Интеграция с TOTP MFA

В данной статье описан процесс интеграции системы многофакторной аутентификации TOTP MFA с AxelNAC.

Создание источника многофакторной аутентификации

Для настройки источника многофакторной аутентификации TOTP MFA выполните следующие действия в веб-интерфейсе AxelNAC:

Шаг 1. Перейдите в раздел **Конфигурация → Интеграция → Многофакторная аутентификация (MFA)** , нажмите **Новая многофакторная аутентификация (MFA)** и в выпадающем списке выберите значение **TOTP**.

Шаг 2. В открывшемся окне заполните все необходимые поля:

- **Имя** — название источника многофакторной аутентификации;
- **Метод RADIUS OTP** — метод использования одноразового пароля, который будет использоваться в RADIUS;
- **Разделитель символов** — символ, используемый для разделения пароля и OTP при выборе метода RADIUS Strip OTP;
- **Продолжительность кеширования** — количество времени, в течение которого AxelNAC будет хранить MFA-информацию пользователя (используется для полей **Strip OTP** и **Second Password Field**, поскольку AxelNAC работает с несколькими запросами RADIUS);
- **Длительность кэширования при валидации после MFA** — срок хранения данных о подтверждении пользователем MFA-аутентификации (представляет собой время между подтверждением на портале и последующим запросом RADIUS).

Ассоциирование источника аутентификации

Многофакторная аутентификация запускается правилом аутентификации во внутреннем источнике. Для этого необходимо создать правило с условием типа memberOf равно cn=otp_user,dc=example,dc=ru и назначить одно из действий:

- **Инициировать RADIUS MFA:** если требуется срабатывание в RADIUS;
- **Инициировать портальную MFA:** если требуется срабатывание в Portal.

Портальная многофакторная аутентификация

Профиль подключения

Предварительно должен иметься профиль подключения, использующий внутренний источник, в котором определено правило аутентификации **Инициировать портальную MFA**, а также должен использоваться модуль корневого портала **Многофакторная аутентификация (MFA)**.

Портал AxelNAC

После входа в портал и регистрации на портале появится QR-код, который нужно отсканировать с помощью устройства (например, Akamai/Goggle/Microsoft/DUO Authenticator). В результате будет сконфигурирована учетная запись с автоматически назначенным именем пользователя и PIN-кодом OTP.

После этого OTP можно будет использовать на портале для регистрации своего устройства.

Многофакторная аутентификация RADIUS

Многофакторная аутентификация с помощью RADIUS зависит от возможностей провайдера MFA, а также от клиента RADIUS.

Простой клиент RADIUS

В этом случае в RADIUS-запросе передаются только имя пользователя и пароль, а единственным доступным методом является push-уведомление. После аутентификации пользователя на его телефон будет отправлено push-уведомление, которое необходимо подтвердить для получения разрешения.

Простой RADIUS-клиент с паролем

В этом сценарии пользователю передается имя пользователя и пароль, но для получения кода пароль может быть разделен специальным символом.

Код OTP (123456).

Код OTP — это код, который пользователь может прочитать на своем устройстве (меняется каждые 30 с).

Push-код (push).

Такой код может иметь вид **push** и **pushx** (**x** — идентификатор телефона в списке, если их несколько). При работе с кодом вида **push**, код будет отправлен на телефон, установленный по умолчанию. При работе с кодом вида **pushx**, **push1** отправит push-код на первый телефон, **push2** — на второй, и так далее. Для предоставления доступа к сети пользователь должен выполнить подтверждение входа на своём телефоне.

SMS-код (sms).

Такой код может иметь вид **sms** и **smsx** (**x** — идентификатор номера телефона в списке, если их несколько) При работе с кодом вида **sms**, код будет отправлен на номер телефона, установленный по умолчанию. При работе с кодом вида **smsx**, **sms1** отправит SMS-код на первый номер телефона, **sms2** — на второй, и так далее. После отправки SMS-сообщений RADIUS-запрос на подключение будет отклонен, клиент RADIUS снова запросит учетные данные. После получения кода по SMS пользователь должен пройти повторную аутентификацию: указать имя пользователя и пароль, а также добавить SMS-код (например, **password,smscode**).

Простой клиент RADIUS со вторым паролем

В этом сценарии VPN-клиент представляет страницу входа в систему с одним именем пользователя, паролем и дополнительным полем пароля. Во втором поле пароля можно задать несколько параметров, например:

Код OTP (123456).

Код OTP — это код, который пользователь может прочитать на своем устройстве (меняется каждые 30 с).

Push-код (push).

Такой код может иметь вид **push** и **pushx** (**x** — идентификатор телефона в списке, если их несколько). При работе с кодом вида **push**, код будет отправлен на телефон, установленный по умолчанию. При работе с кодом вида **pushx**, **push1** отправит push-код на первый телефон, **push2** — на второй, и так далее. Для предоставления доступа к сети пользователь должен выполнить подтверждение входа на своём телефоне.

SMS-код (sms).

Такой код может иметь вид **sms** и **smsx** (**x** — идентификатор номера телефона в списке, если их несколько) При работе с кодом вида **sms**, код будет отправлен на номер телефона, установленный по умолчанию. При работе с кодом вида **smsx**, **sms1** отправит SMS-код на первый номер телефона, **sms2** — на второй, и так далее. После отправки SMS-сообщений RADIUS-запрос на подключение будет отклонен, клиент RADIUS снова запросит учетные данные. После получения кода по SMS пользователь должен пройти повторную аутентификацию: указать имя пользователя и пароль, а также установить полученный по SMS код в поле 2-го пароля.

ID статьи: 597
Последнее обновление: 17 июл., 2024
Обновлено от: Михалева А.
Ревизия: 3
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.0.1 -> AxelNAC. Руководство администратора -> Интеграция с системами многофакторной аутентификации (MFA) -> Интеграция с TOTP MFA
https://docs.axel.pro/entry/597/