Аутентификация с помощью Microsoft Active Directory

В данной статье описано, как настроить аутентификацию пользователей с помощью учетных данных, которые введены в домен. При таком методе аутентификации, AxelNAC может взаимодействовать с контроллером домена для:

- проверки пользователей, подключенных по протоколу EAP-TLS на вхождение в группы домена, для последующей выдачи ролей и доступов;
- проверки учетных данных пользователей по протоколу MS-CHAPv2, для последующей аутентификации их в сети;
- осуществления входа администраторов по доменным УЗ.

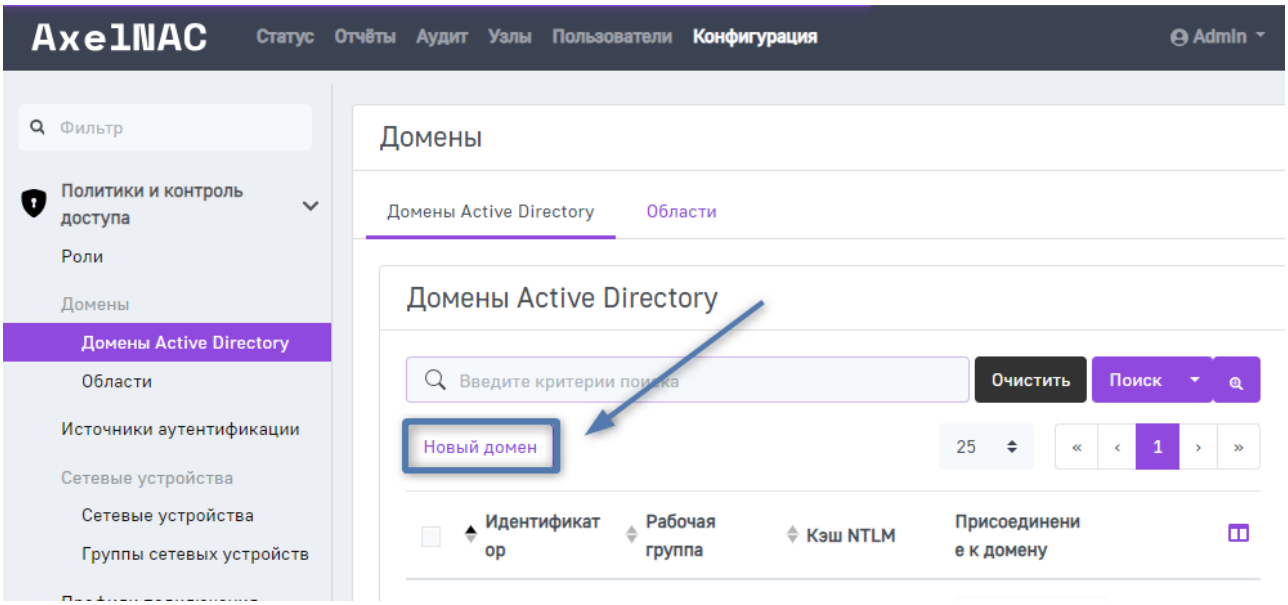
Доменная NTLM-аутентификация

Добавление AxelNAC в домен

Данный шаг необходим только для аутентификации по протоколу MS-CHAPv2. При аутентификации по протоколу EAP-TLS этот шаг можно пропустить.

Для того, чтобы ввести AxelNAC в домен выполните следующие действия:

Шаг 1. В веб-интерфейсе перейдите в раздел **Конфигурация → Политики и контроль доступа → Домены → Домены Active Directory**.



Шаг 2. Нажмите **Новый домен** и в открывшемся окне заполните информацию о домене:

- **Идентификатор** — отображается уникальный идентификатор домена;
- **Рабочая группа** — рабочая группа домена в старом синтаксисе (как в NT4);
- **DNS-имя домена** — FQDN домена (суффикс имен учетных записей);
- **Имя AxelNAC в домене** — имя, которое будет иметь учетная запись сервера в Active Directory;
- **Sticky DC** — предпочтительный контроллер домена для подключения;
- **Сервер(ы) Active Directory** — IP или DNS-имя контроллеров домена;
- **DNS-сервер(ы)** — IP-адрес DNS-сервера домена. Убедитесь, что указанный сервер имеет правильные DNS-записи для домена;
- **Структурное подразделение (OU)** — объект в Active Directory, в котором нужно создать учетную запись компьютера;

Если в пути содержится пробел, его необходимо экранировать обратной косой чертой (пример: Computers/Servers/ Unix systems). В ином случае, система не сможет найти указанный объект.

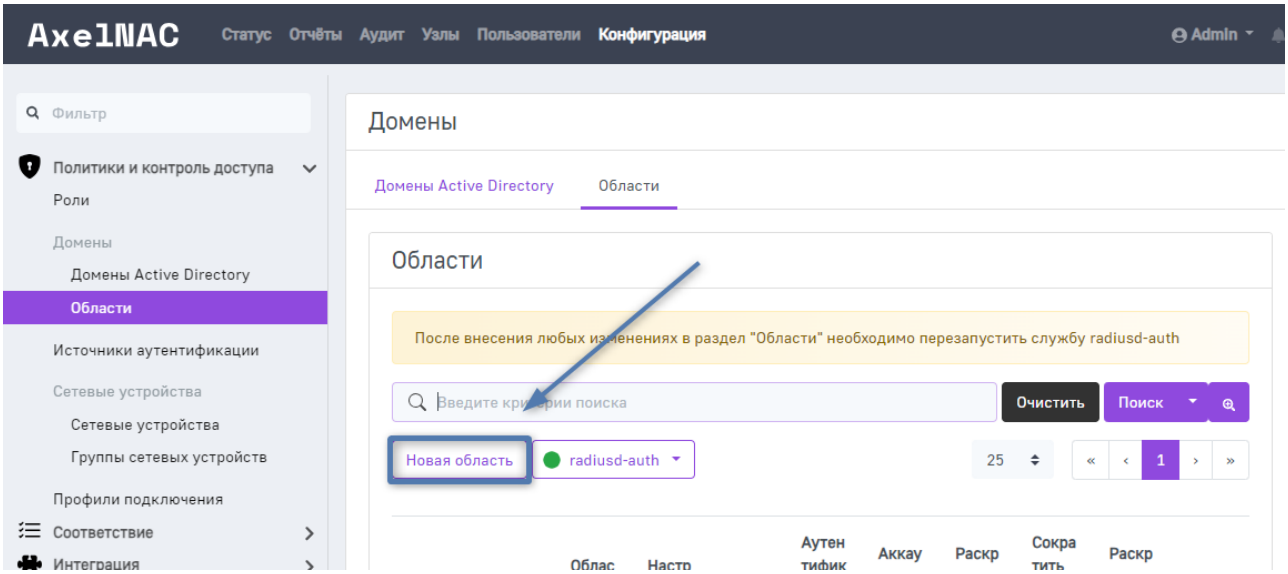
- **Использовать только NTLMv2** — включение этой опции заставляет аутентификацию NTLNM (802.1X в AD) использовать NTLM версии 2;
- **Разрешить при регистрации** — включение этой опции разрешает устройствам в сети регистрации взаимодействовать с контроллером домена.

Если используется кластер Active/Active, каждый член кластера должен присоединяться отдельно. Следуйте инструкциям, приведенным в руководстве по кластеризации AxelNAC.

Конфигурация домена, используемого по умолчанию

В случае, когда для подключения используется единственный домен, необходимо определить его, как домен по умолчанию. Для этого:

Шаг 1. Создайте доменную область в разделе **Конфигурация → Политики и контроль доступа → Домены → Области** .



Шаг 2. В открывшемся окне заполните все необходимые поля на вкладках:

- Основное:
  - **Область** — DNS-имя (FQDN) домена или рабочей группы;
  - **Область Regex** — если значение regex совпадает со значением UserName, AxelNAC будет использовать именно эту конфигурацию области.
- NTLM-аутентификация:
  - **Домен** — домен Active Directory, в который AxelNAC отправляет NTLM-запрос;
  - **eDirectory** — сервер eDirectory, который будет использоваться для аутентификации в этой области.
- Настройки EAP:
  - **EAP** — используемая конфигурация EAP.
- Прокси-сервер FreeRADIUS:
  - **Опции области** — любые опции области, которые нужно добавить в конфигурацию FreeRADIUS;
  - **RADIUS AUTH** — сервер аутентификации RADIUS, на который следует направить запрос;
  - **Тип** — тип пула домашнего сервера для аутентификации;
  - **Авторизоваться из AxelNAC** — включение этой опции определяет, передавать ли запрос в AxelNAC для получения динамического ответа или использовать атрибуты ответа удаленного прокси-сервера;
  - **RADIUS ACCT** — сервер аккаунтинга RADIUS, на который должен быть передан запрос;
  - **Тип** — тип пула домашнего сервера для аккаунтинга.
- Прокси-сервер FreeRADIUS Eduroam:
  - **Опции области Eduroam** — добавление опций Eduroam FreeRADIUS в определение области;
  - **Eduroam RADIUS AUTH** — сервер аутентификации RADIUS Eduroam, на который должен быть передан запрос;
  - **Тип** — тип пула домашнего сервера для аутентификации;
  - **Авторизоваться из AxelNAC** — включение этой опции определяет, передавать ли запрос в AxelNAC для получения динамического ответа или использовать атрибуты ответа удаленного прокси-сервера;
  - **Eduroam RADIUS ACCT** — сервер аккаунтинга RADIUS Eduroam, на который должен быть передан запрос;
  - **Тип** — тип пула домашнего сервера для аккаунтинга.
- Раскрытие:
  - **Раскрыть в портале** — включение этой опции определяет, должны ли имена пользователей, соответствующие этой области, зачищаться при использовании на портале захвата;
  - **Раскрыть в системе администрирования** — включение этой опции определяет, должны ли имена пользователей, соответствующие этой области, удаляться при использовании в интерфейсе администрирования;
  - **Раскрыть в авторизации RADIUS** — включение этой опции определяет, должны ли имена пользователей, соответствующие этой области, зачеркиваться при использовании на этапе авторизации 802.1X;
  - **Пользовательские атрибуты** — включение этой опции определяет, разрешать ли использование пользовательских атрибутов для аутентификации пользователей 802.1X (атрибуты определяются в источнике);
  - **Источник LDAP** — сервер LDAP для запроса пользовательских атрибутов;
  - **Источник LDAP для TTLS PA**P — сервер LDAP, используемый для авторизации и аутентификации по протоколу EAP/TTLS/PAP;
  - **Источник Azure AD для TTLS PAP** — источник Azure AD для аутентификации по протоколу EAP/TTLS/PAP.

Шаг 3. Перезапустите AxelNAC в разделе **Статус → Службы**.

Настройка аутентификации в нескольких доменах

Для того, чтобы реализовать аутентификацию разных групп пользователей в разных доменах, выполните следующие действия:

Шаг 1. Настройте домены в разделе **Конфигурация → Политики и контроль доступа → Домены → Домены Active**

Directory.

Шаг 2. Перейдите в раздел **Конфигурация → Политики и контроль доступа → Домены → Области** и создайте новые области — соответствующую DNS-имени домена, и соответствующую имени рабочей группы.

Шаг 3. Привяжите области созданные области к домену.

Доменная LDAP-аутентификация

Конфигурация источника аутентификации

Для того, чтобы реализовать доменную LDAP-аутентификацию, необходимо создать источник аутентификации Active Directory. Для этого выполните следующие действия:

Шаг 1. Добавьте контроллер домена Microsoft Active Directory в качестве источника аутентификации в AxelNAC. Для этого в разделе **Конфигурация → Политики и контроль доступа → Источники аутентификации** нажмите кнопку **Новый внутренний источник** и выберите **Active Directory** из выпадающего списка.

Шаг 2. В открывшемся окне заполните все необходимые поля.

Для получения дополнительной информации о полях, относящихся к среде Active Directory, воспользуйтесь инструментами Active Directory Explorer (AD Explorer) или AdsiEdit.mmc с сервера Active Directory.

Шаг 3. В созданном новом источнике аутентификации добавьте правила аутентификации с именем **catchall** без каких-либо условий. Нажмите кнопку **Добавить действие** и укажите следующие параметры:

- **Роль** — по умолчанию;
- **Срок предоставления доступа** — 5 дней.

Шаг 4. Убедитесь, что вся введенная информация верна. Для этого нажмите кнопку **Тест** справа от поля **Пароль**. Если появится сообщение с текстом "Успешно проведена валидация с IP-адрес_хоста", источник аутентификации Microsoft Active Directory настроен корректно.

Шаг 5. Сохраните новый источник аутентификации, нажав кнопку **Создать**.

Настройка профиля подключения

После того как создан источник аутентификации, необходимо настроить профиль подключения. Данная процедура необходима для того, чтобы AxelNAC знал, как обрабатывать подключение, которое поступает по проводной или беспроводной (Wi-Fi) сети.

В рассматриваемом примере будет создаваться новый профиль подключения для использования источника аутентификации Active Directory, а также для того, чтобы AxelNAC знал, что нужно автоматически регистрировать все устройства, успешно прошедшие аутентификацию с помощью 802.1X в данном профиле подключения. Для этого необходимо произвести следующую настройку:

Шаг 1. Перейдите в раздел **Конфигурация → Политики и контроль доступа → Профили подключения** и нажмите кнопку **Новый профиль подключения**.

Шаг 2. На открывшейся странице заполните поля следующим образом:

- **Имя профиля:** 8021x;
- **Описание профиля:** Проводное соединение 802.1X;
- **Активировать профиль:** Включено;
- **Регистрировать устройства автоматически:** Включено;
- **Фильтры:** Все;
- **Тип подключения:** Ethernet-EAP;
- **Источники:** Выберите созданный ранее источник аутентификации Active Directory.

Шаг 3. Сохраните изменения конфигурации, нажав **Создать**.

Настройка супликанта на клиентском устройстве

Для того, чтобы клиентское устройство могло быть подключено к серверу, необходимо настроить соединение на устройстве.

Шаг 1. Запустите в Windows сервис **Проводная автонастройка** (dot3svc) и добавьте его в автозагрузку.

Шаг 2. Откройте меню **Сетевые подключения**, затем откройте свойства сетевого интерфейса, по которому организовано подключение.

Шаг 3. На вкладке **Проверка подлинности** установите флажки для всех параметров.

Шаг 4. В поле **Метод проверки подлинности в сети** выберите значение **Microsoft: Protected EAP (PEAP)**.

Шаг 4. Нажмите на кнопку **Параметры** справа от поля выбора метода и снимите флажок с параметра **Подтверждать**

удостоверение сервера с помощью проверки сертификата.

Шаг 6. Перейдите в раздел **Настроить** и установите галочку на все параметры. Затем нажмите **OK** дважды.

Шаг 7. На вкладке **Проверка подлинности** нажмите **Дополнительные параметры**, и в поле **Указать режим проверки подлинности** установите **Проверка подлинности пользователя или компьютера**. Затем нажмите **OK**.

После этого супликант на клиентском устройстве настроен.

ID статьи: 546
Последнее обновление: 14 апр., 2025
Обновлено от: Егоров В.
Ревизия: 9
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.0.1 -> AxelNAC. Руководство администратора -> Источники аутентификации -> Аутентификация с помощью Microsoft Active Directory
https://docs.axel.pro/entry/546/