# МСЭ Checkpoint

Процесс настройки интеграции с МСЭ Checkpoint идентичен процессу настройки с МСЭ Barracuda. Однако, МСЭ Checkpoint поддерживает дополнительный функционал.

## Включение функции Identity Awareness на шлюзе безопасности

Чтобы включить функцию **Identity Awareness**, выполните следующие шаги:

**Шаг 1.** Войдите в систему **SmartDashboard**.

**Шаг 2.** В дереве сетевых объектов (**Network Objects**) разверните ветвь Check Point (**Check Point branch**).

**Шаг 3.** Дважды кликните на шлюзе безопасности (**Security Gateway**), на котором необходимо включить функцию Identity Awareness.

**Шаг 4.** В разделе **Software Blades** на вкладке **Network Security** выберите пункт **Identity Awareness**. Откроется мастер настройки **Identity Awareness Configuration**.

**Шаг 5.** Выберите один или несколько вариантов. Эти опции задают методы получения идентификационных данных управляемых и неуправляемых активов.

**Шаг 6.** Выберите пункт **AD Query** — это позволит шлюзу безопасности беспрепятственно идентифицировать пользователей и компьютеры Active Directory.

**Шаг 7.** Нажмите кнопку **Next**. Откроется окно интеграции с Active Directory.

**Шаг 8.** Выберите Active Directory для настройки из списка, в котором отображаются настроенные учетные единицы LDAP, или создайте новый домен. Если Active Directory еще не настроена, необходимо ввести имя домена, имя пользователя, пароль и учетные данные контроллера домена.

**Шаг 9.** Введите учетные данные Active Directory и нажмите кнопку **Connect** для проверки учетных данных.

Для работы AD Query необходимо указать учетные данные администратора домена

**Шаг 10.** Нажмите **Finish**.

## Включение аккаунтинга RADIUS на шлюзе безопасности

Чтобы включить RADIUS Accounting для шлюза безопасности, выполните следующие действия:

**Шаг 1.** В системе **SmartDashboard** в дереве **Network Objects** откройте шлюз безопасности.

**Шаг 2.** На странице **General Properties** убедитесь, что **Identity Awareness Blade** включен.

**Шаг 3.** На странице **Identity Awareness** выберите **RADIUS Accounting**.

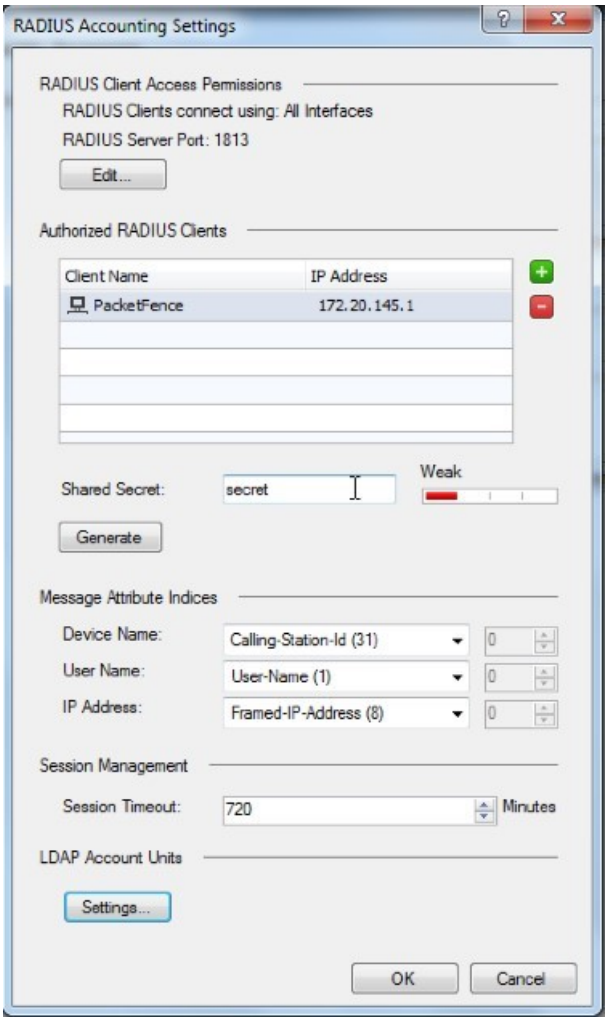
## Настройка RADIUS Accounting на МСЭ

Для того чтобы настроить RADIUS Accounting на МСЭ Checkpoint, выполните следующие действия:

**Шаг 1.** В окне **Check Point Gateway**, панель **Identity Awareness** нажмите кнопку **Settings** (находится справа от опции **RADIUS Accounting**).

**Шаг 2.** В окне **RADIUS Accounting Settings** (см. рисунок ниже) настройте **Message Attribute Indices** следующим образом:

- **Device Name:** Calling-Station-Id (31) — MAC-адрес устройства;
- **User Name:** User-Name (1) — имя пользователя, установленное на портале AxelNAC Portal;
- **IP Address:** Framed-IP-Address (8) — IP-адрес устройства в производственной сети.




## Разрешения клиентского доступа RADIUS

Интерфейсы шлюза должны быть авторизованы для приема соединений от RADIUS аккаунтинга AxelNAC.

Чтобы выбрать интерфейсы шлюза:

**Шаг 1.** В разделе **RADIUS Client Access Permissions** нажмите кнопку **Edit**.

**Шаг 2.** Выберите **All Interfaces** — все интерфейсы шлюза безопасности смогут принимать соединения от клиентов RADIUS Accounting.

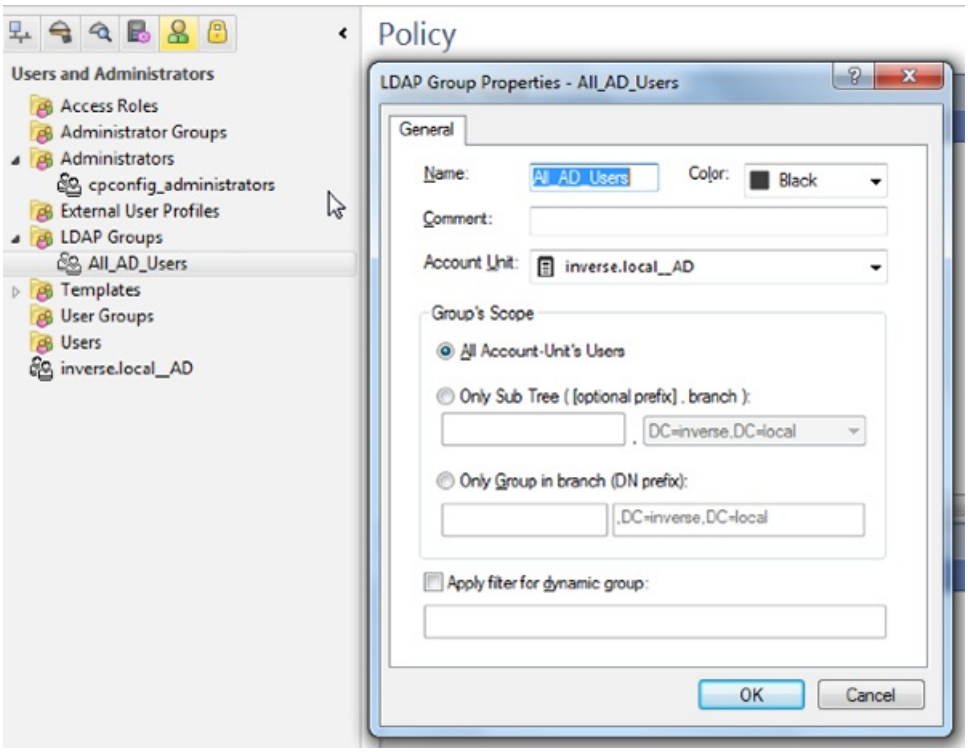
**Шаг 3.** Оставьте порт по умолчанию — 1813.

**Шаг 4.** Нажмите **OK** в обоих окнах для отправки конфигурации.

**Шаг 5.** В системе **SmartDashboard** выберите **Политика — Установить**.

## Группы LDAP

Убедитесь, что в Checkpoint созданы корректные объекты LDAP.




## Процесс верификации

Проверить работу SSO через МСЭ Checkpoint можно с помощью **SmartView Tracker** в разделе **Network & Endpoint Queries → Predefined → Identity Awareness Blade → Login Activity**.

---

ID статьи: 604
Последнее обновление: 3 июл., 2024
Обновлено от: Егоров В.
Ревизия: 1
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.0.1 -> AxelNAC. Руководство администратора -> Реализация SSO через межсетевой экран (МСЭ) -> МСЭ Checkpoint
https://docs.axel.pro/entry/604/