

SAML

AxeINAC поддерживает совместную работу SAML-аутентификации в Captive-портале с другими внутренними источниками для определения уровня авторизации пользователя.

Создание нового источника аутентификации SAML

Для того чтобы создать новый источник аутентификации SAML, нажмите **Новый внутренний источник** в левом верхнем углу таблицы. После этого откроется меню конфигурации нового источника.

Новый источник аутентификации SAML

1

Имя

Требуется указать имя.

2

Описание

Требуется указать Описание.

3

Идентификатор провайдера услуг

Требуется указать ID.

4

Ключ провайдера услуг (x509)

Требуется указать ключ.

5

Сертификат провайдера услуг (x509)

Требуется сертификат.

6

Идентификатор провайдера идентификационных данных

Требуется указать ID.

7

Метаданные провайдера идентификационных данных

Требуется указать метаданные.

8

Сертификат провайдера идентификационных данных (x509)

Требуется сертификат.

9

Сертификат CA провайдера идентификационных данных (x509)

Требуется сертификат.
Если Ваш провайдер идентификационных данных использует самоподписанный сертификат, укажите здесь путь к его сертификату.

10

Атрибут имени пользователя

urn:oid:0.9.2342.19200300.100.1.1

Основной SAML-атрибут, содержащий имя пользователя.

11

Источник аутентификации

Требуется указать Источник.
Источник, используемый для авторизации (сопоставление правил).

Создать

Сбросить

Отмена

В данном меню доступны следующие настройки:

- Имя** — имя источника аутентификации, которое будет отображаться в таблице со списком всех источников аутентификации. Задается при создании источника и не может быть изменено в дальнейшем;
- Описание** — описание источника аутентификации, которое будет отображаться в списке существующих источников аутентификации;
- Идентификатор провайдера услуг** — идентификатор провайдера услуг. Убедитесь, что он соответствует конфигурации провайдера идентификационных данных;
- Ключ провайдера услуг (x509)** — поле для загрузки закрытого ключа, который будет использоваться AxeINAC для подписи своих сообщений провайдеру идентификационных данных;
- Сертификат провайдера услуг (x509)** — поле для загрузки сертификата, связанного с указанным выше ключом;
- Идентификатор провайдера идентификационных данных** — идентификатор провайдера идентификационных данных;

7. **Метаданные провайдера идентификационных данных** — поле для загрузки файла метаданных;
8. **Сертификат провайдера идентификационных данных (x509)** — поле для загрузки сертификата провайдера идентификации;
9. **Сертификат CA провайдера идентификационных данных (x509)** — поле для загрузки сертификата CA провайдера идентификации;
10. **Атрибут имени пользователя** — основной SAML-атрибут, содержащий имя пользователя, который возвращает провайдер идентификационных данных. По умолчанию можно использовать значение **SimpleSAMLphp**. Точный параметр необходимо уточнить в документации SAML-провайдера;
11. **Источник аутентификации** — источник, который будет использоваться для сопоставления имени пользователя с определенными в нем правилами. Это позволяет задать роль и продолжительность доступа пользователя.

Файлы сертификатов, ключей и метаданных могут быть загружены напрямую из веб-интерфейса. Для этого нажмите на значок загрузки файла слева от поля.

Для того чтобы создать новый источник, заполните параметры конфигурации и нажмите **Создать**. Чтобы сбросить введенные параметры на стандартные значения, нажмите **Сбросить**. Для возвращения на предыдущую страницу без сохранения выполненных на странице действий, нажмите **Отменить**.

ID статьи: 703

Последнее обновление: 15 июл., 2025

Обновлено от: Ильина В.

Ревизия: 3

База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.0.1 -> AxelNAC. Руководство по использованию веб-интерфейса -> Меню «Конфигурация» -> Раздел «Политики и контроль доступа» -> Страница «Источники аутентификации» -> Вкладка «Внутренние источники» -> SAML

<https://docs.axel.pro/entry/703/>