

Akamai MFA

В данной статье описано, как настроить интеграцию с Akamai MFA.

Для настройки перейдите в раздел **Конфигурация → Интеграция → Многофакторная аутентификация (MFA)**, нажмите **Новая многофакторная аутентификация (MFA)** и в выпадающем списке выберите **Akamai**.

Новая многофакторная аутентификация (MFA) Akamai

×

| | | | |
|--|---|--|----------------|
| 1 | Имя | <input type="text"/> | ! |
| Требуется указать имя. | | | |
| 2 | ID приложения Akamai MFA | <input type="text"/> | ! |
| Требуется указать ID приложения. | | | |
| 3 | Ключ подписи Akamai MFA | <input type="text"/> ***** | ! |
| Требуется указать Ключ. | | | |
| 4 | Верификационный ключ Akamai MFA | <input type="text"/> ***** | ! |
| Требуется указать Ключ. | | | |
| 5 | Хост Akamai MFA | <input type="text"/> mfa.akamai.com | |
| 6 | Callback URL для переадресации пользователя обратно в AxeINAC | <input type="text"/> http://axelnac_portal_url/mfa | |
| 7 | Метод RADIUS OTP | <input type="text"/> Push | ▼ |
| Укажите метод, который будет использоваться в RADIUS для запуска OTP. | | | |
| 8 | Разделитель символов | <input type="text"/> , | |
| Символ, которым разделяются пароль и код при аутентификации по протоколу RADIUS. | | | |
| 9 | Продолжительность кэширования | <input type="text"/> 60 | секунд |
| Длительность, которая используется для кэширования информации MFA. Она должна примерно соответствовать времени, в течение которого пользователь должен завершить аутентификацию. | | | |
| 10 | Длительность кэширования при валидации после MFA | <input type="text"/> 5 | секунд |
| Срок хранения данных о подтверждении пользователем MFA-автентификации (представляет собой время между подтверждением на портале и последующим запросом RADIUS). | | | |

Создать Сбросить Отмена

В данном меню доступны следующие настройки:

- Имя** — имя конфигурации MFA;
- ID приложения Akamai MFA** — App ID, предоставляемый Akamai;
- Ключ подписи Akamai MFA** — ключ подписи, предоставляемый Akamai;
- Верификационный ключ Akamai MFA** — ключ проверки, предоставляемый Akamai;
- Хост Akamai MFA** — хост (по умолчанию mfa.akamai.com);
- Callback URL для переадресации пользователя обратно в AxeINAC** — параметр, который используется при срабатывании MFA на портале после аутентификации на Akamai Bind v2. Он перенаправляет на этот URL для возврата на портал AxeINAC. Этим значением должно быть FQDN портала с /mfa в конце строки (<https://portal.example.ru/mfa>);
- Метод RADIUS OTP** — метод использования одноразового пароля, который будет использоваться в RADIUS;
- Разделитель символов** — символ, который разделяет пароль и код при аутентификации по протоколу RADIUS;
- Продолжительность кэширования** — время, в течение которого AxeINAC будет хранить MFA-информацию пользователя. Параметр используется для полей **Strip OTP** и **Second Password**, так как AxeINAC работает с несколькими запросами RADIUS;
- Длительность кэширования при валидации после MFA** — время, в течение которого AxeINAC хранит данные о прохождении пользователем MFA-автентификации. Параметр определяет интервал между подтверждением на портале и последующим запросом RADIUS.

Для того чтобы добавить новую конфигурацию MFA, 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: 1366

Последнее обновление: 6 нояб., 2025

Обновлено от: Михалева А.

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 «Интеграция» -> Страница «Многофакторная аутентификация (MFA)» -> Akamai MFA

<https://docs.axel.pro/entry/1366/>