

Расширенный контроль доступа для входа администратора

По умолчанию в веб-интерфейсе AxelNAC разрешен вход по имени пользователя/паролю через любой внутренний источник аутентификации (локальная база данных, LDAP и др.). Если для веб-интерфейса необходимо использовать другие типы аутентификации (например SAML, многофакторную аутентификацию и др.), то для аутентификации администраторов можно использовать все возможности Captive-портала.

Базовая конфигурация

Для того, чтобы выполнить базовую настройку расширенной аутентификации администратора, выполните следующие действия:

Шаг 1. Перейдите в раздел **Конфигурация → Настройки системы → Вход под учетной записью администратора**.

Шаг 2. Активируйте параметр **Статус SSO**. Это необходимо для того, чтобы активировать SSO для входа в веб-интерфейс.

Шаг 3. Если нужно принудительно использовать политику SSO для входа в систему (т. е. отключить имя пользователя/пароль), следует отключить опцию **Разрешить аутентификацию с помощью учетных данных**.

Дополнительно может потребоваться настройка базового адреса SSO Base URL, если доступ к Captive-порталу AxelNAC должен выполняться под именем, отличным от того, которое задано в значениях **Имя хоста** и **Домен**, которые расположены в разделе **Основные настройки**.

Шаг 4. Настройте профиль подключения для аутентификации администраторов. Для этого в разделе **Конфигурация → Политики и контроль доступа → Профили подключения** нажмите **Новый профиль подключения**.

Шаг 5. На открывшейся странице заполните поля следующим образом:

- **Корневой порталный модуль:** Default admin SSO policy;
- **Фильтр:** URI со значением /admin-ssu;
- **Источники:** источники аутентификации, которые должны использоваться для входа в систему.

Шаг 6. Перезапустите службы api-frontend и httpd.portal.

После этого, на странице входа в веб-интерфейс должна отобразиться новая опция с названием Single Sign On. Этот текст можно изменить в разделе конфигурации **Вход под учетной записью администратора**.

Для аутентификации администраторов с помощью этого процесса можно использовать любой механизм аутентификации, применяемый на портале (SAML, Akamai MFA, TOTP и др.). Для настройки каждой функции в профиле подключения, который используется для аутентификации администраторов, обратитесь к соответствующему разделу руководства.

Расширенная конфигурация

Конфигурацию политики доступа на Captive-портале при аутентификации администраторов можно изменить. Модули портала делают этот процесс очень гибким и настраиваемым.

В разделе **Конфигурация → Расширенные настройки доступа → Модули портала** можно изменить SSO-политику по умолчанию (Default admin SSO policy). Также можно создать собственную политику, затем настроить ее в профиле подключения, который аутентифицирует администраторов.

Информация о том, как дополнительно настроить портал захвата, приведена в разделе [Расширенная конфигурация Captive-портала](#).

ID статьи: 66

Последнее обновление: 26 июн., 2024

Обновлено от: Егоров В.

Ревизия: 1

База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 1.0.0 -> AxelNAC. Руководство администратора -> Источники аутентификации -> Расширенный контроль доступа для входа администратора

<https://docs.axel.pro/entry/66/>