0.0.0.0

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

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Save Configuration Ping Logout Refresh Home

Controller Interfaces > Edit < Back Apply

**General Information**

Interface Name	vlan3143
MAC Address	e0:2f:6d:7c:44:44

**Configuration**

Guest Lan

Quarantine

Quarantine Vlan Id

NAS-ID

**Physical Information**

Port Number	1
Backup Port	0
Active Port	1
Enable Dynamic AP Management	<input type="checkbox"/>

**Interface Address**

VLAN Identifier	3143
IP Address	10.31.43.159
Netmask	255.255.255.0
Gateway	10.31.43.1
IPv6 Address	::
Prefix Length	128
IPv6 Gateway	::
Link Local IPv6 Address	fe80::e22f:6dff:fe7c:4440/64

**DHCP Information**

Primary DHCP Server	10.31.40.194
Secondary DHCP Server	
DHCP Proxy Mode	Global
Enable DHCP Option 82	<input type="checkbox"/>
Enable DHCP Option 6 OpenDNS	<input type="checkbox"/>

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

## Настройка WLAN для аутентификации 802.1x.

Для работы аутентификации 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**.

**Security**

**RADIUS Authentication Servers > New**

Server Index (Priority)

Server IP Address(Ipv4/Ipv6)

Shared Secret Format

Shared Secret

Confirm Shared Secret

Key Wrap  (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number

Server Status

Support for CoA

Server Timeout  seconds

Network User  Enable

Management  Enable

Management Retransmit Timeout  seconds

Tunnel Proxy  Enable

IPsec  Enable

**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**.

**Security**

**RADIUS Accounting Servers > New**

Server Index (Priority)

Server IP Address(Ipv4/Ipv6)

Shared Secret Format

Shared Secret

Confirm Shared Secret

Port Number

Server Status

Server Timeout  seconds

Network User  Enable

Tunnel Proxy  Enable

IPsec  Enable

**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 приступить 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»
```

config ap ip default-gateway <ip-address>

config 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 журналы 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

**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:

The screenshot shows the 'WLANs > Edit 'AxeINAC\_EAP'' configuration page. The 'General' tab is selected. The configuration includes: Profile Name: AxeINAC\_EAP; Type: WLAN; SSID: AxeINAC\_EAP; Status: Enabled; Security Policies: [WPA2][Auth(802.1X)]; Radio Policy: All; Interface/Interface Group(G): wlan3143; Multicast Vlan Feature: Disabled; Broadcast SSID: Enabled; NAS-ID: none. There are 'Back' and 'Apply' buttons at the top right.

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

The screenshot shows the 'WLANs > Edit 'AxeINAC\_EAP'' configuration page, specifically the 'Security' tab and 'Layer 2' sub-tab. The configuration includes: Layer 2 Security: WPA+WPA2; MAC Filtering: Disabled; Fast Transition: Disabled; Protected Management Frame (PMF): Disabled; WPA+WPA2 Parameters: WPA Policy: Disabled; WPA2 Policy: Enabled; WPA2 Encryption: AES (checked), TKIP, CCMP256, GCMP128, GCMP256 (all unchecked); OSEN Policy: Disabled; Authentication Key Management: 802.1X (checked), CCKM, PSK (all unchecked). There are 'Back' and 'Apply' buttons at the top right.

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

**General** **Security** **QoS** **Policy-Mapping** **Advanced**

**Layer 2** **Layer 3** **AAA Servers**

Select AAA servers below to override use of default servers on this WLAN

**RADIUS Servers**

RADIUS Server Overwrite interface  Enabled  
 Apply Cisco ISE Default Settings  Enabled

	Authentication Servers	Accounting Servers	EAP Parameters
Server 1	<input checked="" type="checkbox"/> Enabled IP:10.31.40.220, Port:1812	<input checked="" type="checkbox"/> Enabled IP:10.31.40.220, Port:1813	Enable <input type="checkbox"/>
Server 2	None	None	
Server 3	None	None	
Server 4	None	None	
Server 5	None	None	
Server 6	None	None	

**RADIUS Server Accounting**

Interim Update  Interim Interval 0 Seconds

**LDAP Servers**

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

**General** **Security** **QoS** **Policy-Mapping** **Advanced**

Allow AAA Override  Enabled  
 Coverage Hole Detection  Enabled  
 Enable Session Timeout  1800  
 Session Timeout (secs)  
 Aironet IE  Enabled  
 Diagnostic Channel  Enabled  
 Override Interface ACL IPv4 [None] IPv6 [None]  
 Layer2 Acl [None]  
 URL ACL [None]  
 P2P Blocking Action [Disabled]  
 Client Exclusion  Enabled  
 Timeout Value (secs) 180  
 Maximum Allowed Clients 0  
 Static IP Tunneling  Enabled  
 Wi-Fi Direct Clients Policy [Disabled]  
 Maximum Allowed Clients Per AP Radio 200  
 Clear HotSpot Configuration  Enabled  
 Scan Defer Priority 0 1 2 3 4 5 6 7  
        
 Scan Defer Time(msecs) 100

**FlexConnect**

FlexConnect Local Switching  Enabled  
 FlexConnect Local Auth  Enabled  
 Learn Client IP Address  Enabled  
 Vlan based Central Switching  Enabled  
 Central DHCP Processing  Enabled  
 Override DNS  Enabled  
 NAT-PAT  Enabled  
 Central Assoc  Enabled

**Lync**

Lync Server [Disabled]

**11k**

**DHCP**

DHCP Server  Override  
 10.31.40.194  
 DHCP Server IP Addr  
 DHCP Addr. Assignment  Required

**OEAP**

Split Tunnel  Enabled

**Management Frame Protection (MFP)**

MFP Client Protection [Optional]  
 DTIM Period (in beacon intervals)  
 802.11a/n (1 - 255) 1  
 802.11b/g/n (1 - 255) 1 (in beacon in)

**NAC**

NAC State [ISE NAC]  
 Re-anchor Roamed Voice Clients  Enabled  
 KTS based CAC Policy  Enabled

**Radius Client Profiling**

DHCP Profiling   
 HTTP Profiling

**Local Client Profiling**

DHCP Profiling   
 HTTP Profiling

**PMIP**

PMIP Mobility Type   
 PMIP NAI Type [Hexadecimal]  
 PMIP Profile [None]  
 PMIP Realm

**Universal AP Admin Support**

Universal AP Admin

**11v BSS Transition Support**

BSS Transition

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

## Настройка Captive-портала:

**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:

**General** **Security** **QoS** **Policy-Mapping** **Advanced**

Profile Name: MAB\_redirect  
 Type: WLAN  
 SSID: MAB\_redirect  
 Status:  Enabled

Security Policies: **MAC Filtering**  
 (Modifications done under security tab will appear after applying the changes.)

Radio Policy: All  
 Interface/Interface Group(G): vlan3143  
 Multicast Vlan Feature:  Enabled  
 Broadcast SSID:  Enabled  
 NAS-ID: Jet-CSR-WLC5508

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

**General** **Security** **QoS** **Policy-Mapping** **Advanced**

**Layer 2** **Layer 3** **AAA Servers**

Layer 2 Security: None  
 MAC Filtering:

**Fast Transition**  
 Fast Transition: Enable  
 Over the DS:   
 Reassociation Timeout: 20 Seconds

**Lobby Admin Configuration**  
 Lobby Admin Access:

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

**General** **Security** **QoS** **Policy-Mapping** **Advanced**

**Layer 2** **Layer 3** **AAA Servers**

Select AAA servers below to override use of default servers on this WLAN

**RADIUS Servers**  
 RADIUS Server Overwrite interface:  Enabled  
 Apply Cisco ISE Default Settings:  Enabled

	Authentication Servers	Accounting Servers
Server 1	<input checked="" type="checkbox"/> Enabled IP:10.31.40.220, Port:1812	<input checked="" type="checkbox"/> Enabled IP:10.31.40.220, Port:1813
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

**RADIUS Server Accounting**  
 Interim Update:

**LDAP Servers**

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

WLANs > Edit 'MAB\_redirect'

**General** Security QoS Policy-Mapping Advanced

Allow AAA Override  Enabled  
 Coverage Hole Detection  Enabled  
 Enable Session Timeout  1800  
 Session Timeout (secs)  
 Aironet IE  Enabled  
 Diagnostic Channel  Enabled  
 Override Interface ACL IPv4  None IPv6  None  
 Layer2 Acl  None  
 URL ACL  None  
 P2P Blocking Action  Disabled  
 Client Exclusion  Enabled  
 Timeout Value (secs) 180  
 Maximum Allowed Clients 0  
 Static IP Tunneling  Enabled  
 Wi-Fi Direct Clients Policy  Disabled  
 Maximum Allowed Clients Per AP Radio 200  
 Clear HotSpot Configuration  Enabled

DHCP  
 DHCP Server  Override  
 DHCP Server IP Addr 10.31.40.194  
 DHCP Addr. Assignment  Required

OEAP  
 Split Tunnel  Enabled

Management Frame Protection (MFP)  
 MFP Client Protection  Optional

DTIM Period (in beacon intervals)  
 802.11a/n (1 - 255) 1  
 802.11b/g/n (1 - 255) 1

NAC  
 NAC State ISE NAC

WLANs > Edit 'MAB\_redirect'

< Back Apply

**General** Security QoS Policy-Mapping Advanced

Client user idle threshold (0-10000000) 0 Bytes  
 Radius NAI-Realm   
 11ac MU-MIMO   
 WGB PRP  Enabled

Off Channel Scanning Defer  
 Scan Defer Priority 0 1 2 3 4 5 6 7  
 Scan Defer Time(msecs) 100

FlexConnect  
 FlexConnect Local Switching  Enabled  
 FlexConnect Local Auth  Enabled  
 Learn Client IP Address  Enabled  
 Vlan based Central Switching  Enabled  
 Central DHCP Processing  Enabled  
 Override DNS  Enabled  
 NAT-PAT  Enabled

Load Balancing and Band Select  
 Client Load Balancing   
 Client Band Select

Passive Client  
 Passive Client

Voice  
 Media Session Snooping  Enabled  
 Re-anchor Roamed Voice Clients  Enabled  
 KTS based CAC Policy  Enabled

Radius Client Profiling  
 DHCP Profiling   
 HTTP Profiling

Local Client Profiling  
 DHCP Profiling   
 HTTP Profiling

PMIP  
 PMIP Mobility Type

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

## Создание ACL-redirect для режима Local Mode

**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):

Access Control Lists > Edit

< Back Add New Rule

**General**

Access List Name 10.31.40.220\_redirect  
 Deny Counters 0

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

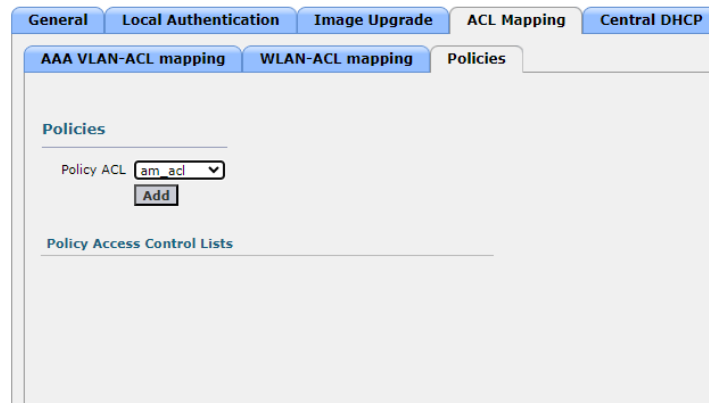
## Создание ACL-redirect для режима Flex Mode

**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**).

Новое сетевое устройство default
✕

Определение
Роли
Режим Inline
RADIUS
SNMP
CLI
Веб-службы

Базовый режим

IP-адрес/MAC-адрес/диапазон (CIDR)	11.31.48.123
Описание	<span style="background-color: #f0f0f0; padding: 2px;">i</span> Значения сетевых устройств по умолчанию
Тип	Cisco Wireless Controller (WLC) <span style="float: right;">▼</span>
Режим	Продуктивный <span style="float: right;">▼</span>
Группа сетевых устройств	default - (Switches Default Values) <span style="float: right;">▼</span>
Метод реавтентификации	RADIUS <span style="float: right;">▼</span>
Реавтентификация на предыдущем сетевом устройстве	<input type="checkbox"/> Нет <small>Данный параметр позволяет выполнять реавтентификацию/CoA на предыдущем коммутаторе, к которому было ранее подключено устройство.</small>
Обеспечение работы внешнего портала	<input checked="" type="checkbox"/> Да <small>Принудительно использовать внешний портал, если это поддерживается сетевым оборудованием.</small>
VoIP	<input type="checkbox"/> По умолчанию (Нет)
Обнаружение VoIP DHCP	<input checked="" type="checkbox"/> По умолчанию (Да) <small>Определить VoIP по отпечатку DHCP.</small>
Динамические Uplink	<input checked="" type="checkbox"/> По умолчанию (Динамический) <small>Автоматическое определение Uplink-портов.</small>

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

**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 реавтентификации** 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**.

Новое сетевое устройство **default** ✕

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

### Назначение VLAN ID

Назначать VLAN ID  По умолчанию (Да)

registration	3143
isolation	1* 3
macDetection	
inline	1* 6
Isolating	
Machine	
REJECT	1* -1
Remediation	

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".

### Назначение URL веб-аутентификации

Назначать URL веб-аутентификации  Да

registration	http://<AxelNAC-ip-address>/Cisco::WLC
isolation	
macDetection	
inline	
Isolating	
Machine	http://<AxelNAC-ip-address>/Cisco::WLC
REJECT	
Remediation	http://<AxelNAC-ip-address>/Cisco::WLC
User	
default	
gaming	
guest	

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

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

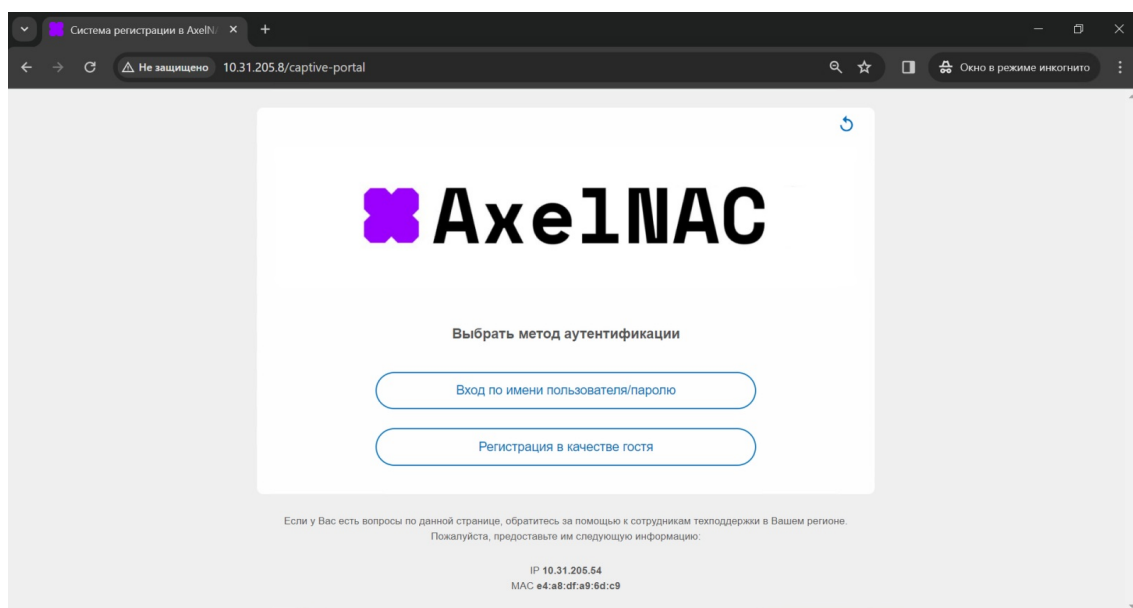
**Шаг 14.** Установите переключатель **Использовать CoA** в положение **Нет**.

**Шаг 15.** Укажите IP-адрес контроллера в поле **IP-адрес контроллера** как на примере.

**Шаг 16.** 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 AxelINAC.



Для того чтобы настроить работу Captive-портал в AxelINAC, 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.

ID статьи: 1043

Последнее обновление: 22 сент., 2025

Обновлено от: Михалева А.

Ревизия: 6

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 Cisco WLC 5500

<https://docs.axel.pro/entry/1043/>