

Интеграция AxelNAC с коммутаторами Eltex MES

В данной статье рассматривается процесс интеграции AxelNAC с коммутаторами Eltex MES.

Убедитесь, что у вас настроена локальная учетная запись администратора на коммутаторе, т.к. после активации 802.1X или MAC-аутентификации коммутатор запросит учетные данные при следующем подключении.

Настройка 802.1x и MAC-авторизации через RADIUS-сервер

Конфигурация RADIUS-сервера

Шаг 1. Для первичной конфигурации необходимо активировать работу RADIUS-сервера. Для этого выполните на коммутаторе следующую команду:

```
radius server enable
```

Шаг 2. Выполните конфигурацию RADIUS-сервера и AAA с помощью следующих команд:

```
!  
aaa authentication dot1x default radius none  
aaa authorization dynamic radius  
aaa accounting dot1x start-stop group radius  
!  
radius-server host 192.168.1.10 encrypted key YourSecret usage all  
radius-server host source-interface vlan 999 #Если необходимо явно указать с какого интерфейса должны отправляться запросы на RADIUS-сервер#
```

Конфигурация интерфейсов

Шаг 1. Активируйте поддержку dot1x и CoA с помощью следующих команд:

```
dot1x system-auth-control  
aaa authorization dynamic radius
```

Шаг 2. Выполните конфигурацию портов с помощью следующего набора команд:

```
interface gigabitethernet1/0/7 ##  
dot1x port-control auto #активация поддержки 802.1x#  
dot1x reauthentication #активация регулярной реаутентификации клиентов#  
dot1x timeout reauth-period 300 #период реаутентификации 300 секунд#  
dot1x host-mode multi-auth #поддержка нескольких одновременных сессий dot1x на одном порте#  
dot1x max-hosts 2 #ограничить количество клиентов dot1x на одном порте 2 сессиями#  
dot1x authentication mac 802.1x #методы аутентификации и их порядок применения#  
dot1x max-login-attempts 5 #количество неуспешных попыток подключения, после которых клиент блокируется#  
dot1x critical-vlan enable #поддержка "bypass vlan" в которую направляется клиент при недоступности RADIUS-серверов#  
dot1x critical-vlan 100 #указание номера "bypass vlan"#  
dot1x radius-attributes vlan static #активация поддержки приема номера vlan от RADIUS-сервера.#  
dot1x radius-attributes vendor-specific data-filter #активация поддержки приема номера ACL от RADIUS-сервера#  
exit
```

Настройка RADIUS-авторизации администраторов

Если ранее выполнялась настройка 802.1x и MAC-авторизации, пропустите шаги 1 и 2.

Для настройки разграничения доступа к сетевому оборудованию, необходимо выполнить следующие действия:

Шаг 1. Активируйте работу RADIUS-сервера с помощью следующей команды:

```
console(config)# radius server enable
```

Шаг 2. Укажите IP-адрес и секретный ключ RADIUS-сервера:

```
console(config)# radius-server host 192.168.1.10 encrypted key YourSecret usage login
```

Если вы планируете использовать dot1x, для параметра **usage** укажите значение **all**.

Шаг 3. Установите способ аутентификации для входа в систему по протоколу RADIUS:

```
console(config)# aaa authentication login authorization default radius local
```

Шаг 4. Установите способ аутентификации при повышении уровня привилегий:

```
console(config)# aaa authentication enable default radius enable
```

Шаг 5. Чтобы не потерять доступ к коммутатору (в случае недоступности RADIUS-сервера), рекомендуется создать учетную запись в локальной базе данных, и задать пароль на привилегированный режим:

```
console(config)# username tester password eltex privilege 15  
console(config)# enable password eltex
```

Конфигурация разграничения доступа

Конфигурация групп и привязка к ним уровней привилегий выполняется с помощью следующего набора команд:

```
radius server group admin  
vlan name test #для доступа к оборудованию с указанного vlan(опционально)
```

```
privilege-level 15
exit
!
radius server group priv1
privilege-level 1
exit
```

Настройка TACACS-авторизации администраторов

Шаг 1. Укажите IP-адрес и секретный ключ TACACS-сервера:

```
console(config)# tacacs-server host 192.168.10.5 key Secret
```

Шаг 2. Установите способ аутентификации для входа в систему по протоколу TACACS+:

```
console(config)# aaa authentication login authorization default tacacs local
```

Шаг 3. Установите способ аутентификации при повышении уровня привилегий:

```
console(config)# aaa authentication enable default tacacs enable
```

Шаг 4. Чтобы не потерять доступ к коммутатору (в случае недоступности TACACS-сервера), рекомендуется создать учетную запись в локальной базе данных, и задать пароль на привилегированный режим:

```
console(config)# username tester password eltex privilege 15
console(config)# enable password eltex
```

Шаг 5. Разрешите ведение аккаунтинга для сессий управления:

```
console(config)# aaa accounting login start-stop group tacacs+
```

Шаг 6. Активируйте ведение аккаунтинга введенных в CLI команд по протоколу TACACS+:

```
console(config)# aaa accounting commands stop-only group tacacs+
```

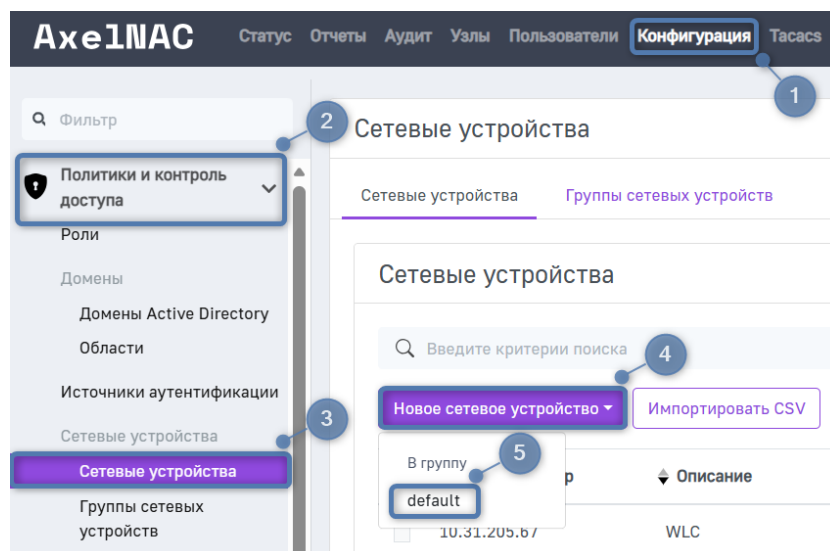
Шаг 7. Активируйте авторизацию вводимых команд на TACACS-сервере:

```
console(config)# aaa authorization commands default group tacacs+ local
```

После этого каждая вводимая команда будет проходить авторизацию на сервере.

Настройка конфигурации коммутатора в AxiNAC

Шаг 1. Перейдите в раздел **Конфигурация** → **Политики и контроль доступа** → **Сетевые устройства**, нажмите 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 заполните поля следующим образом:

- **IP-адрес/MAC-адрес:** укажите IP-адрес коммутатора;
- **Тип:** Eltex MES23xx, MES33xx, MES35xx, MES53xx - Ver4.0.21;
- **Режим:** Продуктивный;
- **Метод реаутентификации:** RADIUS.

Остальные параметры остаются по умолчанию.

Определение	Роли	Режим Inline	RADIUS	SNMP	CLI	Веб-службы	Базовый режим <input type="checkbox"/>
IP-адрес/MAC-адрес	10.10.10.10						
Описание	my_switch						
Тип	Eltex MES23xx, MES33xx, MES35xx, MES53xx - Ver4.0.21						
Режим	Продуктивный						
Группа сетевых устройств	default - (Switches Default Values)						
Метод реавтентификации	RADIUS						
Реавтентификация на предыдущем сетевом устройстве	<input type="checkbox"/> Нет Данный параметр позволяет выполнять реавтентификацию/CoA на предыдущем коммутаторе, к которому было ранее подключено устройство.						
Обеспечение работы внешнего портала	<input type="checkbox"/> По умолчанию (Нет) Принудительно использовать внешний портал, если это поддерживается сетевым оборудованием.						
VoIP	<input type="checkbox"/> По умолчанию (Нет)						
Обнаружение VoIP LLDp	<input checked="" type="checkbox"/> По умолчанию (Да) Определить VoIP по SNMP-запросу в LLDp MIB.						
Обнаружение VoIP CDP	<input checked="" type="checkbox"/> По умолчанию (Да) Определить VoIP по SNMP-запросу в CDP MIB.						
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 3. Переключитесь на вкладку **Роли**. Настройте VLAN и RADIUS DACL (при необходимости), возвращаемые для ролей.

Назначение VLAN ID

Назначать VLAN ID По умолчанию (Да)

registration	30
isolation	66
macDetection	
inline	12 6
Machine	
REJECT	12 -1
User	50
default	
gaming	
guest	20
voice	5

Назначение Downloadable ACL

Назначать Downloadable ACL Да
Добавление списка доступа (ACL) заменяет собой список, который определен непосредственно в конфигурации роли.

registration	ip permit 1 prot=tcp ip_src=10.0.0.3/0.0.0.255 ip_dst=10.0.0.0/255.0.0.0 tcp_port_src=80 tcp_port_dst=443
isolation	

При подключении пользователя определенной роли через контроллер он поместит его в назначенный VLAN из настроек и применит к нему соответствующие правила.

Шаг 4. Перейдите на вкладку **RADIUS** и укажите RADIUS-ключ указанный при настройке RADIUS-сервера на коммутаторе в поле **Секретная фраза**.

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.

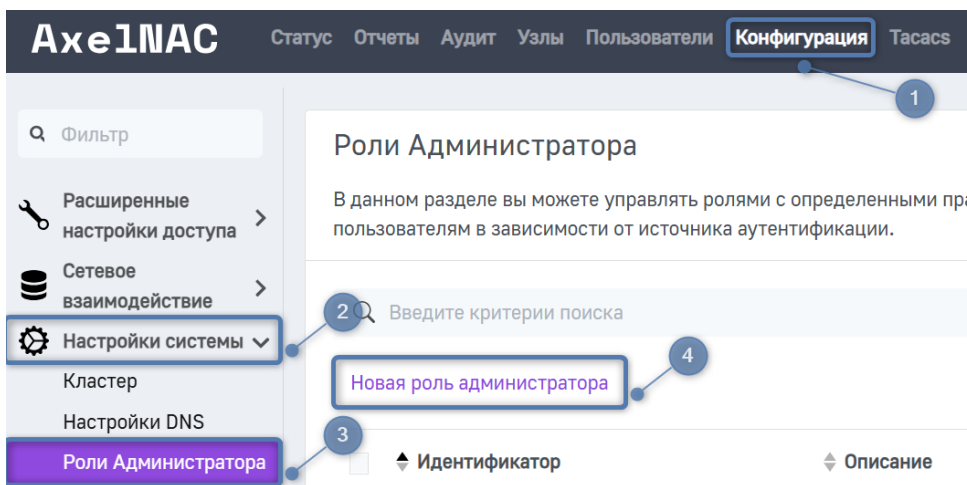
Валидация после MFA По умолчанию (Нет)
Добавить дополнительную проверку в поток RADIUS, чтобы определить, успешно ли пользователь подтвердил MFA.

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

Шаг 5. Нажмите **Создать** в левом нижнем углу окна.

Настройка RADIUS-авторизации администраторов в AxiINAC

Шаг 1. Перейдите в раздел **Конфигурация** → **Настройки системы** → **Роли Администратора**, нажмите кнопку **Новая роль администратора**.



Шаг 2. На открывшейся странице заполните поля следующим образом:

- **Имя:** укажите имя для роли;
- **Описание:** укажите описание роли;
- **Действия:** Switches CLI – Read (3 уровень привилегий).

Новая роль администратора ✕

[Основное](#)
[Настройки пользователя](#)
[Опции узла](#)

Имя

Описание

Действия

Если действия не указаны, администратор не будет иметь доступ к portalу администрирования.

Шаг 3. Нажмите **Создать** в левом нижнем углу окна.

Шаг 4. Создайте аналогичную роль для Switch CLI – write (15 уровень привилегий).

Новая роль администратора ✕

[Основное](#)
[Настройки пользователя](#)
[Опции узла](#)

Имя

Описание

Действия

Если действия не указаны, администратор не будет иметь доступ к portalу администрирования.

Шаг 5. Далее вернуться в раздел **Конфигурация** → **Политики и контроль доступа** → **Сетевые устройства** и выберите нужное устройство;

Шаг 6. На вкладке **RADIUS** включите параметр **Доступ к CLI/VPN разрешен**.

Сетевое устройство 10.10.10.10 **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.

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

Доступ к CLI/VPN разрешен Да
Разрешить данному сетевому оборудованию использовать AxelNAC в качестве RADIUS-сервера для доступа к CLI или VPN.

Шаг 7. Далее перейдите в **Конфигурация → Политики и контроль доступа → Источники аутентификации** и откройте настроенный источник Active Directory.

В данном примере предполагается, что источник аутентификации Active Directory уже настроен. Подробную информацию можно посмотреть в [статье с описанием настройки аутентификации с помощью Microsoft Active Directory](#).

АxelNAC Статус Отчеты Аудит Узлы Пользователи **Конфигурация** Тасасы admin

Источники аутентификации

В данном разделе вы можете указать источники аутентификации для доступа пользователей к Captive-порталу или веб-интерфейсу администратора.

Каждый профиль подключения должен быть связан с одним или несколькими источниками аутентификации, в то время как подключения 802.1X используют для определения роли упорядоченные внутренние источники. В подключениях 802.1X никогда не используются внешние источники.

Введите критерии поиска

25 « < 1 > »

Внутренние источники

Имя	Тип	Описание	
conn_AD	Active Directory	axeldemo	<input type="button" value="Удалить"/> <input type="button" value="Клонировать"/>

Шаг 8. На открывшейся странице заполните следующие настройки:

- **Связанные области:** укажите **<ваш.домен>** и **null** для того, чтобы обрабатывать имя как с доменным суффиксом так и без него;
- **Правила администрирования:** добавьте правило администрирования. Укажите свое условие для проверки пользователей и в **Действия** назначьте **Уровень доступа: switch15**, который мы создали ранее.

Связанные области **axel.pro** **null**

Области, которые будут связаны с данным источником.

Правила аутентификации

Правила администрирования **rule1**

Статус Включено

Имя rule1

Описание

Оператор Все

Условия 1 memberOf равно CN=radius_15, CN=

Действия 1 Уровень доступа switch15

Шаг 9. Нажмите **Создать** в левом нижнем углу окна.

ID статьи: 1047

Последнее обновление: 27 янв., 2026

Обновлено от: Михалева А.

Ревизия: 6

База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.1.0 -> AxelNAC. Руководство по интеграции с сетевым оборудованием -> Интеграция AxelNAC с коммутаторами Eltex MES

<https://docs.axel.pro/entry/1047/>