

Интеграция AxeINAC с контроллерами беспроводного доступа Cisco WLC 5500

В данной статье рассматривается процесс интеграции AxeINAC 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 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:

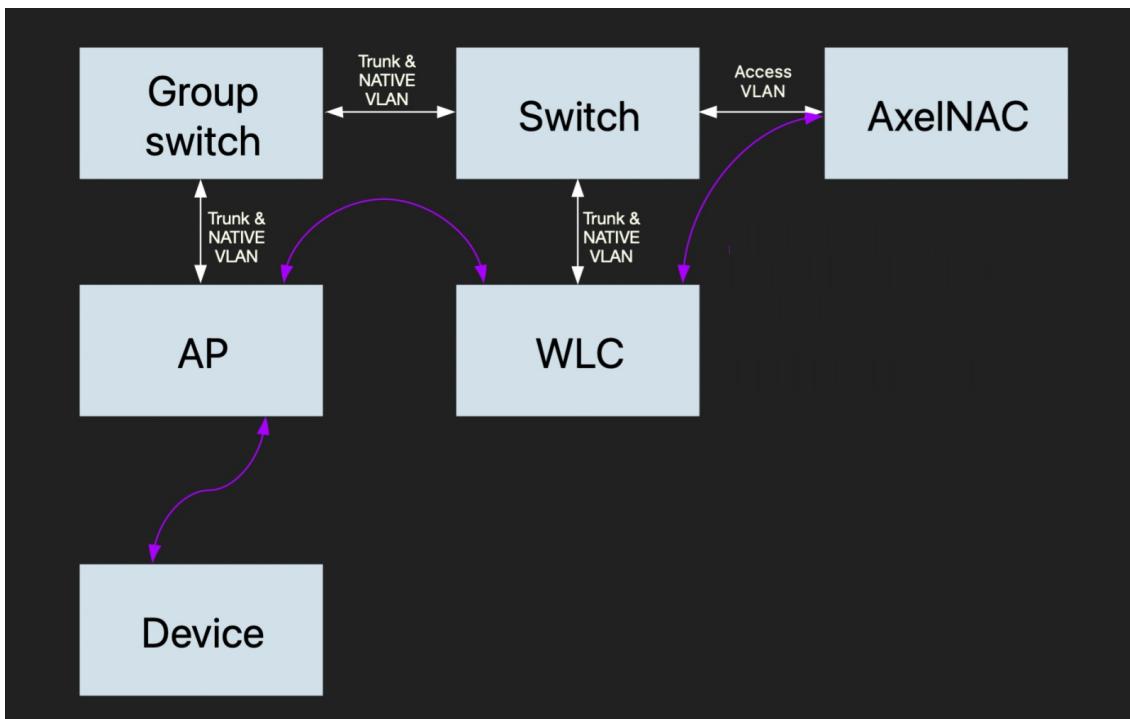


Рисунок 1 — Концептуальная схема соединения сетевого оборудования

Белые стрелки отображают физическое соединение устройств. Фиолетовыми стрелками 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, 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 управляемого интерфейса

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

The screenshot shows the Cisco 5500 Series Wireless Controller's Network Summary dashboard. On the left, a sidebar lists monitoring categories: Network Summary, Rogues, Interferers, Wireless Dashboard, AP Performance, Client Performance, and Best Practices. The main area displays a summary of wireless networks (3 active, 21 rogue), access points (1 active), and clients (0 active). Below this are four cards: ACCESS POINTS BY USAGE (a donut chart for AP_AxeINAC01), OPERATING SYSTEMS (empty), APPLICATIONS BY USAGE (empty), and CLIENTS (a table with columns: Client Identity, Device Type, Usage, Throughput).

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

This screenshot is identical to the one above, but with a red box highlighting the 'Advanced' button in the top right corner of the header. A red arrow points from the text in the previous step to this button, indicating where to click to switch to advanced mode.

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

CISCO

MONITOR WLANs **CONTROLLER** WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Save Configuration | Ping | Logout | Refresh | Home

< Back | Apply

Controller

Interfaces > Edit

General
Icons
Inventory
Interfaces
Interface Groups
Multicast
Network Routes
Redundancy
Internal DHCP Server
Mobility Management
Ports
NTP
CDP
PMIPv6
Tunneling
IPv6
mDNS
Advanced

General Information

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

Configuration

Quarantine:
Quarantine Vlan Id: 0

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:

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.

CISCO

MONITOR WLANs **CONTROLLER** WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Save Configuration | Ping | Logout | Refresh | Home

Controller

Interfaces > Edit

General
Icons
Inventory
Interfaces
Interface Groups
Multicast
Network Routes
Redundancy
Internal DHCP Server
Mobility Management
Ports
NTP
CDP
PMIPv6
Tunneling
IPv6
mDNS
Advanced

General Information

Interface Name: vlan3143
MAC Address: e0:2f:6d:7c:44:40

Configuration

Guest Lan:
Quarantine:
Quarantine Vlan Id: 0
NAS-ID: none

Physical Information

Port Number: 1
Backup Port: 0
Active Port: 1
Enable Dynamic AP Management:

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:
Enable DHCP Option 6 OpenDNS:

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

Настройка WLAN для аутентификации 802.1x.

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

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

The screenshot shows the Cisco Wireless Controller (WLC) web interface. The top navigation bar includes links for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (which is highlighted in orange), MANAGEMENT, COMMANDS, HELP, and FEEDBACK. On the left, a sidebar menu under the Security section lists various AAA components: General, RADIUS (selected), Accounting, Fallback, DNS, Downloaded AVP, TACACS+, LDAP, Local Net Users, MAC Filtering, Disabled Clients, User Login Policies, AP Policies, Password Policies, Local EAP, Advanced EAP, Priority Order, Certificate, Access Control Lists, Wireless Protection Policies, Web Auth, TrustSec SXP, Local Policies, and Advanced.

The main content area is titled "RADIUS Authentication Servers > New". It contains the following configuration fields:

- Server Index (Priority): 3
- Server IP Address(Ipv4/Ipv6): 10.31.205.6
- Shared Secret Format: ASCII
- Shared Secret: (redacted)
- Confirm Shared Secret: (redacted)
- Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
- Port Number: 1812
- Server Status: Enabled
- Support for CoA: Enabled
- Server Timeout: 2 seconds
- Network User: Enable
- Management: Enable
- Management Retransmit Timeout: 2 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 флагок для параметра **Support for CoA**.

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

The screenshot shows the Cisco WLC web interface. The top navigation bar includes links for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (highlighted in orange), MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The sidebar menu under the Security section is identical to the previous screenshot.

The main content area is titled "RADIUS Accounting Servers > New". It contains the following configuration fields:

- Server Index (Priority): 2
- Server IP Address(Ipv4/Ipv6): 10.31.206.6
- Shared Secret Format: ASCII
- Shared Secret: (redacted)
- Confirm Shared Secret: (redacted)
- Port Number: 1813
- Server Status: Enabled
- Server Timeout: 2 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 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:

WLANS > Edit 'AxelNAC_EAP'

< Back Apply

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

Profile Name	AxelNAC_EAP
Type	WLAN
SSID	AxelNAC_EAP
Status	<input checked="" type="checkbox"/> Enabled
Security Policies [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)	
Radio Policy	All
Interface/Interface Group(G)	vlan3143
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
NAS-ID	none

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

WLANS > Edit 'AxelNAC_EAP'

< Back Apply

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

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

Layer 2 Security	WPA+WPA2
MAC Filtering	<input type="checkbox"/>
Fast Transition	
Fast Transition	Disable
Protected Management Frame	
PMF	Disabled
WPA+WPA2 Parameters	
WPA Policy	<input type="checkbox"/>
WPA2 Policy	<input checked="" type="checkbox"/>
WPA2 Encryption	<input checked="" type="checkbox"/> AES <input type="checkbox"/> TKIP <input type="checkbox"/> CCMP256 <input type="checkbox"/> GCMP128 <input type="checkbox"/> GCMP256
OSEN Policy	<input type="checkbox"/>
Authentication Key Management	
802.1X	<input checked="" type="checkbox"/> Enable
CCKM	<input type="checkbox"/> Enable
PSK	<input type="checkbox"/> Enable

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
<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	Enable <input type="checkbox"/>
Server 1 IP:10.31.40.220, Port:1812	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 Interim Interval 0 Seconds

LDAP Servers

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

WLANS > Edit 'AxelNAC_EAP'

General Security QoS Policy-Mapping Advanced

DHCP

DHCP Server Override
Session Timeout (secs) 1800
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

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:

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

Profile Name	MAB_redirect
Type	WLAN
SSID	MAB_redirect
Status	<input checked="" type="checkbox"/> 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	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
NAS-ID	Jet-CSR-WLC5508

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

WLANS > Edit 'MAB_redirect'

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

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

Layer 2 Security	None
MAC Filtering <input checked="" type="checkbox"/>	
Fast Transition	
Fast Transition	<input checked="" type="checkbox"/> Enable
Over the DS	<input checked="" type="checkbox"/>
Reassociation Timeout	20 Seconds
Lobby Admin Configuration	
Lobby Admin Access	<input type="checkbox"/>

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

WLANS > Edit 'MAB_redirect'

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

RADIUS Server Accounting

Interim Update	<input type="checkbox"/>
----------------	--------------------------

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 <input checked="" type="checkbox"/>	Enabled			
Coverage Hole Detection <input checked="" type="checkbox"/>	Enabled			
Enable Session Timeout <input checked="" type="checkbox"/>	1800	Session Timeout (secs)		
Aironet IE	<input checked="" type="checkbox"/>	Enabled		
Diagnostic Channel 18	<input type="checkbox"/>	Enabled		
Override Interface ACL	IPv4 None	IPv6 None		
Layer2 Acl	None			
URL ACL	None			
P2P Blocking Action	Disabled			
Client Exclusion 3	<input checked="" type="checkbox"/>	Enabled	180	Timeout Value (secs)
Maximum Allowed Clients 8	0			
Static IP Tunneling 11	<input type="checkbox"/>	Enabled		
Wi-Fi Direct Clients Policy	Disabled			
Maximum Allowed Clients Per AP Radio	200			
Clear HotSpot Configuration	<input type="checkbox"/>	Enabled		
DHCP				
DHCP Server	<input checked="" type="checkbox"/> Override 10.31.40.194 DHCP Server IP Addr			
DHCP Addr. Assignment	<input checked="" type="checkbox"/> Required			
OEPAP				
Split Tunnel	<input type="checkbox"/> Enabled			
Management Frame Protection (MFP)				
MFP Client Protection 4	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'

General	Security	QoS	Policy-Mapping	Advanced
Client user idle threshold (0-10000000) 0	Bytes			
Radius NAC-Realm				
11ac MU-MIMO	<input checked="" type="checkbox"/>			
WGB PRP	<input type="checkbox"/>	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 2	<input type="checkbox"/>	Enabled		
FlexConnect Local Auth 12	<input type="checkbox"/>	Enabled		
Learn Client IP Address 8	<input checked="" type="checkbox"/>	Enabled		
Vlan based Central Switching 13	<input type="checkbox"/>	Enabled		
Central DHCP Processing	<input type="checkbox"/>	Enabled		
Override DNS	<input type="checkbox"/>	Enabled		
NAT-PAT	<input type="checkbox"/>	Enabled		
Load Balancing and Band Select				
Client Load Balancing	<input type="checkbox"/>			
Client Band Select	<input type="checkbox"/>			
Passive Client				
Passive Client	<input type="checkbox"/>			
Voice				
Media Session Snooping	<input type="checkbox"/> Enabled			
Re-anchor Roamed Voice Clients	<input type="checkbox"/> Enabled			
KTS based CAC Policy	<input type="checkbox"/> Enabled			
Radius Client Profiling				
DHCP Profiling	<input checked="" type="checkbox"/>			
HTTP Profiling	<input checked="" type="checkbox"/>			
Local Client Profiling				
DHCP Profiling	<input type="checkbox"/>			
HTTP Profiling	<input type="checkbox"/>			
PMIP				
PMIP Mobility Type	<input type="checkbox"/>			

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):

Access Control Lists > Edit

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	DSCHP	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	<input checked="" type="checkbox"/>
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	<input checked="" type="checkbox"/>
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any	11067	<input checked="" type="checkbox"/>
4	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	12578	<input checked="" type="checkbox"/>
5	Permit	10.31.40.220 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	2705	<input checked="" type="checkbox"/>
6	Permit	0.0.0.0 / 0.0.0.0	10.31.40.220 / 255.255.255.255	Any	Any	Any	Any	Any	1926	<input checked="" type="checkbox"/>
7	Permit	0.0.0.0 / 0.0.0.0	8.8.8.8 / 255.255.255.255	Any	Any	Any	Any	Any	121439	<input checked="" type="checkbox"/>
8	Permit	8.8.8.8 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	121412	<input checked="" type="checkbox"/>
9	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	105391	<input checked="" type="checkbox"/>

Создание ACL-redirect для режима Flex Mode

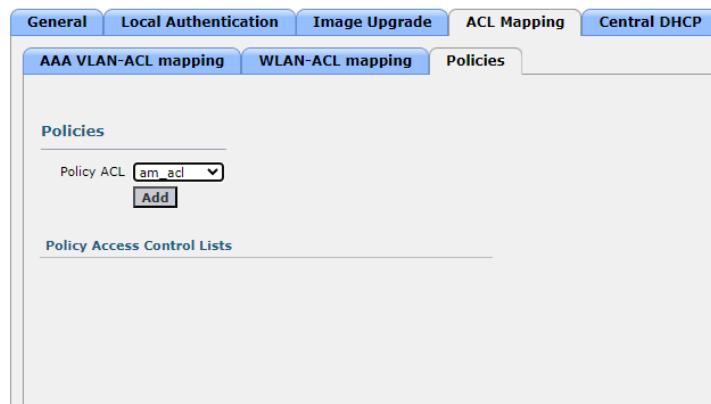
Для создания ACL-redirect для режима Flex Mode выполните следующие действия:

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**).

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						<input checked="" type="checkbox"/>
Описание	<input type="button" value="Значения сетевых устройств по умолчанию"/>						
Тип	Cisco Wireless Controller (WLC)						
Режим	Продуктивный						
Группа сетевых устройств	default - (Switches Default Values)						
Метод реаутентификации	RADIUS						
Реаутентификация на предыдущем сетевом устройстве	<input type="checkbox"/>	Нет					
Данный параметр позволяет выполнять реаутентификацию/СоA 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.							
Динамические UpLink	<input checked="" type="checkbox"/>	По умолчанию (Динамический)					
Автоматическое определение UpLink-портов.							
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 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**.

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**.

Новое сетевое устройство **default**

Определение	Роли	Режим Inline	RADIUS	SNMP	CLI	Веб-службы	Базовый режим
Секретная фраза *****							
<input checked="" type="checkbox"/> Использовать CoA Нет Использовать CoA, если он доступен, для реаутентификации пользователя. Если данный параметр отключен, вместо него будет использоваться RADIUS Disconnect, если он доступен.							
<input checked="" type="checkbox"/> Использовать коннектор для реаутентификации По умолчанию (Да) Использовать доступные коннекторы AxeINAC для выполнения реаутентификации RADIUS. По умолчанию на этом сервере размещён локальный коннектор.							
IP-адрес контроллера 11.31.48.123 <small>Данный IP-адрес будет использоваться для запросов на реаутентификацию. Обычно применяется только для Wi-Fi.</small>							
Disconnect-порт <small>Укажите порт для переадресации запроса Disconnect.</small>							
СоA-порт <small>Укажите порт для переадресации СоA-запроса.</small>							
<input checked="" type="checkbox"/> Валидация после MFA По умолчанию (Нет) <small>Добавить дополнительную проверку в поток RADIUS, чтобы определить, успешно ли пользователь подтвердил MFA.</small>							
<input checked="" type="checkbox"/> Доступ к CLI/VPN разрешён По умолчанию (Нет) <small>Разрешить данному сетевому оборудованию использовать AxeINAC в качестве RADIUS-сервера для доступа к CLI или VPN.</small>							
<input type="button" value="Создать"/> <input type="button" value="Сбросить"/> <input type="button" value="Отмена"/>							

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

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

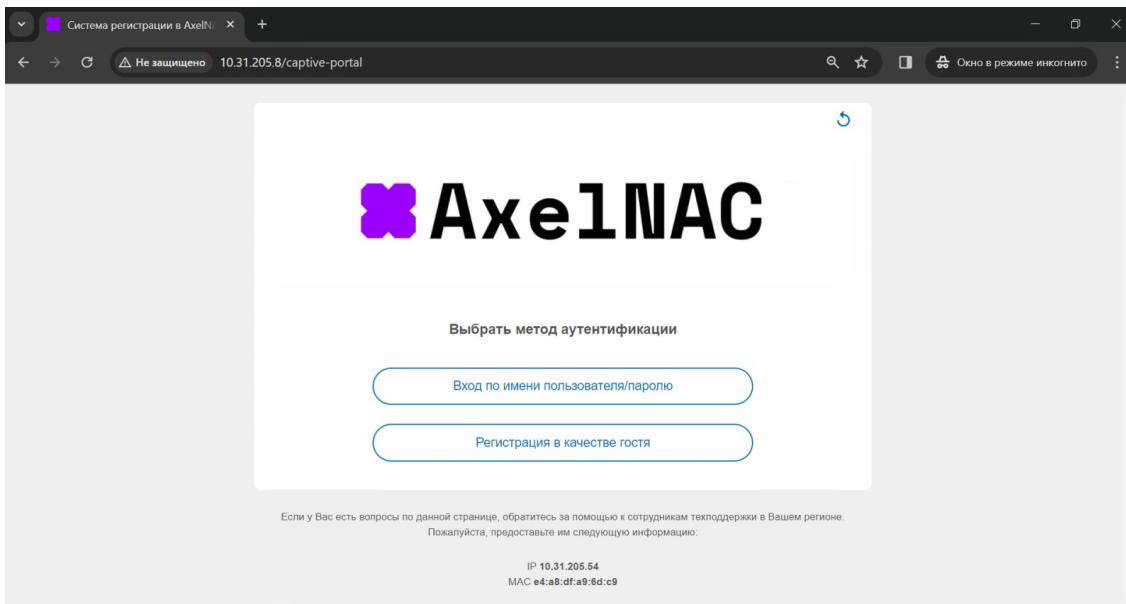
Шаг 15. Активируйте переключатель **Использовать коннектор для реаутентификации**.

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 AxeINAC



Для того чтобы настроить работу Captive-портал в AxeINAC, 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

База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.0.1 -> AxelNAC. Руководство по интеграции с сетевым оборудованием -> Интеграция AxelNAC с контроллерами беспроводного доступа Cisco WLC 5500

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