

Глава 1. Что такое источники аутентификации

Когда клиент успешно проходит аутентификацию — по сертификату, логину и паролю, MAC-адресу или через портал, — AxeINAC должен определить, какие права доступа необходимо предоставить этому пользователю или устройству. Для этого используется **источник аутентификации**.

Источник аутентификации — это компонент, который выполняет проверку данных о пользователе после прохождения аутентификации и возвращает AxeINAC информацию о назначаемой роли, политике доступа, сроке действия сессии и других параметрах подключения. Он связывает результат проверки личности с конкретными сетевыми правами и параметрами, которые будут применены при доступе к инфраструктуре.

Внутренние и внешние источники

Внутренние источники используются для интеграции с корпоративной инфраструктурой и системами каталогов. Они считаются внутренними, так как работают внутри инфраструктуры организации.

Внешние источники — это методы, в которых аутентификация выполняется за пределами корпоративной инфраструктуры. Эти механизмы полезны, когда требуется выдать временный или гостевой доступ.

Правила аутентификации

Для успешной авторизации пользователь должен соответствовать хотя бы одному правилу аутентификации. Правила аутентификации определяются в каждом источнике аутентификации, каждое правило аутентификации может обладать собственным набором критерии соответствия.

Например, правила могут учитывать:

- тип подключения (802.1X, VPN, Captive-portal);
- атрибуты учетной записи в каталоге (например, группа в AD);
- атрибуты сертификата x509;
- подключение из SSID;
- MAC-адрес или принадлежность к профилю устройства.

В случае, если подключаемое устройство не соответствует ни одному из правил аутентификации, будут применены настройки на порту.

Правила администрирования

Помимо правил аутентификации, в некоторых источниках аутентификации применяются **правила администрирования**. Они определяют, как администраторы проходят проверку при доступе к веб-интерфейсу AxeINAC и к сетевому оборудованию через RADIUS.

Зачем все это нужно

Источники аутентификации в AxeINAC обеспечивают проверку пользователей и устройств, назначение ролей и применение сетевых параметров. Внутренние источники работают с корпоративными каталогами и протоколами, внешние — с публичными сервисами и механизмами подтверждения личности. Роль, назначенная по результатам проверки, определяет VLAN и политику доступа, а правила аутентификации описывают требования, которым должно соответствовать устройство.

Так AxeINAC объединяет аутентификацию, определение параметров доступа и управление доступом в единую систему.

ID статьи: 1444

Последнее обновление: 15 дек., 2025

Обновлено от: Ильина В.

Ревизия: 3

База знаний AxeINAC -> Обучающие материалы -> Обучающие курсы -> Конфигурация сетевых соединений -> Раздел 2.

Источники аутентификации -> Глава 1. Что такое источники аутентификации

<https://docs.axel.pro/entry/1444/>