

NAICE

Содержание

Главная	1
Виджеты RADIUS	6
Виджеты TACACS+	20
Виджеты SMS	34
Мониторинг	37
RADIUS	37
Журнал подключений	37
Активные RADIUS-сессии	41
TACACS+	46
Журнал подключений	46
Учёт команд (accounting)	50
Система	53
Системные события	53
Список системных событий	56
Маршруты событий	72
Пользователи и устройства	85
Пользователи системы	85
Учетные записи	85
Роли	104
Сетевые ресурсы	119
Устройства	119
Группы устройств	131
Профили устройств	144
Управление идентификацией	153
Пользователи сети	153
Группы пользователей сети	166
Эндпоинты	177
Группы эндпоинтов	192
Внешние источники идентификации	204
Цепочки идентификаций	231
Доступ к сети	237

Элементы политик	237
Профили авторизации	237
Разрешенные протоколы	241
Условия	245
Словари	257
Лимит RADIUS-сессий	259
Политики RADIUS	262
Политики аутентификации и авторизации	269
Профилирование	275
Условия профилирования	275
Политики профилирования	281
Логические профили	292
Гостевые порталы	297
Гостевые эндпоинты	297
Пользователи портала	300
Конструктор порталов	305
Доступ к оборудованию	316
Элементы политик	237
Условия	316
Наборы команд TACACS+	328
Профили TACACS+	342
Политики TACACS+	346
Настройка политик аутентификации и авторизации	352
Шлюзы уведомлений	359
Управление шлюзами	359
HTTP/HTTPS	363
SMTP	367
Настройки системы	370

Система	53
Общие настройки	370
Сервисы	371
RADIUS	371
TACACS+	373
Журнал событий	374
Лицензирование	374
Подключение к ELM	374
Безопасность и доступ	376
Вход в систему	377
Парольные политики	382
Политика блокировки	384
Двухфакторная аутентификация	387
Взаимодействие с Active Directory	387
Хранилище сертификатов	391
Доверенные сертификаты	391
Серверные сертификаты	398
Решение проблем	398
Логи	399
Узлы	400
Лицензирование	401
Пользовательское соглашение	416
Настройки аккаунта	420

Главная

Описание

Начальная страница системы NAICE представляет собой дашборд, содержащий набор виджетов. Виджеты отображают ключевые показатели работы системы, предоставляя сводную информацию о ее текущем состоянии за последние 24 часа. Реализовано автоматическое обновление данных для всех виджетов с интервалом 2 минуты.

Особенности работы с дашбордом:

- Конфигурация набора виджетов сохраняется индивидуально для каждого пользователя системы;
- Все изменения в расположении и составе набора виджетов применяются только к текущему пользователю системы;
- Система автоматически сохраняет настройки между сеансами работы.

Основные элементы страницы:

- **Панель управления** - расположена в верхней части интерфейса, содержит основные элементы управления дашбордом;
- **Набор виджетов** - настраиваемое рабочее пространство, содержащее информационные виджеты с ключевыми метриками системы.

Просмотр панели дашборда

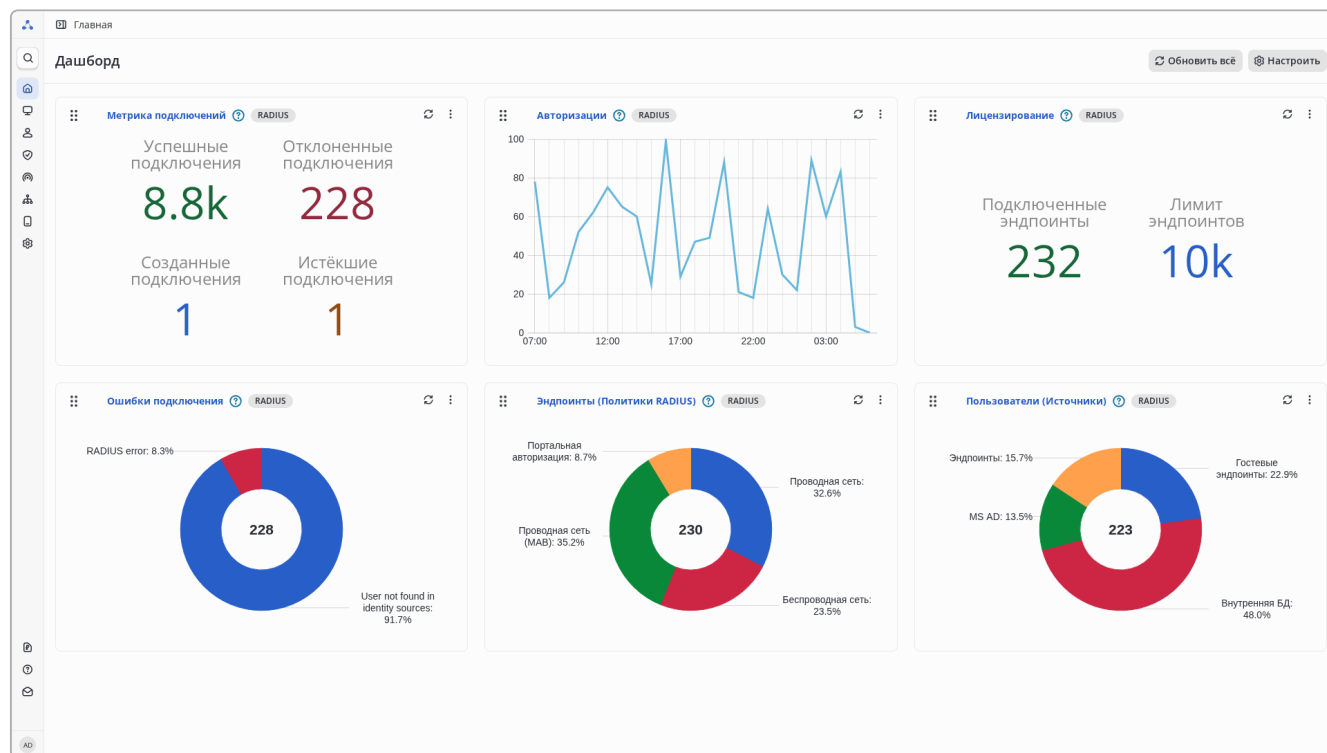


Рисунок 1. Панель управления дашбордом и виджеты, отображаемые на нем

Элементы управления дашбордом:

-  Обновить всё - Обновить данные для всех виджетов, представленных на дашборде.
-  Настроить - Открыть окно настройки панели дашборда.

Каждый виджет состоит из следующих элементов управления:

-  - Служит для изменения порядка виджетов.
- [Авторизации](#) - Наименование виджета. Является гиперссылкой на родительскую страницу.
- RADIUS - тег виджета. Обозначает к какой части функционала относится виджет.
-  - Краткая информация о виджете.
-  - Обновить данные для данного виджета.
-  - Панель действий над виджетом (например, удалить).
- Область визуализации данных в заданном формате отображения.

Настройка отображаемых виджетов на дашборде

Чтобы выбрать виджеты, которые будут отображаться на дашборде, нажмите на  Настроить , после чего откроется окно **Настройки панели дашборда**:

Настройки панели дашборда

Все

RADIUS

TACACS+

CMC

Выбрать все

☐ Активные RADIUS-сессии

ab RADIUS

☒ Авторизации

≈ RADIUS

☐ Эндпоинты (Группы)

⊙ RADIUS

☒ Эндпоинты (Политики RADIUS)

⊙ RADIUS

☐ Эндпоинты (Политики профилирования)

⊙ RADIUS

☐ Устройства (Тип)

▮ RADIUS

☐ Устройства (Локации)

▮ RADIUS

☒ Пользователи (Источники)

⊙ RADIUS

☒ Лицензирование

ab RADIUS

☒ Ошибки подключения

⊙ RADIUS

☐ Всего эндпоинтов

ab RADIUS

☒ Метрика подключений

ab RADIUS

☐ Наборы политик

⊙ RADIUS

☐ Аккаунтинг

≈ TACACS

☐ Авторизации

≈ TACACS

Сбросить

Отмена

Сохранить

Рисунок 2. Окно настройки панели дашборда

Окно **Настройки панели дашборда** содержит следующие элементы управления:

- ☐ - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (добавления или удаления).
- ≈ - Тип отображения данных виджета. Поддерживаются 4 типа отображения данных - график, гистограмма, круговая диаграмма и метрика.
- "Авторизации" - Наименование виджета.
- RADIUS - тег виджета.
- Поле поиска виджетов.

Сбросить - Вернуться к стандартному набору виджетов.

Чтобы добавить или удалить виджет с дашборда, выберите его с помощью чекбокса и нажмите кнопку **Сохранить**. Виджеты с отмеченными чекбоксами будут отображаться на дашборде.

Поиск виджетов

Для более удобной настройки и выбора отображаемых виджетов они сгруппированы на секции, в зависимости от того, к какой части функционала они относятся. Также для большего удобства реализован поиск виджетов по названию.

Настройки панели дашборда

☐ TACACS+ пакеты (Тип)

☐ TACACS+ профили

☐ TACACS+ наборы команд

☐ TACACS+ сессии

☐ TACACS+ аккаунтинг

ab

TACACS

⊙

TACACS

⊙

TACACS

ab

TACACS

ab

TACACS

Сбросить

Отмена

Сохранить

Рисунок 3. Поиск виджетов по названию

Стандартный набор виджетов

При первом входе в систему NAICE по умолчанию отображается **стандартный набор виджетов**.

Стандартный набор виджетов - это предустановленная конфигурация дашборда с виджетами, которая отображается на начальной странице при первом входе в систему NAICE. Данный набор содержит наиболее востребованные виджеты для быстрого понимания текущего состояния системы.

Стандартный набор виджетов можно вернуть с помощью кнопки "Сбросить" в окне [Настройки панели дашборда](#).

Стандартный набор включает в себя следующие виджеты:

- RADIUS Метрика подключений;
- RADIUS Авторизации;
- RADIUS Лицензирование;
- RADIUS Ошибки подключения;
- RADIUS Эндпоинты (Политики доступа);
- RADIUS Пользователи (Источники);

Типы виджетов

Виджеты с типом отображения — График

Функциональные возможности:

- Возможность навигации по графику с помощью клика для детального изучения данных.
- Изменение масштаба и выбор временного диапазона с использованием функции прокрутки.
- При наведении курсора на точку графика отображается количество устройств, а также всплывающая подсказка с указанием времени и даты.
- Возврат к исходному виду отображения по умолчанию осуществляется с помощью соответствующей кнопки в правом верхнем углу виджета.

Виджеты с типом отображения — Метрика

Функциональные возможности:

- Отображение ключевых числовых показателей в компактном формате.
- Поддержка отображения нескольких метрик одновременно.
- Информация представлена в виде чисел, что обеспечивает быстрое восприятие данных.

Виджеты с типом отображения — Гистограмма

Функциональные возможности:

-

Каждый сегмент данных сопровождается названием, расположенным слева, которое соответствует последнему элементу вложенности в группе.

- Значение отображается справа от сегмента данных.
- При наведении курсора на сегмент отображается всплывающая подсказка с подробной информацией об этой области данных в формате - "Полная вложенность от последней дочерней до родительской группы: число".
- Количество отображаемых данных в гистограмме ограничено 10 сегментами.
- Предусмотрен дополнительный сегмент "Другое", содержащий агрегированные данные, не вошедшие в топ-10.

Виджеты с типом отображения — Круговая диаграмма

Функциональные возможности:

- Каждый сегмент данных сопровождается описанием в формате - Название: %.
- При наведении курсора на сегмент отображается всплывающая подсказка с подробной информацией об этой области данных в формате - Название: % - число.
- Количество отображаемых данных в гистограмме ограничено 10 сегментами.
- Предусмотрен дополнительный сегмент "Другое", содержащий агрегированные данные, не вошедшие в топ-10.

Виджеты RADIUS

Список доступных виджетов

Виджет	Тип отображения данных	Краткое описание виджета
Активные RADIUS-сессии	Метрика	Количество активных RADIUS-сессий
Авторизации	График	Количество авторизаций за последние сутки по часам
Лицензирование	Метрика	Текущее количество подключённых эндпоинтов и максимально разрешённое согласно лицензии
Метрика Подключений	Метрика	Количество успешных, отклоненных, созданных и истёкших подключений за последние сутки
Метрика Всего эндпоинтов	Метрика	Общее количество изученных эндпоинтов
Устройства (Тип)	Гистограмма	Количество сетевых устройств, через которые происходило подключение клиента, по типам сетевых устройств

Виджет	Тип отображения данных	Краткое описание виджета
Устройства (Локации)	Гистограмма	Количество сетевых устройств, через которые происходило подключение клиента, по месторасположению сетевых устройств
Эндпоинты (Группы)	Круговая диаграмма	Количество изученных эндпоинтов, проходивших авторизацию за последние сутки, по группам
Эндпоинты (Политики профилирования)	Круговая диаграмма	Количество изученных эндпоинтов, проходивших авторизацию за последние сутки, по политикам профилирования
Эндпоинты (Политики RADIUS)	Круговая диаграмма	Количество изученных эндпоинтов, проходивших авторизацию за последние сутки, по наборам политик
Наборы политик	Круговая диаграмма	Текущее количество срабатываний наборов политик.
Ошибки подключения	Круговая диаграмма	Ошибки подключения клиентов за последние сутки.
Пользователи (Источники)	Круговая диаграмма	Количество уникальных пользователей по источникам их идентификации, проходивших авторизацию за последние сутки
RADIUS-сессии	Метрика	Общее количество сессий за весь период хранения данных. Период хранения отображается в днях.



Каждый виджет имеет определенный тип отображения данных. Изменить тип отображения данных нельзя.



Виджеты с типом отображения "метрика" и "круговая диаграмма" отображают большие числа в сокращенном формате (например, 40k вместо 40123). Точное значение метрики отображается в подсказке при наведении на значение.

Виджет "Активные RADIUS-сессии"

Виджет отображает общее количество активных пользовательских сессий. Все активные сессии можно увидеть в разделе "Мониторинг" [Активные сессии](#)

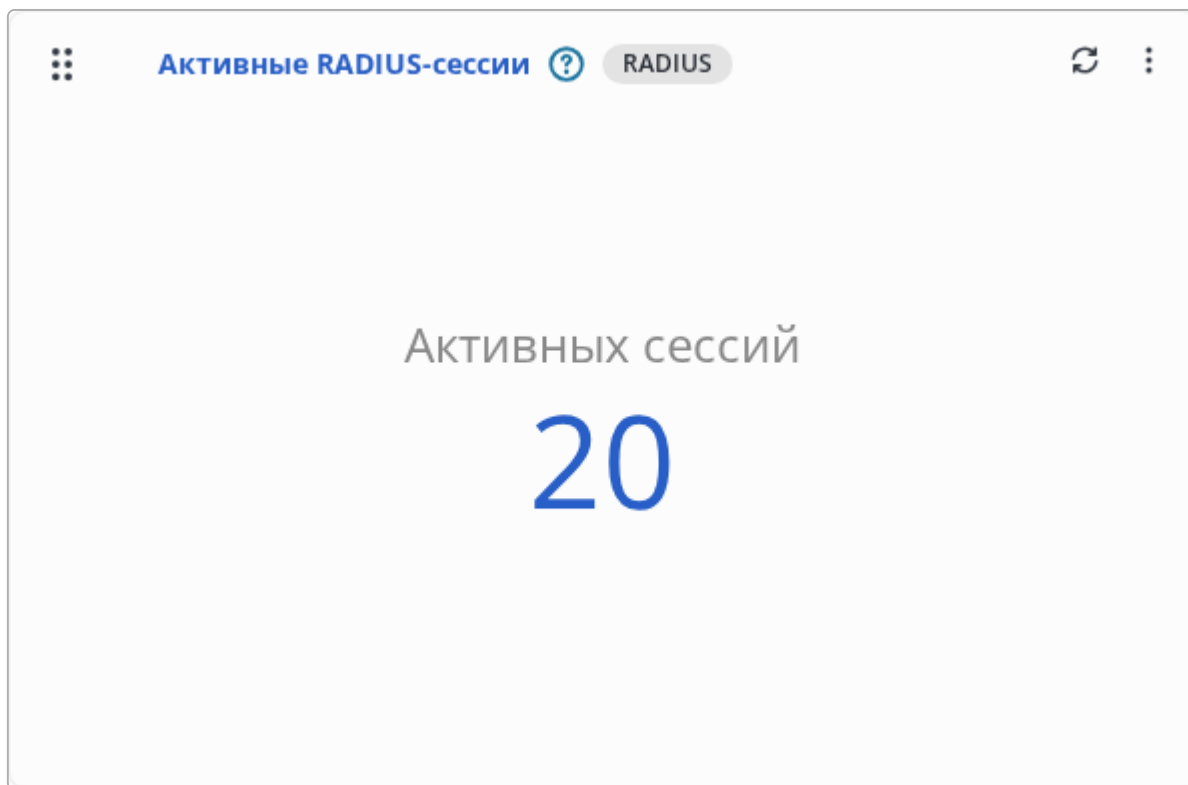


Рисунок 4. Виджет "Активные RADIUS-сессии"

Виджет "Авторизации"

Виджет отображает данные о количестве попыток авторизаций (как успешных, так и отклоненных) в системе за последние сутки по часам, на основе данных [Журнал подключений](#).

Информация визуализирована в виде временного графика, где:

- По вертикальной оси (Y) отображается количественный показатель попыток авторизации;
- По горизонтальной оси (X) представлена временная шкала по часам.

Виджет позволяет оперативно отслеживать активность пользователей, выявлять периоды повышенной активности.

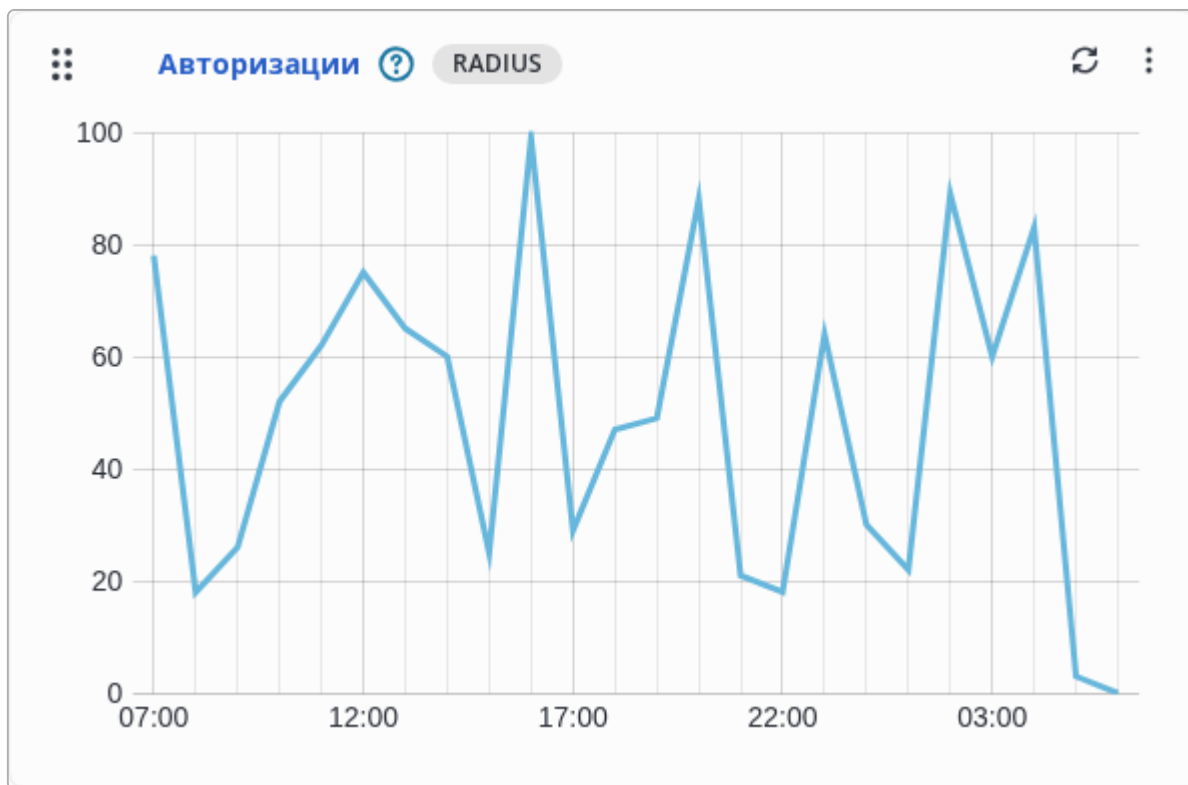


Рисунок 5. Виджет "Авторизации"

Виджет "Метрика подключений"

Виджет отображает данные о количестве успешных и отклонённых подключений за последние сутки на основании данных из [Журнал подключений](#).

Виджет позволяет отследить соотношение состояния сессий (успешных и отклоненных попыток) за сутки.



Рисунок 6. Виджет "Метрика подключений"

Виджет "Лицензирование"

Виджет отображает сводную информацию о [лицензии](#):

- **Подключенные эндпоинты** - Текущее количество успешно авторизованных уникальных эндпоинтов за последние сутки;
- **Лимит эндпоинтов** - Максимально допустимое количество эндпоинтов согласно лицензии.

Виджет позволяет отследить приближение к лимиту по количеству подключенных эндпоинтов.



Рисунок 7. Виджет "Лицензирование"

Виджет "Всего эндпоинтов"

Виджет отображает общее количество изученных эндпоинтов в системе NAICE на основании данных из таблицы [Эндпоинтов](#).

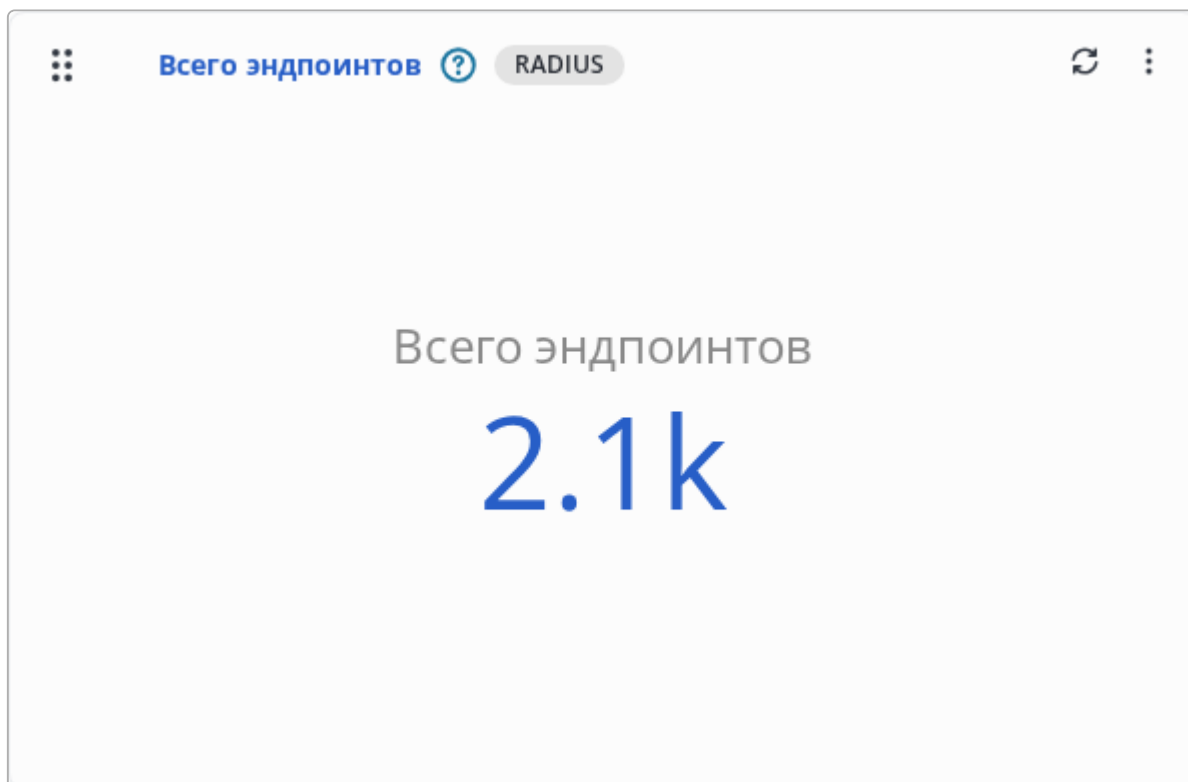


Рисунок 8. Виджет "Всего эндпоинтов"

Виджет "Устройства (Тип)"

Виджет отображает количество сетевых устройств, через которые происходило подключение клиента, по типам сетевых устройств.

Группы устройств, используемые для классификации, берутся из раздела [Группы устройств](#).

Виджет позволяет отследить тенденции востребованности устройств с привязкой к их типу.

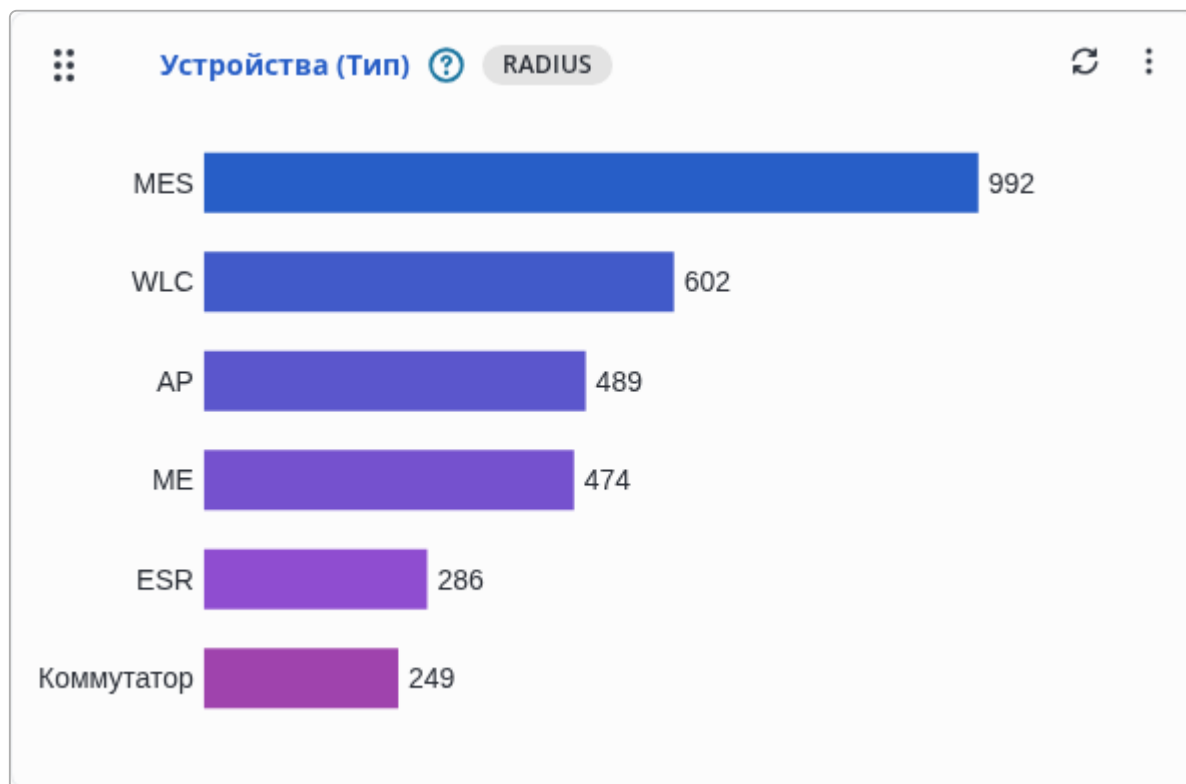


Рисунок 9. Виджет "Устройства (Тип)"

Виджет "Устройства (Локации)"

Виджет отображает количество сетевых устройств, через которые происходило подключение клиента, по месторасположению сетевых устройств.

Группы устройств, используемые для классификации, берутся из раздела [Группы устройств](#).

Виджет позволяет отследить тенденции востребованности устройств с привязкой к их месторасположению.

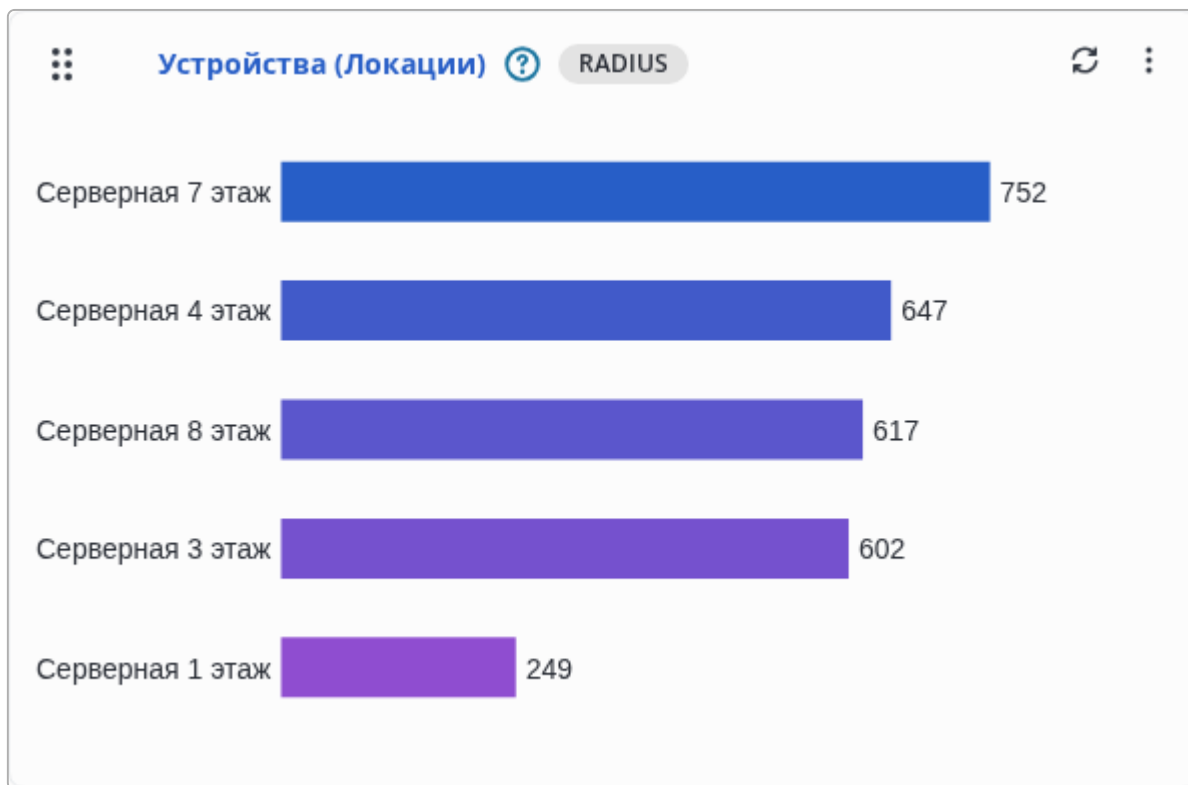


Рисунок 10. Виджет "Устройства (Локации)"

Виджет "Эндпоинты (Группы)"

Виджет отображает количество **изученных** эндпоинтов, проходивших авторизацию за последние сутки, по [Группам эндпоинтов](#) полученным в результате профилирования.

Данные для виджета берутся из таблицы [Эндпоинты](#) и [Журнал подключений](#).

Учитывается последняя группа при переподключении.



- Случайно сгенерированные MAC-адреса не учитываются.
- Известным считается эндпоинт, который присутствует в таблице [Эндпоинты](#).
- При автоматическом режиме новые эндпоинты, добавляемые через RADIUS-запросы, отображаются на виджете только после переподключения, после того как система занесла их в таблицу [Эндпоинты](#).

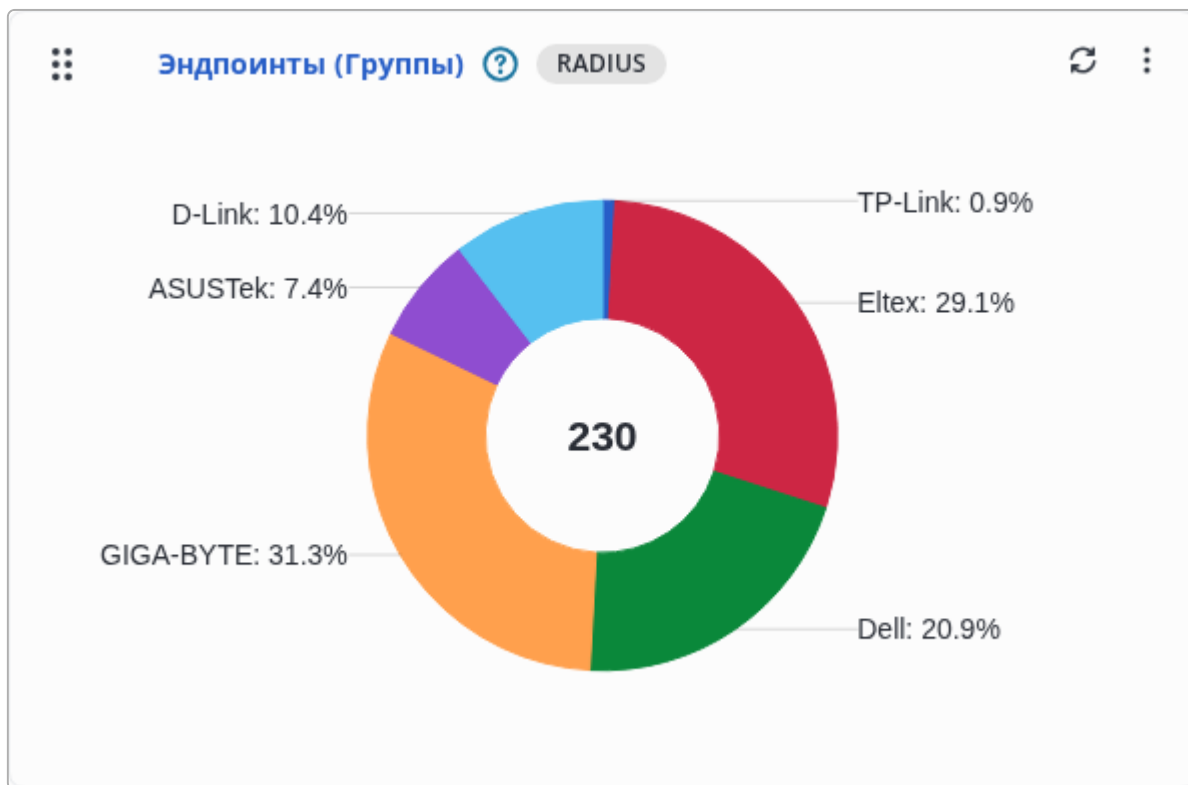


Рисунок 11. Виджет "Эндпоинты (Группы)"

Виджет "Эндпоинты (Политики профилирования)"

Виджет отображает количество **изученных** эндпоинтов, проходивших авторизацию за последние сутки, по [Политикам профилирования](#) полученным в результате профилирования.

Данные для виджета берутся из таблицы [Эндпоинты](#) и [Журнал подключений](#).

Виджет позволяет проанализировать эффективность работы политик профилирования и оценить распределение эндпоинтов по назначенным им политикам профилирования.

Учитывается последняя группа при переподключении.



- Случайно сгенерированные MAC-адреса не учитываются.
- Известным считается эндпоинт, который присутствует в таблице [Эндпоинты](#).
- При автоматическом режиме новые эндпоинты, добавляемые через RADIUS-запросы, отображаются на виджете только после переподключения, после того как система занесла их в таблицу [Эндпоинты](#).

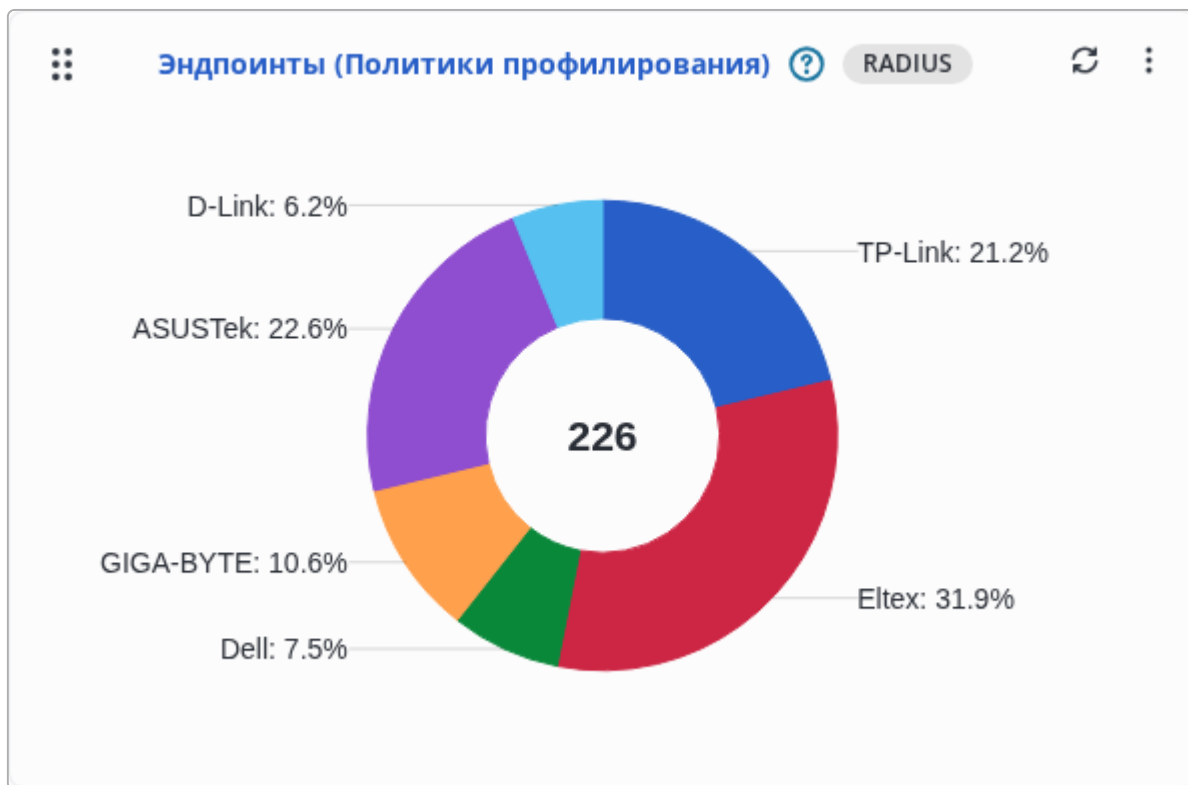


Рисунок 12. Виджет "Эндпоинты (Политики профилирования)"

Виджет "Эндпоинты (Политики RADIUS)"

Виджет отображает количество **изученных** эндпоинтов, проходивших авторизацию за последние сутки, по наборам политик.

Данные для виджета берутся из таблицы [Эндпоинты](#) и [Журнал подключений](#).

Виджет позволяет оценить распределение эндпоинтов по политикам RADIUS.

Учитывается последняя группа при переподключении.



- Случайно сгенерированные MAC-адреса не учитываются.
- Известным считается эндпоинт, который присутствует в таблице [Эндпоинты](#).
- При автоматическом режиме новые эндпоинты, добавляемые через RADIUS-запросы, отображаются на виджете только после переподключения, после того как система занесла их в таблицу [Эндпоинты](#).

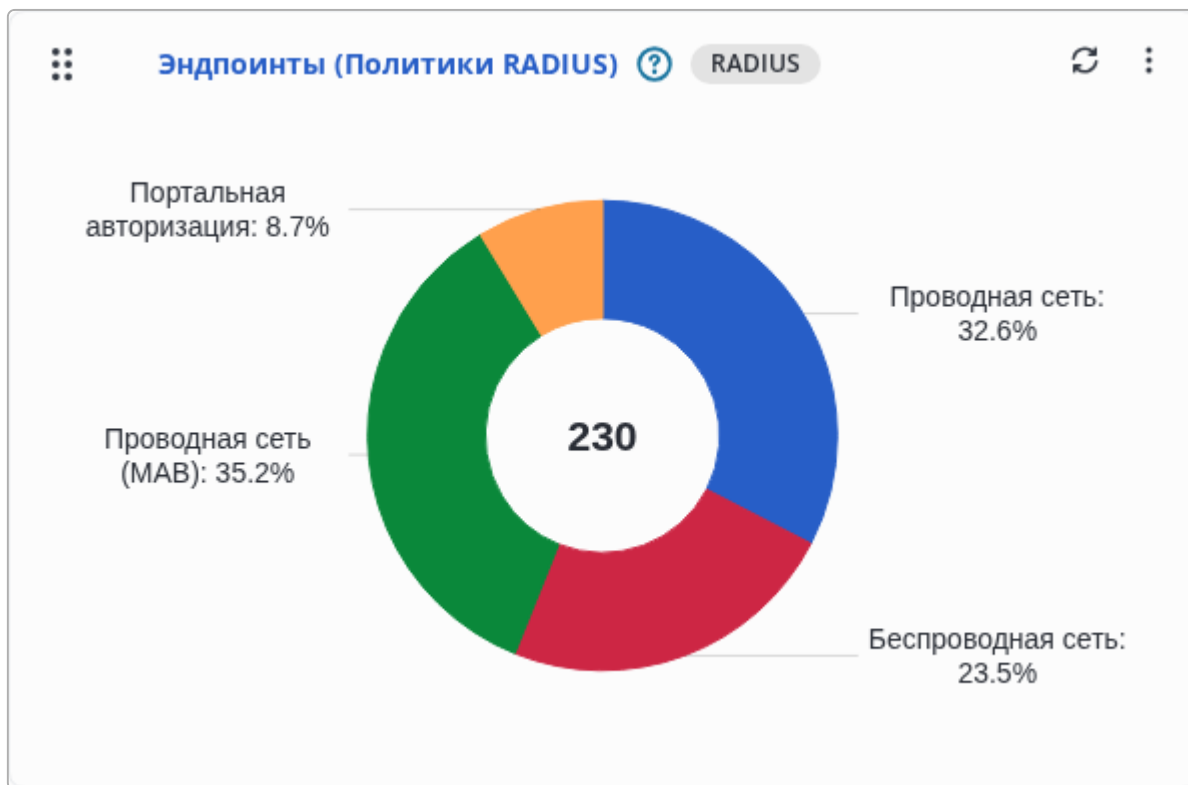


Рисунок 13. Виджет "Эндпоинты (Политики RADIUS)"

Виджет "Пользователи (Источники)"

Виджет отображает количество уникальных пользователей по источникам их идентификации, проходивших авторизацию за последние сутки.

Возможные источники идентификации:

- Internal DB - пользователи из внутренней базы данных системы;
- Endpoints - устройства при авторизации по MAC-адресу (MAB);
- Внешние системы аутентификации (LDAP/Active Directory), настроенные в разделе [Внешние источники идентификации](#).

Виджет позволяет отследить распределение пользователей, прошедших аутентификацию через разные источники идентификации.

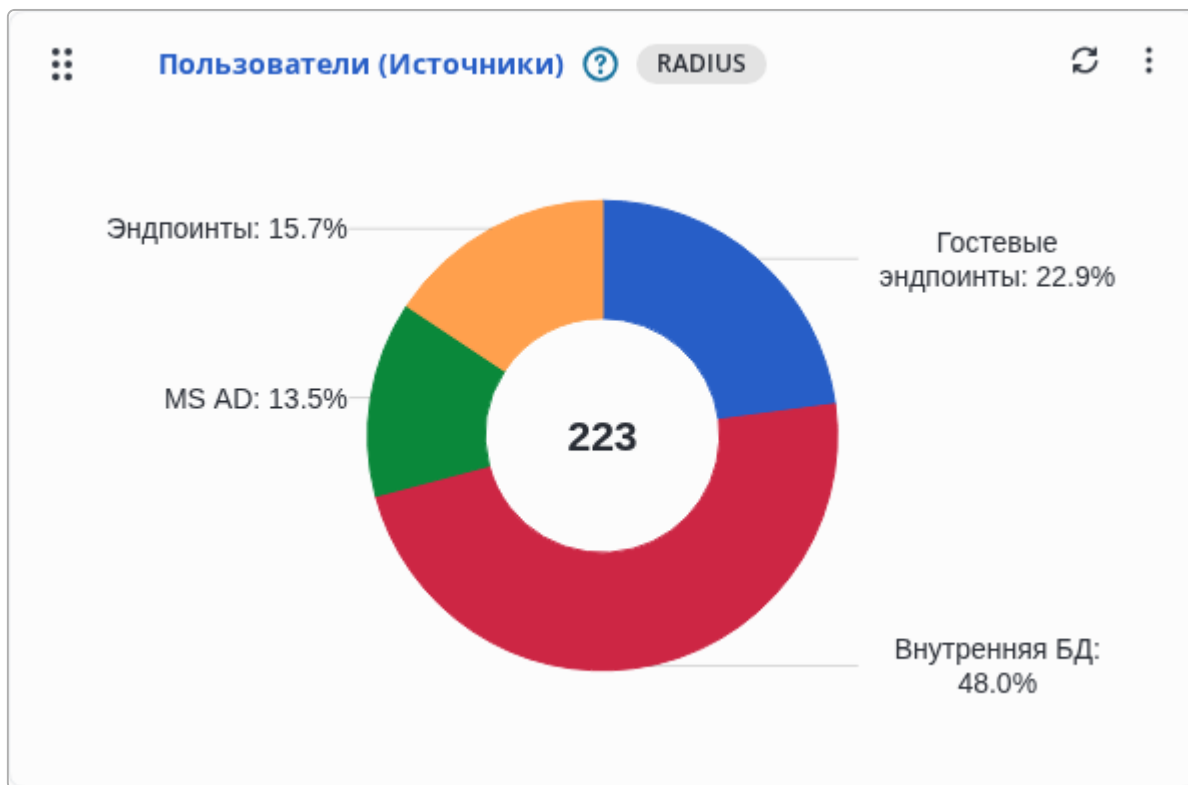


Рисунок 14. Виджет "Пользователи (Источники)"

Виджет "Наборы политик"

Виджет отображает текущее количество срабатываний наборов политик.

Политики с нулевым количеством срабатываний не отображаются.

Данные по количеству срабатываний наборов политик для виджета берутся из списка [Наборов политик](#).

Виджет позволяет отследить частоту применения различных наборов политик для анализа эффективности условий доступа.

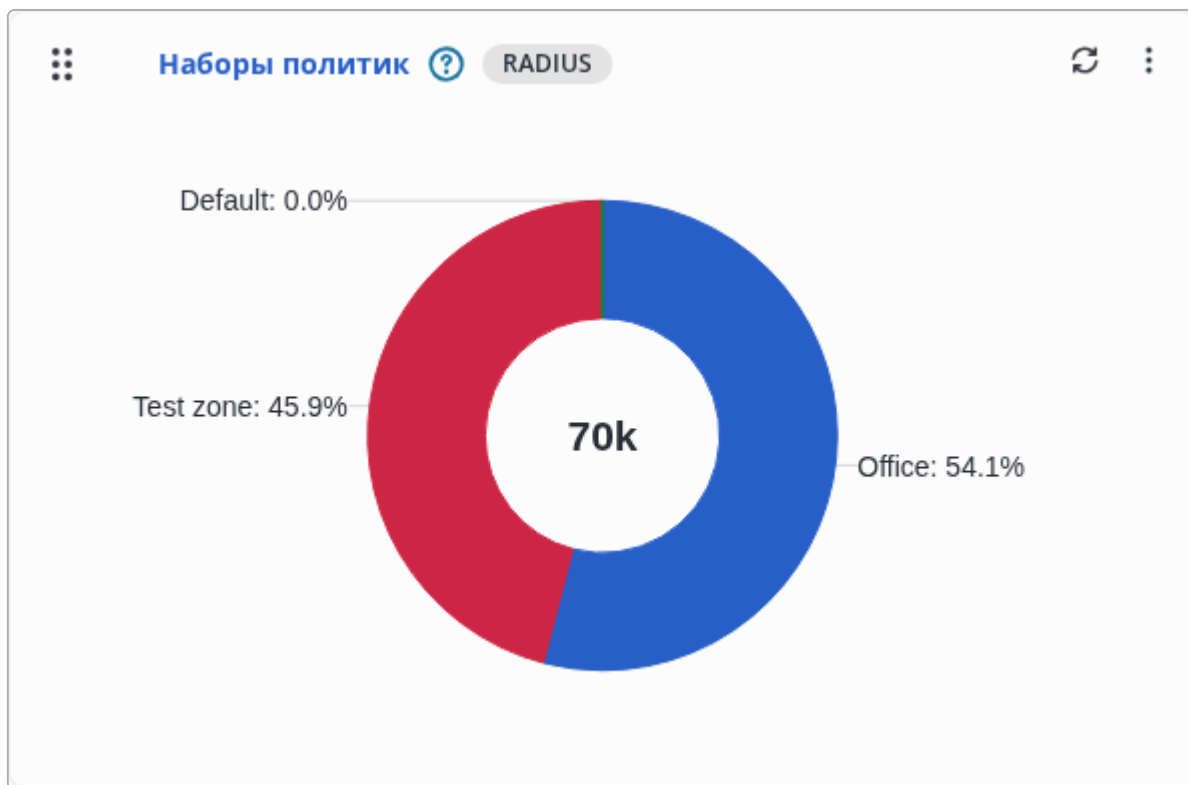


Рисунок 15. Виджет "Наборы политик"

Виджет "Ошибки подключения"

Виджет отображает ошибки подключения клиентов за последние сутки.

Отклонённые политикой доступа подключения не учитываются.

Данные по возникшим ошибкам берутся из [Журнал подключений](#).

Виджет позволяет выявить и классифицировать ошибки при подключении клиентов, исключая случаи преднамеренного блокирования.

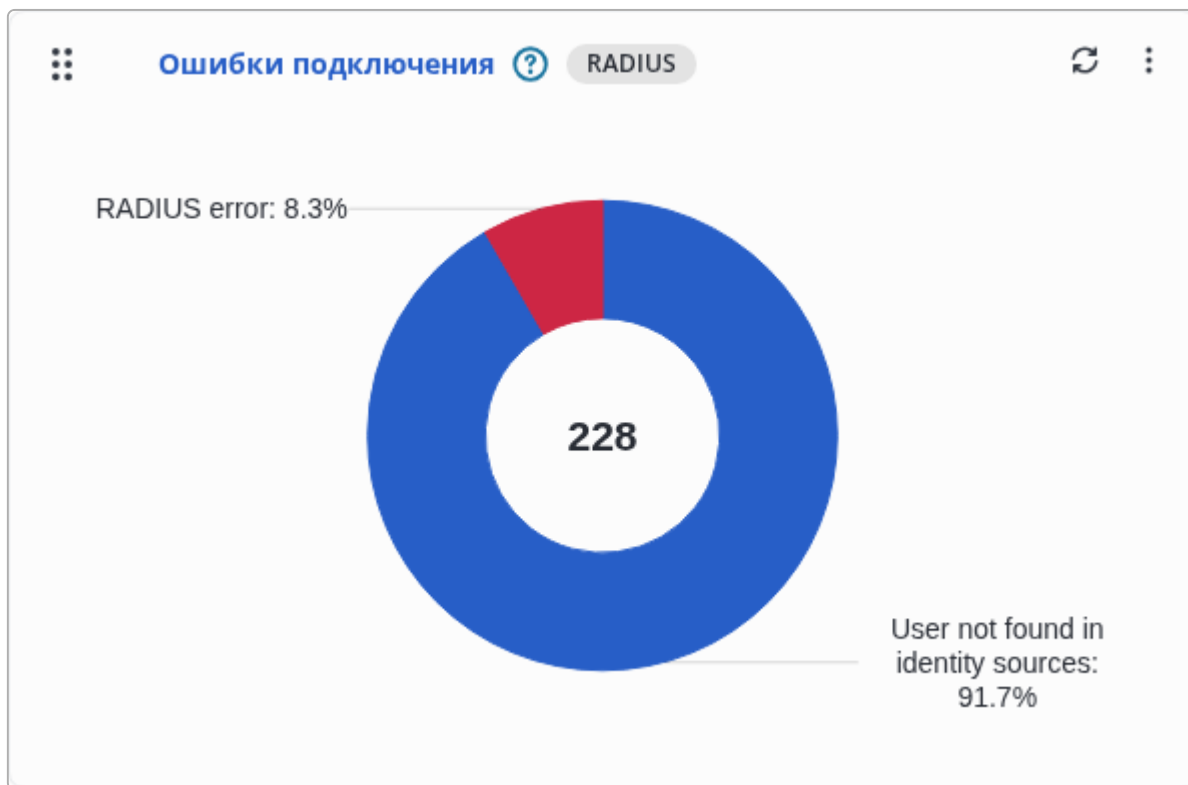


Рисунок 16. Виджет "Ошибки подключения"

Виджет "RADIUS-сессии"

Виджет отображает общее количество RADIUS-сессий за весь период хранения данных, без применения каких-либо фильтров при подсчете. Период хранения также отображается в виджете, единица отображения - дни.

Список сессий можно увидеть в таблице [Журнал подключений](#).

Виджет позволяет оценить объем соответствующей таблицы в базе данных, а также количество подключений пользователей за больший чем сутки период.



Рисунок 17. Виджет "RADIUS-сессии"

Виджеты TACACS+



Данный раздел содержит информацию по настройке функционала, доступ к которому приобретается отдельно с помощью дополнительной опции лицензии NAICE-TACACS+. По вопросам приобретения функционала обращайтесь к Вашему менеджеру или на электронную почту eltex@eltex-co.ru.

Список доступных виджетов

Виджет	Тип отображения данных	Краткое описание виджета
Авторизации	График	Количество авторизаций и аутентификаций сетевых администраторов за последние сутки по часам.
Аккаунтинг	График	Количество запросов аккаунтинга за последние сутки по часам.
Метрика подключений	Метрика	Количество успешных и отклоненных подключений сетевых администраторов за последние сутки.
Пакеты TACACS+ (Тип)	Метрика	Количество пакетов TACACS+ по типу полученных за последние сутки.
Устройства (Тип)	Гистограмма	Количество сетевых устройств, через которые происходило подключение администратора, по типам сетевых устройств.

Виджет	Тип отображения данных	Краткое описание виджета
Устройства (Локации)	Гистограмма	Количество сетевых устройств, через которые происходило подключение администратора, по месторасположению сетевых устройств.
Профили TACACS+	Круговая диаграмма	Текущее количество срабатываний профилей TACACS+.
Наборы команд TACACS+	Круговая диаграмма	Текущее количество срабатываний наборов команд TACACS+.
Наборы политик TACACS+	Круговая диаграмма	Текущее количество срабатываний наборов политик TACACS+.
Ошибки подключения	Круговая диаграмма	Ошибки подключения сетевых администраторов за последние сутки.
Пользователи (Источники)	Круговая диаграмма	Количество уникальных сетевых администраторов по источникам их идентификации, проходивших авторизацию за последние сутки
TACACS+ сессии	Метрика	Общее количество TACACS+ сессий за весь период хранения данных. Период хранения отображается в днях.
TACACS+ аккаунтинг	Метрика	Общее количество TACACS+ аккаунтинга за весь период хранения данных. Период хранения отображается в днях.



Виджеты с типом отображения "метрика" и "круговая диаграмма" отображают большие числа в сокращенном формате (например, 40k вместо 40123). Точное значение метрики отображается в подсказке при наведении на значение.

Виджет "Авторизации"

Виджет отображает данные о количестве попыток авторизаций и аутентификаций на сетевых устройствах (как успешных, так и отклоненных) в системе за последние сутки по часам, на основе данных [Журнала подключений](#).

Информация визуализирована в виде временного графика, где:

- По вертикальной оси (Y) отображается количественный показатель попыток авторизации и аутентификации;
- По горизонтальной оси (X) представлена временная шкала по часам.

Виджет позволяет оперативно отслеживать активность пользователей, выявлять периоды повышенной активности.

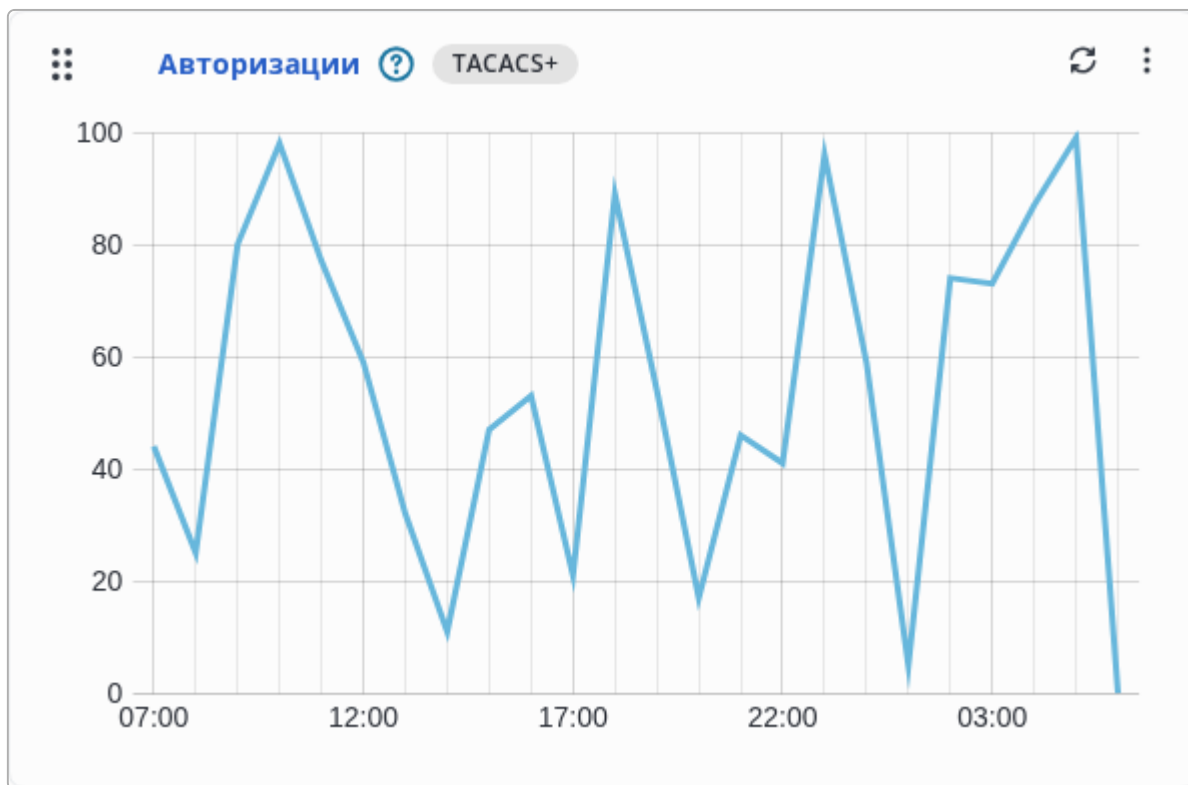


Рисунок 18. Виджет "Авторизации"

Виджет "Аккаунтинг"

Виджет отображает данные о количестве запросов аккаунтинга в системе за последние сутки по часам, на основе данных [Учёт команд](#).

Информация визуализирована в виде временного графика, где:

- По вертикальной оси (Y) отображается количественный показатель запросов аккаунтинга;
- По горизонтальной оси (X) представлена временная шкала по часам.

Виджет позволяет оперативно отслеживать активность пользователей, выявлять периоды повышенной активности.

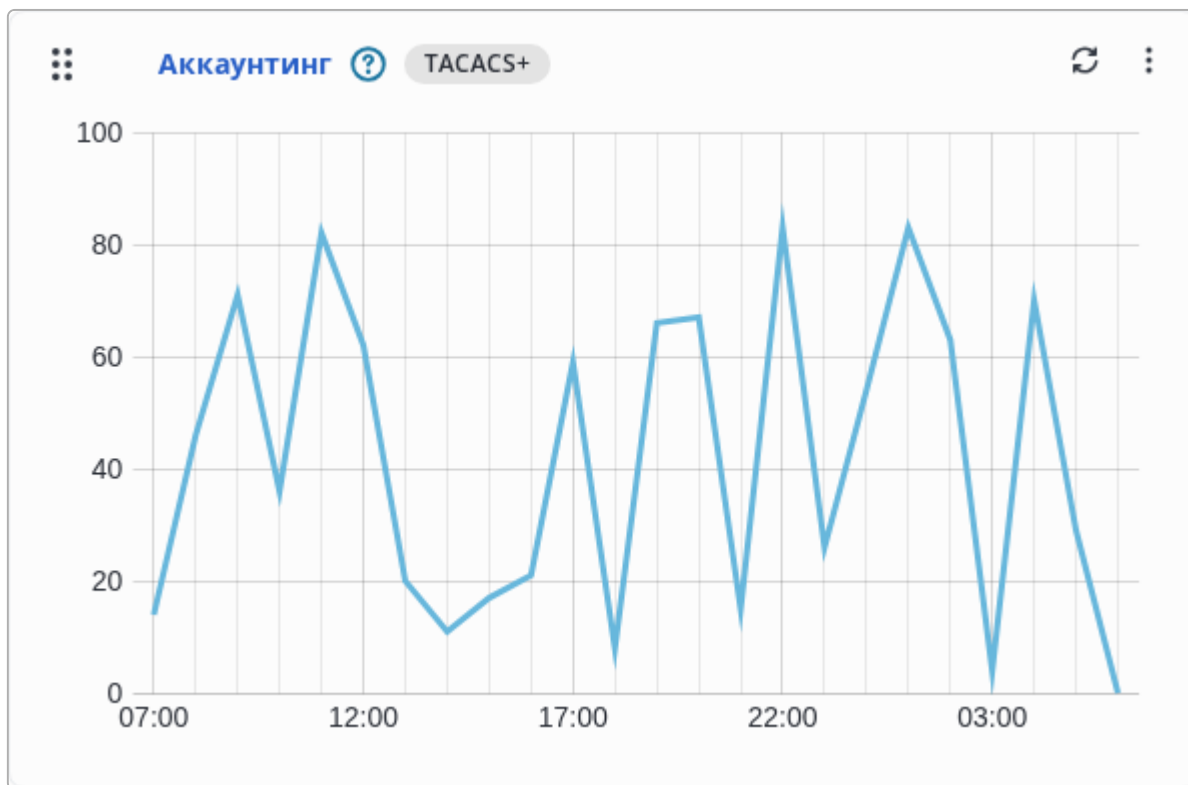


Рисунок 19. Виджет "Аккаунтинг"

Виджет "Метрика подключений"

Виджет отображает данные о количестве успешных и отклонённых подключений на сетевых устройствах за последние сутки на основании данных из [Журнала подключений](#).

Виджет позволяет отследить соотношение состояния сессий (успешных и отклоненных попыток) за сутки.

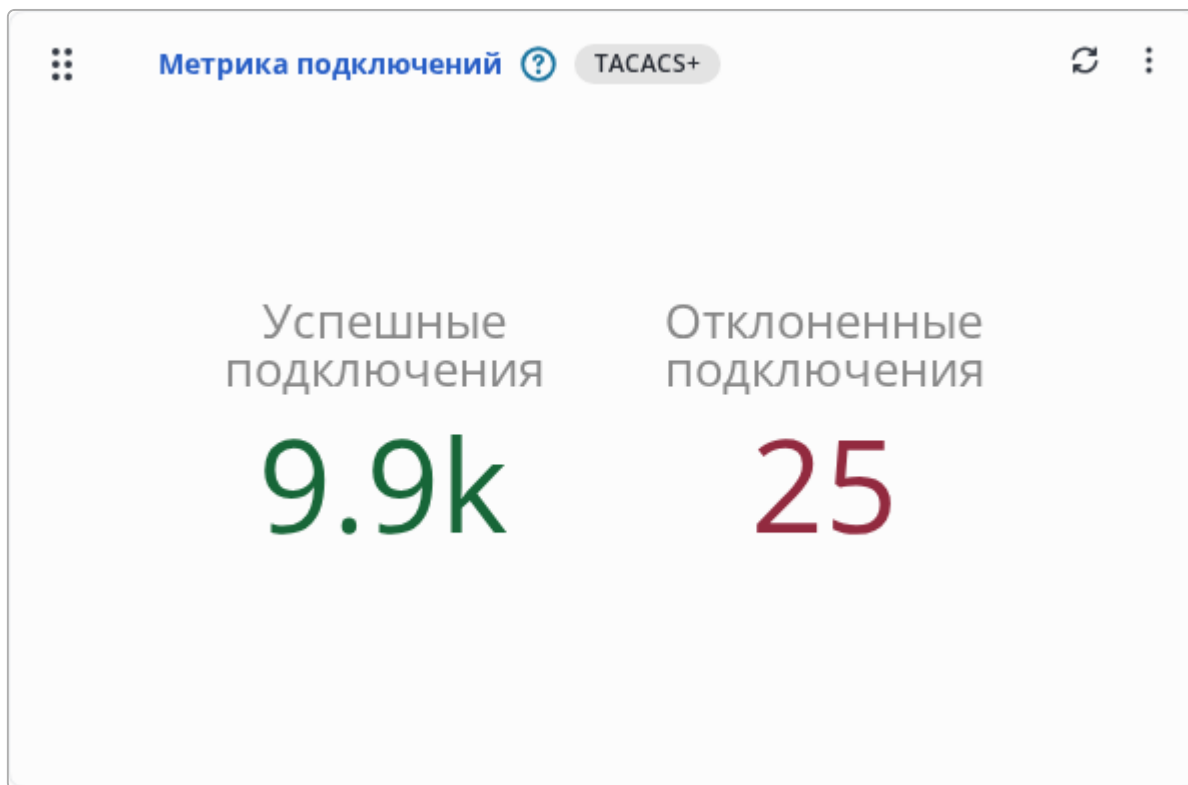


Рисунок 20. Виджет "Метрика подключений"

Виджет "Пакеты TACACS+ (Тип)"

Виджет отображает данные о количестве полученных пакетов TACACS+ на сетевых устройствах по типу пакета за последние сутки на основании данных из [Журнала подключений](#).

Виджет позволяет отследить соотношение пакетов TACACS+ (AUTHENTICATION, AUTHORIZATION, ACCOUNTING)

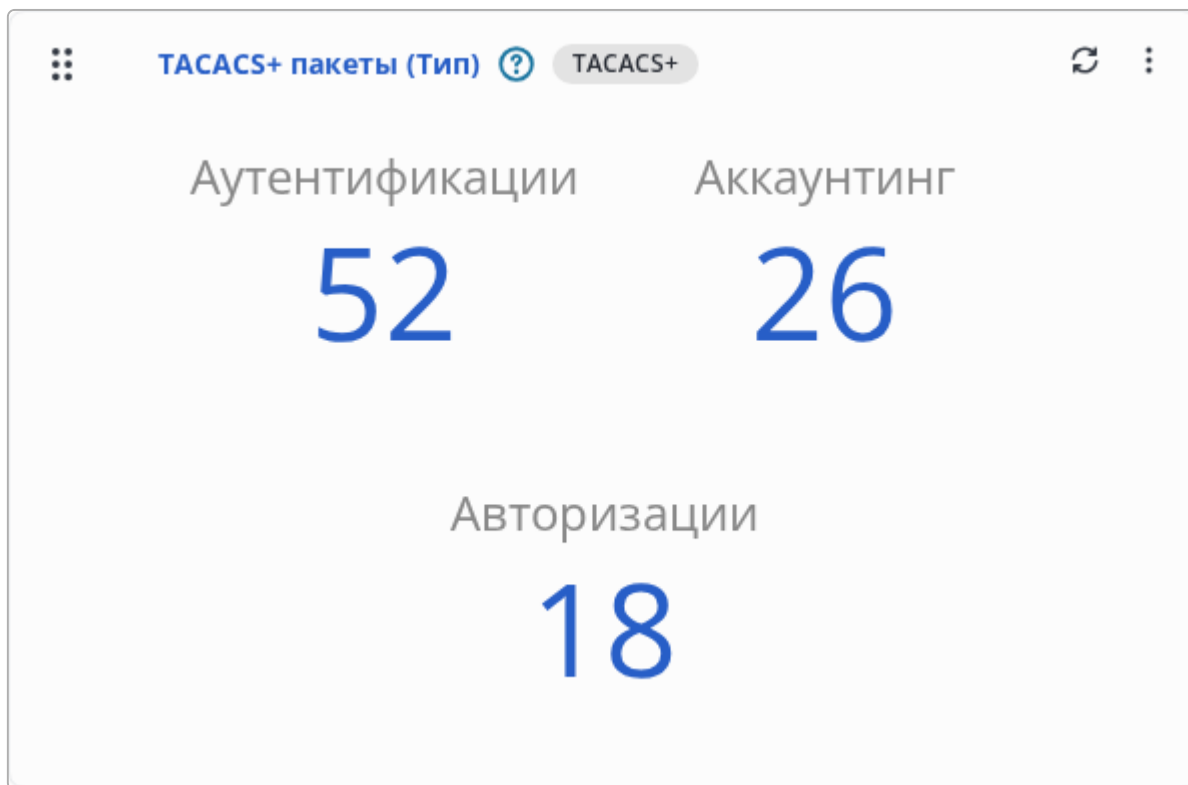


Рисунок 21. Виджет "Пакеты TACACS+ (Тип)"

Виджет "Устройства (Тип)"

Виджет отображает количество сетевых устройств, на которые происходило подключение администратора, по типам сетевых устройств.

Группы устройств, используемые для классификации, берутся из раздела [Группы устройств](#).

Виджет позволяет отследить тенденции востребованности устройств с привязкой к их типу.

Данные виджета заполняются только в случае, когда в условии политик использовался атрибут с типом устройства.

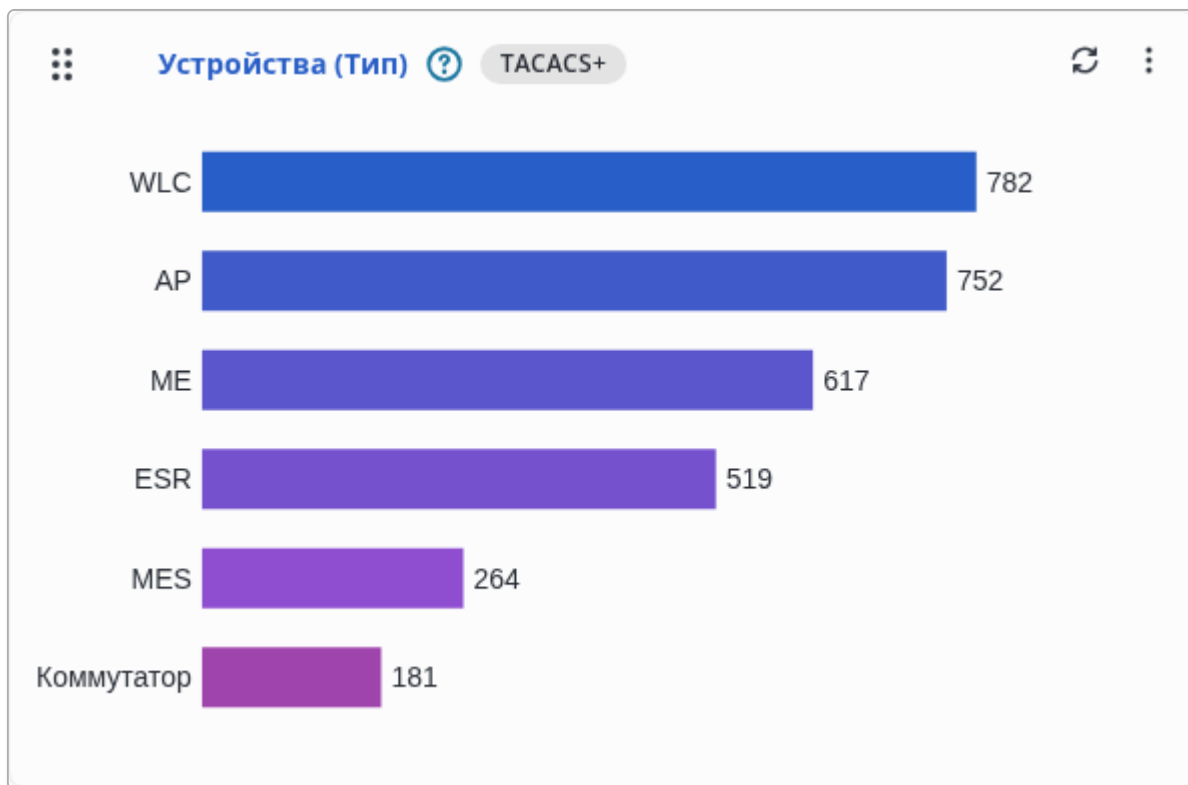


Рисунок 22. Виджет "Устройства (Тип)"

Виджет "Устройства (Локации)"

Виджет отображает количество сетевых устройств, через которые происходило подключение сетевого администратора, по месторасположению сетевых устройств.

Группы устройств, используемые для классификации, берутся из раздела [Группы устройств](#).

Виджет позволяет отследить тенденции востребованности устройств с привязкой к их месторасположению.

Данные виджета заполняются только в случае, когда в условии политик использовался атрибут с локацией устройства.

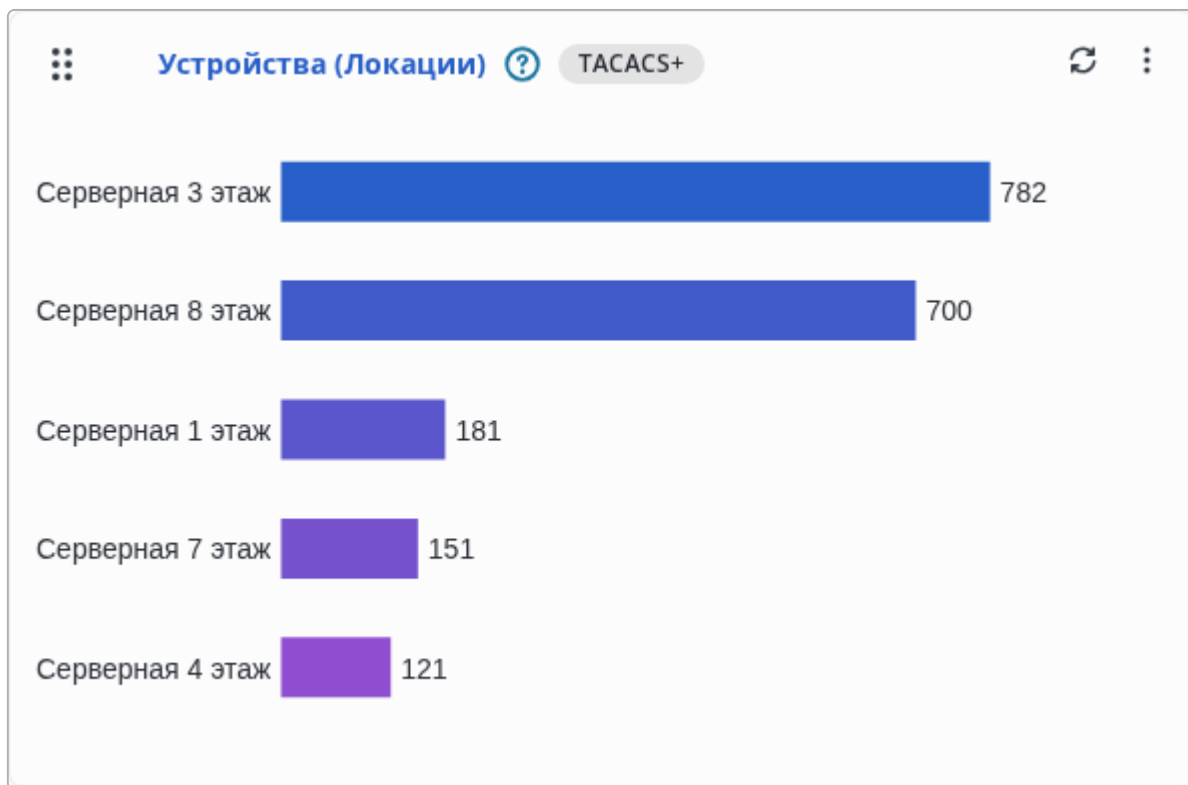


Рисунок 23. Виджет "Устройства (Локации)"

Виджет "Профили TACACS+"

Виджет отображает текущее количество назначенных профилей TACACS+.

Профили с нулевым количеством назначений не отображаются.

Данные по количеству назначенных профилей для виджета берутся из списка [Профилей TACACS](#).

Виджет позволяет отследить частоту применения различных профилей для анализа эффективности условий доступа.

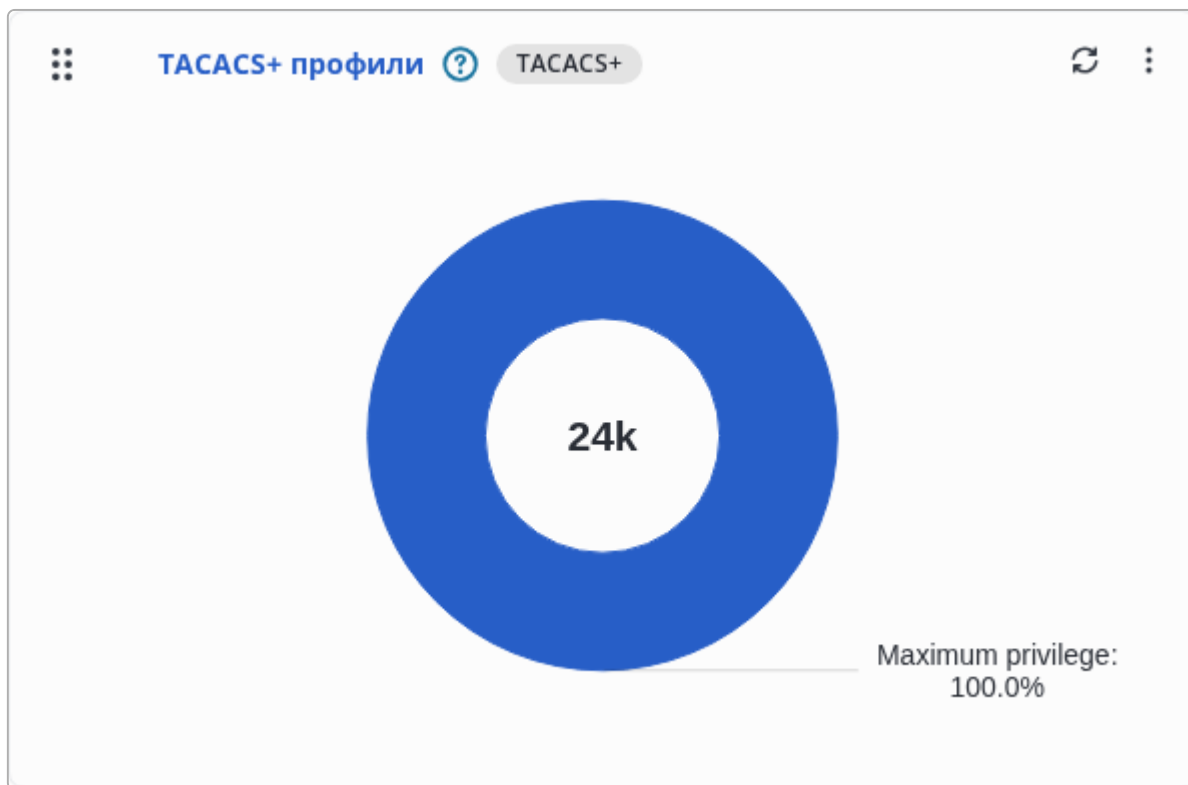


Рисунок 24. Виджет "Профили TACACS+"

Виджет "Наборы команд"

Виджет отображает текущее количество назначенных наборов команд TACACS+.

Наборы команд с нулевым количеством срабатываний не отображаются.

Данные по количеству срабатываний наборов команд для виджета берутся из списка [Наборов команд](#).

Виджет позволяет отследить частоту применения различных наборов команд для анализа эффективности условий доступа.



Рисунок 25. Виджет "Наборы команд"

Виджет "Наборы политик"

Виджет отображает текущее количество срабатываний наборов политик TACACS+.

Политики с нулевым количеством срабатываний не отображаются.

Данные по количеству срабатываний наборов политик для виджета берутся из списка [Наборов политик](#).

Виджет позволяет отследить частоту применения различных наборов политик для анализа эффективности условий доступа.

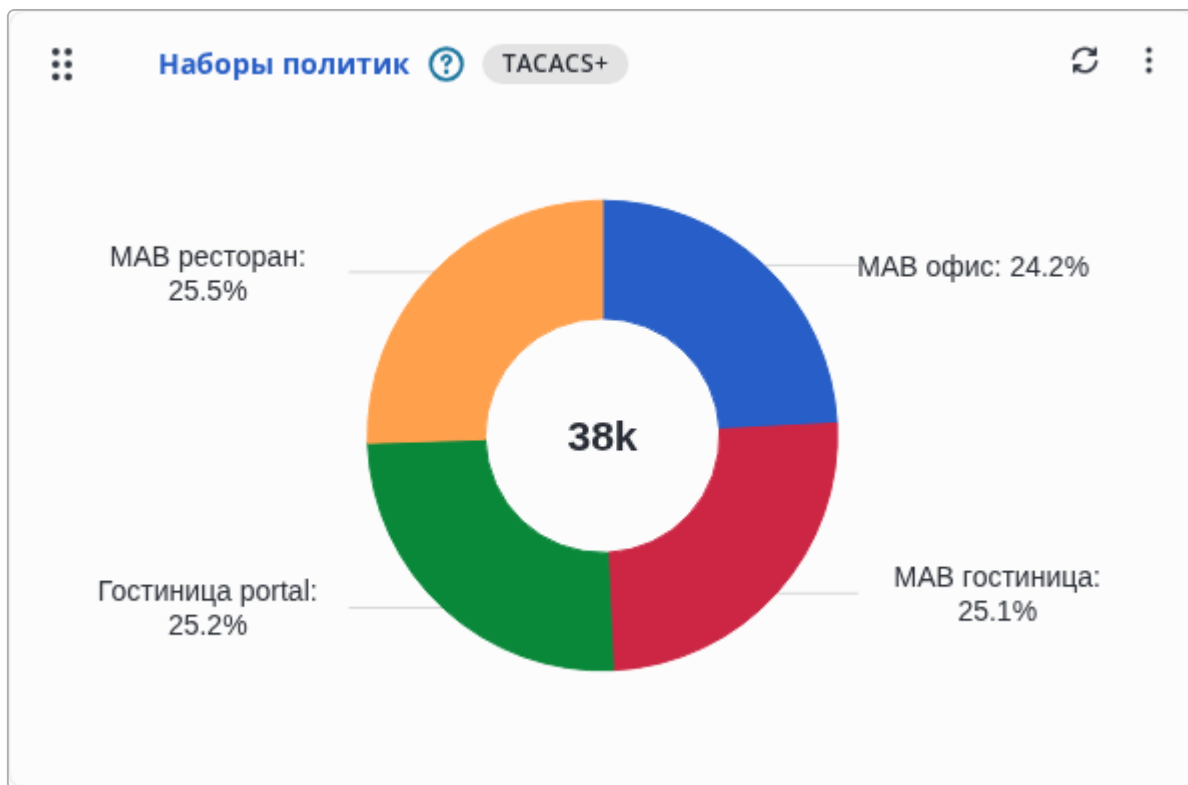


Рисунок 26. Виджет "Наборы политик"

Виджет "Ошибки подключения"

Виджет отображает ошибки подключения администраторов за последние сутки.

Отклонённые политикой доступа подключения не учитываются.

Данные по возникшим ошибкам берутся из [Журнала подключений](#).

Виджет позволяет выявить и классифицировать ошибки при подключении сетевых администраторов, исключая случаи преднамеренного блокирования.

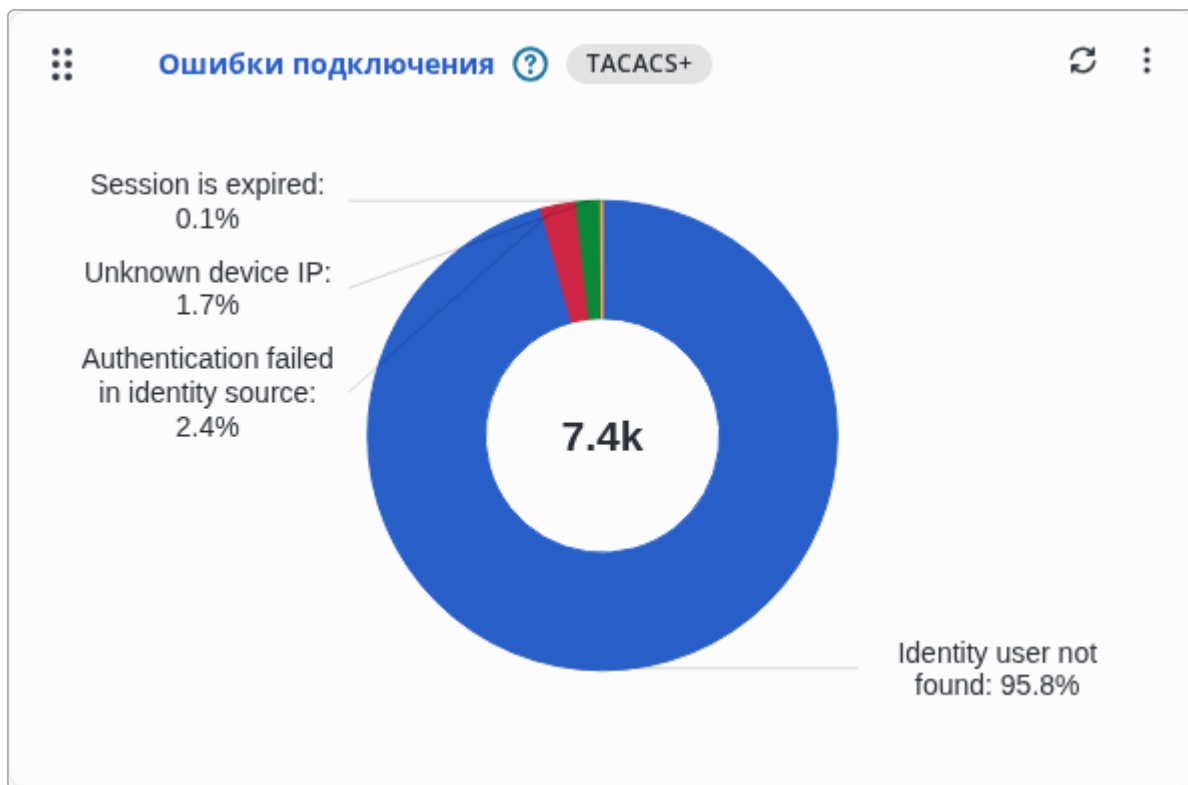


Рисунок 27. Виджет "Ошибки подключения"

Виджет "Пользователи (Источники)"

Виджет отображает количество уникальных сетевых администраторов по источникам их идентификации, проходивших авторизацию за последние сутки.

Возможные источники идентификации:

- Internal DB - пользователи из внутренней базы данных системы;
- Внешние системы аутентификации (LDAP/Active Directory), настроенные в разделе [Внешние источники идентификации](#).

Виджет позволяет отследить распределение администраторов, прошедших аутентификацию через разные источники идентификации.

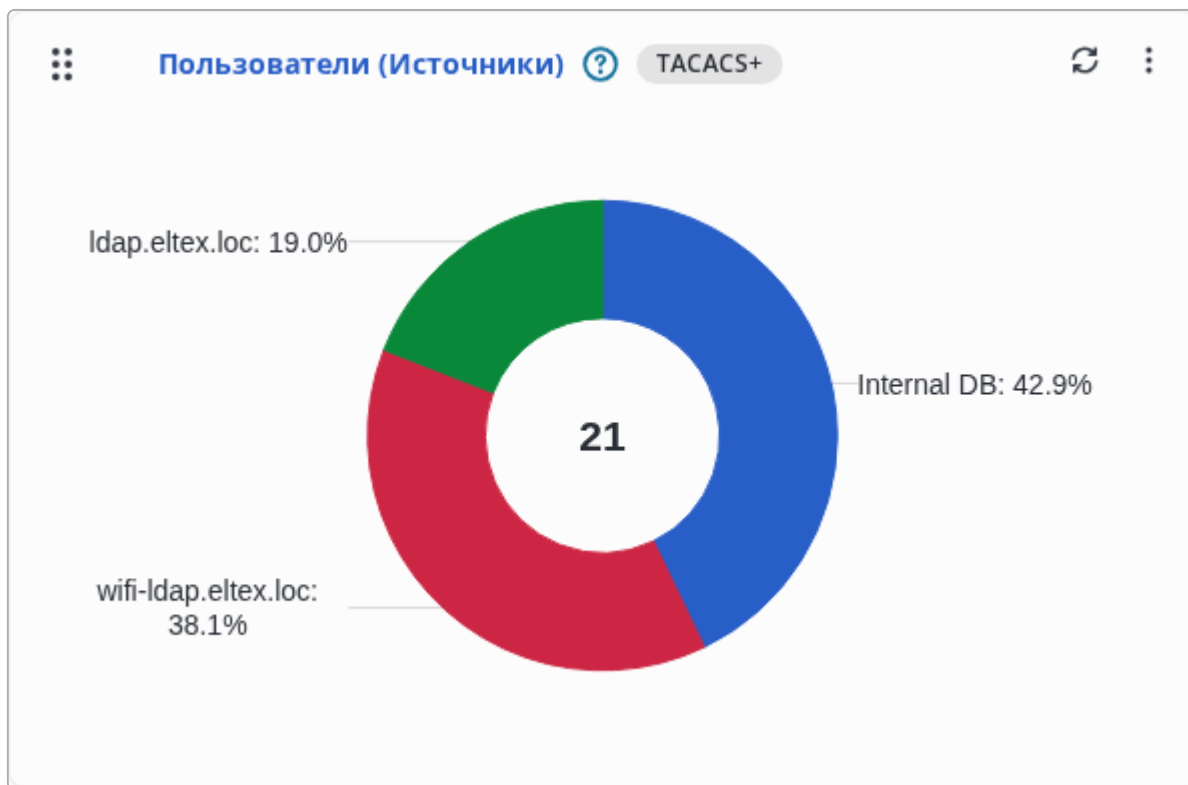


Рисунок 28. Виджет "Пользователи (Источники)"

Виджет "TACACS+ сессии"

Виджет отображает общее количество TACACS+ сессий за весь период хранения данных, без применения каких-либо фильтров при подсчете. Период хранения также отображается в виджете, единица отображения - дни.

Список сессий можно увидеть в таблице [Журнал подключений](#).

Виджет позволяет оценить объем соответствующей таблицы в базе данных, а также количество подключений пользователей за больший чем сутки период.

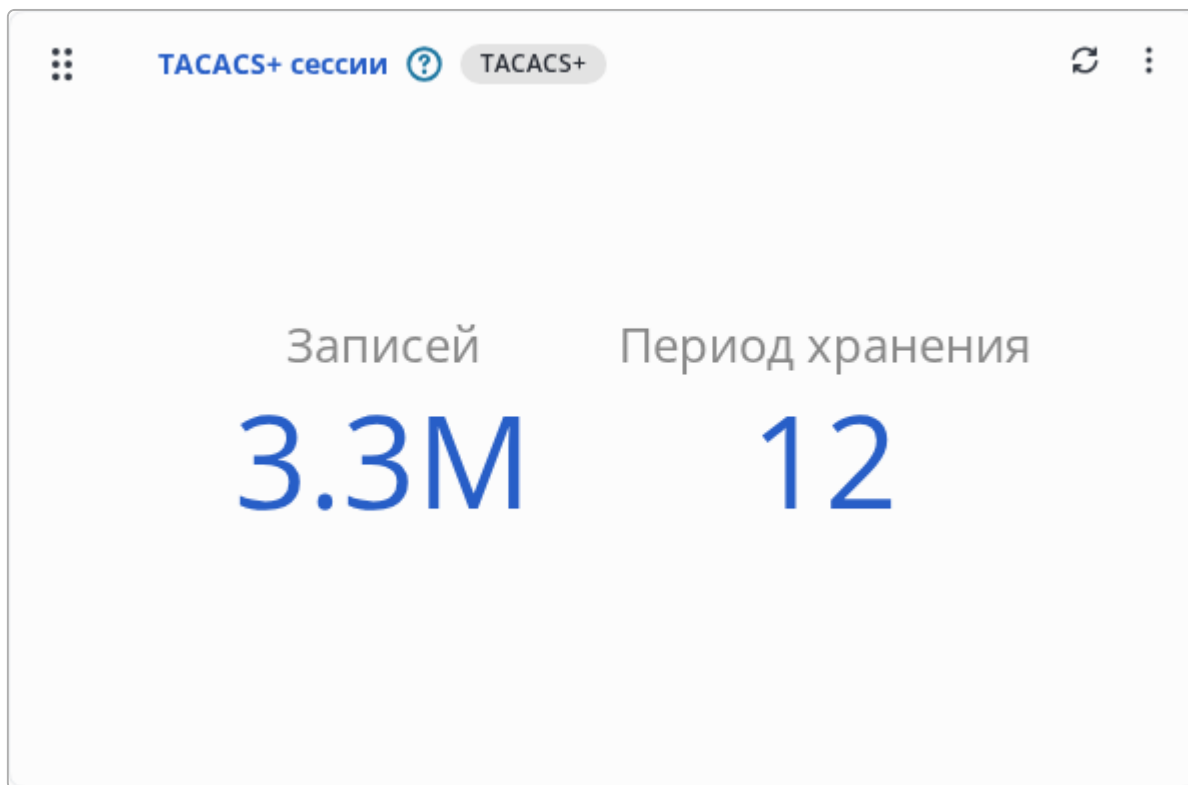


Рисунок 29. Виджет "TACACS+ сессии"

Виджет "TACACS+ аккаунтинг"

Виджет отображает общее количество TACACS+ аккаунтинга за весь период хранения данных, без применения каких-либо фильтров при подсчете. Период хранения также отображается в виджете, единица отображения - дни.

Список сессий аккаунтинга можно увидеть в таблице [Учёт команд \(accounting\)](#).

Виджет позволяет оценить объем соответствующей таблицы в базе данных, а также количество подключений пользователей за больший чем сутки период.

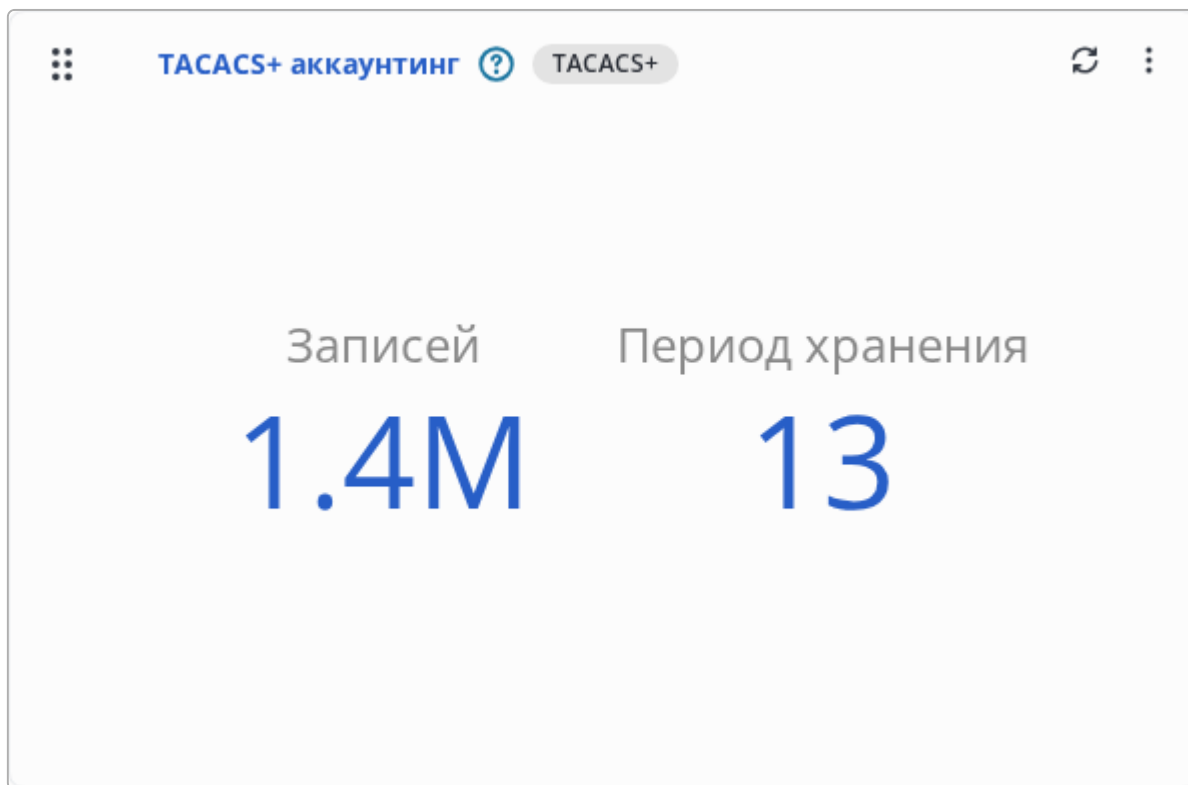


Рисунок 30. Виджет "TACACS+ сессии"

Виджеты SMS



Данный раздел содержит информацию по настройке функционала, доступ к которому открывается с помощью лицензии уровня **ADVANCED**. По вопросам приобретения функционала обращайтесь к Вашему менеджеру или на электронную почту eltex@eltex-co.ru.

Список доступных виджетов

Виджет	Тип отображения данных	Краткое описание виджета
График отправки СМС	График	Количество отправок СМС за последние сутки по часам.
Общее количество СМС	Метрика	Количество успешных и неуспешных отправок СМС за последние сутки.

Виджет "График отправки СМС"

Виджет отображает данные о количестве СМС, отправленных в рамках портальной авторизации, в системе за последние сутки по часам.

Информация визуализирована в виде временного графика, где:

- По вертикальной оси (Y) отображается количественный показатель отправленных СМС;
- По горизонтальной оси (X) представлена временная шкала по часам.

Виджет позволяет оперативно отслеживать активность пользователей, выявлять периоды повышенной активности.

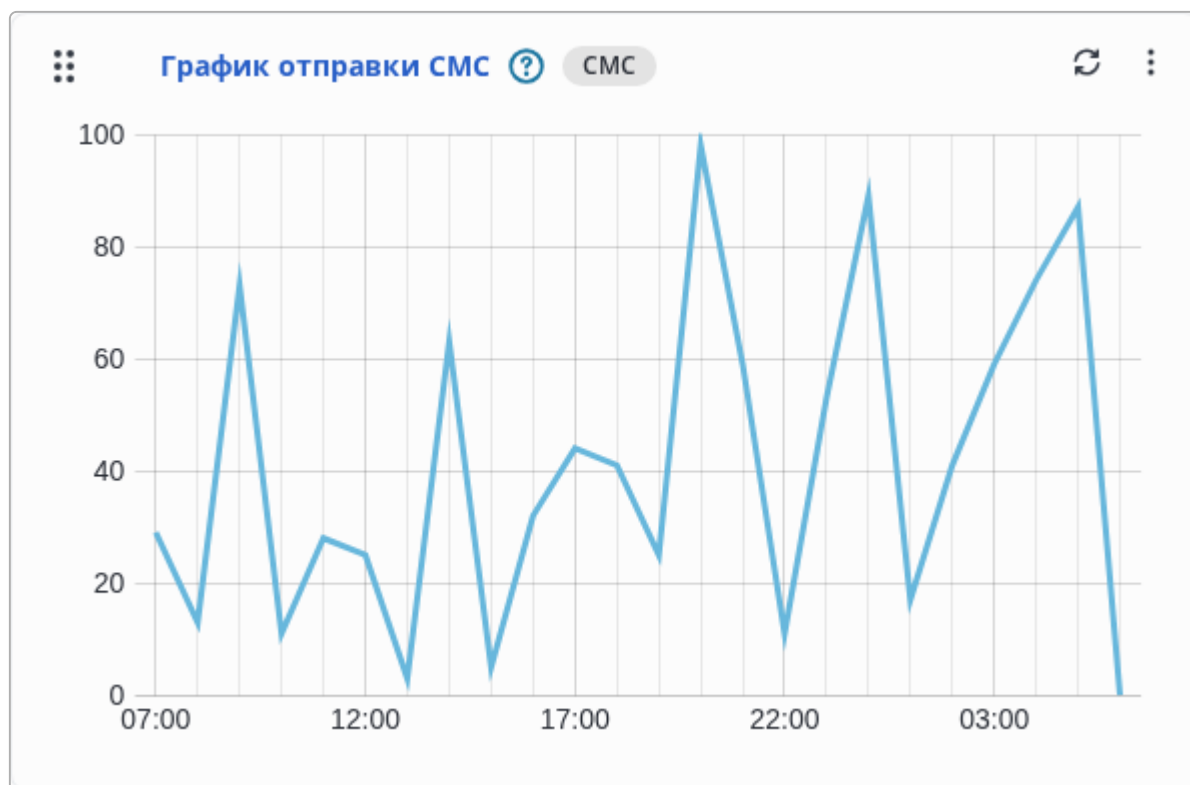


Рисунок 31. Виджет "График отправки СМС"

Виджет "Общее количество СМС"

Виджет отображает данные о количестве успешных и неуспешных отправок СМС.

Виджет позволяет отследить соотношение отправок СМС за сутки.

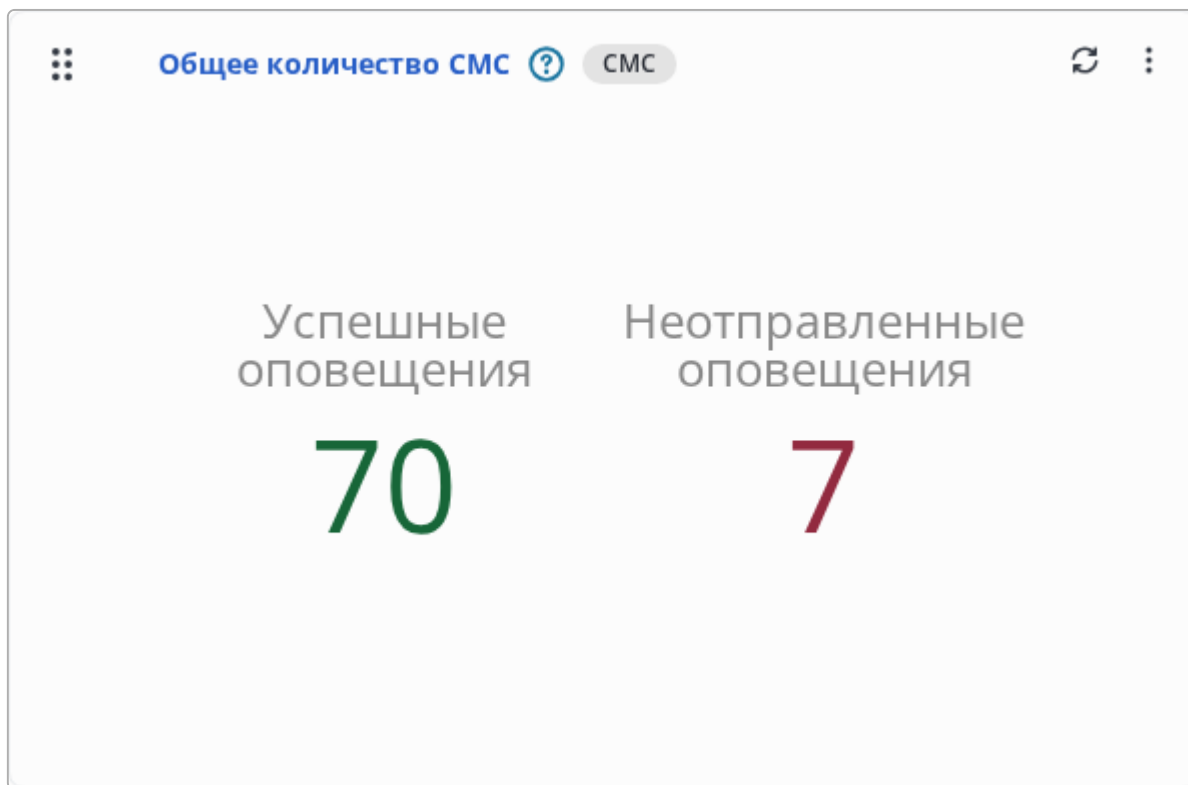


Рисунок 32. Виджет "Общее количество СМС"

Мониторинг

RADIUS

Журнал подключений

Описание

Мониторинг пользовательских сессий позволяет просматривать подключения пользователей за определенный период времени, производить фильтрацию для поиска необходимых записей и анализировать детальную информацию об определенной сессии.

Просмотр списка пользовательских сессий

Мониторинг > RADIUS > Журнал подключений

RADIUS

Журнал подключений

Активные сессии

Каждую минуту

За последние полчаса

Период

Фильтры

Время последней активности	Статус	Подробнее	Имя узла	Пользователь	MAC-адрес клиента	Производитель	Профили авторизации	Имя NAS
02.02.2025 17:01:25	Успешно		naice2.loc	mikhail.grachev	74:56:3C:E7:40:BE	GIGA-BYTE TECHNOLOGY CO.,L...	PermitAccess	sw3103-5
02.02.2025 17:05:15	Успешно		naice1.loc	veronika.karaeva	20:08:C7:28:20:A8	HUAWEI TECHNOLOGIES CO.,L...	PermitAccess	sw3102-2
02.02.2025 17:07:47	Успешно		naice1.loc	alisa.agapova	00:00:40:11:AD:0D	APPLICON, INC.	PermitAccess	sw301-1p
02.02.2025 17:15:32	Успешно		naice2.loc	yuliya.izmailova	A8:A1:59:AD:73:E5	ASRock Incorporation	PermitAccess	sw3101-1t
02.02.2025 17:19:50	Создано		naice3.loc	yuriy.dmitriev	B8:2A:A9:5E:C4:5F	Apple, Inc.	PermitAccess	sw2410-1
02.02.2025 17:23:50	Успешно		naice2.loc	elizar.romanov	C8:A3:62:2C:39:C5	ASIX Electronics Corporation	PermitAccess	wlc281-2
02.02.2025 17:24:50	Успешно		naice1.loc	gleb.chernyahovskiy	5C:E9:31:F9:B5:6F	TP-Link Systems Inc	PermitAccess	sw3101-2t
02.02.2025 17:25:55	Успешно		naice2.loc	svetlana.chagina	FC:70:2E:02:01:4F	Sichuan AI-Link Technology Co...	PermitAccess	sw3101-1p
02.02.2025 17:27:17	Успешно		naice2.loc	dmitriy.volkov	EC:B1:E0:82:9F:40	Eltex Enterprise LTD	PermitAccess	sw3102-1t
02.02.2025 17:28:13	Отклонено		naice3.loc	egor.novikov	34:0A:33:25:70:7E	D-Link International	DenyAccess	sw3101-2
02.02.2025 17:29:23	Успешно		naice2.loc	artem.panchenko	2C:CF:67:10:FC:81	Raspberry Pi (Trading) Ltd	PermitAccess	sw3101-2p
02.02.2025 17:29:45	Истекло		naice1.loc	dariya.harlamova	A8:A1:59:AD:73:E5	ASRock Incorporation	PermitAccess	sw2410-3
02.02.2025 17:29:47	Успешно		naice1.loc	aleksandr.cherkasov	8C:E9:EE:7F:B3:BD	Intel Corporate	PermitAccess	sw2512-1
02.02.2025 17:29:51	Отклонено		naice2.loc	nikita.bondarenko	44:E4:D9:3B:54:41	Cisco Systems, Inc	DenyAccess	sw301-1

Всего элементов: 15

Время последнего обновления: 02.02.2025 17:00:00

Рисунок 33. Таблица со списком сессий пользователей

Таблица по умолчанию содержит колонки:

- Время последней активности — время, когда в рамках данной сессии был получен последний RADIUS-пакет.
- Статус — статус сессии, может принимать значения:
 - Создано — сессия была создана, однако по какой-то причине авторизация не была завершена;
 - Успешно — авторизация была пройдена успешно;
 - Отклонено — авторизация была отклонена;
 - Истекло — сессия была завершена по истечении определенного времени.
- Подробнее — ссылка для открытия детальной страницы сессии, на которой содержится подробная информация о сессии:
 - ссылка доступна.
 - ссылка недоступна. Такая ситуация может возникнуть, когда срок хранения сессий больше времени хранения детальной информации о сессии (7 дней).

Имя узла — имя узла NAICE, которым сформировано событие. Это поле может быть полезно при кластерной установке NAICE.

- **Пользователь** — логин пользователя, с которым проходила авторизация.



Логин пользователя при авторизации в Active Directory всегда отображается в формате UPN (например [username@example.org](#))!

- **MAC клиента** — MAC адрес авторизуемого клиента, который указан в RADIUS-атрибуте Calling-Station-Id (если атрибут отсутствует в RADIUS запросе или не содержит MAC - поле будет пустым).
- **Производитель** — имя организации, которое произвело устройство, проходившее авторизацию.
- **Профили авторизации** — список профилей авторизации, которые были применены по результатам авторизации клиента.
- **Имя NAS** — имя [NAS-устройства](#) в системе.
- **NAS IP** — IP-адрес NAS-устройства, получаемый из RADIUS-атрибута NAS-IP-Address.
- **ID сессии** — идентификатор сессии из RADIUS-атрибута Acct-Session-Id.

Также доступны дополнительные колонки, настраиваемые в  в шапке таблицы:

- **Политика аутентификации** — название правила политики аутентификации, которое было применено в рамках данной сессии;
- **Политика авторизации** — название правила политики авторизации, которое было применено в рамках данной сессии;
- **Причина ошибки подключения** .
- **Тип подключения** — тип подключения, который был определен исходя из настроек [профиля сетевого устройства](#).
- **Протокол аутентификации** — протокол, по которому проходила авторизация (например, PAP).

Элементы управления:

Каждую минуту ▾

За последние полчаса ▾

Период

🗑️ ↺ 📄

Фильтры

Рисунок 34. Настройки отображения активности пользователей

- **Частота обновления** — настройка частоты автоматического перечитывания пользовательских сессий.



При пролистывании первых 25 элементов таблицы параметр "Частота обновления" переходит в состояние "Отключено".

Для возврата нужно либо указать вручную время обновления, либо обновить данные нажатием на кнопку .

- **Промежуток времени** — выбор предопределенного временного периода, в который происходила активность по пользовательским сессиям для отображения, из конечного списка вариантов. При выборе варианта **Произвольный период** требуется настройка поля **Период** .
-

Период — выбор произвольного временного периода, в который происходила активность по пользовательским сессиям для отображения.



Сессии отображаются начиная с 00:00 стартового дня и до 23:59 конечного для выбранного периода. Время учитывает часовой пояс, указанный в разделе [Настройки аккаунта](#) текущего пользователя системы.

- — обновить данные таблицы вручную.
- — открыть окно настройки отображаемых колонок таблицы.
- **Фильтры** — открыть окно настройки фильтрации.

Фильтрация настраивается в следующем окне:

Фильтры

Пользователь Введите логин	MAC-адрес клиента ? FF:FF:FF:00:00:00	Статус Выберите статус
Тип подключения Выберите тип	Имя NAS Введите имя NAS	NAS IP 0.0.0.0
Протокол аутентификации Выберите протокол		

Заккрыть **Применить**

Рисунок 35. Окно настройки фильтрации записей

Фильтрация записей доступна по параметрам "Пользователь", "MAC клиента", "Статус", "Тип подключения", "Имя NAS", "NAS IP" и "Протокол аутентификации".

В поле ввода MAC-адреса клиента доступен ввод только цифр 16-ичной системы счисления. Разделители октетов (двоеточия) вводятся автоматически.

Доступен поиск по частичному совпадению байтового представления.



Для поиска по части MAC-адреса необходимо, чтобы все доступные для поиска октеты адреса были указаны полностью.
Например, поиск по запросу "AA:BB:CC" возможен, по запросу "A:BB:C" - нет.

Кнопка **Сбросить все** предназначена для сброса настроенных параметров поиска. Она отображается только при настройке хотя бы одного фильтра.

В настройках таблицы можно сменить состав отображаемых колонок.

Кнопка **Сбросить все** предназначена для сброса настроенных колонок к состоянию по умолчанию (неактивно, пока состоянию по умолчанию не изменено).

Настройки таблицы

☐ Показывать все колонки

☒ Время последней активности
☒ Статус
☒ Подробнее
☒ Имя узла
☒ Пользователь
☒ MAC-адрес клиента
☒ Производитель

ОтменаСохранить

Рисунок 36. Окно настройки отображаемых колонок в таблице

Просмотр детальной информации о сессии

Для просмотра детальной информации о сессии из таблицы со всеми сессиями необходимо кликнуть на  в колонке "Подробнее" для выбранной сессии.

Мониторинг
RADIUS
Пользовательские сессии
NAS IP: 235.240.189.197
session ID: F79B...

← NAS IP: 235.240.189.197
session ID: F79B58BF

Общая информация

CoA запросы

Общая информация		Детали аутентификации	
Session status	ACCEPTED	Event	SUCCESS
Event	SUCCESS	Username	tester
Username	tester	Calling-Station-id	4C:12:2D:26:F1:84
Calling-Station-id	4C:12:2D:26:F1:84	Vendor	Dell
Vendor	Dell	Session creation timestamp	14.11.2025 12:23:47
Authentication policy	Default	Session updating timestamp	14.11.2025 12:23:47
Authorization policy	Test Authorization rule	Identity source	Internal DB
Authorization profile	common_acl	Authentication protocol	PAP
		Authorization profile	common_acl
		Network device	Anna:AE15C3DB
		Service Type	Framed-User

Прочие атрибуты

Результат

```
[
  {
    "name": "control:Use-MS-AD",
    "type": "integer",
    "value": {
      "1"
    }
  }
]
```

Рисунок 37. Детальная информация о сессии

Информация на странице разделена на 4 блока:

- Общая информация** — краткая и наиболее важная информация о сессии;

40

Детали аутентификации — детальная информация, которая может быть полезная для отладки;

- Прочие атрибуты — содержание пакета, полученного NAICE от RADIUS-сервера;
- Результат — список атрибутов, которыми был обогащен ответ клиенту в результате авторизации (например, атрибуты для выдачи VLAN или ACL). Если выдача дополнительных атрибутов не настроена в профиле авторизации, то список будет пуст.

Также в отдельной вкладке можно посмотреть ассоциированные с этой сессией CoA-запросы.

Время	Тип CoA запроса	Статус запроса	Тип RADIUS запроса	Статус ответа	Тип RADIUS ответа
14.11.2025 06:58:11	Re-auth	В процессе	CoA-Request	Не выполнено	No response
Запрос		Ответ			
Поля запроса		Список атрибутов			
Packet Identifier	0x24	lorem		amet	
Length	118	amet		ipsum	
Authenticator	dd131c2326cc018c028d6db5f7312843	ipsum		sit	
Code	43	sit		elit	
13.11.2025 22:39:30	Disconnect	Отклонен	No request	Не выполнено	No response

Рисунок 38. Список CoA-запросов

Активные RADIUS-сессии

Описание

Раздел *Активные RADIUS-сессии* предназначен для мониторинга пользовательских сессий, находящихся в активном состоянии в реальном времени. Журнал позволяет просматривать информацию о каждой сессии, фильтровать записи и вручную завершать зависшие сессии.

Просмотр списка активных сессий

Время последней активности	Пользователь	Источник идентификации	MAC-адрес клиента	Имя узла	Дата создания записи	NAS IP	ID сессии
02.02.2025 17:01:25	mikhail.grachev	mikhail.grachev	74:56:3C:E7:40:BE	naice2.loc	02.02.2025 17:01:25	172.16.0.210	ccc061bc-6440-3cda-4ec1-d...
02.02.2025 17:05:15	veronika.karaeva	veronika.karaeva	20:0B:C7:28:20:A8	naice1.loc	02.02.2025 17:05:15	172.16.0.211	9abd5e49-1dde-8a5c-a89e-8...
02.02.2025 17:07:47	alisa.agapova	alisa.agapova	00:00:40:11:AD:0D	naice1.loc	02.02.2025 17:07:47	172.16.0.219	5acb0e42-73d1-e2b0-b61f-b...
02.02.2025 17:15:32	yuliya.izmailova	yuliya.izmailova	A8:A1:59:AD:73:E5	naice2.loc	02.02.2025 17:15:32	172.16.2.44	a21b1ee0-46fb-938c-0a26-2...
02.02.2025 17:19:50	yuriy.dmitriev	yuriy.dmitriev	B8:2A:A9:5E:C4:5F	naice3.loc	02.02.2025 17:19:50	172.16.0.38	c1db4306-5804-ccfd-28fe-fc...
02.02.2025 17:23:50	elizar.romanov	elizar.romanov	C8:A3:62:2C:39:C5	naice2.loc	02.02.2025 17:23:50	172.16.1.149	5538bc15-a11e-cec7-d5eb-6...
02.02.2025 17:24:50	gleb.chernyahovskiy	gleb.chernyahovskiy	5C:E9:31:F9:B5:6F	naice1.loc	02.02.2025 17:24:50	172.16.2.45	06d2ae68-21d9-8c2c-c8b8-b...
02.02.2025 17:25:55	svetlana.chagina	svetlana.chagina	FC:70:2E:02:01:4F	naice2.loc	02.02.2025 17:25:55	172.16.0.194	5667376d-87a2-a3c3-c7bf-4...
02.02.2025 17:27:17	dmitriy.volkov	dmitriy.volkov	EC:B1:E0:82:9F:40	naice2.loc	02.02.2025 17:27:17	172.16.2.47	a4274bf3-7882-ceed-b78c-df...
02.02.2025 17:28:13	egor.novikov	egor.novikov	34:0A:33:25:70:7E	naice3.loc	02.02.2025 17:28:13	172.16.0.193	a25bd1c1-b488-151d-022b-...
02.02.2025 17:29:23	artem.panchenko	artem.panchenko	2C:CF:67:10:FC:81	naice2.loc	02.02.2025 17:29:23	172.16.0.196	889ab8e7-545e-a92e-4251-5...
02.02.2025 17:29:45	dariya.harlamova	dariya.harlamova	A8:A1:59:AD:73:E5	naice1.loc	02.02.2025 17:29:45	172.16.1.150	bbec4c65-3bde-a771-385d-4...

Всего элементов: 12

Время последнего обновления: 02.02.2025 17:00:00

Рисунок 39. Таблица активных RADIUS-сессий

Таблица содержит следующие колонки:

Время последней активности - время, когда по данной сессии был получен последний RADIUS Accounting пакет.

- **Пользователь** - логин пользователя, от имени которого было произведено подключение.
- **Источник идентификации** - наименование источника аутентификации, которому принадлежит подключенный пользователь.
- **MAC-адрес клиента** - MAC-адрес авторизуемого устройства, который указан в RADIUS-атрибуте Calling-Station-Id.
- **Имя узла** - имя узла NAICE, обработавший пакет, по которому была создана сессия.
- **Дата создания записи** - дата и время, когда сессия была создана.
- **NAS IP** - IP-адрес NAS-устройства, получаемый из RADIUS-атрибута NAS-IP-Address.

Элементы управления:

Каждую минуту

▼

За последние полчаса

▼

Период

↺

↻

☰

☒

Фильтры

Рисунок 40. Настройки отображения активных сессий

- **Частота обновления** - настройка частоты автоматического перечитывания данных об активных сессиях.



При пролистывании первых 25 элементов таблицы параметр "Частота обновления" переходит в состояние "Отключено". Для возврата нужно либо указать вручную время обновления, либо обновить данные нажатием на кнопку

- **Промежуток времени** - выбор predetermined временного периода для отображения сессий из списка вариантов. При выборе варианта **Произвольный период** требуется настройка поля **Период**.
- **Период** - выбор произвольного временного периода для отображения сессий.
- - обновить данные таблицы вручную.
- - открыть окно настройки отображаемых колонок таблицы.
- - завершить выбранные сессии. Кнопка отключена, если не выбрана ни одна активная сессия.
- **Фильтры** - открыть окно настройки фильтрации.

Фильтрация настраивается в следующем окне:

Фильтры

Пользователь

Введите логин

Источник идентификации

Выберите источник

MAC-адрес клиента ?

FF:FF:FF:00:00:00

NAS IP

0.0.0.0

Заккрыть

Применить

Рисунок 41. Окно настройки фильтрации записей

Фильтрация записей доступна по параметрам: "Пользователь", "Источник идентификации", "MAC-адрес клиента" и "NAS IP".

Кнопка **Заккрыть** закрывает окно фильтрации без применения изменений. Кнопка **Применить** применяет настроенные фильтры к таблице.

Доступен поиск по частичному совпадению для текстовых полей.



Для поиска по части MAC-адреса необходимо, чтобы все доступные для поиска октеты адреса были указаны полностью.
Например, поиск по запросу "AA:BB:CC" возможен, по запросу "A:BB:C" - нет.

В настройках таблицы  можно сменить состав отображаемых колонок.

Кнопка **Сбросить все** предназначена для сброса настроенных колонок к состоянию по умолчанию (неактивно, пока состоянию по умолчанию не изменено).

Настройки таблицы

☒ Показывать все колонки

☒ Время последней активности

☒ Пользователь

☒ Источник идентификации

☒ MAC-адрес клиента

☒ Имя узла

☒ Время создания

☒ NAS IP

Отмена Сохранить

Рисунок 42. Окно настройки отображаемых колонок в таблице

Завершение активной сессии

Для завершения активной сессии необходимо на странице просмотра, используя чекбокс ☐, выбрать необходимую сессию и в панели над таблицей нажать на ☒.



Сессия закрывается только в системе NAICE. CoA-запрос не отправляется, фактическое сетевое подключение может остаться активным.

Завершить сессию?

RADIUS-сессия пользователя mikhail.grachev в системе NAICE будет завершена.
CoA-запрос отправлен не будет.
Фактическое сетевое подключение может остаться активным.

Отмена Подтвердить

Рисунок 43. Подтверждение завершения одной сессии

При нажатии на кнопку завершения появляется модальное окно с информацией о том, что RADIUS-сессия пользователя будет завершена в системе NAICE и CoA-запрос отправлен не будет.

Для массового завершения сессий используйте чекбоксы в первой колонке таблицы:

Время последней активности	Пользователь	Источник идентификации	MAC-адрес клиента	Имя узла	Дата создания записи	NAS IP	ID сессии
☒ 02.02.2025 17:01:25	mikhail.grachev	mikhail.grachev	74:56:3C:E7:40:BE	naice2.loc	02.02.2025 17:01:25	172.16.0.210	ccc061bc-6440-3cda-4ec1-d...
☐ 02.02.2025 17:05:15	veronika.karaeva	veronika.karaeva	20:0B:C7:28:20:A8	naice1.loc	02.02.2025 17:05:15	172.16.0.211	9abd5e49-1dde-8a5c-a89e-8...
☐ 02.02.2025 17:07:47	alisa.agapova	alisa.agapova	00:00:40:11:AD:0D	naice1.loc	02.02.2025 17:07:47	172.16.0.219	5ac00e42-73d1-e2b0-b61f-b...
☐ 02.02.2025 17:15:32	yuliya.izmailova	yuliya.izmailova	A8:A1:59:AD:73:E5	naice2.loc	02.02.2025 17:15:32	172.16.2.44	a21b1ee0-46fb-938c-0a26-2...
☐ 02.02.2025 17:19:50	yuriy.dmitriev	yuriy.dmitriev	B8:2A:A9:5E:C4:5F	naice3.loc	02.02.2025 17:19:50	172.16.0.38	c1db4306-5804-ccfd-28fe-fc...
☐ 02.02.2025 17:23:50	elizar.romanov	elizar.romanov	C8:A3:62:2C:39:C5	naice2.loc	02.02.2025 17:23:50	172.16.1.149	5538bc15-a11e-cec7-d5eb-6...
☐ 02.02.2025 17:24:50	gleb.chernyahovskiy	gleb.chernyahovskiy	5C:E9:31:F9:B5:6F	naice1.loc	02.02.2025 17:24:50	172.16.2.45	06d2ae88-21d9-8c2c-c8b8-b...
☐ 02.02.2025 17:25:55	svetlana.chagina	svetlana.chagina	FC:70:2E:02:01:4F	naice2.loc	02.02.2025 17:25:55	172.16.0.194	5667376d-87a2-a3c3-c7bf-4...
☐ 02.02.2025 17:27:17	dmitriy.volkov	dmitriy.volkov	EC:B1:E0:82:9F:40	naice2.loc	02.02.2025 17:27:17	172.16.2.47	a4274bf3-7882-ecbc-78c7-df...
☐ 02.02.2025 17:28:13	egor.novikov	egor.novikov	34:0A:33:25:70:7E	naice3.loc	02.02.2025 17:28:13	172.16.0.193	a25bd1c1-b488-151d-022b-...
☐ 02.02.2025 17:29:23	artem.panchenko	artem.panchenko	2C:CF:67:10:FC:81	naice2.loc	02.02.2025 17:29:23	172.16.0.196	889ab8e7-545e-a92e-4251-5...
☐ 02.02.2025 17:29:45	dariya.harlamova	dariya.harlamova	A8:A1:59:AD:73:E5	naice1.loc	02.02.2025 17:29:45	172.16.1.150	bbec4c65-3bde-a771-385d-4...

Рисунок 44. Чекбокс выделения сессии

После выделения одной или нескольких сессий кнопка становится активной и позволяет завершить все выбранные сессии:

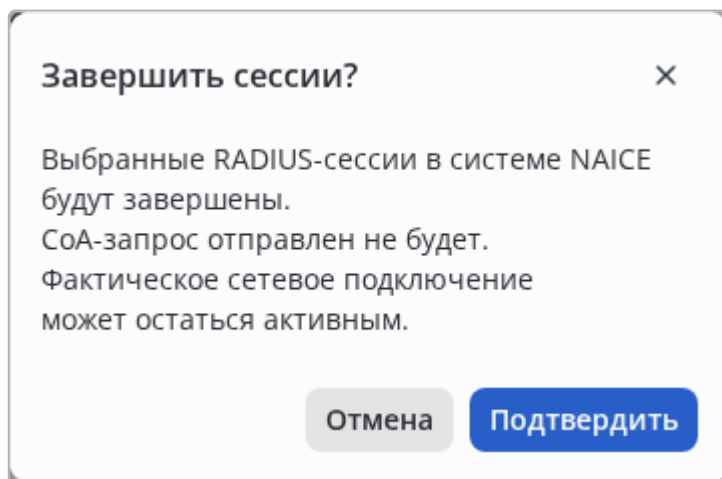


Рисунок 45. Подтверждение завершения нескольких сессий

Действие кнопки завершения аналогично получению RADIUS Accounting Stop пакета - сессия закрывается в системе NAICE и освобождается квота для подключения нового пользователя.



Для использования кнопки завершения сессии необходимы привилегии на редактирование журнала мониторинга активных сессий.

Как завершается сессия

Сессия считается активной с момента успешной аутентификации пользователя и отображается в таблице до одного из следующих событий:

- Получение пакета *RADIUS Accounting Stop* - сессия завершается автоматически, квота одновременных подключений освобождается.
- Таймаут неактивности - если в течение заданного периода по сессии не поступают Accounting пакеты (Interim-Update), система автоматически завершает сессию. Время жизни настраивается в разделе [Лимит RADIUS-сессий](#).
-

Ручное завершение администратором - сессия закрывается в системе NAICE, квота одновременных подключений освобождается. CoA-запрос не отправляется.

После завершения сессия исключается из списка активных и перестает учитываться при проверке ограничения одновременных сессий. В [журнале событий](#) фиксируется событие с указанием причины закрытия сессии.

TACACS+

Журнал подключений



Данный раздел содержит информацию по настройке функционала, доступ к которому приобретается отдельно с помощью дополнительной опции лицензии NAICE-TACACS+. По вопросам приобретения функционала обращайтесь к Вашему менеджеру или на электронную почту eltex@eltex-co.ru.

Описание

Журнал подключений TACACS+ позволяет просматривать подключения администраторов сетевых устройств по протоколу TACACS+ за определенный период времени, производить фильтрацию для поиска необходимых записей и анализировать детальную информацию об определенном запросе.

Просмотр списка подключений TACACS+

TACACS+										
Журнал подключений										
Учёт команд (accounting)										
Каждую минуту За последний месяц Период										
Время подключения	Статус	Подробнее	Имя узла	Тип пакета	Пользователь	Имя устройства	Причина ошибки	Адрес пользователя	Уровень привилегий	ID сессии
02.02.2025 10:00:00	Успешно		naice1.loc	AUTHENTICATION	mikhail.grachev	sw3102-5		192.168.0.210	1	8981842260656128
02.02.2025 09:48:00	Успешно		naice3.loc	AUTHORIZATION	veronika.karaeva	sw3102-2		192.168.0.211	1	6488106203086848
02.02.2025 09:43:00	Успешно		naice3.loc	AUTHORIZATION	alisa.agapova	sw301-1p		192.168.0.219	15	839972996807936
02.02.2025 09:38:00	Успешно		naice2.loc	AUTHORIZATION	yuliy.izmailova	sw3101-1t		192.168.2.44	7	show port-security
02.02.2025 09:38:00	Успешно		naice1.loc	AUTHORIZATION	yuriy.dmitriev	sw2410-1		192.168.0.38	1	show version
02.02.2025 09:28:00	Успешно		naice1.loc	AUTHENTICATION	elizar.romanov	wlc281-2		192.168.1.149	1	2723169678917632
02.02.2025 09:27:00	Успешно		naice3.loc	AUTHORIZATION	gleb.chernyakovskiy	sw3101-2t		192.168.2.45	15	switchport access vlan 16
02.02.2025 09:25:00	Успешно		naice2.loc	AUTHORIZATION	svetlana.chagina	sw3101-1p		192.168.0.194	7	show flow-control
02.02.2025 09:21:00	Успешно		naice2.loc	AUTHORIZATION	dmitriy.volkov	sw3102-1t		192.168.2.47	15	interface switchport trunk
02.02.2025 09:20:00	Отклонено		naice1.loc	AUTHORIZATION	egor.novikov	sw3101-2	Command not defined in...	192.168.0.193	1	show running-config
02.02.2025 09:20:00	Успешно		naice1.loc	AUTHORIZATION	artem.panchenko	sw3101-3p		192.168.0.196	1	show spanning-tree
02.02.2025 09:18:00	Успешно		naice3.loc	AUTHENTICATION	dariya.harlamova	sw2410-3		192.168.1.150	15	167768286242432
02.02.2025 09:14:00	Успешно		naice3.loc	AUTHENTICATION	aleksandr.cherkasov	sw2512-1		192.168.0.46	1	show bootvar
02.02.2025 09:12:00	Отклонено		naice2.loc	AUTHENTICATION	nikita.bondarenko	sw301-1	Identity user not found	192.168.0.218	1	3112534305406976
02.02.2025 09:14:00	Успешно		naice1.loc	AUTHORIZATION	denis.kastanaev	sw2410-2		192.168.1.148	15	interface GigabitEthernet...

Рисунок 46. Таблица со списком подключений по TACACS+

Таблица по умолчанию содержит колонки:

- Время подключения — время, когда была произведена попытка подключения.
- Статус — статус сессии, может принимать значения:
 - Успешно — авторизация/аутентификация была пройдена успешно;
 - Отклонено — авторизация/аутентификация была отклонена;
 - Истекло — сессия была завершена по истечении определенного времени;
- Подробнее — ссылка для открытия детальной страницы, на которой содержится подробная информация о подключении.
- Имя узла — имя узла NAICE, которым сформировано событие. Это поле может быть полезно при кластерной установке NAICE.

Тип пакета — может принимать значения "AUTHENTICATION" или "AUTHORIZATION" в зависимости от запроса.

- Пользователь — логин администратора, с которым проходило подключение.
- Имя устройства — имя [сетевого устройства](#), на котором происходило подключение.
- Причина ошибки — описание ошибки, повлекшей неуспешную аутентификацию или авторизацию.
- Адрес пользователя — IP адрес устройства, с которого администратор выполнял подключение.
- Уровень привилегий — значение уровня привилегий, назначенного администратору в рамках данного подключения.
- Команда — название команды на сетевом устройстве, на авторизацию которой производился запрос.
- ID сессии — идентификатор сессии TACACS+.

Также доступны дополнительные колонки, настраиваемые в  в шапке таблицы:

- IP устройства — адрес устройства, на которое выполнялось подключение.
- Политика аутентификации — название правила политики аутентификации, которое было применено в рамках данной сессии.
- Политика авторизации — название правила политики авторизации, которое было применено в рамках данной сессии.
- Порт — название протокола или номер порта, по которому было выполнено подключение на устройство.
- Тип устройства — тип устройства, который был определен исходя из настроек [устройства](#).
- Местоположение устройства — местоположение устройства, которое определяется из настроек [устройства](#).
- Профиль TACACS — название профиля TACACS, назначенного администратору в результате авторизации.
- Набор команд — название набора команд, доступных администратору для выполнения на устройстве.

Элементы управления:



Рисунок 47. Настройки отображения подключений в журнале

- Частота обновления — настройка частоты автоматического перечитывания сессий TACACS.
- Промежуток времени — выбор фиксированного временного периода, в который происходила активность по сессиям для отображения.
- Период — выбор произвольного временного интервала, в который происходила активность по сессиям для отображения.

 — обновить данные таблицы вручную.

-  — открыть окно настройки отображаемых колонок таблицы.
-  **Фильтры** — открыть окно настройки фильтрации.



При пролистывании первых 25 элементов таблицы параметр "Частота обновления" переходит в состояние "Отключено". Для возврата нужно либо указать вручную время обновления, либо обновить данные нажатием на кнопку .

Фильтрация настраивается в следующем окне:

Фильтры

Тип пакета Выберите тип	Пользователь Введите логин	Статус Выберите статус
IP устройства 0.0.0.0	Имя устройства Введите имя	Адрес пользователя 0.0.0.0
Порт Введите порт	Команда Введите команду	

Рисунок 48. Окно настройки фильтрации записей

Фильтрация записей доступна по параметрам "Тип пакета", "Пользователь", "Статус", "IP устройства", "Имя устройства", "Адрес пользователя", "Порт" и "Команда".



Для адресов устройства и пользователя доступен поиск по частичному совпадению любого октета/октетов IP-адреса.

Кнопка **Сбросить все** предназначена для сброса настроенных параметров поиска.

В настройках таблицы  можно сменить состав отображаемых колонок.

Кнопка **Сбросить все** предназначена для сброса настроенных колонок к состоянию по умолчанию (неактивно, пока состоянию по умолчанию не изменено).

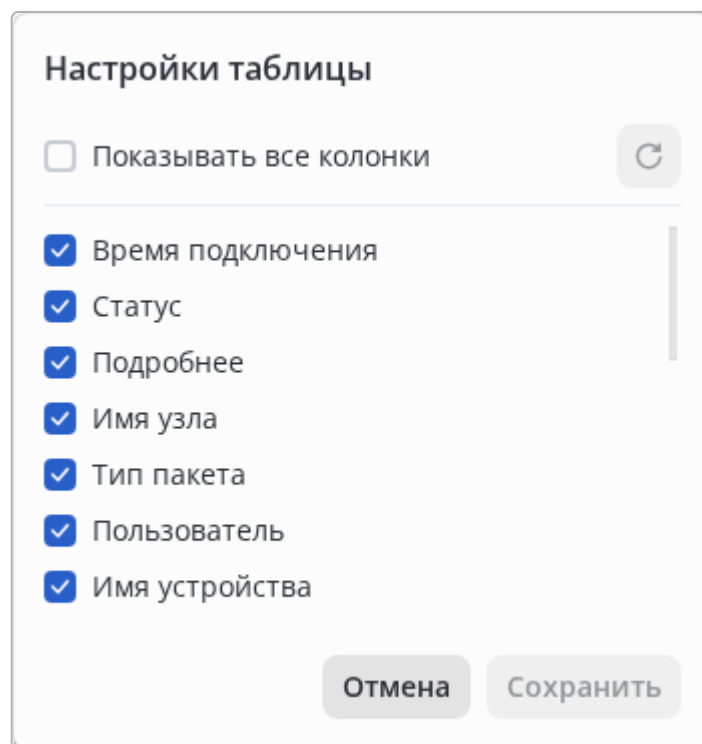


Рисунок 49. Окно настройки отображаемых колонок в таблице

Просмотр детальной информации о подключении

Для просмотра детальной информации о подключении из таблицы с журналом подключений необходимо кликнуть на  в колонке "Подробнее" для выбранной сессии.

Общая информация	
Packet type	AUTHENTICATION
STATUS	PASS
Session ID	525945328
Message Text	Device-Administration: Command Authorization succeeded
Username	denis.smirnov
Authorization policy	SC >> Authorization Rule 1
Matched Command Set	allow-all
Command From Device	tacacs-server host 100.110.3.81 key testing123
Детали аутентификации	
Event	SUCCESS
Параметры пакета TACACS	
Authentication Method	TacacsPlus
Authentication Privilege Level	15
Authentication Type	PAP
Authentication Service	Login

Рисунок 50. Детальная информация о сессии

Информация на странице разделена на 4 блока:

- **Общая информация** — краткая и наиболее важная информация о сессии;

Детали аутентификации — детальная информация об аутентификации, которая может быть полезная для отладки;

- Детали авторизации — детальная информация об авторизации, которая может быть полезная для отладки;
- Параметры пакета TACACS — прочие атрибуты, полученные NAICE в запросе TACACS.



Отображение блоков "Детали аутентификации" и "Детали авторизации" зависит от типа пакета в сессии.

Учёт команд (accounting)



Данный раздел содержит информацию по настройке функционала, доступ к которому приобретается отдельно с помощью дополнительной опции лицензии NAICE-TACACS+. По вопросам приобретения функционала обращайтесь к Вашему менеджеру или на электронную почту eltex@eltex-co.ru.

Описание

Журнал учета команд TACACS+ позволяет просматривать информацию о действиях администраторов сетевых устройств по протоколу TACACS+ за определенный период времени, производить фильтрацию для поиска необходимых записей.

Просмотр списка учета команд TACACS+

The screenshot shows the 'TACACS+' section with the 'Accounting' tab selected. It displays a table of command logs with columns for connection time, event type, user, command, device name, IP address, and user address. The table contains 5 entries. At the bottom, it indicates 'Всего элементов: 5' and 'Время последнего обновления: 02.02.2025 10:00:00'.

Время подключения ↓	Тип события	Пользователь	Команда	Имя устройства	IP устройства	Адрес пользователя
02.02.2025 10:00:00	COMMAND	Hayley	sumptus volo thorax	Hayley Device	117.143.110.35	240.50.199.204
02.02.2025 09:00:00	LOGIN	Edythe	adnuo maxime natus	Edythe Device	173.234.54.233	67.76.125.149
02.02.2025 08:00:00	LOGOUT	Kyler	aer amplius tersus	Kyler Device	192.109.225.246	2.169.127.159
02.02.2025 07:00:00	LOGIN	Janie	undique civitas fugit	Janie Device	5.101.6.27	7.130.63.26
02.02.2025 06:00:00	LOGIN	Salma	admiratio tyrannus talio	Salma Device	38.190.41.50	240.148.95.248

Рисунок 51. Таблица со списком учета команд по TACACS+

Таблица по умолчанию содержит колонки:

- Время подключения - время, когда была произведена попытка подключения.
- Тип события - В зависимости от события может принимать значения: LOGIN - для событий входа, COMMAND - для событий команды, EXIT - для событий выхода.
- Пользователь - логин администратора, с которым проходило подключение.
- Команда - название команды, которая выполнялась на сетевом устройстве.
- Имя устройства - имя [сетевого устройства](#), на котором происходило подключение.

IP устройства - адрес устройства, на которое выполнялось подключение.

- Адрес пользователя - IP адрес устройства, с которого администратор выполнял подключение.
- ID сессии - идентификатор сессии TACACS+.

Также доступны дополнительные колонки, настраиваемые в  в шапке таблицы:

- Уровень привилегий - значение уровня привилегий, назначенного администратору в рамках данного подключения.
- Порт - название протокола или номер порта, по которому было выполнено подключение на устройство.
- Метод аутентификации - метод аутентификации пользователя, с помощью которого происходил учет команды.
- Сервис аутентификации - имя сервиса аутентификации, через который происходил учет команды.
- Протокол аутентификации - название протокола аутентификации, по которому происходил учет команды.
- Аргументы запроса - аргументы запроса, по которому происходил учет команды.

Элементы управления:

Каждую минуту

▼

За последний месяц

▼

Период

☰

🔄

🔍

🔍 Фильтры

Рисунок 52. Настройки отображения подключений в журнале

- Частота обновления - настройка частоты автоматического перечитывания событий TACACS.
- Промежуток времени - выбор временного периода, в который происходила активность по сессиям для отображения.
- Период - выбор произвольного временного интервала, в который происходила активность по сессиям для отображения.
-  - обновить данные таблицы вручную.
-  - открыть окно настройки отображаемых колонок таблицы.
-  **Фильтры** - открыть окно настройки фильтрации.



При пролистывании первых 25 элементов таблицы параметр "Частота обновления" переходит в состояние "Отключено". Для возврата нужно либо указать вручную время обновления, либо обновить данные нажатием на кнопку .

Фильтрация настраивается в следующем окне:

Фильтры

Пользователь Введите логин

IP устройства 0.0.0.0

Имя устройства Введите имя

Адрес пользователя 0.0.0.0

Порт Введите порт

Команда Введите команду

Заккрыть Применить

Рисунок 53. Окно настройки фильтрации записей

Фильтрация записей доступна по параметрам "Пользователь", "IP устройства", "Имя устройства", "Адрес пользователя", "Порт" и "Команда".



Для адресов устройства и пользователя доступен поиск по частичному совпадению любого октета/октетов IP-адреса.

Кнопка **Сбросить все** предназначена для сброса настроенных параметров поиска.

В настройках таблицы  можно сменить состав отображаемых колонок.

Кнопка **Сбросить все** предназначена для сброса настроенных колонок к состоянию по умолчанию (неактивно, пока состоянию по умолчанию не изменено).

Настройки таблицы

☐ Показывать все колонки

☒ Время подключения

☒ Тип события

☒ Пользователь

☒ Команда

☒ Имя устройства

☒ IP устройства

☒ Адрес пользователя

Отмена Сохранить

Рисунок 54. Окно настройки отображаемых колонок в таблице

Система

Системные события

Описание

Журнал системных событий отображает информацию о происходящих в системе событиях, таких как активация лицензии, вход/выход администратора из системы, создание, редактирование, удаление различных записей и т.п. Со списком возможных событий можно ознакомиться на странице [:system/list-events.html](http://system/list-events.html).

Для удобства анализа событий существует возможность выбрать период возникновения событий, их уровень критичности, к какой группе относятся события. Так же доступен поиск определенного события тексту его сообщения.

Просмотр системных событий

Мониторинг > Система > Системные события

Система

Системные события

Маршруты событий

Каждую минуту

Фильтры

Поиск по сообщениям

Дата	Имя узла	Уровень	Сообщение
02.02.2025 10:00:00	naice1.eltex.loc	ERROR	Журнал событий - Язык журнала событий: en → de
02.02.2025 09:00:00	naice3.eltex.loc	DEBUG	Срок хранения сессий, дней: 16 → 9.
02.02.2025 08:00:00	naice3.eltex.loc	DEBUG	Парольные политики - Пароль пользователей системы не должен содержать логин: включено → выключено
02.02.2025 07:00:00	naice3.eltex.loc	DEBUG	Парольные политики - Отправлять уведомления о создании пользователя системы: включено → выключено
02.02.2025 06:00:00	naice1.eltex.loc	DEBUG	Журнал событий - Срок хранения событий в журнале, дней: 12 → 14
02.02.2025 05:00:00	naice2.eltex.loc	WARNING	Журнал событий - Срок хранения событий в журнале, дней: 13 → 13
02.02.2025 04:00:00	naice3.eltex.loc	WARNING	Срок хранения сессий, дней: 2 → 22
02.02.2025 03:00:00	naice2.eltex.loc	DEBUG	Срок хранения сессий, дней: 11 → 29
02.02.2025 02:00:00	naice1.eltex.loc	DEBUG	Порт аутентификации и учета команд(accounting): 62687 → 38620.
02.02.2025 01:00:00	naice1.eltex.loc	INFO	Парольные политики - Пароль пользователей системы должен содержать заглавные буквы: включено → выключено
02.02.2025 00:00:00	naice1.eltex.loc	INFO	Парольные политики - Пароль пользователей системы должен содержать строчные буквы: включено → выключено
01.02.2025 23:00:00	naice3.eltex.loc	INFO	Парольные политики - Пароль пользователей системы должен содержать заглавные буквы: включено → выключено
01.02.2025 22:00:00	naice1.eltex.loc	DEBUG	Парольные политики - Отправлять уведомления об изменении данных существующего пользователя системы: включено → выключено
01.02.2025 21:00:00	naice3.eltex.loc	ERROR	Парольные политики - Пароль пользователей системы не должен содержать логин: включено → выключено
01.02.2025 20:00:00	naice2.eltex.loc	INFO	Парольные политики - Шлюз для отправки email уведомлений: выключено → SMTP Gateway

Всего элементов: 23

Время последнего обновления: 02.02.2025 10:00:01

Рисунок 55. Таблица со списком системных событий

Таблица по умолчанию содержит колонки:

- Дата - дата и время события.
- Имя узла - имя узла NAICE, которым сформировано событие. Это поле может быть полезно при кластерной установке NAICE.
- Уровень - уровень логирования события.
- Сообщение - текстовое описание события.

Так же доступны дополнительные колонки, настраиваемые через  в шапке таблицы:

- IP-адрес - адрес хоста, вызвавшего создание события.
- Группа - группа, к которой относится событие. Со списком возможных групп событий можно также ознакомиться на странице [:system/list-events.html](http://system/list-events.html).
- Ключ - результат выполнения действий, отраженных в событии.
-

Автор - логин **пользователя системы**, инициировавшего событие. Если событие было вызвано логикой работы самой системы, то отображается логин **system**.

- Роль - **роль** системного пользователя, вызвавшего событие.



Колонки **Дата** и **Сообщение** не могут быть отключены.

Рисунок 56. Настройка отображаемых колонок таблицы системных событий

Для сброса всех настроек к состоянию по умолчанию используется кнопка  в верхнем правом углу модального окна.

Элементы управления:

-  **Фильтры** - Открыть окно настройки фильтрации.
-  - Открыть окно настройки отображаемых колонок таблицы.
-  - Изменить текущий порядок сортировки. Сортировка доступна только по колонке **Дата**.
-  - обновить данные таблицы вручную.
- **Частота обновления** - настройка частоты автоматического перечитывания системных событий.



При проматывании первых 25 элементов таблицы параметр "Частота обновления" переходит в состояние "Отключено". Для возврата нужно либо указать ручную время обновления, либо обновить страницу браузера.

- **Поиск по сообщениям** - регистронезависимый поиск в колонке **Сообщение**.

🔍

Поиск по сообщениям

Рисунок 57. Поиск по сообщениям



Для сброса выражения поиска необходимо нажать кнопку **×** справа в форме поиска.

Кнопка не отображается, пока не введено какое-либо значение.

Фильтрация настраивается в следующем окне:

Фильтры

Выберите период

Период

Уровень

Выберите уровень

Группа

Выберите группу

Ключ

Выберите ключ

Автор

Введите логин

Роль

Введите роль

IP

0.0.0.0

Заккрыть

Применить

Рисунок 58. Окно настройки фильтрации записей

Фильтрация записей доступна по параметрам:

- **Выберите период** - позволяет выбрать временной период с точностью до даты и времени.
- **Уровень** - позволяет выбрать уровень отображаемых событий:
 - **INFO** - отображать события уровня **INFO**, **WARNING**, **ERROR**.
 - **DEBUG** - отображать события всех уровней.
 - **WARNING** - отображать события уровня **WARNING**, **ERROR**.
 - **ERROR** - отображать события уровня **ERROR**.
- **Группа** - выбор отображаемой группы событий.
- **Ключ** - выбор типа события из определенной группы. Если группа не выбрана - выбор ключа недоступен.
- **Автор** - фильтр по **пользователю системы**, инициировавшему события.
- **Роль** - **роль** системного пользователя, связанная с событием.
- **IP-адрес** - фильтр по адресу хоста, с которого было инициировано событие. Доступна фильтрация по частичному совпадению любого октета/октетов.

Для сброса всех настроек к состоянию по умолчанию используется кнопка **Сбросить все** в верхнем правом углу окна выбора параметров фильтрации. Кнопка становится видима только если выбран хотя бы один фильтр.

Список системных событий



Содержание поля **Сообщение** для событий отображается в соответствии с языком, выбранным в настройке **Язык системы** в разделе [Общие настройки](#)



Некоторые функции, описанные на данной странице, доступны только при наличии расширенной лицензии. Такие функции помечены специальными метками в виде цветных значков рядом с наименованием.

События — Лицензирование

Название события	Описание	Уровень	Сообщение	Источник
Активация лицензии	Активация лицензии — результат успешного общения с ELM или локальная проверка PLR	INFO	Лицензия <productId> успешно активирована	Gulo
Загрузка файла лицензии	Загрузка файла лицензии	INFO	Лицензия <fileType> для <productId> успешно загружена для <hostname>	Пользователь / UI
Демо режим	Продукт запущен в демо режиме	WARNING	Продукт запущен в демо режиме	Gulo
Лицензия принята	Лицензия успешно применена (в сервисах, предоставляющих услугу — Ovis, Aquila)	DEBUG	Лицензия <productId> применена в <service>. Параметры: <params>	Ovis / Aquila
Функциональность ограничена	Ограничение доступа к функционалу (по разным причинам)	WARNING	Ограничение доступа к функционалу	Ovis / Aquila
Лицензия удалена	Лицензия удалена	INFO	Лицензия <productId> удалена	Пользователь / UI
Ошибка активации лицензии	Ошибка активации лицензии	ERROR	Ошибка активации лицензии <productId>: <error>	Gulo

Название события	Описание	Уровень	Сообщение	Источник
Обновление файла лицензии	Лицензия переведена в статус (init - ready, вручную - backup и т.п.)	DEBUG	Лицензия <productId> переведена в статус <status>	Gulo
Успешное создание файла активации лицензии	Файл активации сформирован (после обращения к EPG-сервису)	INFO	Файл активации сформирован для <productId>	Gulo
Ошибка создания файла активации лицензии	Ошибка формирования файла активации (ошибка обращения к EPG-сервису)	ERROR	Ошибка формирования файла активации для <productId> : <error>	Gulo
Файл лицензии с ключом продукта уже существует	PK-файл уже существует	ERROR	PK-файл для <hostname> уже существует	Ursus
Ошибка загрузки файла лицензии	Ошибка загрузки файла лицензии	ERROR	Ошибка загрузки <fileType> файла лицензии для <productId> на <hostname>	Gulo
Запущена активация лицензии	Запущена активация лицензии	INFO	Активирует лицензию <productId>.	Gavia
Создание файла активации лицензии	Создание файла активации лицензии	INFO	Создаёт файл активации для лицензии <productId>.	Gavia
Причина сброса лицензии	Произошёл сброс лицензии и передана причина сброса.	ERROR	Лицензия будет сброшена. <dropReason>	Gulo
Достигнут лимит гостевых эндпоинтов демо лицензии	Превышен лимит гостевых эндпоинтов в демо-режиме	WARNING	Превышен лимит в демо режиме на <limit> гостевых эндпоинтов	Gulo

Название события	Описание	Уровень	Сообщение	Источник
Ошибка инициализации в реципиенте	Ошибка инициализации лицензии в реципиенте	ERROR	При применении лицензии произошла ошибка в работе сервиса	Gulo

События — RADIUS-аутентификация

Название события	Описание	Уровень	Сообщение	Источник
Создана RADIUS-сессия	Создана новая RADIUS-сессия	INFO	RADIUS сессия-создана.	Ovis
Успешная RADIUS-аутентификация	RADIUS-сессия успешно прошла аутентификацию	INFO	RADIUS-сессия прошла аутентификацию.	Ovis
Истекла RADIUS-сессия	RADIUS-сессия истекла	INFO	RADIUS-сессия протухла.	Ovis
Отклонена RADIUS-сессия	RADIUS-сессия отклонена	WARNING	RADIUS-сессия отклонена.	Ovis
Ручное завершение активной RADIUS-сессии	Активная RADIUS-сессия была завершена пользователем системы	INFO	RADIUS-сессия пользователя <code><identityUserName></code> (mac <code><userMAC></code> , nasIp <code><userIp></code>) остановлена администратором <code><adminLogin></code>	Gavia
Автоматическое завершение активной RADIUS-сессии	Активная RADIUS-сессия была завершена автоматически	INFO	RADIUS-сессия пользователя <code><identityUserName></code> (mac <code><userMAC></code> , nasIp <code><userIp></code>) остановлена автоматически	Ovis

События — Обновление привилегий ролей

Название события	Описание	Уровень	Сообщение	Источник
Пользователь системы создан	Создан новый пользователь системы	INFO	Создан пользователь системы с логином <code><login></code> и ролью <code><role></code> .	Пользователь / UI
Пользователь системы изменен	Изменены данные пользователя системы	INFO	Изменен пользователь системы с логином <code><login></code> и ролью <code><role></code> .	Пользователь / UI

Название события	Описание	Уровень	Сообщение	Источник
Параметры учетной записи изменены пользователем	Пользователь изменил параметры своей учетной записи	INFO	Пользователь с логином <login> и ролью <role> изменил параметры своей учетной записи.	Пользователь / UI
Создана роль	Создана новая роль RBAC	INFO	Создана роль с именем <role>.	Пользователь / UI
Изменена роль	Изменены параметры роли RBAC	INFO	Отредактирована роль с именем <role>.	Пользователь / UI
Удалены роли	Удалены роли RBAC	INFO	Роли с именами <roles> были удалены.	Пользователь / UI

События — Обновление сетевых ресурсов

Название события	Описание	Уровень	Сообщение	Источник
Создано сетевое устройство	Создано новое сетевое устройство	INFO	Сетевое устройство <deviceName> было создано.	Пользователь / UI
Изменено сетевое устройство	Изменены параметры сетевого устройства	INFO	Сетевое устройство <deviceName> было изменено.	Пользователь / UI
Удалены сетевые устройства	Удалены сетевые устройства	INFO	Сетевые устройства <devicesNames> были удалены.	Пользователь / UI
Создана сетевая группа	Создана новая сетевая группа	INFO	Сетевая группа <groupName> была создана.	Пользователь / UI
Изменена сетевая группа	Изменены параметры сетевой группы	INFO	Сетевая группа <groupName> была изменена.	Пользователь / UI
Удалены сетевые группы	Удалены сетевые группы	INFO	Сетевые группы <groupsNames> были удалены.	Пользователь / UI

Название события	Описание	Уровень	Сообщение	Источник
Создан сетевой профиль	Создан новый сетевой профиль	INFO	Сетевой профиль <profileName> был создан.	Пользователь / UI
Изменен сетевой профиль	Изменены параметры сетевого профиля	INFO	Сетевой профиль <profileName> был изменен.	Пользователь / UI
Удалены сетевые профили	Удалены сетевые профили	INFO	Сетевые профили <profilesNames> были удалены.	Пользователь / UI

События — Обновление элементов управления идентификацией

Название события	Описание	Уровень	Сообщение	Источник
Создан пользователь сети	Создан новый пользователь сети	INFO	Пользователь сети <identityUserName> был создан.	Пользователь / UI
Изменен пользователь сети	Изменены параметры пользователя сети	INFO	Пользователь сети <identityUserName> был изменен.	Пользователь / UI
Удалены пользователи сети	Удалены пользователи сети	INFO	Пользователи сети <identityUsersNames> были удалены.	Пользователь / UI
Создана группа пользователей сети	Создана новая группа пользователей сети	INFO	Группа пользователей сети <identityUsersGroupName> была создана.	Пользователь / UI
Изменена группа пользователей сети	Изменены параметры группы пользователей сети	INFO	Группа пользователей сети <identityUsersGroupName> была изменена.	Пользователь / UI
Удалены группы пользователей сети	Удалены группы пользователей сети	INFO	Группы пользователей сети <identityUsersGroupsNames> были удалены.	Пользователь / UI

События — Обновление цепочки идентификации

Название события	Описание	Уровень	Сообщение	Источник

Название события	Описание	Уровень	Сообщение	Источник
Изменена цепочка идентификации	Изменены параметры цепочки идентификации	INFO	Цепочка идентификации <identitySequenceName> была изменена.	Пользователь / UI
Удалены цепочки идентификации	Удалены цепочки идентификации	INFO	Цепочки идентификации <identitySequencesNames> были удалены.	Пользователь / UI

События — Обновление внешних источников идентификации

Название события	Описание	Уровень	Сообщение	Источник
Создан внешний источник идентификации	Создан новый внешний источник идентификации	INFO	Внешний источник идентификации <externalSourceName> был создан.	Пользователь / UI
Изменен внешний источник идентификации	Изменены параметры внешнего источника идентификации	INFO	Внешний источник идентификации <externalSourceName> был изменен.	Пользователь / UI
Удалены внешние источники идентификации	Удалены внешние источники идентификации	INFO	Внешние источники идентификации <externalSourcesNames> были удалены.	Пользователь / UI
Пароль доменного компьютера успешно изменён	Пароль доменного компьютера успешно изменён	INFO	Успешное автоматическое изменение системой пароля у доменного компьютера <externalSourceComputerName> во внешнем источнике <externalSourceName> .	Ursus
Ошибка при изменении пароля доменного компьютера	Ошибка при изменении пароля доменного компьютера	ERROR	Произошла ошибка при автоматическом изменении пароля системой у доменного компьютера <externalSourceComputerName> во внешнем источнике <externalSourceName> .	Ursus

События — Обновление политик RADIUS

Название события	Описание	Уровень	Сообщение	Источник
Созданы наборы политик RADIUS	Созданы новые наборы политик RADIUS	INFO	Наборы политик <radiusPolicySetName> созданы.	Пользователь / UI
Изменены наборы политик RADIUS	Изменены параметры наборов политик RADIUS	INFO	Наборы политик <radiusPolicySetName> изменены.	Пользователь / UI
Удалены наборы политик RADIUS	Удалены наборы политик RADIUS	INFO	Наборы политик <radiusPolicySetName> удалены.	Пользователь / UI
Создан профиль авторизации RADIUS	Создан новый профиль авторизации RADIUS	INFO	Профиль авторизации <radiusAuthProfileName> создан.	Пользователь / UI
Изменен профиль авторизации RADIUS	Изменены параметры профиля авторизации RADIUS	INFO	Профиль авторизации <radiusAuthProfileName> изменен.	Пользователь / UI
Удалены профили авторизации RADIUS	Удалены профили авторизации RADIUS	INFO	Профили авторизации <radiusAuthProfilesNames> удалены.	Пользователь / UI
Создан список разрешенных протоколов RADIUS	Создан новый список разрешенных протоколов RADIUS	INFO	Список разрешенных протоколов <radiusAllowedProtocolName> создан.	Пользователь / UI
Изменен список разрешенных протоколов RADIUS	Изменены параметры списка разрешенных протоколов RADIUS	INFO	Список разрешенных протоколов <radiusAllowedProtocolName> изменен.	Пользователь / UI
Удалены списки разрешенных протоколов RADIUS	Удалены списки разрешенных протоколов RADIUS	INFO	Список разрешенных протоколов <radiusAllowedProtocolNames> удален.	Пользователь / UI
Создано условие RADIUS	Создано новое условие для политик RADIUS	INFO	Условие <radiusConditionName> создано.	Пользователь / UI

Название события	Описание	Уровень	Сообщение	Источник
Изменено условие RADIUS	Изменены параметры условия для политик RADIUS	INFO	Условие <radiusConditionName> изменено.	Пользователь / UI
Удалены условия RADIUS	Удалены условия для политик RADIUS	INFO	Условия <radiusConditionNames> удалены.	Пользователь / UI

События — Обновление профилирования

Название события	Описание	Уровень	Сообщение	Источник
Создана политика профилирования	Создана новая политика профилирования	INFO	Политика профилирования <policyName> была создана.	Пользователь / UI
Изменена политика профилирования	Изменены параметры политики профилирования	INFO	Политики профилирования <policyName> были изменены.	Пользователь / UI
Удалены политики профилирования	Удалены политики профилирования	INFO	Политики профилирования <policiesNames> были удалены.	Пользователь / UI
Создано условие профилирования	Создано новое условие профилирования	INFO	Условие профилирования <conditionName> было создано.	Пользователь / UI
Изменено условие профилирования	Изменены параметры условия профилирования	INFO	Условие профилирования <conditionName> было изменено.	Пользователь / UI
Удалены условия профилирования	Удалены условия профилирования	INFO	Условия профилирования <conditionsNames> были удалены.	Пользователь / UI
Создан логический профиль	Создан новый логический профиль.	INFO	Логический профиль <logicalProfileName> был создан.	Пользователь / UI
Изменён логический профиль	Изменены параметры логического профиля.	INFO	Логический профиль <logicalProfileName> был изменён.	Пользователь / UI

Название события	Описание	Уровень	Сообщение	Источник
Создан лог-коллектор	Создан новый лог-коллектор	INFO	Лог коллектор <logCollectorName> был создан.	Пользователь / UI
Изменен лог-коллектор	Изменены параметры лог-коллектора	INFO	Лог коллектор <logCollectorName> был изменен.	Пользователь / UI
Удалены лог-коллекторы	Удалены лог-коллекторы	INFO	Лог коллекторы <logCollectorsNames> были удалены.	Пользователь / UI
Пользователь отправил тестовое событие в лог коллектор	Пользователь отправил тестовое событие в лог коллектор.	INFO	Пользователь отправил тестовое событие в лог коллектор.	Пользователь / UI

События — Пользовательские сессии

Название события	Описание	Уровень	Сообщение	Источник
Создание пользовательской сессии	Пользователь вошел в систему	INFO	Пользователь <login> вошел в систему с правами <authorities> с IP <userId>.	Пользователь / UI
Завершение пользовательской сессии	Пользователь вышел из системы.	INFO	Пользователь <login> аутентифицированный через <sourceName> вышел из системы с ip <userId>.	Пользователь / UI
Разрыв пользовательской сессии	Сессия пользователя была прервана системой.	INFO	Сессия пользователя <login> аутентифицированного через <sourceName> с ip <userId> разорвана.	Пользователь / UI
Пользовательская сессия истекла	Сессия пользователя истекла.	INFO	Сессия пользователя <login> аутентифицированного через <sourceName> с ip <userId> истекла.	Пользователь / UI
Ошибка аутентификации: неверный логин	Попытка аутентификации с неверным логином.	WARNING	Пользователь провалил аутентификацию с логином <login> через источник <externalSourceName> с ip <userId>, неверный логин.	Пользователь / UI

Название события	Описание	Уровень	Сообщение	Источник
Ошибка аутентификации: неверный пароль	Попытка аутентификации с неверным паролем.	WARNING	Пользователь провалил аутентификацию с логином <login> через источник <externalSourceName> с ip <userIp> , неверный пароль.	Пользователь / UI
Ошибка аутентификации: пользователь деактивирован	Попытка аутентификации с деактивированным пользователем.	WARNING	Пользователь провалил аутентификацию с логином <login> через источник <externalSourceName> с ip <userIp> , отключенный аккаунт.	Пользователь / UI
Ошибка аутентификации: пустой логин	Попытка аутентификации с пустым логином.	ERROR	Попытка аутентификации через источник <externalSourceName> без логина с ip <userIp> .	Пользователь / UI
Ошибка аутентификации: пустой пароль	Попытка аутентификации с пустым паролем.	WARNING	Пользователь провалил аутентификацию с логином <login> через источник <externalSourceName> с ip <userIp> , пустой пароль.	Пользователь / UI
Ошибка аутентификации: роль не найдена	Попытка аутентификации с неподходящей ролью.	WARNING	Пользователь провалил аутентификацию с логином <login> через источник <externalSourceName> с ip <userIp> , подходящая роль не найдена.	Пользователь / UI
Ошибка аутентификации: внешний источник недоступен	Попытка аутентификации с недоступным внешним источником.	WARNING	Пользователь провалил аутентификацию с логином <login> через источник <externalSourceName> с ip <userIp> , внешний источник недоступен.	Пользователь / UI

Название события	Описание	Уровень	Сообщение	Источник
Остальные ошибки аутентификации	Остальные ошибки возникающие в ходе аутентификации	ERROR	Пользователь провалил аутентификацию с логином <login> через источник <externalSourceName> с ip <userIp>, ошибка: <error>.	Пользователь / UI

События — Обновление эндпоинтов

Название события	Описание	Уровень	Сообщение	Источник
Создан эндпоинт	Создан новый эндпоинт	INFO	Эндпоинт <endpointName> был создан.	Пользователь / UI
Изменены эндпоинты	Изменены параметры эндпоинтов	INFO	Эндпоинты <endpointsNames> были изменены.	Пользователь / UI
Удалены эндпоинты	Удалены эндпоинты	INFO	Эндпоинты <endpointsNames> были удалены.	Пользователь / UI
Создана группа эндпоинтов	Создана новая группа эндпоинтов	INFO	Группа эндпоинтов <endpointsGroupName> была создана.	Пользователь / UI
Изменена группа эндпоинтов	Изменены параметры группы эндпоинтов	INFO	Группа эндпоинтов <endpointsGroupName> была изменена.	Пользователь / UI
Удалены группы эндпоинтов	Удалены группы эндпоинтов	INFO	Группы эндпоинтов <endpointsGroupsNames> были удалены.	Пользователь / UI

События — Обновление настроек сервисов

Название события	Описание	Уровень	Сообщение	Источник
Запрос на изменение настроек сервисов	Изменение настроек сервисов	DEBUG	Произведен запрос на изменение настройки сервисов: <serviceName> <serviceName>.	Phoca
Применение настройки сервиса	Настройка сервиса применена	DEBUG	Применена настройка для сервиса <serviceName>.	<serviceName>

Название события	Описание	Уровень	Сообщение	Источник
Запрос на изменение настроек контейнеров	Изменение настроек контейнеров	DEBUG	Произведен запрос на изменение настройки контейнеров: <containerName> <containerName>.	Phoca
Применение настройки контейнера	Настройка контейнера применена	DEBUG	Применена настройка для контейнера <containerName>.	<containerName>

События — Обновление настроек системы

Название события	Описание	Уровень	Сообщение	Источник
Применение настроек системы	Изменение настроек системы	INFO	Изменены следующие параметры: - Настройка 1: "значение 1" → "значение 2" - Настройка 2: включено → выключено	Пользователь / UI

События — Обновление настроек сертификатов

Название события	Описание	Уровень	Сообщение	Источник
Создание доверенного сертификата	Доверенный сертификат был создан	INFO	Доверенный сертификат <certName> был создан.	Пользователь / UI
Изменение доверенного сертификата	Доверенный сертификат был изменен	INFO	Доверенный сертификат <certName> был изменен.	Пользователь / UI
Удаление доверенного сертификата	Доверенный сертификат был удален	INFO	Доверенные сертификаты <certNames> были удалены.	Пользователь / UI
Изменение статуса доверенного сертификата	Статус доверенного сертификата был изменен	WARNING	Статус доверенного сертификата <certName> был изменен на <status>.	Пользователь / UI
Истекает срок действия доверенного сертификата	Срок действия доверенного сертификата скоро кончится	WARNING	Доверенный сертификат <certificateName> истечёт <expirationDate> (через <daysLeft> дн.).	Phoca

Название события	Описание	Уровень	Сообщение	Источник
Срок действия доверенного сертификата истек	Закончился срок действия доверенного сертификата	ERROR	Срок действия доверенного сертификата <certificateName> истёк <expirationDate> .	Phoca

ADVANCED События — Портальные ошибки аутентификации и уведомлений

Название события	Описание	Уровень	Сообщение	Источник
Сервис аутентификации не доступен	Сервис портала недоступен.	ERROR	Сервис аутентификации <service> недоступен.	Castor
Ошибка отправки СМС сообщения	Произошла ошибка при отправке СМС при портальной авторизации.	ERROR	Ошибка отправки СМС на номер телефона <target> на портале <portalName> : <error> .	Castor

ADVANCED События — СМС-шлюз

Название события	Описание	Уровень	Сообщение	Источник
Получено демо СМС	Получено СМС от демо-шлюза.	INFO	Получено демо смс: <smsMessage>.	Bubo
Ошибка отправки уведомления на почту	Уведомление об ошибке при отправке электронного письма	ERROR	Ошибка при отправке электронного письма на адрес <email>: <error>	Bubo

ADVANCED События — TACACS+ Аутентификация

Название события	Описание	Уровень	Сообщение	Источник
Начало аутентификации доступа TACACS+	Пользователь начал аутентификацию доступа через TACACS+	INFO	Пользователь <suser> начал аутентификацию через <tacacsProtocol> .	Aquila

Название события	Описание	Уровень	Сообщение	Источник
Ошибка аутентификации доступа TACACS+	Пользователь не прошел аутентификацию доступа через TACACS+	INFO	Пользователь <suser> провалил аутентификацию через <tacacsProtocol>.	Aquila
Начало аутентификации enable TACACS+	Пользователь начал аутентификацию для изменения уровня привилегий	INFO	Пользователь <suser> начал изменение уровня привилегий на <privilegeLevel> через <tacacsProtocol>.	Aquila
Успешная аутентификация enable TACACS+	Пользователь успешно изменил уровень привилегий	INFO	Пользователь <suser> успешно изменил уровень привилегий на <privilegeLevel> через <tacacsProtocol>.	Aquila
Ошибка аутентификации enable TACACS+	Пользователь не смог изменить уровень привилегий	INFO	Пользователь <suser> провалил изменение уровня привилегий на <privilegeLevel> через <tacacsProtocol>.	Aquila

ADVANCED События — TACACS+ Авторизация

Название события	Описание	Уровень	Сообщение	Источник
Успешная авторизация доступа TACACS+	Пользователь успешно прошел авторизацию доступа	INFO	Пользователь <suser> прошел авторизацию через TACACS+.	Aquila
Ошибка авторизации доступа TACACS+	Пользователь не прошел авторизацию доступа	INFO	Пользователь <suser> провалил авторизацию через TACACS+.	Aquila
Успешная авторизация команды TACACS+	Пользователь авторизован для выполнения команды	INFO	Пользователь <suser> авторизован для выполнения команды <tacacsCommand>.	Aquila

Название события	Описание	Уровень	Сообщение	Источник
Ошибка авторизации команды TACACS+	Пользователь не авторизован для выполнения команды	INFO	Пользователь <user> провалил авторизацию для выполнения команды <tacacsCommand> .	Aquila

ADVANCED События — Учет активности TACACS+

Название события	Описание	Уровень	Сообщение	Источник
TACACS+ логин	Пользователь вошел в систему	INFO	Пользователь <user> вошел.	Aquila
TACACS+ логат	Пользователь вышел из системы	INFO	Пользователь <user> вышел.	Aquila
TACACS+ выполнение команды	Пользователь выполнил команду	INFO	Пользователь <user> выполнил команды <tacacsCommand> .	Aquila
Неизвестное событие TACACS+ accounting	Неизвестное событие аккаунтинга	INFO	Неизвестное событие аккаунтинга для пользователя <user>.	Aquila

ADVANCED События — Обновление порталов

Название события	Описание	Уровень	Сообщение	Источник
Создан портал	Создан новый портал	INFO	Портал <portalName> был создан.	Пользователь / UI
Изменен портал	Изменены параметры портала	INFO	Портал <portalName> был изменён.	Пользователь / UI
Удален портал	Удален портал	INFO	Портал <portalName> был удалён.	Пользователь / UI

ADVANCED События — Обновление политики TACACS+

Название события	Описание	Уровень	Сообщение	Источник
Создан набор политик TACACS+	Создан новый набор политик TACACS+	INFO	Набор политик TACACS+ <tacacsPolicySetName> был создан.	Пользователь / UI

Название события	Описание	Уровень	Сообщение	Источник
Изменены наборы политик TACACS+	Изменены параметры наборов политик TACACS+	INFO	Наборы политик TACACS+ <tacacsPolicySetsNames> были изменены.	Пользователь / UI
Удалены наборы политик TACACS+	Удалены наборы политик TACACS+	INFO	Наборы политик TACACS+ <tacacsPolicySetsNames> были удалены.	Пользователь / UI
Создан профиль TACACS+	Создан новый профиль TACACS+	INFO	Профиль TACACS+ <tacacsProfileName> был создан.	Пользователь / UI
Изменен профиль TACACS+	Изменены параметры профиля TACACS+	INFO	Профиль TACACS+ <tacacsProfileName> был изменен.	Пользователь / UI
Удалены профили TACACS+	Удалены профили TACACS+	INFO	Профили TACACS+ <tacacsProfilesNames> были удалены.	Пользователь / UI
Создан набор команд TACACS+	Создан новый набор команд TACACS+	INFO	Набор команд TACACS+ <tacacsCommandName> был создан.	Пользователь / UI
Изменен набор команд TACACS+	Изменены параметры набора команд TACACS+	INFO	Набор команд TACACS+ <tacacsCommandName> был изменен.	Пользователь / UI
Удалены наборы команд TACACS+	Удалены наборы команд TACACS+	INFO	Наборы команд TACACS+ <tacacsCommandsNames> были удалены.	Пользователь / UI
Создано условие TACACS+	Создано новое условие для политик TACACS+	INFO	Условие TACACS+ <tacacsConditionName> было создано.	Пользователь / UI
Изменено условие TACACS+	Изменены параметры условия для политик TACACS+	INFO	Условие TACACS+ <tacacsConditionName> было изменено.	Пользователь / UI

Название события	Описание	Уровень	Сообщение	Источник
Удалены условия TACACS+	Удалены условия для политик TACACS+	INFO	Условия TACACS+ <tacacsConditionsName> были удалены.	Пользователь / UI

ADVANCED События — Обновление шлюзов уведомлений

Название события	Описание	Уровень	Сообщение	Источник
Создание шлюза уведомлений	Создан новый шлюз уведомления	INFO	Шлюз уведомления <notificationGateway> был создан.	Пользователь / UI
Обновление шлюза уведомлений	Изменены параметры шлюза уведомления	INFO	Шлюз уведомления <notificationGateway> был изменён.	Пользователь / UI
Удаление шлюза уведомлений	Удалены шлюзы уведомления	INFO	Шлюзы уведомления <notificationGateways> были удалены.	Пользователь / UI

ADVANCED События — Обновление пользователей гостевых порталов

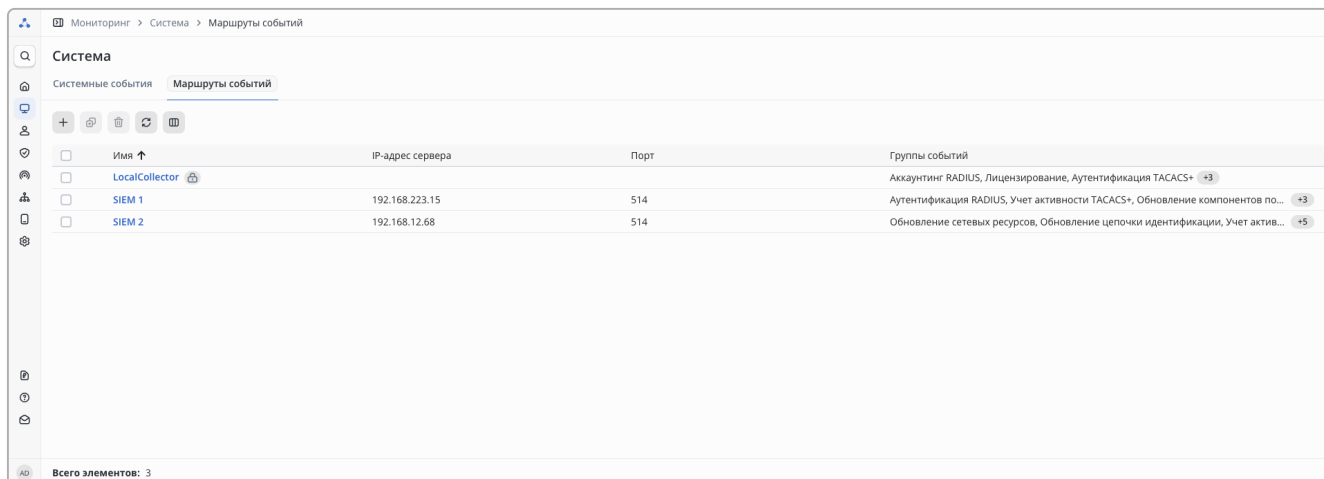
Название события	Описание	Уровень	Сообщение	Источник
Создан порталный пользователь	Создан новый порталный пользователь	INFO	Портальный пользователь <portalUserName> был создан.	Пользователь / UI
Изменен порталный пользователь	Изменены параметры порталного пользователя	INFO	Портальный пользователь <portalUserName> был изменён.	Пользователь / UI
Удалены порталные пользователи	Удалены порталные пользователи	INFO	Портальные пользователи <portalUsersNames> были удалены.	Пользователь / UI

Маршруты событий

Описание

Маршруты событий позволяют настраивать сбор и отправку событий системы по группам в формате "CEF" во внешние системы централизованного логирования и мониторинга событий - например, в SIEM-системы или лог-коллекторы. Это обеспечивает централизованный сбор, анализ и хранение событий, упрощая диагностику, аудит и контроль безопасности.

Просмотр маршрутов событий



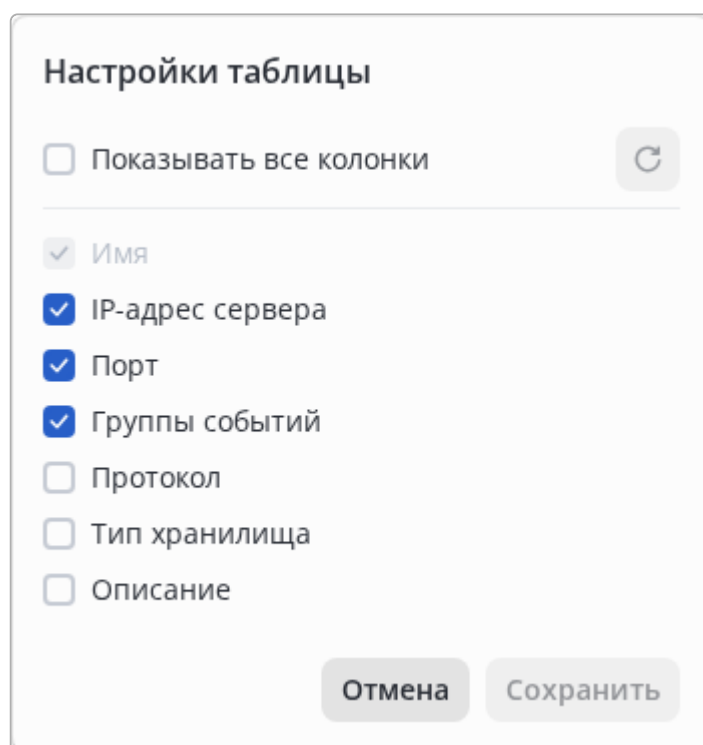
Имя	IP-адрес сервера	Порт	Группы событий
LocalCollector			Аккаунтинг RADIUS, Лицензирование, Аутентификация TACACS+ +3
SIEM 1	192.168.223.15	514	Аутентификация RADIUS, Учет активности TACACS+, Обновление компонентов по... +3
SIEM 2	192.168.12.68	514	Обновление сетевых ресурсов, Обновление цепочки идентификации, Учет актив... +5

Рисунок 59. Таблица со списком маршрутов событий

Таблица содержит следующие колонки:

- Имя - уникальное имя маршрута.
 -  - данная запись является системной и недоступна для удаления или редактирования.
- IP-адрес сервера - IP-адрес внешнего сервера-получателя логов.
- Порт - номер сетевого порта, на который будут отправляться события.

Настройка колонок таблицы маршрутов осуществляется в дополнительном меню доступном по нажатию кнопки 



Настройки таблицы

☐ Показывать все колонки

☒ Имя

☒ IP-адрес сервера

☒ Порт

☒ Группы событий

☐ Протокол

☐ Тип хранилища

☐ Описание

Отмена Сохранить

Рисунок 60. Настройка колонок таблицы

Полный список доступных колонок таблицы:

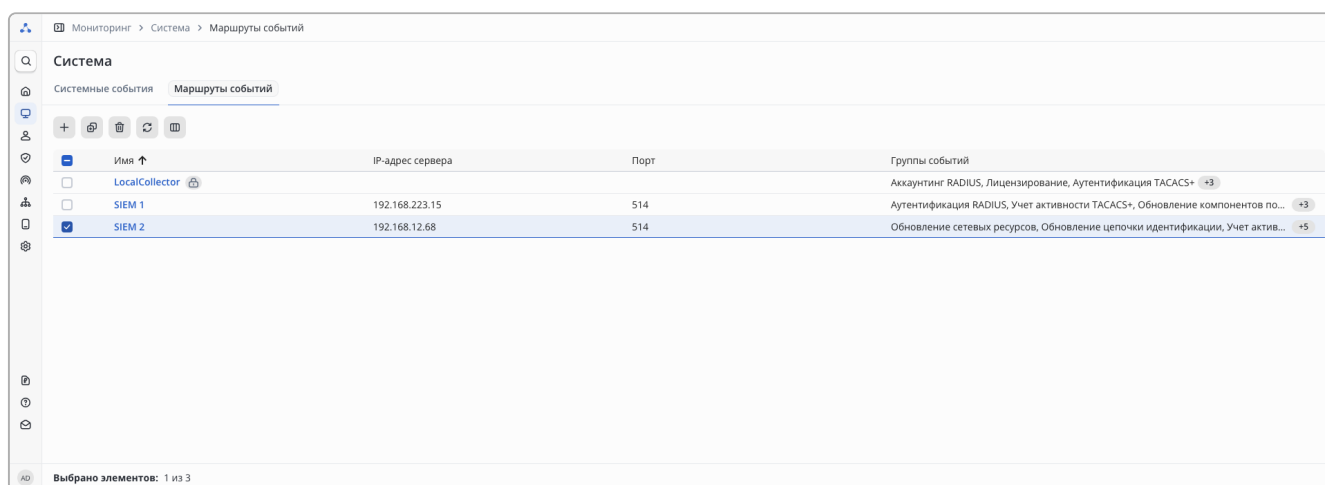
Имя - уникальное имя маршрута.

- IP-адрес сервера - IP-адрес сервера, принимающего события.
- Порт - номер сетевого порта, на который отправляются события.
- Группы событий - список групп событий, события которых будут отправляться по этому маршруту. В поле отображается сокращенный список (например, "Обновление привилегий ролей, Обновление внешних источников... +20"), при наведении курсора отображается полный список.
- Протокол - протокол передачи данных (UDP или TCP).
- Тип хранилища - тип хранилища маршрута событий (все созданные пользователем системы маршруты будут храниться в хранилище "Пользовательское").
- Описание - произвольное описание маршрута.

Страница содержит следующие элементы управления:

-  - Добавить новый элемент.
-  - Дублировать выбранный чекбоксом элемент. Становится активным, если выбран только один элемент в списке.
-  - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
-  - Обновить данные.
-  - Изменить текущий порядок сортировки (доступно на колонках "Имя", "Протокол", "Тип хранилища")
- ☐ - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (удаления или дублирования).

В нижней части страницы отображается общее количество элементов таблицы, а также количество выбранных чекбоксами элементов.



Имя	IP-адрес сервера	Порт	Группы событий
LocalCollector			Аккаунтинг RADIUS, Лицензирование, Аутентификация TACACS+ +3
SIEM 1	192.168.223.15	514	Аутентификация RADIUS, Учет активности TACACS+, Обновление компонентов по... +3
SIEM 2	192.168.12.68	514	Обновление сетевых ресурсов, Обновление цепочки идентификации, Учет актив... +5

Выбрано элементов: 1 из 3

Рисунок 61. Счетчик маршрутов

Системный маршрут событий

В таблице уже по умолчанию присутствует маршрут событий `LocalCollector` типа `Системное хранилище`.

Данный маршрут необходим для сбора событий "внутри" системы NAICE и их последующего хранения в локальной базе данных:

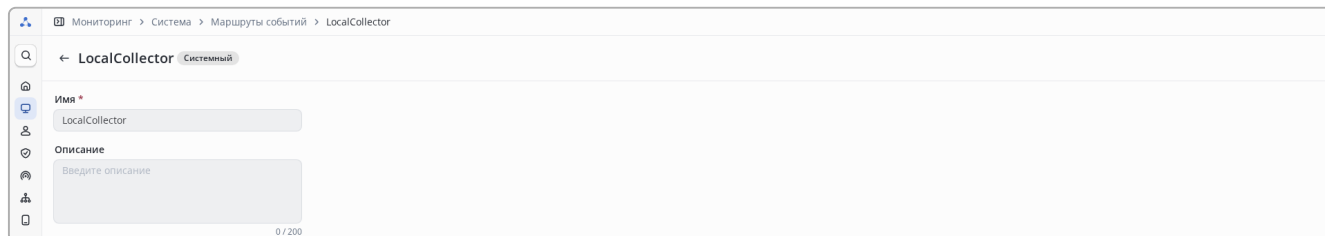


Рисунок 62. Системный маршрут "LocalCollector"

Маршрут `LocalCollector` уже содержит список выбранных обязательных групп событий сохраняемых в локальную базу данных и отображаемых в [журнале системных событий](#), они отображаются как заблокированные и не доступны для редактирования, другие группы можно редактировать при необходимости:

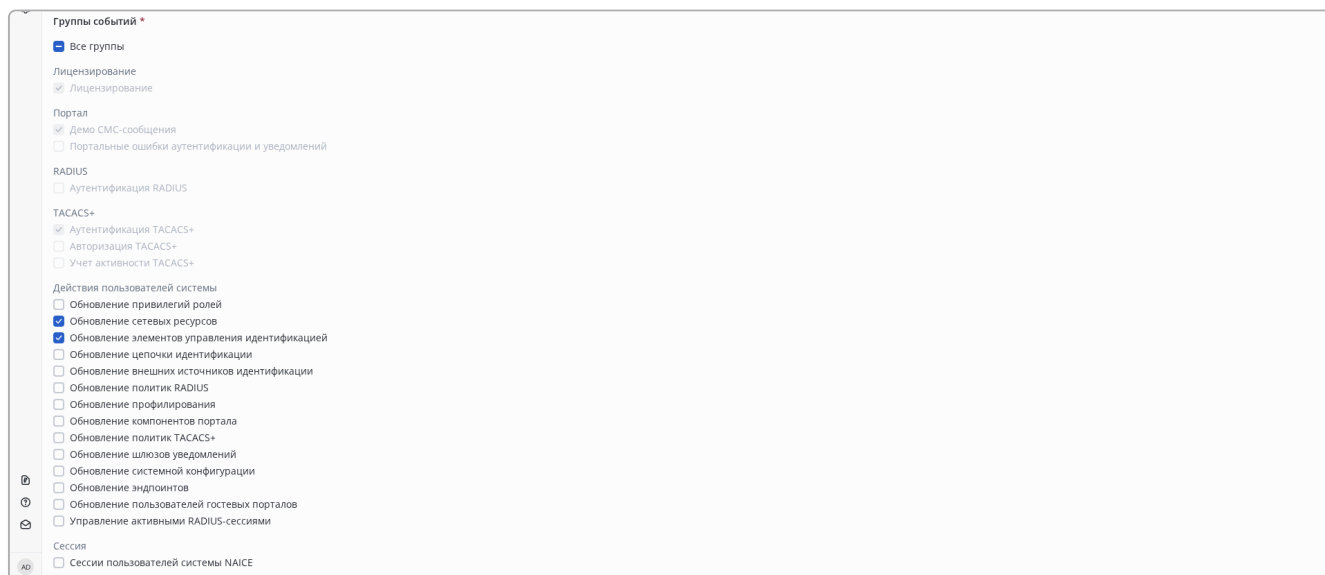


Рисунок 63. Группы маршрута "LocalCollector"

Отключение доступных к редактированию групп внутри системного маршрута приведет, к тому, что они не будут сохраняться в локальной базе данных и соответственно не будут отображаться в [журнале системных событий](#).

Список ограничений действий пользователя системы по отношению к системному маршруту:



- Удалить системный маршрут невозможно.
- Поля «Имя» и «Описание» недоступны для редактирования пользователем системы в системном маршруте.
- Некоторые группы выбраны в системном маршруте по умолчанию, они являются обязательными и не могут быть отредактированы, остальные группы редактируются.
- Создавать новые маршруты с типом «Системное хранилище» нельзя. Все маршруты, созданные пользователем системы, автоматически получают тип «Пользовательский».

Добавление маршрута событий

Добавление маршрутов осуществляется по нажатию кнопки 

В открывшемся окне создания нового маршрута заполнить следующие поля:

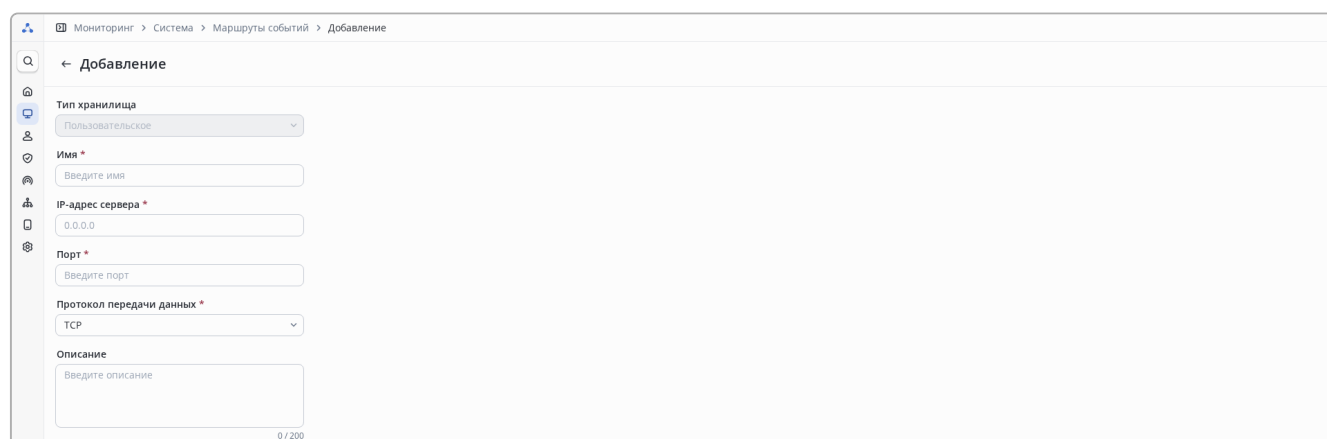


Рисунок 64. Добавление нового маршрута (настройка основных полей)

- **Имя *** - уникальное имя для идентификации маршрута.
- **IP-адрес сервера *** - IP-адрес внешнего сервера, на который будут отправляться события.
- **Порт *** - номер сетевого порта, на котором внешний сервер ожидает события.
- **Протокол передачи данных *** - протокол передачи событий. Доступны TCP и UDP.
- **Описание** - произвольное текстовое описание маршрута.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

Ниже в разделе "Группы событий" необходимо выбрать события для отправки:

Группы событий *

☒ Все группы

Лицензирование

☐ Лицензирование

Портал

☐ Демо СМС-сообщения

☒ Портальные ошибки аутентификации и уведомлений

RADIUS

☒ Аутентификация RADIUS

TACACS+

☒ Аутентификация TACACS+

☒ Авторизация TACACS+

☐ Учет активности TACACS+

Действия пользователей системы

☐ Обновление привилегий ролей

☐ Обновление сетевых ресурсов

☐ Обновление элементов управления идентификацией

☐ Обновление цепочки идентификации

☐ Обновление внешних источников идентификации

☐ Обновление политик RADIUS

☐ Обновление профилирования

☐ Обновление компонентов портала

☐ Обновление политик TACACS+

☐ Обновление шлюзов уведомлений

☐ Обновление системной конфигурации

☐ Обновление эндпоинтов

☐ Обновление пользователей гостевых порталов

☐ Управление активными RADIUS-сессиями

Сессия

☐ Сессии пользователей системы NAICE

Отмена Добавить и продолжить **Добавить**

Рисунок 65. Добавление нового маршрута (выбор групп событий)

Описание групп:

- **Все группы** - выбор всех возможных групп событий.
- **Лицензирование** - события, связанные с лицензированием.
- **Портал** - события, связанные с "Демо СМС-сообщениями" для порталных пользователей, а также ошибками, связанными с порталной аутентификацией.
- **RADIUS** события, связанные с RADIUS-аутентификацией.
- **TACACS+** - события, связанные с аутентификацией, авторизацией и учетом активности в рамках TACACS+.
- **Действия пользователей системы** - события обновления конфигураций различных записей NAICE (привилегий ролей пользователей системы NAICE, сетевых ресурсов, наборов политик и т.д.).
- **Сессия** - события, связанные с сессиями пользователей системы NAICE.

Для добавления маршрута событий в системе предусмотрены две кнопки добавления, различающиеся последующим поведением:

- **"Добавить и продолжить"** - после нажатия форма не закрывается, становится доступной кнопка **"Отправить пробное событие"**.
- **"Добавить"** - после нажатия выполняется перенаправление на страницу списка маршрутов событий.

Отправка пробных событий

Работу пользовательского маршрута можно проверить отправкой пробного события во внешнюю систему. Для этого необходимо нажать кнопку **"Отправить пробное событие"**.



Кнопка **"Отправить пробное событие"** неактивна до момента, пока не выбраны никакие группы событий, а сам маршрут не сохранен.



Результат отправки пробного события зависит от выбранного транспортного протокола. При использовании протокола UDP подтверждение получения пробного события со стороны внешнего сервера невозможно в силу реализации самого протокола. При использовании протокола TCP подтверждение получения пробного события возможно и будет отражено в окне результата отправки отправки.

Результат проверки отправки пробного события может быть одним из следующих:

- Пробное событие успешно отправлено. Проверьте SIEM-систему - Пробное событие отправлено по протоколу UDP.
- Пробное событие успешно отправлено - Пробное событие отправлено успешно по протоколу TCP.
- Время истекло. Пробное событие не было отправлено - Со стороны внешней системы не получен ответ для установления TCP-сессии доставки пробного события.
- SIEM-система недоступна - означает, что TCP-сессию для отправки пробного события установить не удалось (при установке TCP-сессии получен отказ или установка TCP-сессии завершилась ошибкой).

Примеры окон результата отправки пробных событий:

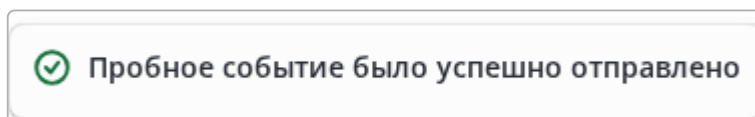


Рисунок 66. Схема без резервирования, пробное событие успешно отправлено, протокол TCP

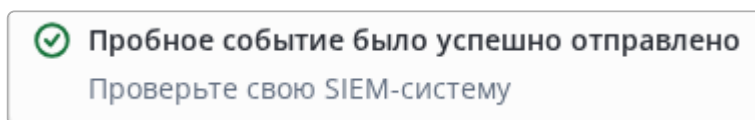


Рисунок 67. Схема без резервирования, пробное событие отправлено, протокол UDP

В случае использования схемы с резервированием отправка пробных событий будет осуществляться с обоих хостов NAICE, поэтому в окне результата отправки события будут сразу два сервиса.

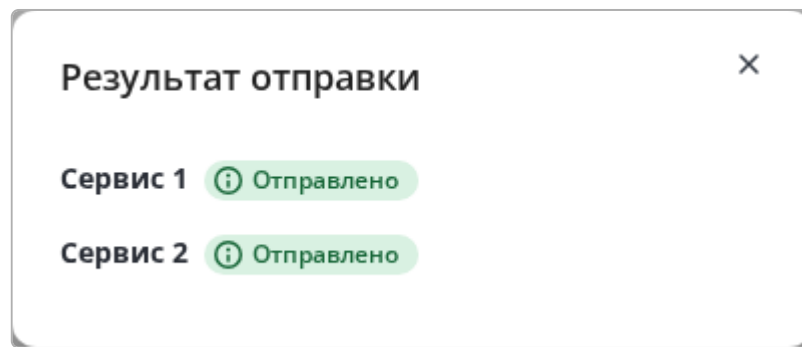


Рисунок 68. Схема с резервированием, пробное событие успешно отправлено для обоих хостов, протокол TCP

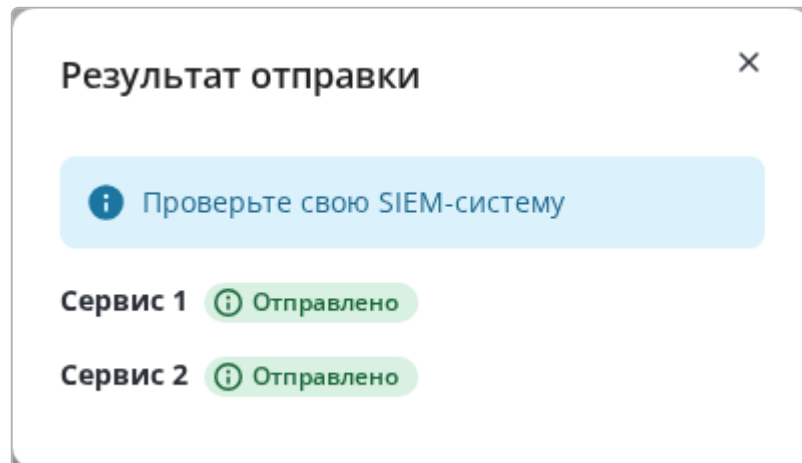


Рисунок 69. Схема с резервированием, пробное событие отправлено для обоих хостов, протокол UDP

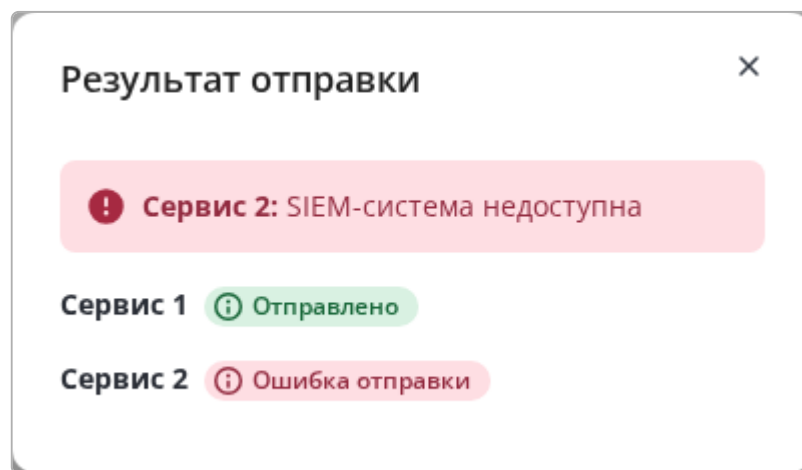


Рисунок 70. Схема с резервированием, ошибка отправки пробного события для одного из хостов, протокол TCP

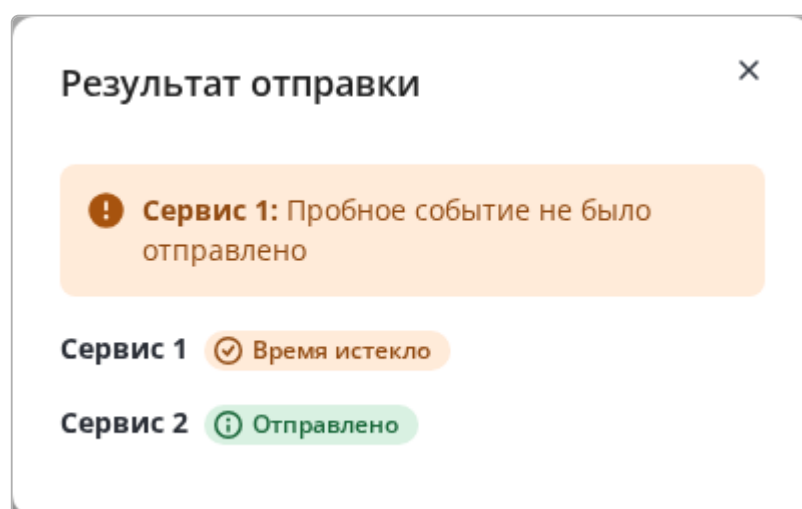


Рисунок 71. Схема с резервированием, время отправки пробного события истекло для одного из хостов, протокол TCP

Редактирование маршрута событий

Для редактирования маршрута на странице **Маршруты событий** выберите нужный маршрут и перейдите к редактированию, нажав на его имя в колонке **Имя**.

☐	Имя ↑
☐	LocalCollector
☐	SIEM 1

Рисунок 72. Гиперссылка на страницу редактирования маршрута

Форма редактирования идентична форме добавления маршрутов событий.



При внесении изменений в форму кнопка **"Отправить пробное событие"** становится недоступной. Повторная активация кнопки происходит только после сохранения изменений.

Мониторинг > Система > Маршруты событий > SIEM 1

← SIEM 1

Тип хранилища
Пользовательское

Имя *
SIEM 1

IP-адрес сервера *
192.168.223.15

Порт *
515

Протокол передачи данных *
UDP

Описание
Введите описание

0 / 200

Рисунок 73. Редактирования полей маршрута

Группы событий *

☒ Все группы

Лицензирование
☒ Лицензирование

Портал
☐ Демо СМС-сообщения
☒ Портальные ошибки аутентификации и уведомлений

RADIUS
☒ Аутентификация RADIUS

TACACS+
☐ Аутентификация TACACS+
☐ Авторизация TACACS+
☒ Учет активности TACACS+

Действия пользователей системы
☐ Обновление привилегий ролей
☐ Обновление сетевых ресурсов
☐ Обновление элементов управления идентификацией
☐ Обновление цепочки идентификации
☐ Обновление внешних источников идентификации
☐ Обновление политик RADIUS
☐ Обновление профилирования
☒ Обновление компонентов портала
☐ Обновление политик TACACS+
☐ Обновление шлюзов уведомлений
☒ Обновление системной конфигурации
☐ Обновление эндпоинтов
☐ Обновление пользователей гостевых порталов

Сессия
☐ Сессии пользователей системы NAICE

Отмена Сохранить и продолжить Сохранить

Рисунок 74. Редактирования групп маршрута

Для сохранения изменений в системе предусмотрены две кнопки, различающиеся последующим поведением:

- **"Сохранить и продолжить"** - после нажатия форма не закрывается, кнопка **"Отправить пробное событие"** снова становится доступной.
- **"Сохранить"** - после нажатия выполняется перенаправление на страницу списка маршрутов событий.

Дублирование маршрута событий

Для дублирования маршрута необходимо отметить чекбокс слева от нужного маршрута в таблице:

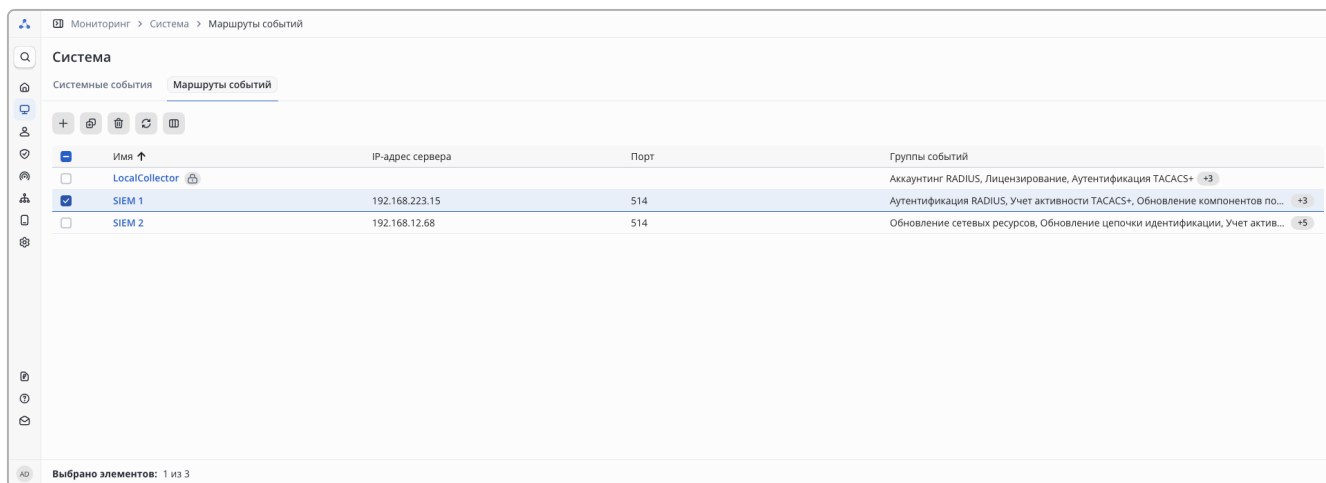


Рисунок 75. Выбор маршрута для дублирования

Затем нажать на кнопку дублирования маршрута  над таблицей.

Откроется форма, аналогичная форме добавления маршрута, где все поля будут заполнены значениями из выбранного маршрута. По умолчанию к значению в поле **Имя** добавляется "_copy". Можно задать любое другое имя, которое еще не используется в системе.

← Дублирование

Тип хранилища
Пользовательское

Имя *
SIEM 1_copy

IP-адрес сервера *
192.168.223.15

Порт *
514

Протокол передачи данных *
UDP

Описание
Введите описание

0 / 200

Рисунок 76. Поля настроек внутри маршрута при дублировании

Или выбрать иные группы сообщений при необходимости:

Рисунок 77. Группы сообщений внутри маршрута при дублировании

Для добавления маршрута событий в системе предусмотрены две кнопки добавления, различающиеся последующим поведением:

- **"Добавить и продолжить"** - после нажатия форма не закрывается, становится доступной кнопка **"Отправить пробное событие"**.
- **"Добавить"** - после нажатия выполняется перенаправление на страницу списка маршрутов событий.

Удаление маршрута событий

Для удаления одного или нескольких маршрутов отметьте один или более чекбоксов слева от нужных маршрутов в таблице:

Имя ↑	IP-адрес сервера	Порт	Группы событий
☐ LocalCollector			Аккаунтинг RADIUS, Лицензирование, Аутентификация TACACS+ +3
☐ SIEM 1	192.168.223.15	514	Аутентификация RADIUS, Учет активности TACACS+, Обновление компонентов по... +3
☒ SIEM 2	192.168.12.68	514	Обновление сетевых ресурсов, Обновление цепочки идентификации, Учет актив... +5

Рисунок 78. Выбор маршрута для удаления

Затем нажать на кнопку удаления маршрута  над таблицей.

После удаления маршрута события перестанут отправляться на указанный в маршруте сервер. Подтвердить или отменить действие можно в окне:



Удаление элементов требует подтверждения в модальном окне. Выбранные элементы будут удалены только после явного подтверждения операции.

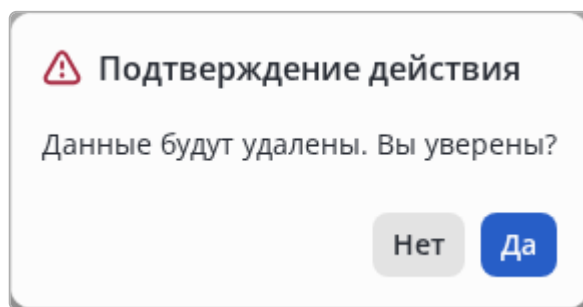


Рисунок 79. Диалоговое окно подтверждения действия

Пользователи и устройства

Пользователи системы

Учетные записи

Описание

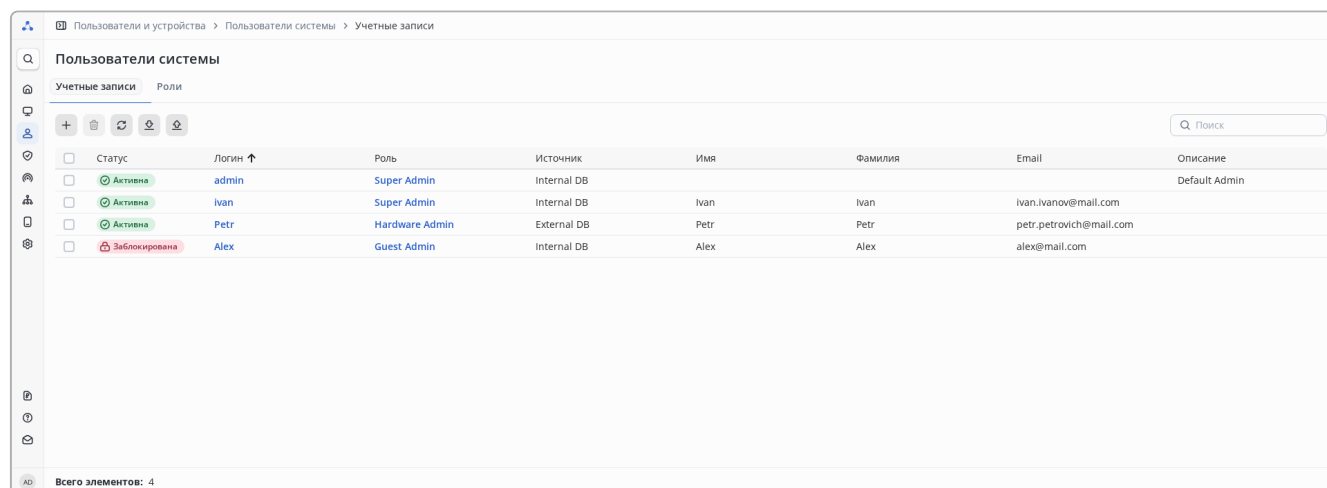
Раздел предназначен для управления учетными данными пользователей системы NAICE.

Учетные записи пользователей системы подразделяются на два типа:

- **Локальные** — создаются непосредственно в системе NAICE (источник `Internal DB`);
- **Внешние** — создаются автоматически при первом успешном прохождении аутентификации через [внешний источник идентификации](#).

[Настройки аккаунта](#) текущего пользователя системы доступны на любой странице при нажатии на **AD** в нижнем левом углу окна в меню.

Просмотр всех учетных записей пользователей системы



The screenshot shows a web interface for managing system users. At the top, there's a breadcrumb trail: 'Пользователи и устройства > Пользователи системы > Учетные записи'. Below this is a search bar and tabs for 'Учетные записи' (selected) and 'Роли'. A table lists four users with columns for checkboxes, status, login, role, source, name, surname, email, and description. The status column uses color-coded icons: green for 'Активна' and red for 'Заблокирована'. The bottom of the interface shows a footer with 'AD' and 'Всего элементов: 4'.

☐	Статус	Логин ↑	Роль	Источник	Имя	Фамилия	Email	Описание
☐	Активна	admin	Super Admin	Internal DB				Default Admin
☐	Активна	Ivan	Super Admin	Internal DB	Ivan	Ivan	ivan.ivanov@mail.com	
☐	Активна	Petr	Hardware Admin	External DB	Petr	Petr	petr.petrovich@mail.com	
☐	Заблокирована	Alex	Guest Admin	Internal DB	Alex	Alex	alex@mail.com	

Рисунок 80. Таблица с перечнем учетных записей пользователей системы на странице просмотра

На странице отображается таблица, содержащая перечень всех локальных и внешних учетных записей пользователей системы.

Таблица содержит следующую информацию о пользователях системы:

- **Статус** — состояние учетной записи, определяющее возможность авторизации в системе:
 - **Активна** — пользователь может войти в систему;
 - **Выключена** — пользователь не может войти в систему. Для учетной записи может быть указан период отключения и причина отключения;
 - **Заблокирована** — пользователь временно заблокирован, например, после превышения лимита неудачных попыток входа.

Логин — логин пользователя системы (должен быть уникальным и не содержать пробелов);

- **Роль** — **роль** пользователя системы. Является гиперссылкой на страницу просмотра/редактирования этой роли;
- **Источник** — указывает на происхождение учетной записи: **Internal DB** (создана в системе NAICE) или наименование **внешнего источника** (создана автоматически при успешной аутентификации через внешний источник);
- **Имя** — имя пользователя системы;
- **Фамилия** — фамилия пользователя системы;
- **Email** — адрес электронной почты пользователя системы;
- **Описание** — произвольное описание.

Допускается сортировка в прямом и обратном порядке по всем колонкам таблицы. По умолчанию сортировка выполняется в прямом (алфавитном) порядке по колонке **Логин**.



При наведении курсора мыши на статус учётной записи в таблице отображается всплывающая подсказка с детальной информацией: период действия статуса (дата и время начала и окончания) и причина его применения.

Элементы управления:

- — Добавить новый элемент.
- — Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- — Обновить данные таблицы.
- — Позволяет загрузить данные из csv-файла.
- — Позволяет выгрузить данные в csv-файл.
- ☐ — Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).
- — Изменить текущий порядок сортировки.
- **Поиск** — Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.

Внешние учетные записи пользователей системы

Внешние учетные записи (их локальные копии) создаются автоматически в системе при первом успешном входе пользователя через внешний источник идентификации.

Для просмотра учетной записи внешнего пользователя системы необходимо на странице со списком нажать на логин. После этого откроется страница просмотра внешней учетной записи пользователя системы:

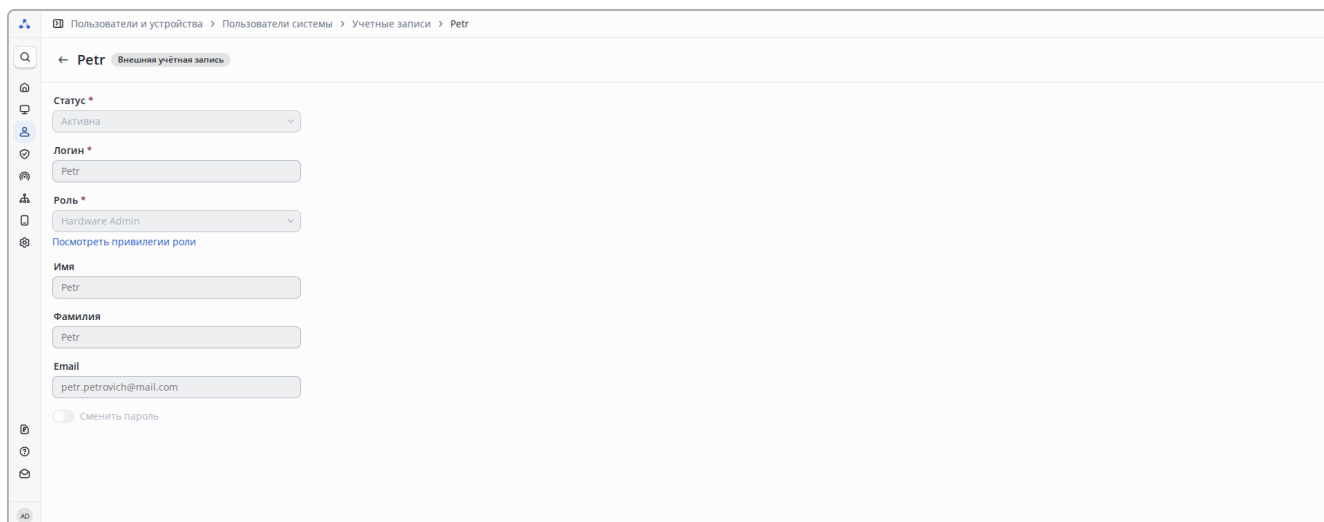


Рисунок 81. Форма просмотра учетной записи внешнего пользователя системы

Форма просмотра внешней учетной записи содержит следующие поля:

- **Статус** — состояние учетной записи, определяющее возможность авторизации. Для внешних учетных записей статусы **Активна** и **Выключена** берутся из внешнего источника идентификации и недоступны для изменения в NAICE;
 - Искключение: если учетная запись имеет статус **Заблокирована**, администратор может вручную снять блокировку, изменив статус на **Активна**.
- **Логин** — идентификатор пользователя во внешней системе (не должен превышать 100 символов):
 - Для учетных записей из **Active Directory** логин всегда отображается в формате **UPN** (User Principal Name) с указанием домена;
 - Для учетных записей из **OpenLDAP** логин соответствует значению атрибута, заданного в поле **Subject name attribute** при настройке внешнего источника;
- **Роль** — **роль** внешнего пользователя системы, назначаемая автоматически по результатам сопоставления групп, в которых состоит пользователь, с группами, указанными в настройках внешних ролей NAICE. Определяет уровень доступа к функционалу системы;
- **Имя**, **Фамилия**, **Email** — персональные данные пользователя. Заполняются значениями из соответствующих атрибутов, настроенных в блоке «Сопоставление информации о пользователях системы» при настройке внешнего источника.

Кнопка "**Посмотреть привилегии роли**" открывает окно с таблицей привилегий выбранной роли:

- Наименования привилегий;
- Статусы выданных прав:
 -  — у пользователя есть доступ,
 -  — доступ не предусмотрен,
 -  — у пользователя нет доступа.



Редактирование внешних учетных записей запрещено. Все изменения должны вноситься непосредственно во внешнем источнике идентификации.

Исключение: снятие блокировки, если учетная запись была заблокирована политикой блокировки.

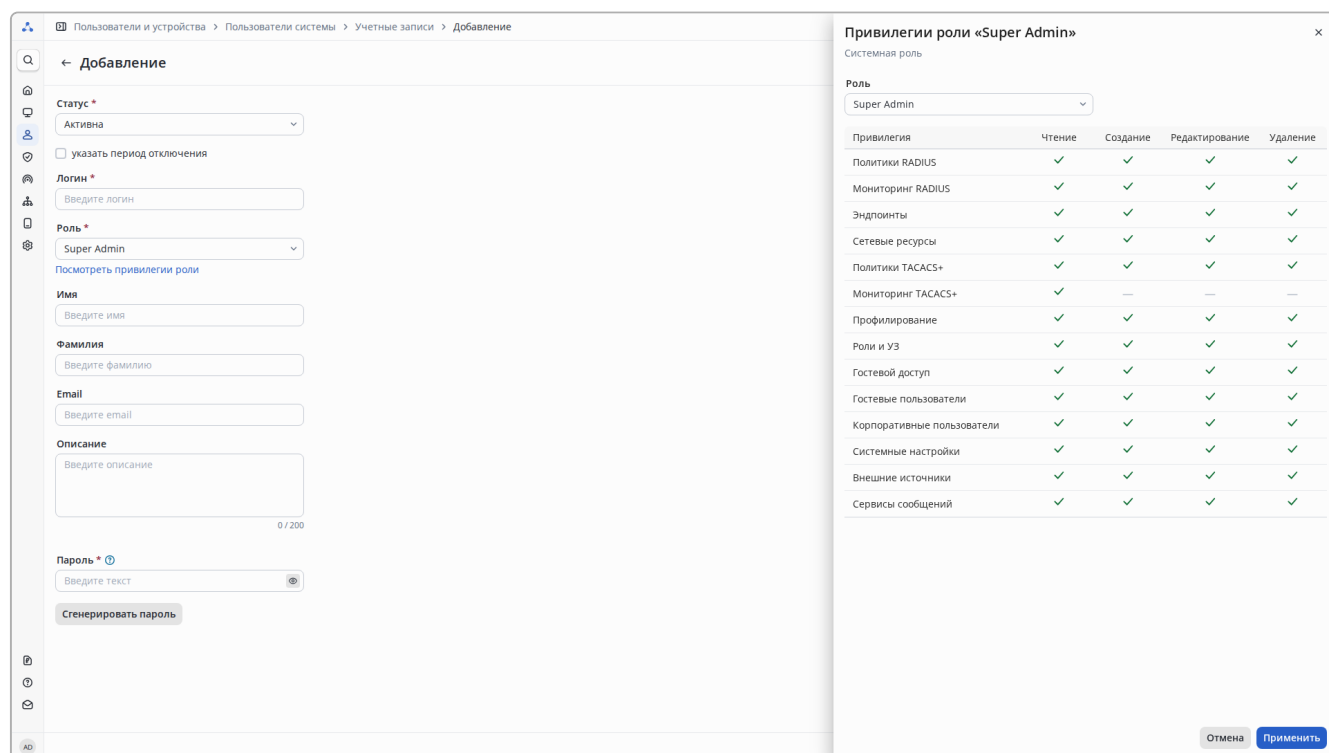


При каждом последующем входе в систему выполняется синхронизация внешней учетной записи:

- **обновление атрибутов** (Статус, Имя, Фамилия, Email) в соответствии с текущими данными из внешнего источника;
- **повторное вычисление роли** на основе актуального состава групп пользователя во внешнем источнике.

Добавление учетной записи пользователя системы

Для добавления учетной записи пользователя системы необходимо нажать  на панели действий, расположенной над таблицей.



Привилегия	Чтение	Создание	Редактирование	Удаление
Политики RADIUS	✓	✓	✓	✓
Мониторинг RADIUS	✓	✓	✓	✓
Эндпоинты	✓	✓	✓	✓
Сетевые ресурсы	✓	✓	✓	✓
Политики TACACS+	✓	✓	✓	✓
Мониторинг TACACS+	✓	—	—	—
Профилирование	✓	✓	✓	✓
Роли и УЗ	✓	✓	✓	✓
Гостевой доступ	✓	✓	✓	✓
Гостевые пользователи	✓	✓	✓	✓
Корпоративные пользователи	✓	✓	✓	✓
Системные настройки	✓	✓	✓	✓
Внешние источники	✓	✓	✓	✓
Сервисы сообщений	✓	✓	✓	✓

Рисунок 82. Страница добавления учетной записи пользователя системы

Форма добавления пользователя системы включает в себя следующие поля:

- **Статус *** — определяет текущее состояние учетной записи. Позволяет разрешить или запретить пользователю вход в систему. По умолчанию установлено значение **Активна**;
- **Логин *** (максимальная длина - 100 символов);
- **Роль *** — выбор **роли** для пользователя системы. Роль определяет уровень доступа к функционалу системы;

Имя (максимальная длина - 100 символов);

- Фамилия (максимальная длина - 100 символов);
- Email (максимальная длина - 200 символов);
- Описание (максимальная длина - 200 символов);
- Пароль * (максимальная длина - 72 символа). По нажатию на  можно включить отображение вводимого пароля, по умолчанию текст скрыт. Пароль должен соответствовать текущей [парольной политике](#).

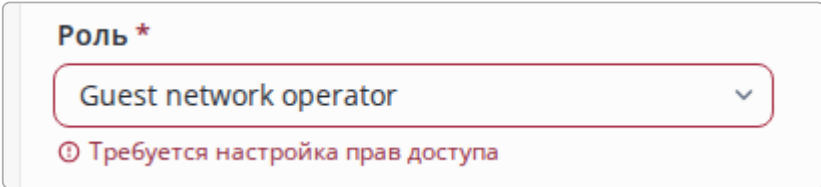
* — поля, обязательные для заполнения.



Нельзя назначить учетной записи роль, права которой превышают права текущего пользователя.



После повышения уровня лицензии может потребоваться дополнительная настройка привилегий. Роли, требующие донастройки, помечаются предупреждением:



Роль *

Guest network operator

⚠ Требуется настройка прав доступа

Рисунок 83. Предупреждение "Требуется настройка прав доступа"

Кнопка ["Посмотреть привилегии роли"](#) открывает окно с таблицей привилегий выбранной роли:

- Наименования привилегий;
- Статусы выданных прав:
 -  — у пользователя есть доступ,
 -  — доступ не предусмотрен,
 -  — у пользователя нет доступа.

В окне с помощью выпадающего списка **Роль** предусмотрена возможность просмотреть права доступа, назначенные другим ролям. При нажатии кнопки **"Применить"** роль будет перевыбрана в форме добавления учетной записи.

Пароль для пользователя системы можно сгенерировать, нажав на кнопку **"Сгенерировать пароль"**, либо указать вручную. Сгенерированный пароль помещается в поле **Новый пароль**, его можно скопировать по клику на .

Для создания учетной записи необходимо нажать кнопку **"Добавить"**.

Редактирование учетной записи пользователя системы

Для редактирования учетной записи пользователя системы необходимо на странице со списком нажать на логин:

☐	Статус	Логин ↑
☐	✔ Активна	admin
☐	✔ Активна	ivan
☐	✔ Активна	Petr
☐	🔒 Заблокирована	Alex

Рисунок 84. Гиперссылка на страницу редактирования учетной записи пользователя системы

После этого откроется страница редактирования учетной записи пользователя системы, аналогичная странице добавления:

The screenshot shows a web interface for editing a user. The breadcrumb trail at the top is: Пользователи и устройства > Пользователи системы > Учетные записи > ivan. The left sidebar contains icons for various system functions. The main form area is titled '← ivan' and includes the following fields and controls:

- Статус ***: A dropdown menu currently showing 'Активна'.
- ☐ **указать период отключения**: An unchecked checkbox.
- Логин ***: A text input field containing 'ivan'.
- Роль ***: A dropdown menu currently showing 'Super Admin'.
- [Посмотреть привилегии роли](#): A link below the role dropdown.
- Имя**: A text input field containing 'Ivan'.
- Фамилия**: A text input field containing 'Ivan'.
- Email**: A text input field containing 'ivan.ivanov@mail.com'.
- Описание**: A text area with the placeholder 'Введите описание' and a character count '0 / 200'.
- ☐ **Сменить пароль**: An unchecked checkbox.

Рисунок 85. Форма редактирования пользователя системы

Для изменения пароля пользователя системы необходимо включить переключатель "**Сменить пароль**", после чего ввести желаемый пароль в соответствующие поля.



После сохранения изменений для логина, пароля и/или роли сессия будет прервана — потребуется повторная авторизация.



Запрещено редактировать свою учетную запись. Для изменения данных своей учетной записи перейдите в раздел [Настройки аккаунта](#).

После внесения изменений необходимо нажать кнопку **"Сохранить"**. Кнопка скрыта, пока не будет изменено хотя бы одно поле.

Кнопка **"Отмена"** осуществляет сброс внесенных изменений до исходного состояния.

Управление статусом учетной записи

В поле **Статус** задается состояние учетной записи пользователя системы.

Доступны следующие значения:

Статус	Описание
Активна	Пользователь может войти в систему.
Выключена	Пользователь не может войти в систему. При выборе этого статуса можно указать период отключения и причину отключения.
Заблокирована	Пользователь временно заблокирован. Статус присваивается автоматически при срабатывании политики блокировки и не может быть установлен вручную.



Для того, чтобы пользователи получали email-уведомления об изменениях статуса их учетной записи (блокировка, отключение, разблокировка), необходимо настроить отправку уведомлений в разделе **Настройки системы** → **Безопасность и доступ** → [«Парольная политика»](#).

Плановое отключение учетной записи

Для активной учетной записи можно заранее указать период отключения.

Чтобы задать период отключения, активируйте чекбокс **«Указать период отключения»**.

Статус *

Активна

☒ указать период отключения

Период отключения УЗ *

09.05.2026 00:00 – бессрочно

Причина отключения

Введите причину

0 / 200

Рисунок 86. Форма редактирования учетной записи с плановым отключением

При активации планового отключения становятся доступными следующие поля:

- **Период отключения УЗ** — интервал, в течение которого учетная запись будет недоступна.
 - **Дата и время начала** — с этого момента учетная запись будет отключена;
 - **Дата и время окончания** — после этого момента доступ будет восстановлен.
- **Причина отключения** — пояснение причины отключения учетной записи.

Дата начала

09.05.2026 00:00

Дата окончания

ДД.ММ.ГГГГ 44:MM

Оставьте поля пустыми для бессрочного отключения

Сбросить Отмена Применить

Рисунок 87. Окно выбора периода планового отключения учетной записи



- Дата и время **начала** обязательны для заполнения и должны быть позже текущего момента.
- Если дата и время **окончания** не указаны, учетная запись будет отключена бессрочно.

Отключение учетной записи

Для запрета авторизации пользователя измените значение поля **Статус** на **Выключена**.

Статус *

Выключена

Период отключения УЗ *

08.05.2026 10:15 – бессрочно

Причина отключения

Введите причину

0 / 200

Рисунок 88. Выключение локальной учетной записи

При отключении учетной записи становятся доступными дополнительные поля:

- **Период отключения УЗ** — интервал, в течение которого учетная запись будет недоступна. В поле начала автоматически подставляется текущее время (момент сохранения изменений);
- **Причина отключения** — пояснение причины отключения учетной записи.

Если дата и время **окончания** периода не указаны, учетная запись будет отключена бессрочно.

Заблокированная учетная запись

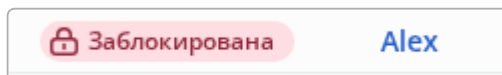


Рисунок 89. Заблокированная учетная запись в таблице

Учетная запись может быть автоматически заблокирована системой при срабатывании **политики блокировки** — например, после превышения допустимого количества неудачных попыток входа.

Статус **Заблокирована** присваивается автоматически и **не может быть установлен вручную** через форму редактирования. Снять блокировку можно только одним из способов:

- автоматически — после истечения времени блокировки, заданного в политике;
- вручную — администратор может разблокировать учетную запись, изменив статус на **Активна**.

Локальная учетная запись

Для локальной учетной записи в форме редактирования отображаются сведения о блокировке:

Рисунок 90. Форма редактирования заблокированной локальной учетной записи

Доступны следующие поля:

- **Период блокировки УЗ** — временной интервал, в течение которого учетная запись остается заблокированной;

- **Причина блокировки** — причина, по которой учетная запись была заблокирована (формируется системой автоматически).

Администратор может изменить состояние заблокированной учетной записи:

- чтобы **разблокировать** учетную запись, измените значение поля **Статус** на **Активна**;
- чтобы **отключить** учетную запись (например, для временного запрета доступа), измените значение поля **Статус** на **Выключена**.

После изменения статуса сохраните изменения, нажав кнопку **«Сохранить»**.

Внешняя учетная запись

Для внешней учетной записи сведения о блокировке отображаются в форме просмотра:

The screenshot shows a web interface for managing users. The breadcrumb trail is: Пользователи и устройства > Пользователи системы > Учетные записи > ivan. The page title is 'ivan' with a sub-tab 'Внешняя учетная запись'. The form contains the following fields:

- Статус ***: A dropdown menu currently set to 'Заблокирована'.
- Период блокировки УЗ ***: A date range field showing '08.05.2026 10:15 - 08.05.2026 10:30'.
- Причина блокировки**: A text area containing 'Пользователь заблокирован политикой блокировки'.
- Логин ***: A text field with the value 'ivan'.
- Роль ***: A dropdown menu set to 'Hardware Admin'.
- Имя**: A text field with the value 'ivan'.
- Фамилия**: A text field with the value 'ivan'.
- Email**: A text field with the value 'ivan.ivanov@mail.com'.
- Сменить пароль**: A toggle switch currently turned off.

Рисунок 91. Форма просмотра заблокированной внешней учетной записи

Для заблокированной внешней учетной записи доступны поля:

- **Период блокировки УЗ** — временной интервал, в течение которого учетная запись остается заблокированной;
- **Причина блокировки** — причина, по которой учетная запись была заблокирована (формируется системой автоматически).

Администратор может изменить состояние заблокированной внешней учетной записи, изменив значение поля **Статус** на **Активна**.

Удаление учетной записи пользователя системы

Для удаления учетной записи пользователя системы в таблице необходимо выделить чекбокс слева от учетной записи, которую требуется удалить, и нажать кнопку  на панели действий, расположенной над таблицей.



Если у выбранного пользователя системы (как локального, так и внешнего) была открыта сессия, она будет немедленно прекращена.

Пользователи и устройства > Пользователи системы > Учетные записи

Пользователи системы

Учетные записи Роли

Статус

Статус	Логин	Роль	Источник	Имя	Фамилия	Email	Описание
☐ Активна	admin	Super Admin	Internal DB				Default Admin
☒ Активна	Ivan	Super Admin	Internal DB	Ivan	Ivan	Ivan.Ivanov@mail.com	
☐ Активна	Petr	Hardware Admin	External DB	Petr	Petr	petr.petrovich@mail.com	
☐ Заблокирована	Alex	Guest Admin	Internal DB	Alex	Alex	alex@mail.com	

Выбрано элементов: 1 из 4

Рисунок 92. Выбор учетных записей пользователей системы в таблице для удаления



Удаление элементов требует подтверждения в модальном окне. Выбранные элементы будут удалены только после явного подтверждения операции.

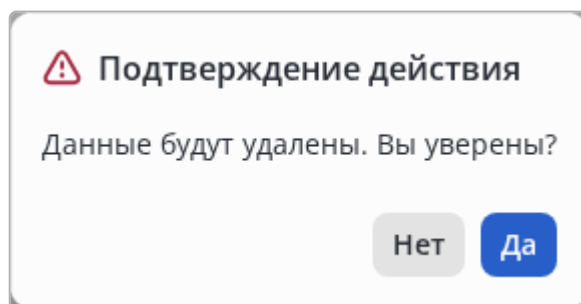


Рисунок 93. Диалоговое окно подтверждения действия



Нельзя удалить учетную запись, под которой выполнен текущий вход в систему.

Импорт

NAICE поддерживает импорт данных из CSV-файлов.

Предварительная подготовка перед импортом

1. Создайте или проверьте наличие необходимых связанных записей (например, профиль устройства).
2. Ознакомьтесь с требованиями к CSV-файлу:
 - Файл должен быть в кодировке UTF-8;
 - Разделитель полей: запятая (,)
 - Разделитель строк/текста: двойная кавычка (")
 - Заголовки и значения должны быть взяты в двойные кавычки (")
 - Максимальный размер файла 2МБ.
3. Проверьте содержимое файла на наличие лишних кавычек перед импортом;

Проверьте то что значения, содержащие двойную кавычку (") или слэш (/) правильно экранированы.

- Значения, содержащие двойную кавычку (") экранируются с помощью \"
- Значения, содержащие слэш (/) экранируются с помощью \/

Правильное написание значений (с экранированием помощью \) на примере содержания файла для импорта набора команд TACACS:

"name:Required"	"description"	"permit_unmatch ed(true/false)"	"commands(Grant/command/argume nts/enabled;...)"
"command_set"	"\"Test command set\""	"false"	"PERMIT/\"show/vlan 1 2 \"/true"

Некорректное написание значений (без экранирования) на примере содержания файла для импорта набора команд TACACS:

"name:Required"	"description"	"permit_unmatch ed(true/false)"	"commands(Grant/command/argume nts/enabled;...)"
"command_set"	"Test command set"	"false"	"PERMIT/show/vlan 1 2 /true"



Игнорирование экранирования приведёт к некорректному распознаванию данных.

Порядок выполнения импорта

Для импорта данных из CSV-файла нажмите  на панели действий, расположенной над таблицей. После чего откроется окно:

Импорт

При импорте дублирующиеся данные не будут перезаписаны или отредактированы - система пропустит их. Если вы хотите изменить старые данные, удалите их из системы вручную перед импортом.

Внимательно ознакомьтесь с [Документацией](#) , чтобы импорт прошёл без ошибок.

Выберите файл*
Максимальный размер файла 2МБ

 **Загрузите** или перетащите сюда

Поле обязательно для заполнения

Источник данных *

NAICE

☐ Игнорировать существующие данные 

☐ Остановить импорт при первой ошибке

Отмена

Импорт

Рисунок 94. Окно Импорта

Импорт данных из CSV-файла выполняется в несколько шагов:

1. Выберите необходимый CSV-файл, перетащив его в поле загрузки или выбрав через проводник, нажав кнопку "**Загрузите**";



Измененный CSV-файл нужно загрузить повторно, чтобы применить правки.

2. Выберите источник данных, если он заранее не определён;
3. При необходимости активируйте флаги импорта:

Игнорировать существующие данные

- Если переключатель включен — дубликаты записей считаются предупреждением.
- Если переключатель выключен — дубликаты расцениваются как ошибка.

Остановить импорт при первой ошибке

- Если переключатель включен — импорт останавливается при первой же ошибке. Будут импортированы только записи, которые были успешно обработаны до её возникновения.

Если переключатель выключен — ошибочные строки пропускаются, импорт продолжается до конца. Будут импортированы только валидные записи.

4. Для того чтобы импорт начался, нажмите кнопку **"Импорт"**.



При импорте дублирующиеся данные перезаписаны или отредактированы не будут - система пропустит их. Если вы хотите изменить старые данные, удалите их из системы вручную перед импортом.

Просмотр отчета по импорту

Сразу после завершения обработки файла откроется окно отчёта по импорту.

Если все записи в файле были обработаны корректно, вы увидите окно:

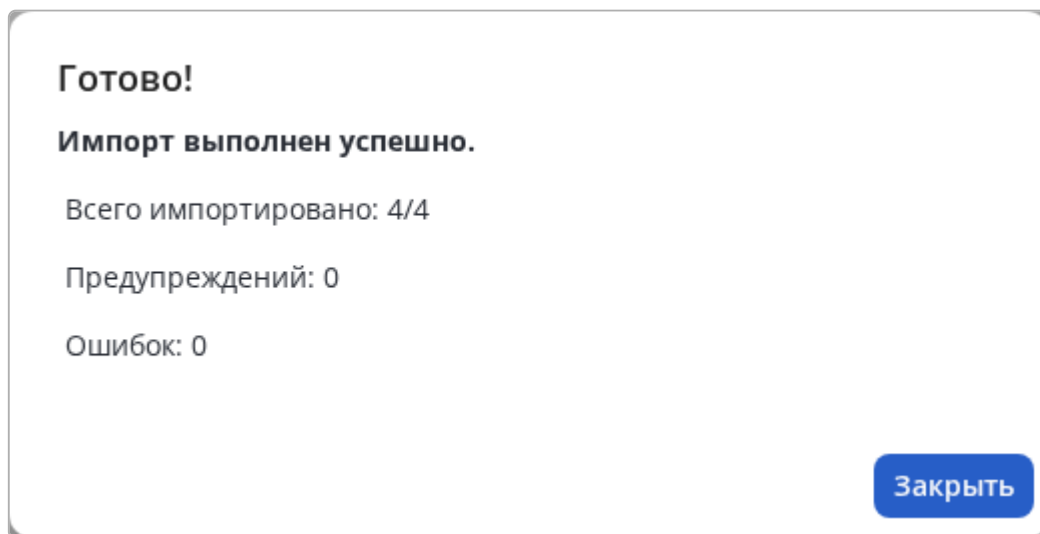


Рисунок 95. Отчет импорта (все записи обработаны корректно)

Блок с общей информацией содержит:

- **Всего импортировано** - Счётчик того, сколько записей было импортировано из общего импортируемого количества строк;
- **Предупреждений** - Количество возникших предупреждений;
- **Ошибок** - Количество возникших ошибок.

Если не все записи были обработаны корректно, вы увидите окно:

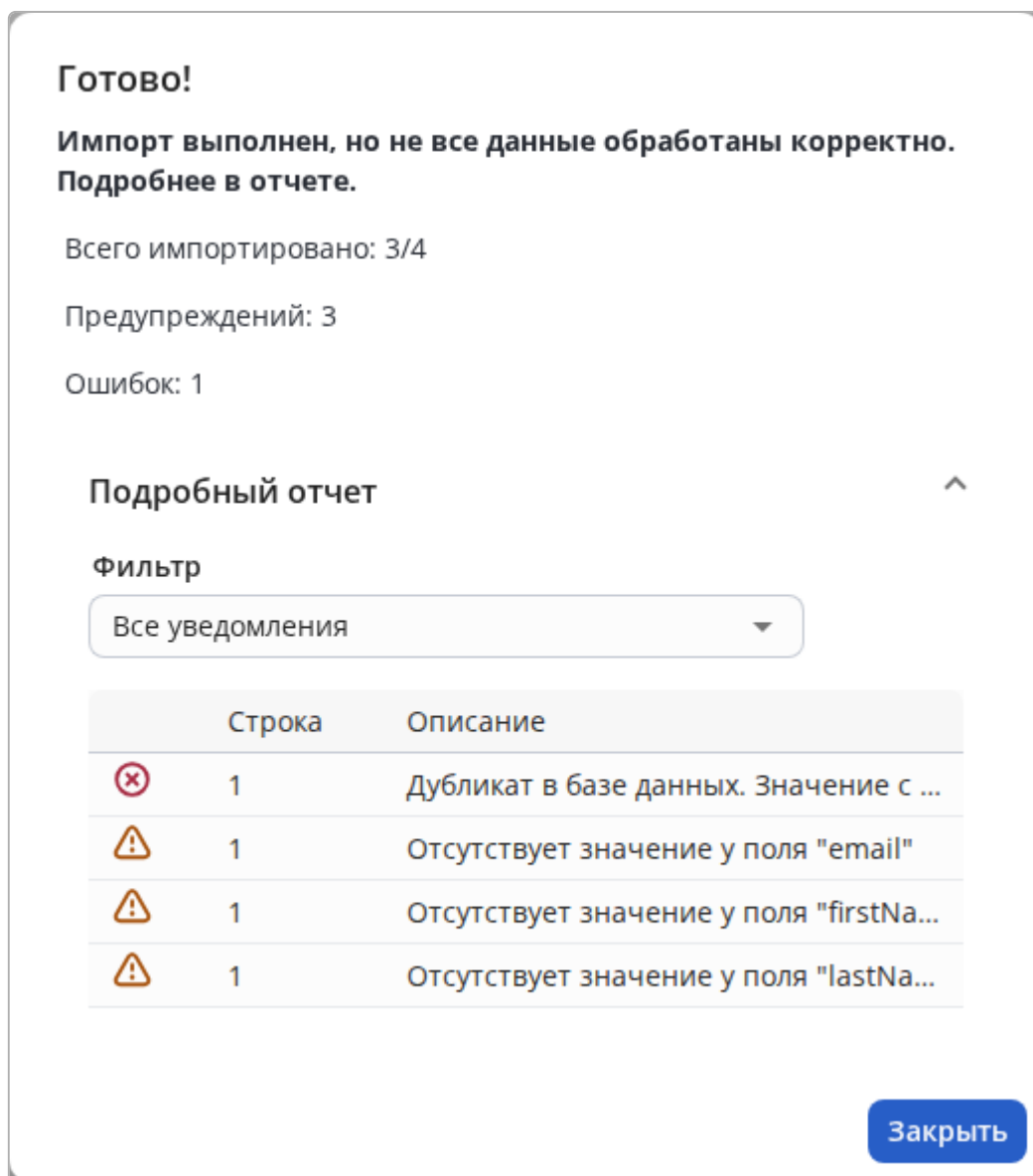


Рисунок 96. Отчет импорта (записи обработаны с ошибками/предупреждениями)

Подробный отчет содержит следующую информацию:

- **Фильтр** - Выпадающий список, в котором можно выбрать отображаемые уведомления (Все уведомления, Только ошибки или Только предупреждения)

Таблица уведомлений содержит колонки:

- **Строка** - Номер строки в CSV-файле, где обнаружена ошибка или предупреждение;
- **Описание** - Детальное текстовое объяснение ошибки или предупреждения.



Для просмотра полного текста описания наведите курсор мыши на соответствующую строку - во всплывающей подсказке отобразится полный текст сообщения об ошибке или предупреждении.

Особенности импорта учетных записей пользователей системы



Для импорта учетных записей пользователей системы в качестве источника данных поддерживается только NAICE.



Импорт внешних учетных записей не поддерживается.

В таблице ниже приведен список полей, их обязательность, описание и требования:

Поле	Описание	Требования
login:Required	Логин пользователя системы	Обязательное поле Максимальная длина - 100 символов Должен быть уникальным Нельзя использовать пробелы
role:Required	Роль пользователя системы	Обязательное поле Роль должна существовать в системе
password:Required	Пароль пользователя системы. Может быть импортирован как в захешированном, так и в открытом виде	Обязательное поле Максимальная длина - 72 символа Должен соответствовать текущей парольной политике Нельзя использовать символы <code>№</code> , <code>`</code>
isEncrypted:Required	Флаг хэширования пароля. Показывает, в каком виде передается пароль	Обязательное поле Возможные значения: - <code>true</code> — передаваемый пароль захеширован - <code>false</code> — пароль передается в открытом виде и будет захеширован во время импорта
status:Required	Статус пользователя	Обязательное поле Возможные значения: - <code>ENABLED</code> — пользователь включен - <code>DISABLED</code> — пользователь выключен - <code>BLOCKED</code> — пользователь заблокирован
disableStartTime	Время, с которого пользователь выключен	Время в формате <code>YYYY-MM-DDTHH:MM:SSZ</code> Используется, если для пользователя задан период отключения
disableEndTime	Время, до которого пользователь выключен	Время в формате <code>YYYY-MM-DDTHH:MM:SSZ</code> Если значение не указано, пользователь будет выключен бесечно
disableReason	Причина отключения пользователя	Максимальная длина - 200 символов

Поле	Описание	Требования
firstName	Имя пользователя системы	Максимальная длина - 100 символов
lastName	Фамилия пользователя системы	Максимальная длина - 100 символов
email	Адрес электронной почты	Максимальная длина - 200 символов Формат: admin123@gmail.com Недопустимые символы: • кириллические буквы (а-я)(А-Я) • пробел • двойные кавычки " • символ номера № • точка с запятой ; • двоеточие : • запятая , • круглые скобки () • квадратные скобки [] • знаки больше/меньше < > • обратный слэш \
description	Произвольное описание	Максимальная длина - 200 символов

Пример корректного содержания файла:

"login: Required"	"role: Required"	"password: Required"	"is Encrypted: Required"	"status: Required"	"first Name"	"last Name"	"email"	"description"	"disableStart Time"	"disableReason"	"timeout"	"activateEmailOpt"	"backupCode"
"administrator"	"Super Admin"	"password"	"false"	"ENABLED"	"Иван"	"Иванов"	"ivanov@testru"	"Default"	"2026-05-26T11:22:07Z"	"2026-05-26T13:00:00Z"	"Много наблюдал"	"/MCCYJRAE4p6F..."	"\$2a\$10\$gVJsW..."

Получение CSV-файла шаблона описано далее в разделе «Экспорт».



Значения, содержащие двойную кавычку (") или слэш (/), должны быть экранированы с помощью \. Игнорирование экранирования приведет к некорректному распознаванию данных.



Все импортированные записи получают источник Internal DB (внутренняя база данных системы NAICE).

Экспорт

NAICE поддерживает экспорт данных в формате CSV. Значения и заголовки обрамляются **двойными кавычками**, разделитель полей: **запятая (,)**.

Процедура экспорта

Доступны два режима экспорта данных:

- **Экспорт всего** - Выгрузка всех записей текущего раздела. Системные записи исключаются из экспорта;
- **Экспорт выбранного** - Выгрузка только отмеченных чекбоксом записей.

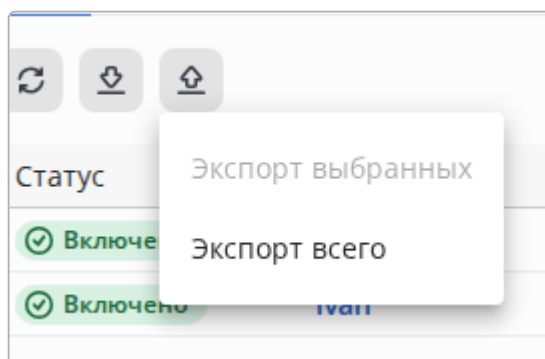


Рисунок 97. Окно выбора режима экспорта



Значения содержащие двойную кавычку (") или слэш (/) будут экранированы с помощью \".

Экспорт всех записей

На панели действий над таблицей нажмите  и выберите режим **"Экспорт всего"**. В открывшемся окне подтвердите действие кнопкой **"Экспорт"**:

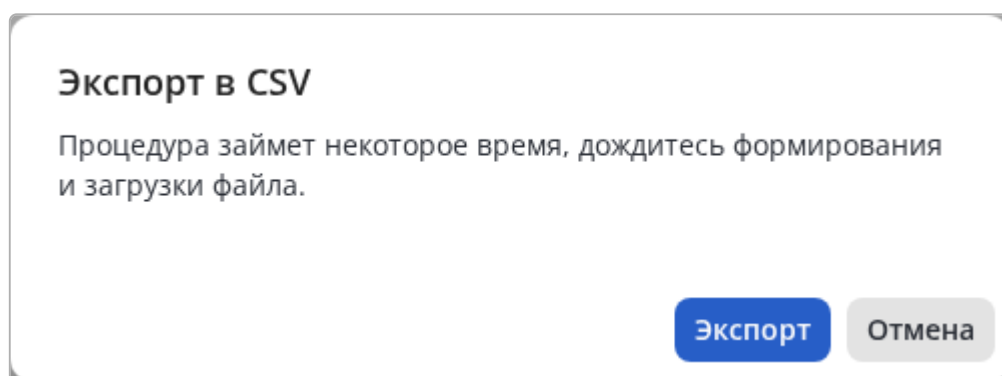


Рисунок 98. Экспорт всего

После нажатия кнопки **"Экспорт"** на устройство выгрузится файл, содержащий все записи из текущего раздела.

Экспорт выбранных записей

На панели действий над таблицей нажмите  и выберите режим **"Экспорт выбранных"**. В открывшемся окне подтвердите действие кнопкой **"Экспорт"**:

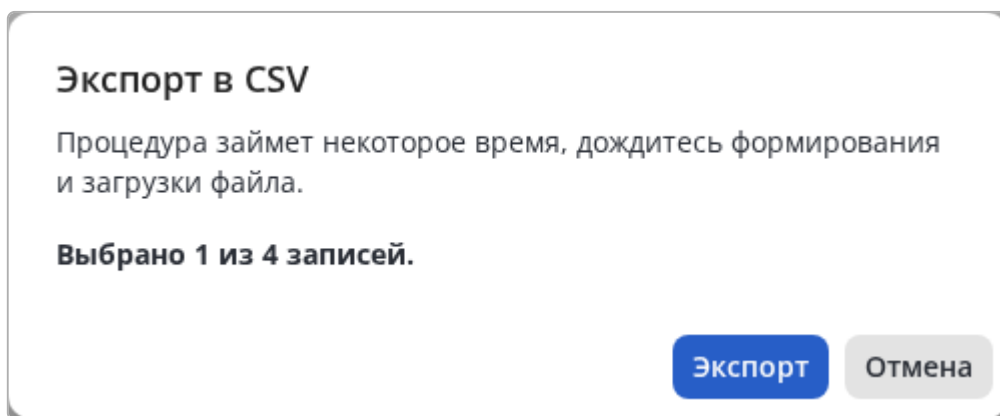


Рисунок 99. Экспорт выбранных

После нажатия кнопки **"Экспорт"** на устройство выгрузится файл, содержащий только отмеченные записи.



При **открытии** CSV-файлов в качестве разделителя полей **всегда** используйте **запятую (,)**, разделителем строк/текста могут быть **двойные кавычки (")** или **пустое значение**.



При **сохранении** CSV-файлов в качестве разделителя полей **всегда** используйте **запятую (,)**, а разделитель строк/текста - **пустое значение**.

Если при открытии файла использовался разделитель строк — двойная кавычка (**"**), то значения, содержащие символы двойной кавычки (**"**) или слэша (**/**), экранированные как ****, могут при сохранении получить лишнюю кавычку (**"**) после (****). Проверьте файл в текстовом редакторе и удалите лишние кавычки, если они появились.

Шаблон

Если в таблице отсутствуют записи (либо присутствуют только системные), при выборе режима **"Экспорт всего"** будет сформирован CSV-файл, содержащий исключительно заголовки столбцов. Данный файл может быть использован в качестве **шаблона** для подготовки данных перед импортом.

Особенности экспорта учетных записей пользователей системы

При экспорте учитывайте следующие особенности:

- **Пароли** выгружаются из базы данных в зашифрованном виде (алгоритм **Bcrypt**). Восстановление исходных паролей невозможно.
- **Внешние учетные записи** также включаются в экспортируемый CSV-файл.



Для корректного импорта внешних учетных записей в целевую систему необходимо:

1. Предварительно создать в NAICE **внешний источник идентификации** (AD, LDAP), соответствующий экспортированным записям.
2. Настроить **внешние роли** для сопоставления групп.

Если внешний источник или роли отсутствуют, импорт внешних УЗ будет невозможен.

Структура CSV-файла для учетных записей пользователей системы описана в разделе [«Особенности импорта учетных записей пользователей системы»](#).

Роли

Описание

Раздел предназначен для управления правами доступа пользователей системы NAICE.

В NAICE предусмотрено два типа ролей:

- **Внутренние роли** — назначаются вручную локальным учетным записям.
- **Внешние роли** — назначаются автоматически внешним учетным записям на основе проверки принадлежности пользователя к группам во внешнем источнике идентификации.

Уровни доступа

Система поддерживает пять уровней доступа для каждой привилегии:

Уровень	Описание
0 (Выключено)	Доступ к функционалу отсутствует. Связанные разделы не отображаются в интерфейсе.
1 (Чтение)	Просмотр данных и разделов, связанных с привилегией.
2 (Создание)	Создание новых записей в дополнение к просмотру.
3 (Редактирование)	Изменение существующих записей в дополнение к просмотру и созданию.
4 (Удаление)	Полный доступ, включая удаление записей.

Каждый последующий уровень доступа включает в себя возможности предыдущего.



Некоторые привилегии (например, связанные с мониторингом) имеют максимальный уровень доступа 1 (только чтение).

Предустановленные роли



Удаление и редактирование предустановленных ролей запрещено.

Система включает следующие предустановленные роли для типовых сценариев использования:

- **Super Admin** — полный доступ ко всему функционалу.
- **Network Admin** управление сетевым доступом.
- **Hardware Admin** — управление сетевыми устройствами.
- **System Admin** — администратор системы.
- **Guest Admin** — управление гостевой сетью.
- **Guest Operator** — оператор гостевой сети.
- **Monitor** — мониторинг и просмотр данных.

Уровни привилегий для предустановленных ролей

Привилегия	Super Admin	Network Admin	Hardware Admin	System Admin	Guest Admin	Guest Operator	Monitor
Политики RADIUS	4	4	0	4	1	0	1
Мониторинг RADIUS	4	4	0	4	4	1	1
Эндпоинты	4	4	0	4	0	0	1
Сетевые ресурсы	4	4	4	4	1	0	1
Политики TACACS+	4	0	4	4	0	0	1
Мониторинг TACACS+	1	0	1	1	0	0	1
Профилирование	4	4	0	4	1	0	1
Роли и УЗ	4	0	0	1	0	0	0
Гостевой доступ	4	1	0	4	4	1	1
Гостевые пользователи	4	4	0	4	4	4	0
Корпоративные пользователи	4	4	4	4	0	0	0
Системные настройки	4	0	0	4	0	0	0
Внешние источники	4	1	1	4	0	0	1
Сервисы сообщений	4	1	0	4	1	1	1

Привилегии и разделы системы

В данном разделе приведен полный перечень привилегий системы NAICE и соответствующих им разделов интерфейса.

Разделы, не требующие привилегий

Следующие разделы доступны всем авторизованным пользователям системы независимо от назначенных ролей:

- **Настройки аккаунта** — управление собственными учетными данными.
- **Документация** — встроенная справочная информация.
- **Дашборд** — доступность виджетов на главной странице зависит от выданных привилегий.
- **Системные события** — доступность групп событий определяется привилегиями пользователя.

Разделы, управляемые привилегиями



Условные обозначения в таблице:

- **— (прочерк)** в колонке **Особенности доступа** означает, что для данной привилегии действуют [стандартные правила уровней доступа](#).

Если в колонке указан текст, значит есть дополнительные условия, описанные в ячейке.

Привилегия	Раздел	Особенности доступа	Уровень лицензии
Политики RADIUS	Доступ к сети → Элементы политик: → Профили авторизации → Разрешенные протоколы → Условия → Словари → Лимит RADIUS-сессий	Лимит RADIUS-сессий: • 1-3 уровни доступа - права только <i>Чтение</i> • <i>Управление</i> функционалом становится доступным с 4 уровня	BASIC
	Доступ к сети: → Политики RADIUS	• 1-3 уровни: только <i>чтение</i> • <i>Полное управление</i>, сброс счетчиков становится доступным с 4 уровня	BASIC
	Пользователи и устройства → Управление идентификацией: → Цепочки идентификации	—	BASIC

Привилегия	Раздел	Особенности доступа	Уровень лицензии
Мониторинг RADIUS	Мониторинг → RADIUS: → Журнал подключений → Активные сессии	Активные сессии: • 1-3 уровни доступа - права только Чтение • Завершение активной сессии становится доступным с 4 уровня	BASIC
Эндпоинты	Пользователи и устройства → Управление идентификацией: → Эндпоинты → Группы эндпоинтов	Группы эндпоинтов: • <i>Создание/удаление</i> группы эндпоинтов становится доступно со 2 уровня • <i>Добавление/удаление</i> эндпоинтов в группы становится доступно с 3 уровня	BASIC
Сетевые ресурсы	Пользователи и устройства → Сетевые ресурсы: → Устройства → Группы устройств → Профили устройств	—	BASIC
Политики TACACS+	Доступ к оборудованию → Элементы политик: → Условия → Наборы команд TACACS+ → Профили TACACS+ → Словари	—	Доп. модуль TACACS+
	Доступ к оборудованию: → Политики TACACS+	• 1-3 уровни: только чтение • <i>Полное управление</i> , сброс счетчиков становится доступным с 4 уровня	Доп. модуль TACACS+
	Пользователи и устройства → Управление идентификацией: → Цепочки идентификации	—	BASIC
Мониторинг TACACS+	Мониторинг → TACACS+: → Журнал подключений → Учет команд (accounting)	—	Доп. модуль TACACS+

Привилегия	Раздел	Особенности доступа	Уровень лицензии
Роли и УЗ	Пользователи и устройства → Пользователи системы: → Учетные записи → Роли	—	BASIC
Гостевой доступ	Гостевые порталы → Управление порталами: → Конструктор порталов	—	ADVANCED
	Пользователи и устройства → Управление идентификацией: → Цепочки идентификации	—	BASIC
Гостевые пользователи	Гостевые порталы → Управление порталами: → Гостевые эндпоинты → Пользователи порталов	—	ADVANCED
Корпоративные пользователи	Пользователи и устройства → Управление идентификацией: → Пользователи сети → Группы пользователей сети	Группы пользователей сети: • <i>Создание/удаление</i> групп пользователей становится доступно со 2 уровня • <i>Добавление/удаление</i> пользователей в группы становится доступно с 3 уровня	BASIC
Системные настройки	Мониторинг → Система: → Маршруты событий	• Отправка пробного события становится доступным со 2 уровня	BASIC
	Настройки системы	• 1-3 уровни: только <i>чтение</i> • 4 уровень: <i>полное управление</i>	BASIC
	Лицензирование	• 0-3 уровни: только <i>чтение</i> • 4 уровень: <i>полное управление</i>	—
Внешние источники	Пользователи и устройства → Управление идентификацией: → Внешние источники идентификации	• Проверка связи с сервером доступна начиная с 1 уровня • <i>Добавление</i> групп и атрибутов становится доступным со 2 уровня • <i>Удаление</i> групп и атрибутов становится доступным с 3 уровня	BASIC
Сервисы сообщений	Шлюзы уведомлений: → Управление шлюзами	• Отправка тестового СМС/письма становится доступным со 2 уровня	BASIC

Привилегия	Требует наличия (минимум на чтение)
Политики RADIUS	Сетевые ресурсы , Профилирование , Гостевой доступ
Политики TACACS+	Сетевые ресурсы
Эндпоинты	Профилирование
Роли и УЗ	Внешние источники
Гостевые пользователи	Гостевой доступ
Гостевой доступ	Сервисы сообщений
Системные настройки	Внешние источники , Сервисы сообщений

Просмотр списка ролей

Статус	Роль	Тип	Описание
Недоступно	AD_Operators	Внешняя	
Доступно	Guest Admin	Внутренняя	System role for guest network administrator
Доступно	Guest Operator	Внутренняя	System role for guest network operator
Доступно	Hardware Admin	Внутренняя	System role for hardware access administrator
Доступно	Monitor	Внутренняя	System role for monitoring only with read-only privileges
Доступно	Network Admin	Внутренняя	System role for network access administrator
Доступно	read	Внутренняя	
Доступно	Super Admin	Внутренняя	System role with privileges for all pages and actions
Доступно	System Admin	Внутренняя	System role for system administrator

Рисунок 100. Таблица с перечнем ролей

На странице отображается таблица со всеми ролями системы. Таблица содержит следующие колонки:

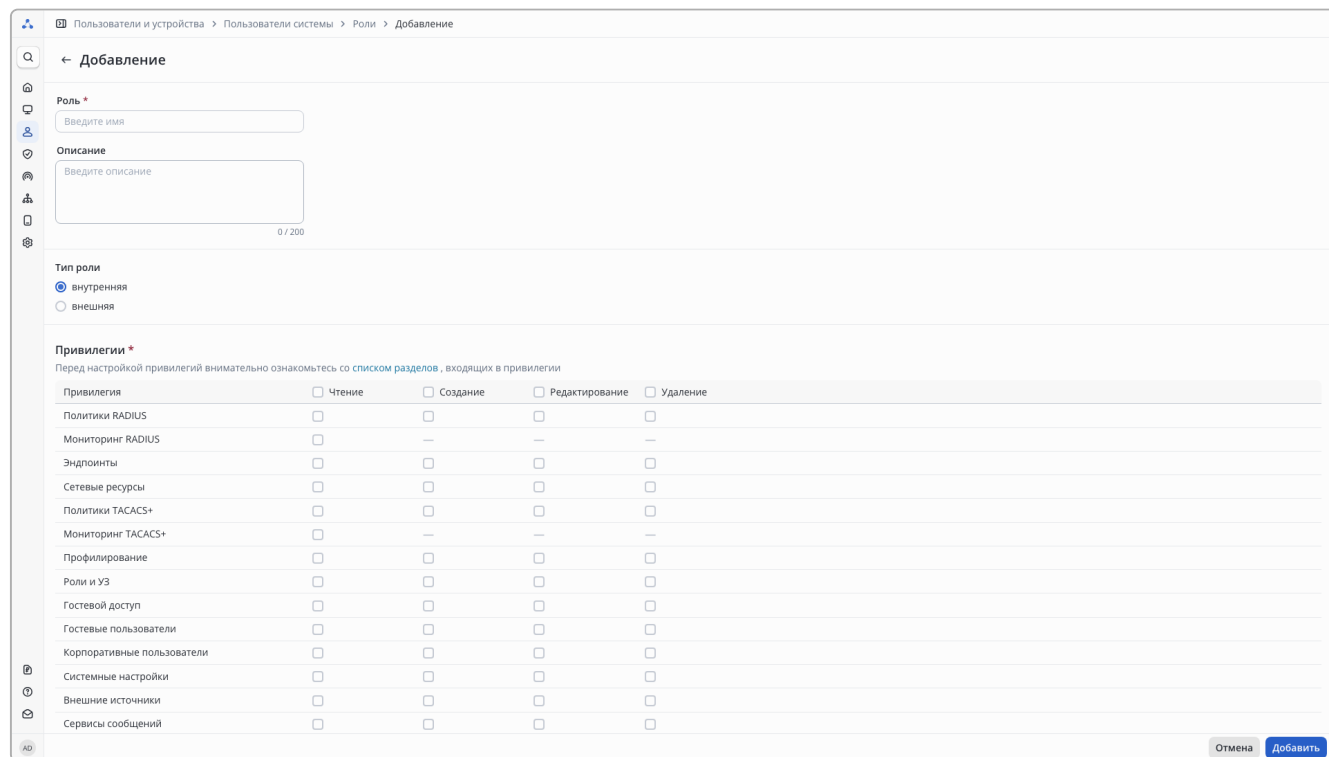
- Роль — имя роли.
 - данная запись является системной и недоступна для удаления или редактирования.
 - предупреждение: указывает на некорректную настройку роли.
- Тип — тип роли: **внутренняя** (назначается вручную) или **внешняя** (назначается автоматически по группам из внешнего источника).
- Статус — доступность роли для назначения:
 - Доступно** — роль может быть назначена пользователям;
 - Недоступно** — внешняя роль с некорректными настройками (например, при смене одного внешнего источника на другой или при отключении внешней аутентификации). Такие роли не могут быть назначены пользователям до исправления конфигурации.
- Описание — произвольное описание роли.

-  — Добавить новый элемент.
-  — Дублировать выбранный чекбоксом элемент. Становится активным, если выбран только один элемент в списке.
-  — Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
-  — Обновить данные таблицы.
- ☐ — Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).
-  — Изменить текущий порядок сортировки.

Добавление роли

Для добавления новой роли необходимо нажать кнопку  на панели действий над таблицей.

Добавление внутренней роли



← Добавление

Роль *

Введите имя

Описание

Введите описание

0 / 200

Тип роли

☒ внутренняя

☐ внешняя

Привилегии *

Перед настройкой привилегий внимательно ознакомьтесь со списком разделов, входящих в привилегии

Привилегия	☐ Чтение	☐ Создание	☐ Редактирование	☐ Удаление
Политики RADIUS	☐	☐	☐	☐
Мониторинг RADIUS	☐	☐	☐	☐
Эндоинты	☐	☐	☐	☐
Сетевые ресурсы	☐	☐	☐	☐
Политики TACACS+	☐	☐	☐	☐
Мониторинг TACACS+	☐	☐	☐	☐
Профилирование	☐	☐	☐	☐
Роли и УЗ	☐	☐	☐	☐
Гостевой доступ	☐	☐	☐	☐
Гостевые пользователи	☐	☐	☐	☐
Корпоративные пользователи	☐	☐	☐	☐
Системные настройки	☐	☐	☐	☐
Внешние источники	☐	☐	☐	☐
Сервисы сообщений	☐	☐	☐	☐

Отмена **Добавить**

Рисунок 101. Форма добавления внутренней роли

Форма содержит следующие поля:

- **Роль *** — имя роли.
- **Описание** — произвольное описание (максимальная длина - 200 символов).
- **Тип роли *** — выбрать значение "внутренняя".
- **Привилегии *** — таблица настройки прав доступа. Требуется выбрать уровень хотя бы для одной привилегии.

* — поля, обязательные для заполнения.



Нельзя создать роль с правами выше, чем у текущего пользователя.

Для добавления роли необходимо нажать кнопку "Добавить".

Добавление внешней роли

Пользователи и устройства > Пользователи системы > Роли > Добавление

← Добавление

Роль *
Введите имя

Описание
Введите описание
0 / 200

Тип роли
☐ внутренняя
☒ внешняя

Источник аутентификации
MS AD

Для назначения роли требуется
☒ состоять во всех указанных группах (AND)
☐ состоять хотя бы в одной из указанных групп (OR)

Группы из службы каталогов *
Поиск +

Привилегии *
Перед настройкой привилегий внимательно ознакомьтесь со списком разделов, входящих в привилегии

Привилегия	☐ Чтение	☐ Создание	☐ Редактирование	☐ Удаление
Политики RADIUS	☐	☐	☐	☐
Мониторинг RADIUS	☐	—	—	—
Эндпоинты	☐	☐	☐	☐
Сетевые ресурсы	☐	☐	☐	☐
Политики TACACS+	☐	☐	☐	☐
Мониторинг TACACS+	☐	—	—	—
Профилирование	☐	☐	☐	☐
Роли и уз	☐	☐	☐	☐
Гостевой доступ	☐	☐	☐	☐
Гостевые пользователи	☐	☐	☐	☐
Корпоративные пользователи	☐	☐	☐	☐
Системные настройки	☐	☐	☐	☐

Отмена **Добавить**

Рисунок 102. Форма добавления внешней роли

Форма содержит следующие поля:

- **Роль *** — наименование роли.
- **Описание** — произвольное описание (максимальная длина - 200 символов).
- **Тип роли *** — выбрать значение "внешняя".
- **Источник аутентификации** — внешний источник идентификации, группы которого используются для сопоставления.



Поле заполняется автоматически на основе конфигурации раздела «Вход в систему» и не требует ручного выбора. В качестве значения подставляется источник, указанный в поле "Источник аутентификации" при включенной опции "Использовать внешний источник идентификации в качестве основного источника аутентификации".

- **Для назначения роли требуется** — выбор условия при проверке принадлежности пользователей к группам из службы каталогов.

состоять во всех указанных группах (логическое «И») — роль назначается только пользователям, состоящим одновременно **во всех** выбранных группах. Является значением по умолчанию.

- состоять хотя бы в одной из указанных групп (логическое «ИЛИ») — роль назначается пользователям, состоящим **хотя бы в одной** из выбранных групп. Становится доступен только при указании двух и более групп.

Правила совместимости групп и логики:

- Запрещено создание двух и более ролей с одинаковым набором групп и *одинаковой* логикой.
- Группы, которые уже используются в какой-либо роли с логикой «ИЛИ», нельзя повторно использовать в другой роли с логикой «ИЛИ».
- Допустимо создание ролей с одинаковым набором групп и *разной* логикой («И» и «ИЛИ»), **за исключением случаев, когда набор состоит из одной группы:**
 - Группа, которая является **единственной** в роли с логикой «И», не может быть использована в роли с логикой «ИЛИ».
 - Группа, которая уже используется **в любой роли с логикой «ИЛИ»**, не может быть использована в качестве единственной в роли с логикой «И».

- Группы из службы каталогов * — для выбора доступны группы, которые были добавлены при настройке соответствующего внешнего источника (вкладка «Группы»).

The screenshot shows a UI element titled 'Группы из службы каталогов * ?'. Below the title is a search input field with the placeholder text 'Поиск'. To the right of the input field is a dropdown arrow icon and a plus sign icon.

Для того что бы увидеть список групп из внешнего истоника необходимо нажать на поле "Поиск" и в выпадающем списке выбрать нужное значение.

The screenshot shows the search results for the query 'test'. The input field contains 'test' and has a clear button (x) and a dropdown arrow. Below the input field, a list of results is displayed, with the first result being 'CN=Admins,OU=Groups,OU=Company,DC=test, DC=loc'. The list is partially obscured by a blue selection box.

При выборе групп из внешнего источника доступна фильтрация по имени группы. Фильтрация регистронезависимая, отображает все группы попавшие под фильтр.

Группы из службы каталогов * ?

CN=Admins,OU=Groups,OU=Company... ▾ +

Необходимо добавить хотя бы одну группу.

- **Привилегии *** — таблица настройки прав доступа. Требуется выбрать уровень хотя бы для одной привилегии.

* — поля, обязательные для заполнения.



Нельзя создать роль с правами выше, чем у текущего пользователя.

Для создания роли необходимо нажать кнопку "Добавить".

Условия получения внешней роли

- Роль должна иметь статус **Доступно**. Роли со статусом **Недоступно** не назначаются.
- Связанный с ролью внешний источник должен быть **доступен** и корректно настроен.
- Пользователь должен удовлетворять условию, заданному в настройках роли:
 - при логике «И» — состоять во всех группах, перечисленных в настройках роли;
 - при логике «ИЛИ» — состоять хотя бы в одной из указанных групп.



Назначение роли проверяется и пересчитывается **при каждом входе** пользователя на основе актуального состава групп.

Выбор роли при множественном соответствии

Если пользователь соответствует условиям нескольких внешних ролей, назначение выполняется по следующему алгоритму:

1. Приоритет AND перед OR

В первую очередь рассматриваются роли с логикой AND. Если найдена хотя бы одна подходящая AND-роль, роли с логикой OR не рассматриваются.

2. Выбор среди AND-ролей

Из всех подходящих AND-ролей выбирается та, которая требует наличия наибольшего количества групп. Если таких ролей несколько, приоритет отдаётся роли, созданной раньше (с меньшим идентификатором).

3. Выбор среди OR-ролей

Если подходящих AND-ролей нет, система проверяет подходящие OR-роли. Если таких ролей несколько, приоритет отдаётся роли, созданной раньше (с меньшим идентификатором).

Редактирование роли

Для редактирования роли необходимо на странице со списком нажать на имя роли в общей таблице.

☐	Статус	Роль ↑
☐	⊗ Недоступно	AD_Operators ⚠
☐	✓ Доступно	Guest Admin 🔒
☐	✓ Доступно	Guest Operator 🔒
☐	✓ Доступно	Hardware Admin 🔒
☐	✓ Доступно	Monitor 🔒
☐	✓ Доступно	Network Admin 🔒
☐	✓ Доступно	read
☐	✓ Доступно	Super Admin 🔒
☐	✓ Доступно	System Admin 🔒

Рисунок 103. Гиперссылка на страницу редактирования роли

После этого откроется страница редактирования роли, аналогичная странице добавления.



Изменение типа роли запрещено, если роль назначена хотя бы одному пользователю системы.

Редактирование внутренней роли

Пользователи и устройства

Пользователи системы

Роли

Radius policy

← Radius policy

⚠

При изменении привилегий роли сессии пользователей с этой ролью прервутся - потребуется повторная авторизация

Роль *

Radius policy

Описание

Role description

16 / 200

Тип роли

☒ внутренняя
☐ внешняя

Привилегии *

Перед настройкой привилегий внимательно ознакомьтесь со списком разделов, входящих в привилегии

Привилегия	Чтение	Создание	Редактирование	Удаление
Политики RADIUS	☒	☒	☒	☐
Мониторинг RADIUS	☐	☐	☐	☐
Эндпоинты	☐	☐	☐	☐
Сетевые ресурсы	☐	☐	☐	☐
Политики TACACS+	☐	☐	☐	☐
Мониторинг TACACS+	☐	☐	☐	☐
Профилирование	☒	☐	☐	☐
Роли и уз	☐	☐	☐	☐
Гостевой доступ	☒	☐	☐	☐
Гостевые пользователи	☐	☐	☐	☐
Корпоративные пользователи	☐	☐	☐	☐
Системные настройки	☐	☐	☐	☐
Внешние источники	☐	☐	☐	☐
Сервисы сообщений	☒	☐	☐	☐

Отмена

Сохранить

Рисунок 104. Форма редактирования внутренней роли



После сохранения изменений в **привилегиях роли** все активные сессии пользователей с этой ролью будут завершены — потребуется повторная авторизация.

После внесения изменений необходимо нажать кнопку **"Сохранить"**. Кнопка становится активной при наличии изменений.

Кнопка **«Отмена»** осуществляет сброс внесенных изменений до исходного состояния.

Редактирование внешней роли

Пользователи и устройства > Пользователи системы > Роли > AD_Operators

← AD_Operators

При изменении привилегий роли сессии пользователей с этой ролью прервутся - потребуется повторная авторизация

Роль *

AD_Operators

Описание

Введите описание

0 / 200

Тип роли

☐ внутренняя

☒ внешняя

Источник аутентификации

MS AD

Для назначения роли требуется

☒ состоять во всех указанных группах (AND)

☐ состоять хотя бы в одной из указанных групп (OR)

Группы из службы каталогов *

CN=Admins,OU=Groups,OU=Company...

Привилегии *

Перед настройкой привилегий внимательно ознакомьтесь со списком разделов, входящих в привилегии

Привилегия	☒ Чтение	☒ Создание	☒ Редактирование	☐ Удаление
Политики RADIUS	☒	☒	☒	☐
Мониторинг RADIUS	☐	☐	☐	☐
Эндпоинты	☐	☐	☐	☐
Сетевые ресурсы	☐	☐	☐	☐
Политики TACACS+	☐	☐	☐	☐
Мониторинг TACACS+	☐	☐	☐	☐
Профилирование	☒	☐	☐	☐
Роли и УЗ	☐	☐	☐	☐
Гостевой доступ	☒	☐	☐	☐
Гостевые пользователи	☐	☐	☐	☐
Корпоративные пользователи	☐	☐	☐	☐
Системные настройки	☐	☐	☐	☐
Внешние источники	☐	☐	☐	☐
Сервисы сообщений	☒	☐	☐	☐

Отмена Сохранить

Рисунок 105. Форма редактирования внешней роли



После сохранения изменений в **привилегиях роли** или **составе групп внешнего источника** все активные сессии пользователей с этой ролью будут немедленно завершены — потребуется повторная авторизация.

После внесения изменений необходимо нажать кнопку **"Сохранить"**. Кнопка становится активной при наличии изменений.

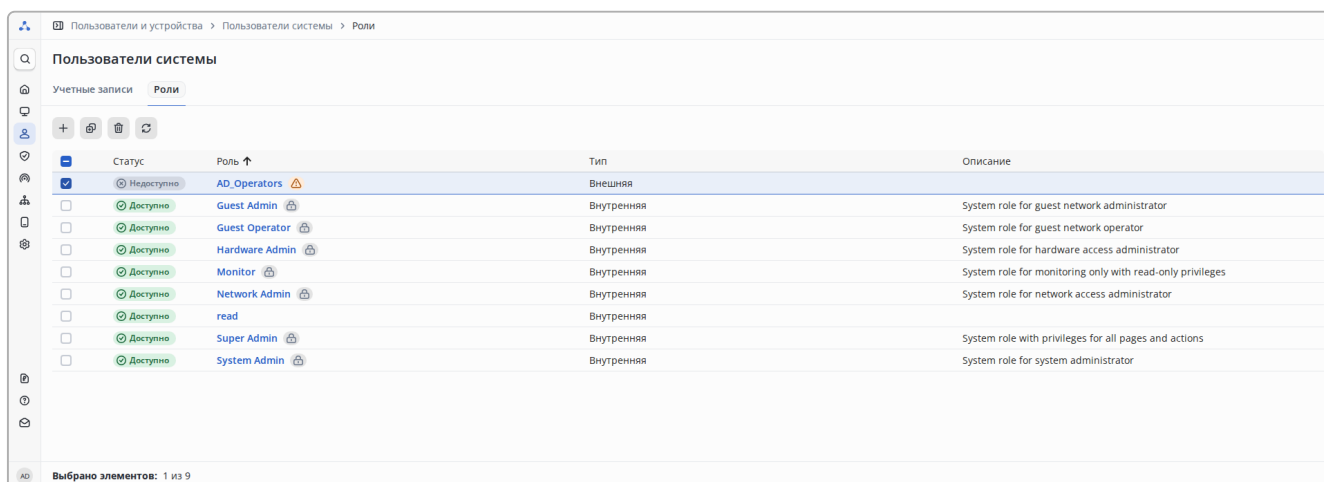
Кнопка **«Отмена»** осуществляет сброс внесенных изменений до исходного состояния.

Удаление роли

Для удаления необходимо выделить чекбокс слева от ролей, которые требуется удалить, и нажать кнопку  на панели действий, расположенной над таблицей.



Нельзя удалить роль, которая назначена пользователю системы.



Статус	Роль	Тип	Описание
Недоступно	AD_Operators	Внешняя	
Доступно	Guest Admin	Внутренняя	System role for guest network administrator
Доступно	Guest Operator	Внутренняя	System role for guest network operator
Доступно	Hardware Admin	Внутренняя	System role for hardware access administrator
Доступно	Monitor	Внутренняя	System role for monitoring only with read-only privileges
Доступно	Network Admin	Внутренняя	System role for network access administrator
Доступно	read	Внутренняя	
Доступно	Super Admin	Внутренняя	System role with privileges for all pages and actions
Доступно	System Admin	Внутренняя	System role for system administrator

Рисунок 106. Выбор ролей в таблице для удаления



Удаление элементов требует подтверждения в модальном окне. Выбранные элементы будут удалены только после явного подтверждения операции.

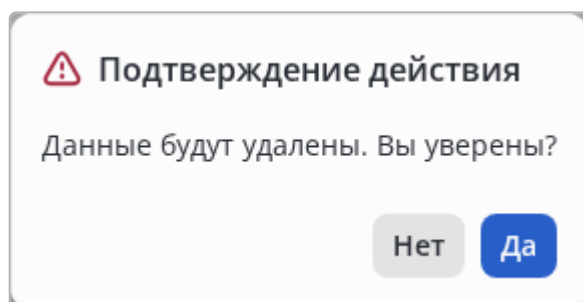


Рисунок 107. Диалоговое окно подтверждения действия

Особенности при смене внешнего источника

При изменении конфигурации входа в систему (раздел «Вход в систему») все внешние роли, связанные со **старым источником**, автоматически переходят в статус  **Недоступно**.



Рисунок 108. Предупреждение о смене источника

Смена основного источника аутентификации

При переключении с одного внешнего источника на другой (например, с MS Active Directory на OpenLDAP) форма недоступной внешней роли будет выглядеть следующим образом:

Пользователи и устройства > Пользователи системы > Роли > AD_Operators

← AD_Operators

Изменился источник входа. Эта роль больше не может быть выдана — смените группы из службы каталогов

Роль *

AD_Operators

Описание

Введите описание

0 / 200

Тип роли

☐ внутренняя

☒ внешняя

Источник аутентификации

MS AD

Для назначения роли требуется

☒ состоять во всех указанных группах (AND)

☐ состоять хотя бы в одной из указанных групп (OR)

Группы из службы каталогов

CN=Admins,OU=Groups,OU=Company...

Группы из старого источника

Привилегии *

Перед настройкой привилегий внимательно ознакомьтесь со списком разделов, входящих в привилегии

Привилегия	Чтение	Создание	Редактирование	Удаление
Политики RADIUS	☒	☒	☒	☐
Мониторинг RADIUS	☐	☐	☐	☐
Эндпоинты	☐	☐	☐	☐
Сетевые ресурсы	☒	☐	☐	☐
Политики TACACS+	☐	☐	☐	☐
Мониторинг TACACS+	☐	☐	☐	☐
Профилирование	☒	☐	☐	☐
Роли и узлы	☐	☐	☐	☐
Гостевой доступ	☒	☐	☐	☐
Гостевые пользователи	☐	☐	☐	☐
Корпоративные пользователи	☐	☐	☐	☐

Отмена Сохранить

Рисунок 109. Форма редактирования недоступной внешней роли (смена источника)

- В **Источник аутентификации** автоматически подставляется **актуальный источник** (текущий основной источник из настроек входа).
- Ранее выбранные группы подсвечиваются как устаревшие.



Дублирование роли позволяет быстро создать ее копию с актуальным источником. Группы из старого источника при этом не переносятся.

Отключение использования внешнего источника

При отключении использования внешнего источника (снятие чекбокса "Использовать внешний источник идентификации в качестве основного") форма недоступной внешней роли будет выглядеть следующим образом:

Рисунок 110. Форма редактирования недоступной внешней роли (отключен внешний вход)

- В блоке **Тип роли** вариант **"внешняя"** заблокирован — выбрать можно только тип **"внутренняя"**.
- Блоки, связанные с внешней аутентификацией (**Источник аутентификации** и **Группы из службы каталогов**), недоступны для редактирования.



Дублирование недоступной внешней роли требует смены типа роли на **"внутренняя"**.

Особенности при изменении уровня лицензии

Повышение уровня лицензии

После повышения уровня лицензии может потребоваться дополнительная настройка привилегий. Роли, требующие донастройки, помечаются предупреждением:

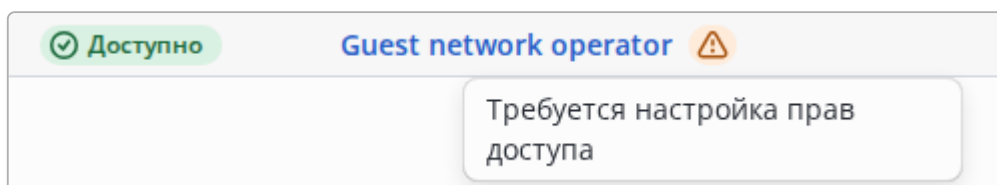


Рисунок 111. Предупреждение о необходимости донастройки роли

Пользователи с такими ролями увидят системное уведомление в интерфейсе:

Рисунок 112. Уведомление в навигационном меню "Требуется настройка роли"

Понижение уровня лицензии

При редактировании роли, содержащей привилегии, не входящие в текущую лицензию, права на эти привилегии будут сброшены после подтверждения сохранения:

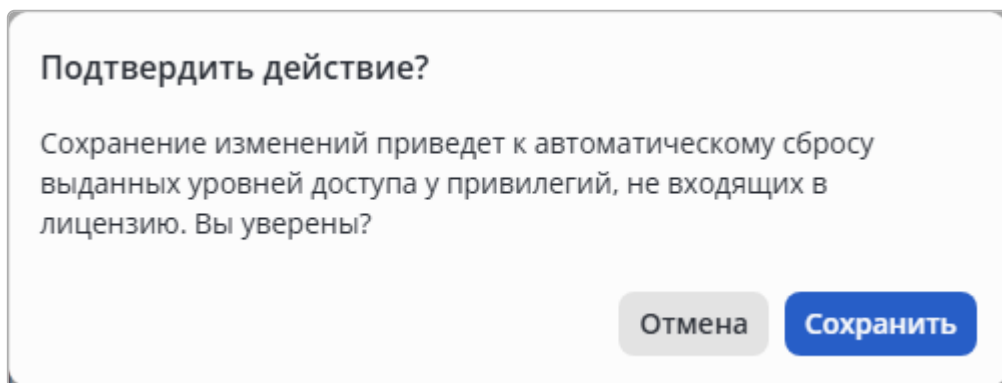


Рисунок 113. Подтверждение сохранения изменений

Сетевые ресурсы

Сетевое устройство (authenticator, NAS - Network Access Server) - стационарное устройство, обеспечивающее подключение клиентских устройств к сети и реализующее их аутентификацию с использованием протокола 802.1x, MAB или портальной авторизации.

Управление сетевыми устройствами выполняется в меню "Пользователи и устройства" → "Сетевые ресурсы".

Содержит разделы:

- [Устройства](#) - раздел настроек взаимодействия с сетевыми устройствами;
- [Группы устройств](#) - раздел настроек групповых признаков, которые могут использоваться при настройке сетевых устройств;
- [Профили устройств](#) - профили, описывающие особенности взаимодействия сетевых устройств по протоколам RADIUS и TACACS+.

Устройства

Описание

Сетевое устройство (аутентификатор, NAS - Network Access Server) - стационарное устройство, обеспечивающее подключение клиентских устройств к сети и реализующее их аутентификацию с использованием протокола 802.1x, MAB или других видов подключений.

Раздел "Устройства" отвечает за просмотр, добавление, удаление, редактирование сетевых устройств в системе NAICE.



Если устройство не было добавлено в систему, то запрос на авторизацию по RADIUS-протоколу от него не будет обработан!

Важно понимать — создание нового устройства невозможно без созданного [профиля устройства](#).

Просмотр списка сетевых устройств

Имя	IPv4	Профиль	Протоколы	Местоположение	Тип устройства	Описание
Renoir	10.25.96.105	Eltex MES	RADIUS TACACS+	Building 1 < All Locations	Eltex < All Device Types	
Samsung_Catharine_430	63.238.75.65	Eltex MES	RADIUS TACACS+	Building 1 < All Locations	Eltex < All Device Types	

Рисунок 114. Таблица с перечнем сетевых устройств на странице просмотра

На данной странице содержится таблица со списком всех сетевых устройств, добавленных в систему.

Таблица содержит колонки:

- Имя** — наименование сетевого устройства.
- IPv4** — IP-адрес, предназначенный для взаимодействия с устройством (IPv4).
- Профиль** — назначенный профиль устройству. Является гиперссылкой на страницу просмотра/редактирования настроек данного профиля устройства.
- Протоколы** — показывает статус настройки протоколов RADIUS и TACACS.
 - Серый** статус - протокол в выбранном профиле выключен;
 - Красный** статус - протокол в выбранном профиле включен, но секрет в настройках устройства не указан;
 - Зеленый** статус - протокол в выбранном профиле включен, секрет в настройках устройства указан.
- Местоположение** — группа, определяющая местоположение устройства.
- Тип устройства** — группа, определяющая тип устройства.
- Описание** — произвольное описание устройства.



При наведении на строку с интересующим профилем появляется подсказка  при нажатии на которую можно посмотреть настройки для данного профиля.

Возможна сортировка в прямом и обратном порядке по колонкам "Имя", "IPv4", "Профиль". По умолчанию сортировка выполняется в прямом алфавитном порядке по колонке "Имя".

Элементы управления:

-  — Добавить новый элемент.
-  — Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
-  — Обновить данные таблицы.
-  — Позволяет загрузить данные из csv-файла.
-  — Позволяет выгрузить данные в csv-файл.
- ☐ — Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).
-  — Изменить текущий порядок сортировки.
-  Поиск — Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.



В данный момент IPv4 - единственный признак, по которому система определяет, с каким устройством идёт работа.
Доступно только полное совпадение по IP, а значит адреса всех устройств должны быть добавлены в систему явно.

Добавление сетевого устройства

Для добавления сетевого устройства нажмите .

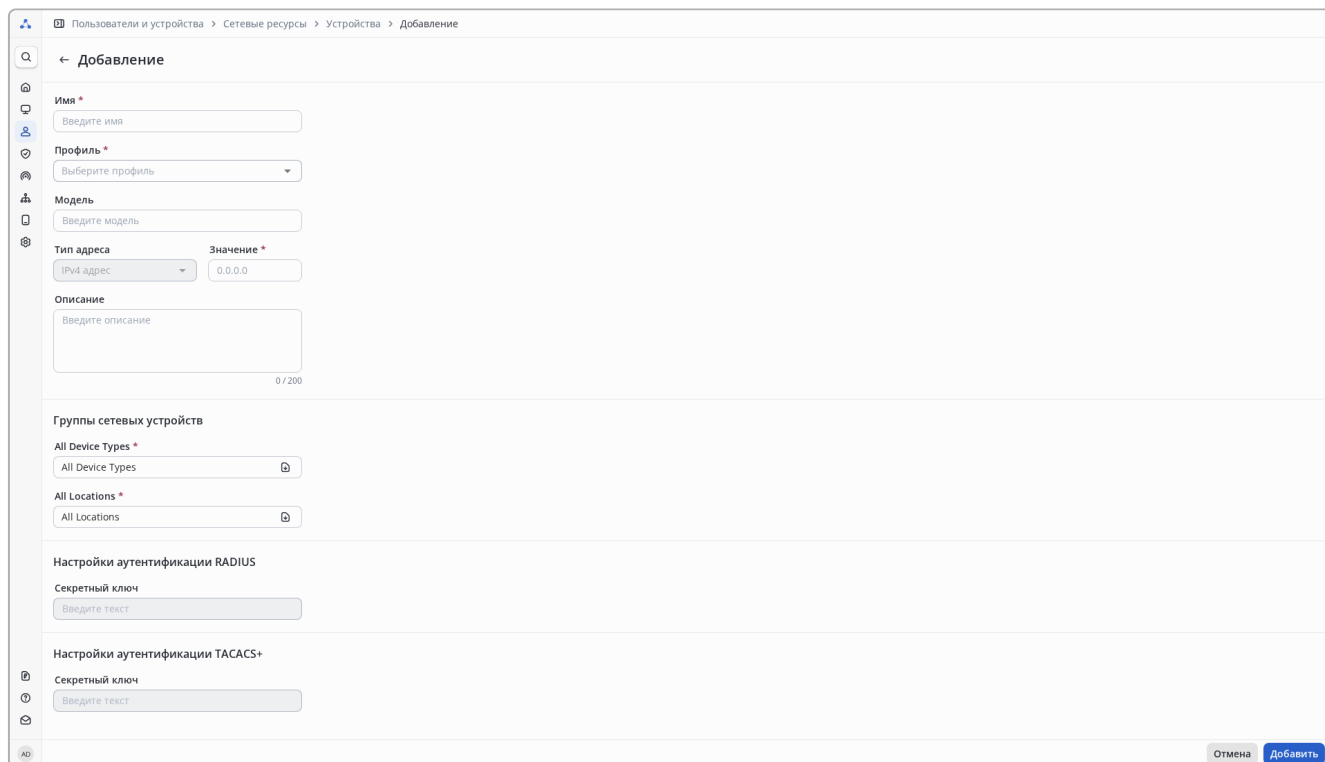


Рисунок 115. Страница добавления сетевого устройства

В открывшейся форме можно заполнить следующие параметры:

•

Имя * - наименование сетевого устройства; должно быть уникально в рамках списка сетевых устройств. Максимальная длина - 200 символов.

- **Профиль *** - выбор [профиля сетевого устройства](#).
- **Модель** - модель сетевого устройства. Максимальная длина - 100 символов.
- **IPv4 *** - IP-адрес сетевого устройства. Запись в виде четырех чисел от 0 до 255, разделенных точками.
- **Описание** - произвольное описание. Максимальная длина - 200 символов.

Группы сетевых устройств - выбор групп типа и локации сетевого устройства. Если выбор не сделать - будут назначены группы по умолчанию (т.е. корневые).

При создании новой корневой группы, как это описано в разделе [Группы устройств](#), в списке *Группы сетевых устройств* они будут появляться автоматически.

Настройка аутентификации RADIUS содержит:

- Секретный ключ для взаимодействия с сетевым устройством по протоколу RADIUS. Является обязательным полем, если в выбранном профиле включен протокол RADIUS. Длина от 1 до 200 символов.

TACACS+ **Настройка аутентификации TACACS+** содержит:

- Секретный ключ для взаимодействия с сетевым устройством по протоколу TACACS+. Длина от 0 до 64 символов.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

После ввода необходимых данных нажмите кнопку "Добавить".

Редактирование сетевого устройства

Для редактирования сетевого устройства необходимо на странице со списком нажать на его имя.

☐	Имя ↑
☐	Renoir
☐	Samsung_Catharine_430

Рисунок 116. Гиперссылка на страницу редактирования устройства

После этого откроется окно редактирования, аналогичное странице добавления.

Пользователи и устройства > Сетевые ресурсы > Устройства > Renoir

← Renoir

Имя *

Renoir

Профиль *

Eltex MES

Модель

MES2324P

Тип адреса

IPv4 адрес

Значение *

10.25.96.105

Описание

Введите описание

0 / 200

Группы сетевых устройств

All Device Types *

Eltex

All Locations *

Building 1

Настройки аутентификации RADIUS

Секретный ключ *

.....

Настройки аутентификации TACACS+

Секретный ключ

Введите текст

Рисунок 117. Страница редактирования устройства



RADIUS-сервер, находящийся в составе NAICE, кэширует сетевые устройства при их добавлении в систему. В случае ошибки при указании секретного ключа и последующем редактировании на корректный ключ эти данные в кэше не будут обновлены. В этом случае выполните рестарт docker-контейнера naice-radius для перечитывания новых данных из базы данных.

После редактирования необходимо нажать на кнопку **"Сохранить"**. Кнопка скрыта, пока не будет внесено хотя бы одно изменение.

Кнопка **"Отмена"** осуществляет сброс внесенных изменений до исходного состояния.

Удаление сетевого устройства

Для удаления в окне со списком надо выделить чекбокс слева от наименования сетевых устройств, которые требуется удалить, и нажать кнопку  вверху слева.

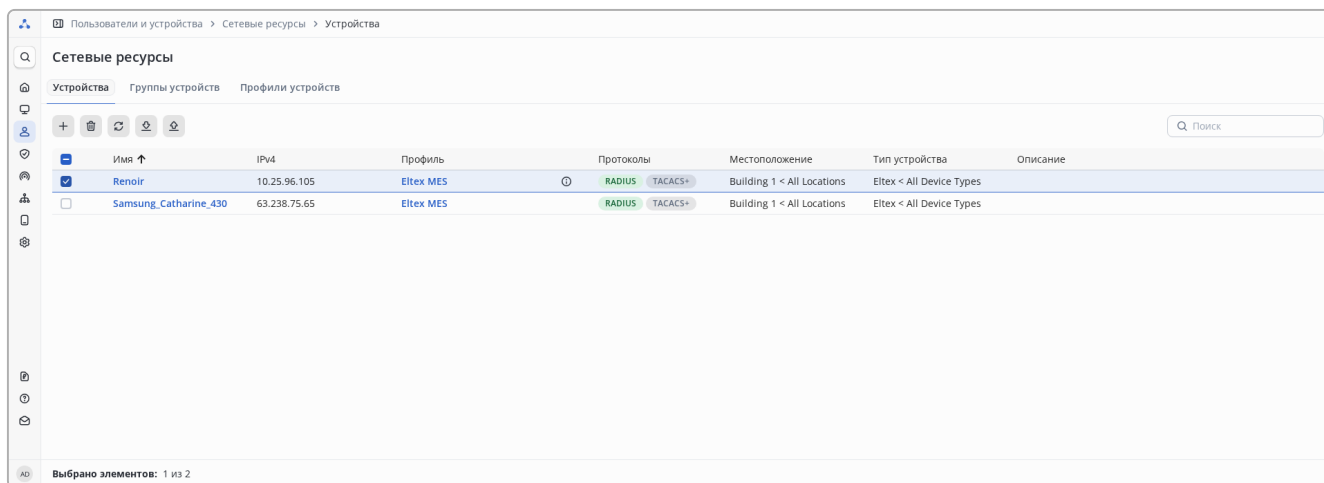


Рисунок 118. Выбор устройства в таблице для удаления



Удаление элементов требует подтверждения в модальном окне. Выбранные элементы будут удалены только после явного подтверждения операции.

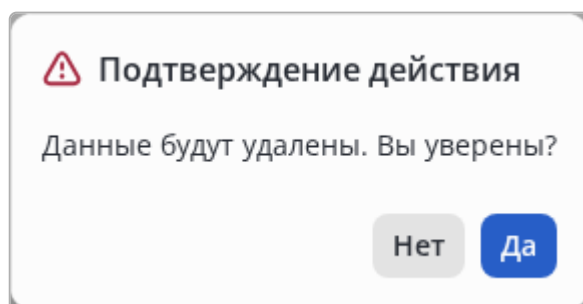


Рисунок 119. Диалоговое окно подтверждения действия

Импорт

NAICE поддерживает импорт данных из CSV-файлов.

Предварительная подготовка перед импортом

1. Создайте или проверьте наличие необходимых связанных сущностей (например, профиль устройства).
2. Ознакомьтесь с требованиями к CSV-файлу:
 - Файл должен быть в кодировке UTF-8;
 - Разделитель полей: запятая (,)
 - Разделитель строк/текста: двойная кавычка (")
 - Заголовки и значения должны быть взяты в двойные кавычки (")
 - Максимальный размер файла 2МБ.
3. Проверьте содержимое файла на наличие лишних кавычек перед импортом;
4. Проверьте то что значения, содержащие двойную кавычку (") или слэш (/) правильно экранированы.

Значения, содержащие двойную кавычку (") экранируются с помощью \

- Значения, содержащие слэш (/) экранируются с помощью \

Правильное написание значений (с экранированием при помощи \) на примере содержания файла для импорта набора команд TACACS:

"name:Required"	"description"	"permit_unmatched(true/false)"	"commands(Grant/command/arguments/enabled;...)"
"command_set"	"\"Test command set\""	"false"	"PERMIT/\"show/vlan 1 2 \"/true"

Некорректное написание значений (без экранирования) на примере содержания файла для импорта набора команд TACACS:

"name:Required"	"description"	"permit_unmatched(true/false)"	"commands(Grant/command/arguments/enabled;...)"
"command_set"	"Test command set"	"false"	"PERMIT/show/vlan 1 2 /true"



Игнорирование экранирования приведёт к некорректному распознаванию данных.

Порядок выполнения импорта

Для импорта данных из CSV-файла нажмите  на панели действий, расположенной над таблицей. После чего откроется окно:

Импорт

При импорте дублирующиеся данные не будут перезаписаны или отредактированы - система пропустит их. Если вы хотите изменить старые данные, удалите их из системы вручную перед импортом.

Внимательно ознакомьтесь с [Документацией](#) , чтобы импорт прошёл без ошибок.

Выберите файл*
Максимальный размер файла 2МБ

 **Загрузите** или перетащите сюда

Поле обязательно для заполнения

Источник данных *

NAICE

☐ Игнорировать существующие данные 

☐ Остановить импорт при первой ошибке

☐ Автоматически создать недостающие записи 

Отмена

Импорт

Рисунок 120. Окно импорта

Импорт данных из CSV-файла выполняется в несколько шагов:

1. Выберите необходимый CSV-файл, перетащив его в поле загрузки или выбрав через проводник, нажав кнопку "Загрузите";



Измененный CSV-файл нужно загрузить повторно, чтобы применить правки.

2. Выберите источник данных, если он заранее не определён;
3. При необходимости активируйте флаги импорта:

Игнорировать существующие данные

- Если переключатель включен — дубликаты записей считаются предупреждением.
- Если переключатель выключен — дубликаты расцениваются как ошибка.

Остановить импорт при первой ошибке

-

Если переключатель включен — импорт останавливается при первой же ошибке. Будут импортированы только записи, которые были успешно обработаны до её возникновения.

- Если переключатель выключен — ошибочные строки пропускаются, импорт продолжается до конца. Будут импортированы только валидные записи.

Автоматически создать недостающие записи

- Если переключатель включен — при выполнении импорта недостающие записи будут заполнены автоматически. Перечень автозаполняемых записей можно узнать при наведении на подсказку справа от переключателя.
- Если переключатель выключен — все требуемые поля необходимо заполнить вручную.

4. Для того чтобы импорт начался, нажмите кнопку **"Импорт"**.



При импорте дублирующиеся данные перезаписаны или отредактированы не будут - система пропустит их. Если вы хотите изменить старые данные, удалите их из системы вручную перед импортом.

Просмотр отчета по импорту

Сразу после завершения обработки файла откроется окно отчёта по импорту.

Если все записи в файле были обработаны корректно, вы увидите окно:

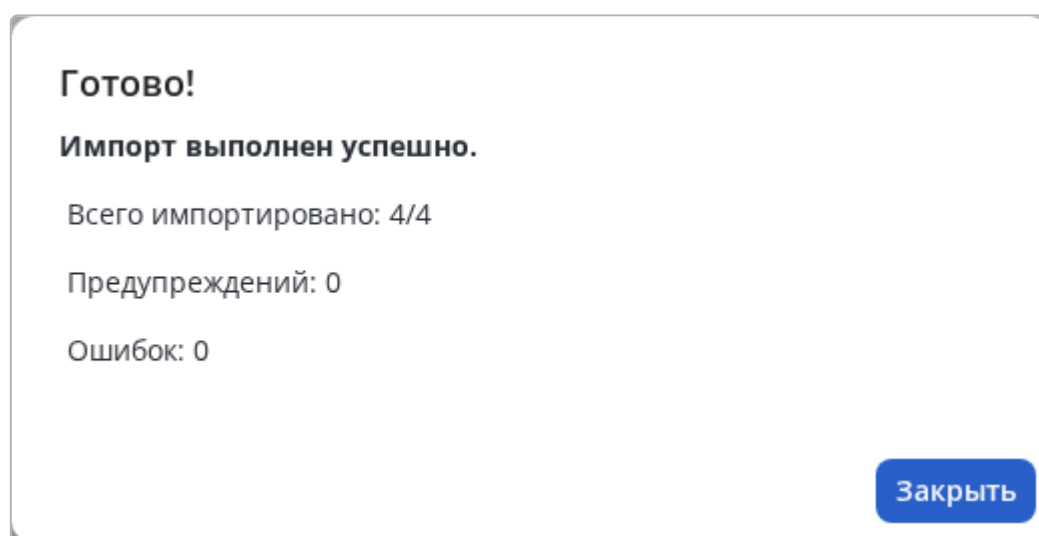


Рисунок 121. Отчет импорта (все записи обработаны корректно)

Блок с общей информацией содержит:

- **Всего импортировано** - Счётчик того, сколько записей было импортировано из общего импортируемого количества строк;
- **Предупреждений** - Количество возникших предупреждений;
- **Ошибок** - Количество возникших ошибок.

Если не все записи были обработаны корректно, вы увидите окно:

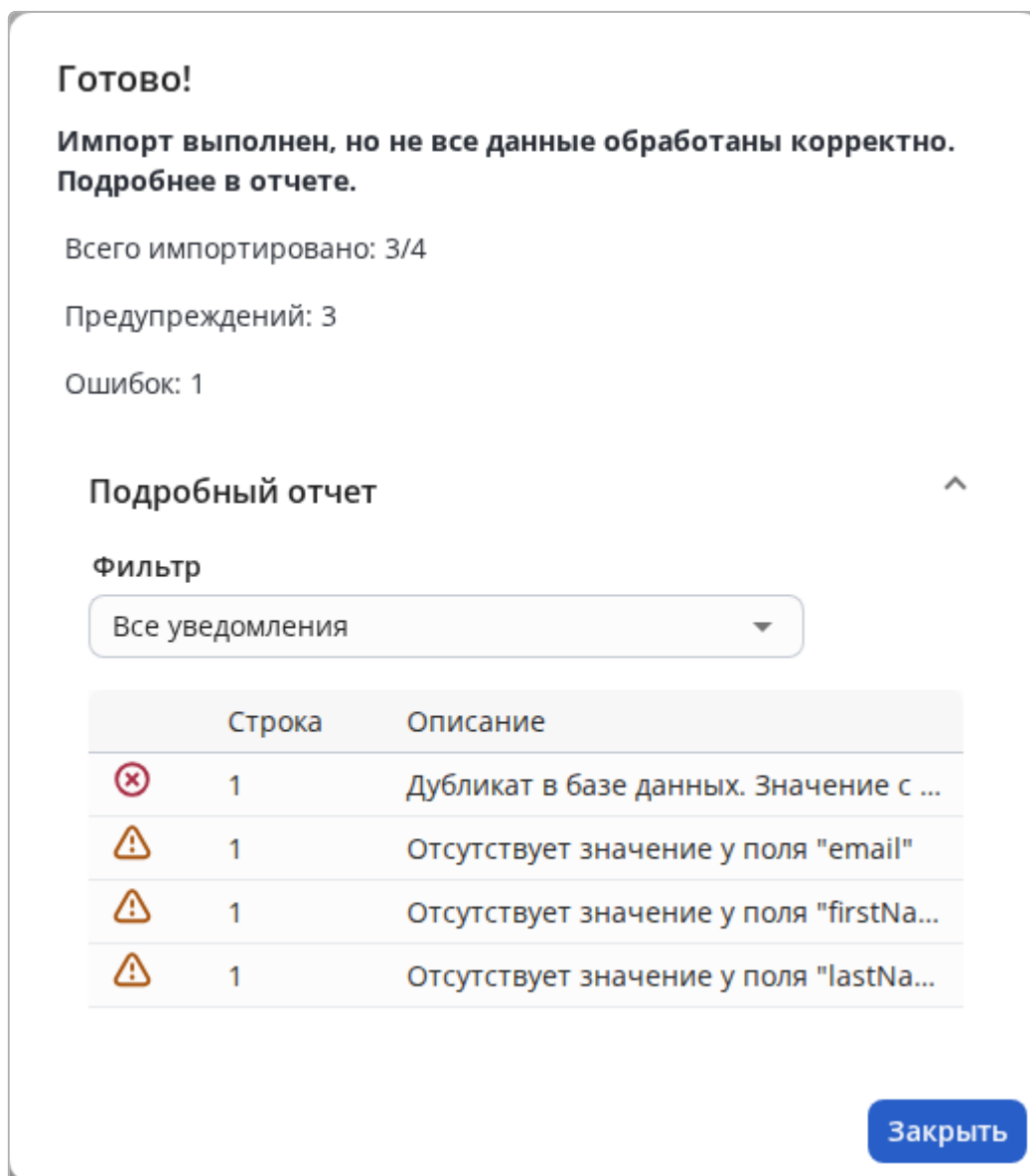


Рисунок 122. Отчет импорта (записи обработаны с ошибками/предупреждениями)

Подробный отчет содержит следующую информацию:

- **Фильтр** - Выпадающий список, в котором можно выбрать отображаемые уведомления (Все уведомления, Только ошибки или Только предупреждения)

Таблица уведомлений содержит колонки:

- **Строка** - Номер строки в CSV-файле, где обнаружена ошибка или предупреждение;
- **Описание** - Детальное текстовое объяснение ошибки или предупреждения.



Для просмотра полного текста описания наведите курсор мыши на соответствующую строку - во всплывающей подсказке отобразится полный текст сообщения об ошибке или предупреждении.

Особенности импорта устройств



Для устройств сети в качестве источника данных поддерживан только NAICE

В таблице ниже приведен список полей, их обязательность, описание и требования:

Поле	Описание	Требования
name:Required	Имя сетевого устройства	Обязательное поле Должно быть уникальным Максимальная длина - 100 символов
description	Произвольное описание устройства	Максимальная длина - 200 символов
ip_address:Required	IP-адрес устройства (IPv4)	Обязательное поле Должен быть уникальным Формат: четыре числа 0-255, разделенные точками
model_name	Модель сетевого устройства	Максимальная длина - 100 символов
network_device_profile:Required	Профиль сетевого устройства	Обязательное поле Профиль должен существовать в системе
network_device_groups	Группы устройства в которые будет входить устройство (указывается полный путь)	Группы должны существовать в системе Формат: группа#подгруппа Разделитель путей: ;
radius_secret	Секретный ключ RADIUS	Обязателен при включенном RADIUS в профиле Длина: 1-200 символов Запрещены пробелы
tacacs_secret	Секретный ключ TACACS+	Максимальная длина - 64 символа Запрещены пробелы



Если для устройства не указаны группы в `network_device_groups` или группы будут не найдены, ему будут назначены корневые группы.

Пример корректного содержания файла:

"name:Required"	"description"	"ip_address:Required"	"model_name"	"network_device_profile:Required"	"network_device_groups"	"radius_secret"	"tacacs_secret"
"MES"	""	"10.25.96.105"	"MES2324P"	"Eltex MES"	"All Locations#Building 1;All Device Types#Eltex"	"secret123"	"secret123"

Получение CSV-файла шаблона описано далее в разделе "Экспорт".

Экспорт

NAICE поддерживает экспорт данных в формате CSV. Значения и заголовки обрамляются **двойными кавычками**, разделитель полей: **запятая (,)**.

Процедура экспорта

Доступны два режима экспорта данных:

- **Экспорт всего** - Выгрузка всех записей текущего раздела. Системные записи исключаются из экспорта;
- **Экспорт выбранного** - Выгрузка только отмеченных чекбоксом записей.

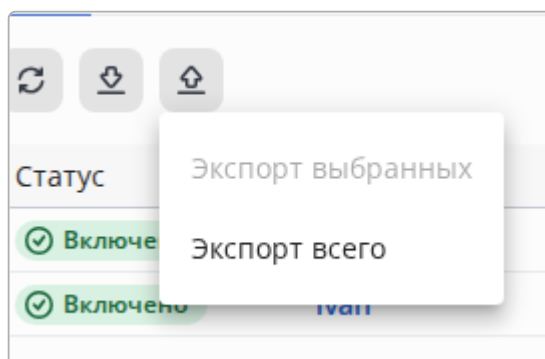


Рисунок 123. Окно выбора режима экспорта



Значения содержащие двойную кавычку (") или слэш (/) будут экранированы с помощью \".

Экспорт всех записей

На панели действий над таблицей нажмите  и выберите режим **"Экспорт всего"**. В открывшемся окне подтвердите действие кнопкой **"Экспорт"**:

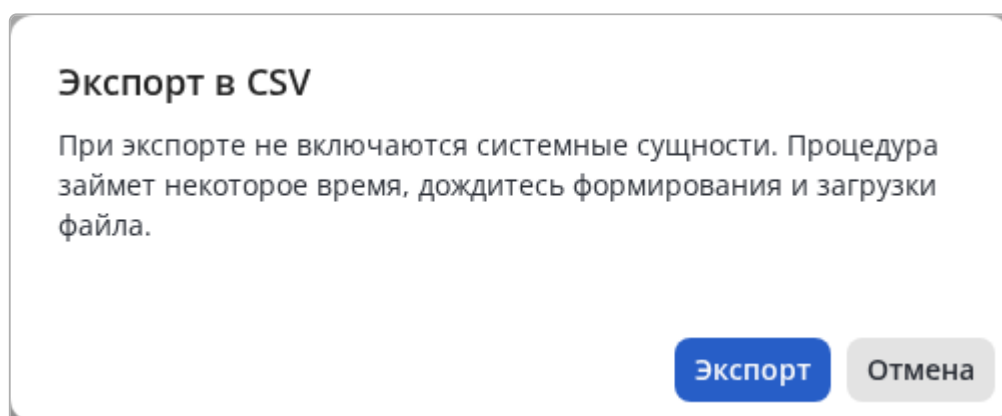


Рисунок 124. Экспорт всего

После нажатия кнопки **"Экспорт"** на устройство выгрузится файл, содержащий все записи из текущего раздела.

Экспорт выбранных записей

На панели действий над таблицей нажмите  и выберите режим "Экспорт выбранных". В открывшемся окне подтвердите действие кнопкой "Экспорт":

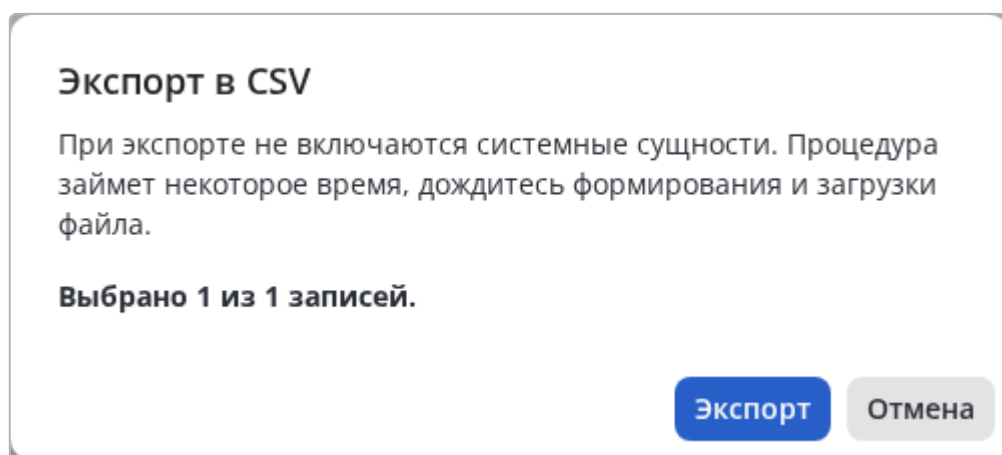


Рисунок 125. Экспорт выбранных

После нажатия кнопки "Экспорт" на устройство выгрузится файл, содержащий только отмеченные записи.



При **открытии** CSV-файлов в качестве разделителя полей **всегда** используйте **запятую (,)**, разделителем строк/текста могут быть **двойные кавычки (")** или **пустое значение**.

При **сохранении** CSV-файлов в качестве разделителя полей **всегда** используйте **запятую (,)**, а разделитель строк/текста - **пустое значение**.



Если при открытии файла использовался разделитель строк — двойная кавычка ("), то значения, содержащие символы двойной кавычки (") или слэша (/), экранированные как \", могут при сохранении получить лишнюю кавычку (") после (\"). Проверьте файл в текстовом редакторе и удалите лишние кавычки, если они появились.

Шаблон

Если в таблице отсутствуют записи (либо присутствуют только системные), при выборе режима "Экспорт всего" будет сформирован CSV-файл, содержащий исключительно заголовки столбцов. Данный файл может быть использован в качестве **шаблона** для подготовки данных перед импортом.

Особенности экспорта устройств



Полный путь до подгруппы в которую входит устройство будет прописан через разделитель - #. Каждый отдельный путь до группы будет отделен с помощью - ; .

Структура CSV-файла для устройств сети описана в разделе "Особенности импорта устройств".

Группы устройств

Описание

Группы устройств предназначены для агрегации сетевых устройств по различным признакам, с дальнейшей возможностью определения различных сценариев авторизации для разных групп в разделах [Политики RADIUS](#) или [Политики TACACS+](#).

Просмотр групп

На данной странице содержится таблица со списком всех групп.

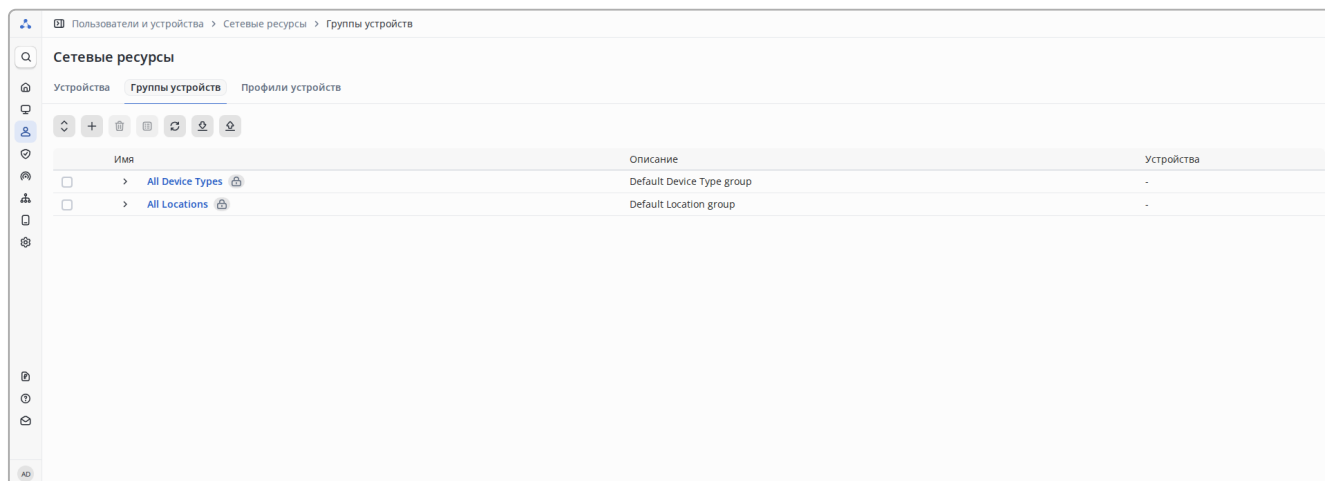


Рисунок 126. Страница просмотра списка групп

По умолчанию существуют две корневые группы:

- **All Device Types** — предназначена для формирования групп по признакам типа сетевых устройств
- **All Locations** — предназначена для формирования групп по признакам локации сетевых устройств.

Данные группы являются системными и не могут быть удалены или изменены.

При необходимости можно добавить новые пользовательские корневые группы. Таким образом администратор может создать любую иерархию устройств, группируя их по любым признакам, где *признак* выносится в Имя корневой группы, а *значения признака* в Имена дочерних групп.

Таблица содержит колонки:

- **Имя** - наименование группы;
 - — Данная запись является системной и недоступна для удаления или редактирования.
- **Описание** — произвольное описание группы;
- **Устройства** — количество устройств в группе; для корневых групп количество устройств не отображается.

Сортировка не предусмотрена.

Элементы управления:

-  — Раскрыть все группы.
-  — Добавить группу.
-  — Удалить группу (неактивно, пока не выбрана группа).
-  — Показать устройства группы и ее подгрупп (неактивно, пока не выбрана группа).
-  — Обновить данные таблицы.
-  — Позволяет загрузить данные из csv-файла.
-  — Позволяет выгрузить данные в csv-файл.
-  — Раскрыть список подгрупп группы.
-  — Свернуть список подгрупп группы.
- ☐ — Чекбокс для выделения группы (можно выбрать только одну группу).

Добавление группы

Добавление корневой группы

Для добавления корневой группы нажмите  вверху слева от списка групп когда не выбрана ни одна группа.

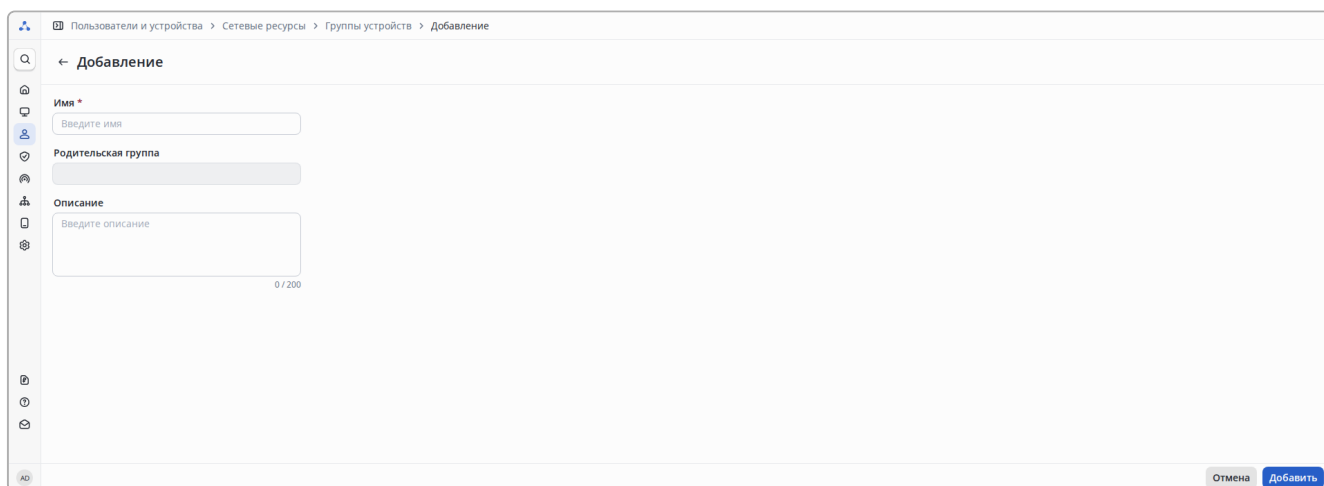


Рисунок 127. Страница добавление группы

В открывшемся окне можно заполнить:

- **Имя *** - наименование группы. Максимальная длина — 100 символов.
- **Описание** - описание. Максимальная длина — 200 символов.
- **Родительская группа** — заполняется автоматически, значение берется от группы для которой выполняется создание подгруппы. При создании корневой группы поле будет пустое.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

После ввода необходимых данных нажмите кнопку "Добавить".

Добавление подгруппы в существующую группу

Для добавления группы в существующую группу необходимо выбрать её чекбоксом слева от наименования и нажать **+**.

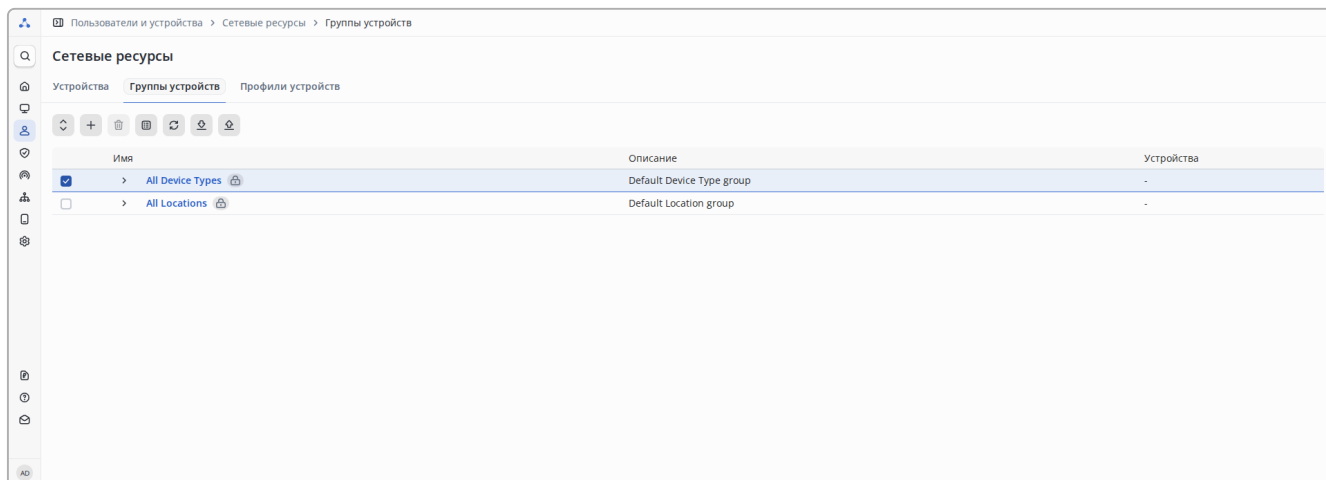


Рисунок 128. Страница с выбором корневой группы для добавления дочерней группы

При добавлении подгруппы в поле "Родительская группа" отображается наименование и ID родительской группы. Данное поле не может быть изменено.

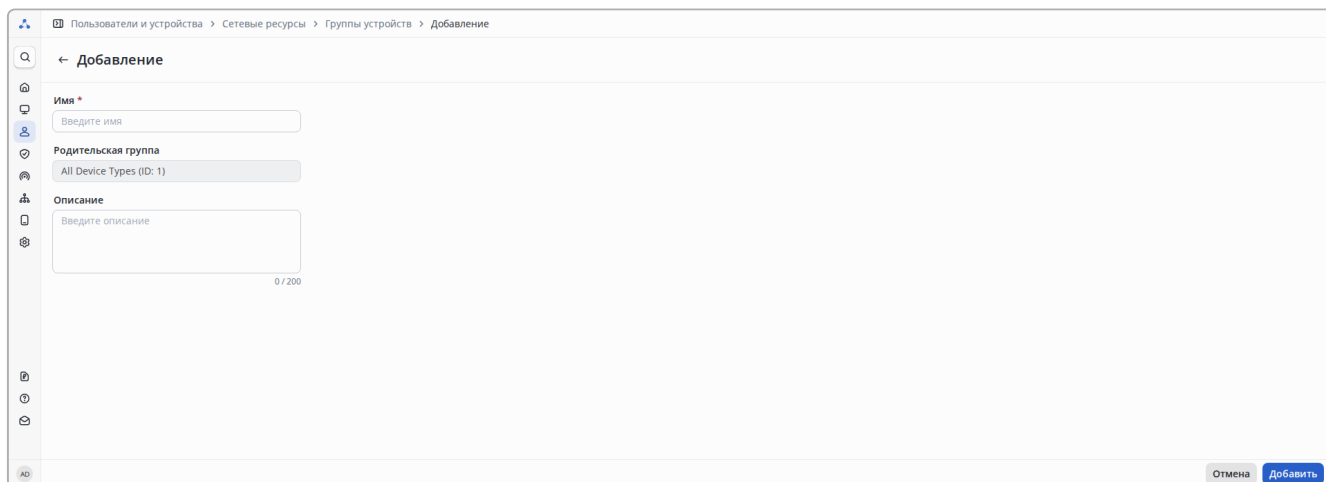


Рисунок 129. Страница с добавлением дочерней группы

Редактирование группы

Для редактирования группы необходимо нажать на её наименование.

Рисунок 130. Страница редактирования группы

После редактирования необходимо нажать на кнопку **"Сохранить"**. Кнопка скрыта, пока не будет внесено хотя бы одно изменение.

Кнопка **"Отмена"** осуществляет сброс внесенных изменений до исходного состояния.



Изменить "Родительскую группу" нельзя. Процедура перемещения подгруппы в другую родительскую не предусмотрена. Для её изменения надо удалить группу и создать ее в качестве подгруппы иной группы.

Удаление группы

Для удаления в окне со списком надо выделить чекбокс слева от наименования и нажать кнопку  вверху слева.

Имя	Описание	Устройства
☐ > All Device Types	Default Device Type group	-
☐ > All Locations	Default Location group	-
☒ Building 1		1

Рисунок 131. Страница с выделенной группой для удаления



Удаление элементов требует подтверждения в модальном окне. Выбранные элементы будут удалены только после явного подтверждения операции.

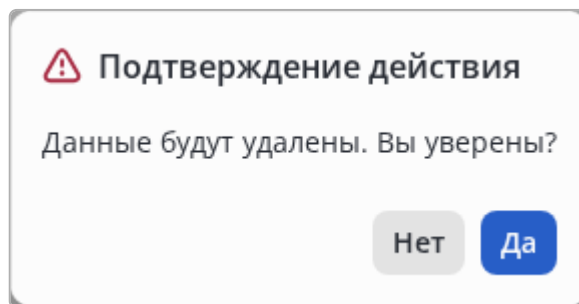


Рисунок 132. Диалоговое окно подтверждения действия



Ограничения:

- нельзя выбрать и удалить несколько групп;
- нельзя удалить системные группы "All Device Types" и "All Locations";
- нельзя удалить группу содержащую подгруппы;
- нельзя удалить группу, которая назначена сетевому устройству.

Просмотр устройств в группе

Просмотр устройств в группе возможен двумя способами:

- просмотр устройств в группе и ее подгруппах через выбор группы и нажатие на  ;
- просмотр устройств только этой группы через нажатие на счетчик напротив группы в колонке "Устройства".

В обоих случаях в правой части экрана будет открыта боковая панель с таблицей устройств в группе.

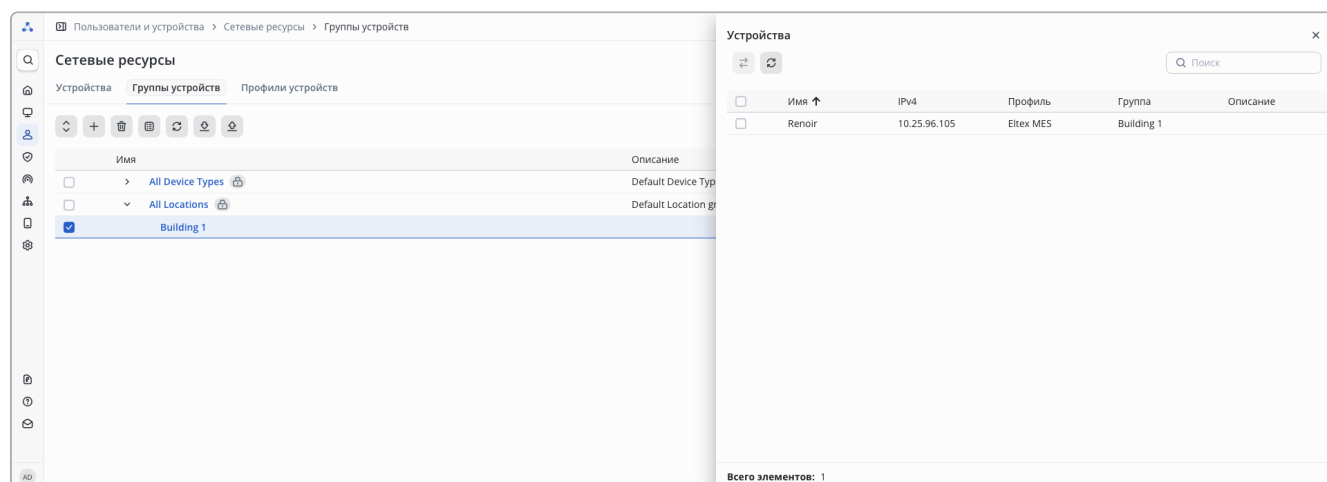


Рисунок 133. Панель просмотра устройств в группе

Таблица содержит колонки:

- **Имя** — имя устройства;
- **IPv4** — IPv4-адрес устройства;
- **Профиль** — профиль устройства;

Группа — подгруппа устройства в рамках данной корневой группы. Не отображается, если панель открыта при нажатии на счетчик устройств.

- **Описание** — произвольное описание устройства.

Сортировка доступна по колонкам "Имя" и "IPv4". По умолчанию сортировка выполняется в прямом (алфавитном) порядке по колонке "Имя".

-  — Переместить устройства в другую группу (неактивно, пока не выбран хоть один элемент).
-  — Обновить данные таблицы.
-  **Поиск** — Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
- ☐ — Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий.
-  — Изменить текущий порядок сортировки.

Перемещение устройства в другую группу

Для перемещения устройств в другую группу в окне со списком устройств отметьте чекбоксом слева те устройства, которые необходимо переместить. После нажатия на кнопку перемещения устройства  откроется окно с выбором группы для перемещения в рамках этой же корневой группы.

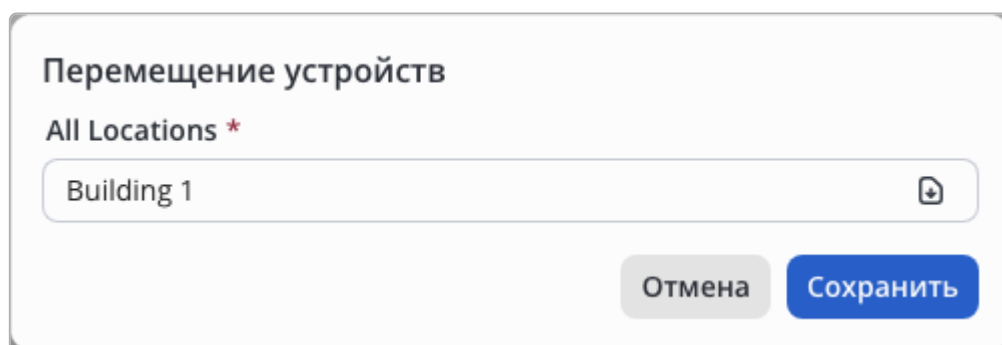


Рисунок 134. Панель перемещения устройств в группу

Группа выбирается из списка, открывающегося по нажатию на .

Импорт

NAICE поддерживает импорт данных из CSV-файлов.

Предварительная подготовка перед импортом

1. Создайте или проверьте наличие необходимых связанных записей (например, профиль устройства).
2. Ознакомьтесь с требованиями к CSV-файлу:
 - Файл должен быть в кодировке UTF-8;
 - Разделитель полей: запятая (,)
 - Разделитель строк/текста: двойная кавычка (")

Заголовки и значения должны быть взяты в двойные кавычки (")

- Максимальный размер файла 2МБ.

3. Проверьте содержимое файла на наличие лишних кавычек перед импортом;

4. Проверьте то что значения, содержащие двойную кавычку (") или слэш (/) правильно экранированы.

- Значения, содержащие двойную кавычку (") экранируются с помощью \
- Значения, содержащие слэш (/) экранируются с помощью \

Правильное написание значений (с экранированием помощью \) на примере содержания файла для импорта набора команд TACACS:

"name:Required"	"description"	"permit_unmatch ed(true/false)"	"commands(Grant/command/argume nts/enabled;...)"
"command_set"	"\"Test command set\""	"false"	"PERMIT/\"show/vlan 1 2 \"/true"

Некорректное написание значений (без экранирования) на примере содержания файла для импорта набора команд TACACS:

"name:Required"	"description"	"permit_unmatch ed(true/false)"	"commands(Grant/command/argume nts/enabled;...)"
"command_set"	"Test command set"	"false"	"PERMIT/show/vlan 1 2 /true"



Игнорирование экранирования приведёт к некорректному распознаванию данных.

Порядок выполнения импорта

Для импорта данных из CSV-файла нажмите  на панели действий, расположенной над таблицей. После чего откроется окно:

Импорт

При импорте дублирующиеся данные не будут перезаписаны или отредактированы - система пропустит их. Если вы хотите изменить старые данные, удалите их из системы вручную перед импортом.

Внимательно ознакомьтесь с [Документацией](#) , чтобы импорт прошёл без ошибок.

Выберите файл*
Максимальный размер файла 2МБ

 **Загрузите** или перетащите сюда

Поле обязательно для заполнения

Источник данных *

NAICE

☐ Игнорировать существующие данные 

☐ Остановить импорт при первой ошибке

Отмена

Импорт

Рисунок 135. Окно Импорта

Импорт данных из CSV-файла выполняется в несколько шагов:

1. Выберите необходимый CSV-файл, перетащив его в поле загрузки или выбрав через проводник, нажав кнопку "**Загрузите**";



Измененный CSV-файл нужно загрузить повторно, чтобы применить правки.

2. Выберите источник данных, если он заранее не определён;
3. При необходимости активируйте флаги импорта:

Игнорировать существующие данные

- Если переключатель включен — дубликаты записей считаются предупреждением.
- Если переключатель выключен — дубликаты расцениваются как ошибка.

Остановить импорт при первой ошибке

- Если переключатель включен — импорт останавливается при первой же ошибке. Будут импортированы только записи, которые были успешно обработаны до её возникновения.

Если переключатель выключен — ошибочные строки пропускаются, импорт продолжается до конца. Будут импортированы только валидные записи.

4. Для того чтобы импорт начался, нажмите кнопку **"Импорт"**.



При импорте дублирующиеся данные перезаписаны или отредактированы не будут - система пропустит их. Если вы хотите изменить старые данные, удалите их из системы вручную перед импортом.

Просмотр отчета по импорту

Сразу после завершения обработки файла откроется окно отчёта по импорту.

Если все записи в файле были обработаны корректно, вы увидите окно:

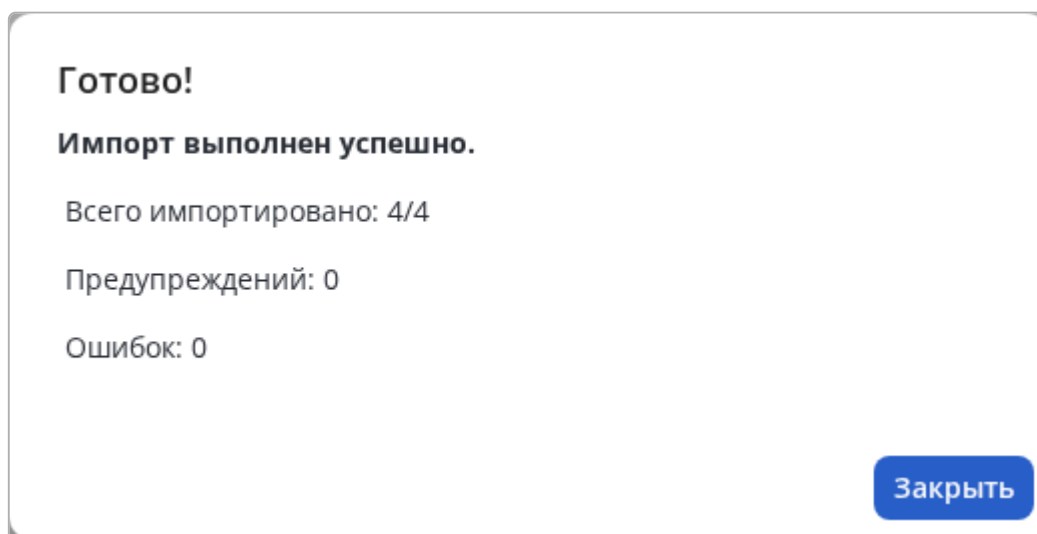


Рисунок 136. Отчет импорта (все записи обработаны корректно)

Блок с общей информацией содержит:

- **Всего импортировано** - Счётчик того, сколько записей было импортировано из общего импортируемого количества строк;
- **Предупреждений** - Количество возникших предупреждений;
- **Ошибок** - Количество возникших ошибок.

Если не все записи были обработаны корректно, вы увидите окно:

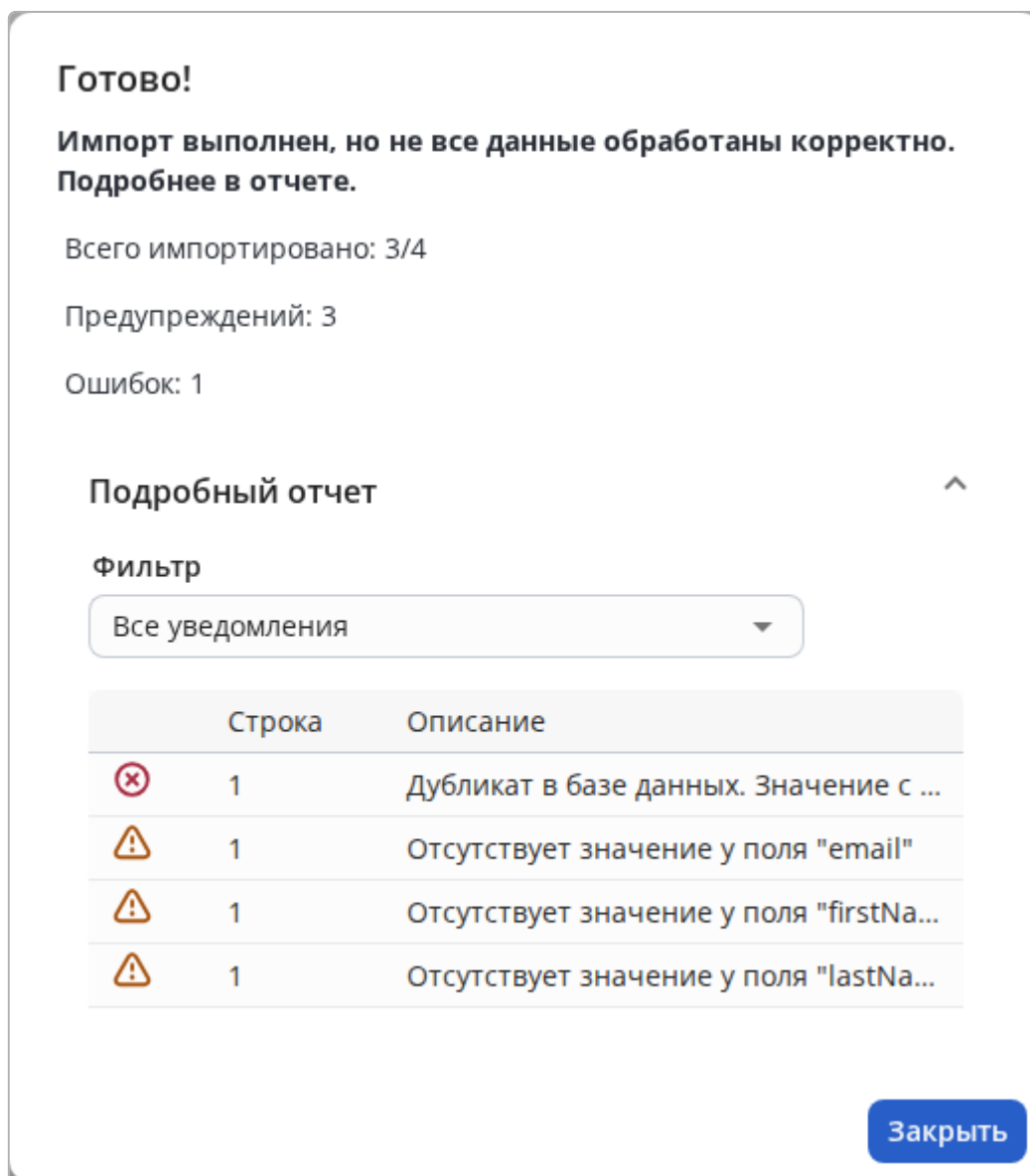


Рисунок 137. Отчет импорта (записи обработаны с ошибками/предупреждениями)

Подробный отчет содержит следующую информацию:

- **Фильтр** - Выпадающий список, в котором можно выбрать отображаемые уведомления (Все уведомления , Только ошибки или Только предупреждения)

Таблица уведомлений содержит колонки:

- **Строка** - Номер строки в CSV-файле, где обнаружена ошибка или предупреждение;
- **Описание** - Детальное текстовое объяснение ошибки или предупреждения.



Для просмотра полного текста описания наведите курсор мыши на соответствующую строку - во всплывающей подсказке отобразится полный текст сообщения об ошибке или предупреждении.

Особенности импорта групп устройств



Для групп устройств в качестве источника данных поддержан только **NAICE**

В таблице ниже приведен список полей, их обязательность, описание и требования:

Поле	Описание	Требования
name:Required	Имя группы (указывается полный путь)	Обязательное поле Формат: группа#подгруппа
description	Произвольное описание группы	Максимальная длина - 200 символов



Если в системе нет промежуточной корневой/дочерней группы, она создается автоматически.

Пример корректного содержания файла:

"name:Required"	"description"
"All Device Types#Switch"	""

Получение CSV-файла шаблона описано далее в разделе "Экспорт".

Экспорт

NAICE поддерживает экспорт данных в формате CSV. Значения и заголовки обрамляются **двойными кавычками**, разделитель полей: **запятая (,)**.

Процедура экспорта

Доступны два режима экспорта данных:

- **Экспорт всего** - Выгрузка всех записей текущего раздела. Системные записи исключаются из экспорта;
- **Экспорт выбранного** - Выгрузка только отмеченных чекбоксом записей.

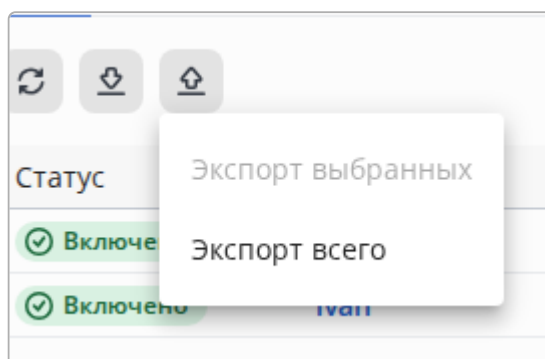


Рисунок 138. Окно выбора режима экспорта



Значения содержащие двойную кавычку (") или слэш (/) будут экранированы с помощью \".

Экспорт всех записей

На панели действий над таблицей нажмите  и выберите режим "Экспорт всего". В открывшемся окне подтвердите действие кнопкой "Экспорт":

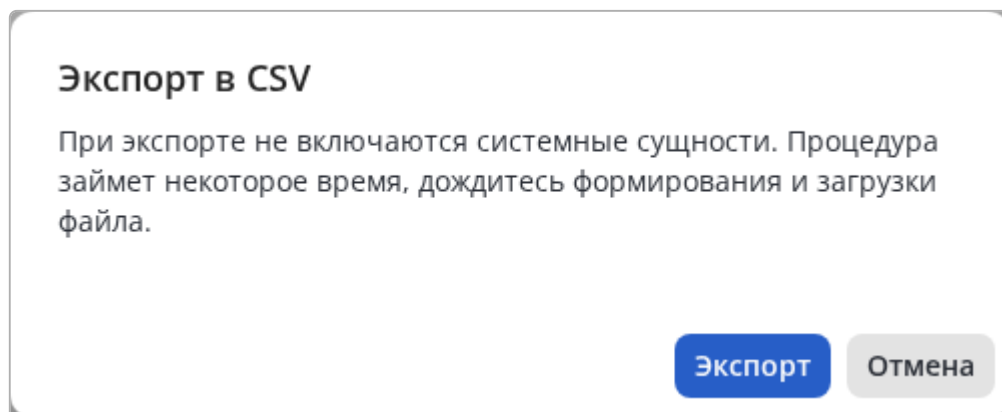


Рисунок 139. Экспорт всего

После нажатия кнопки "Экспорт" на устройство выгрузится файл, содержащий все записи из текущего раздела.

Экспорт выбранных записей

На панели действий над таблицей нажмите  и выберите режим "Экспорт выбранных". В открывшемся окне подтвердите действие кнопкой "Экспорт":

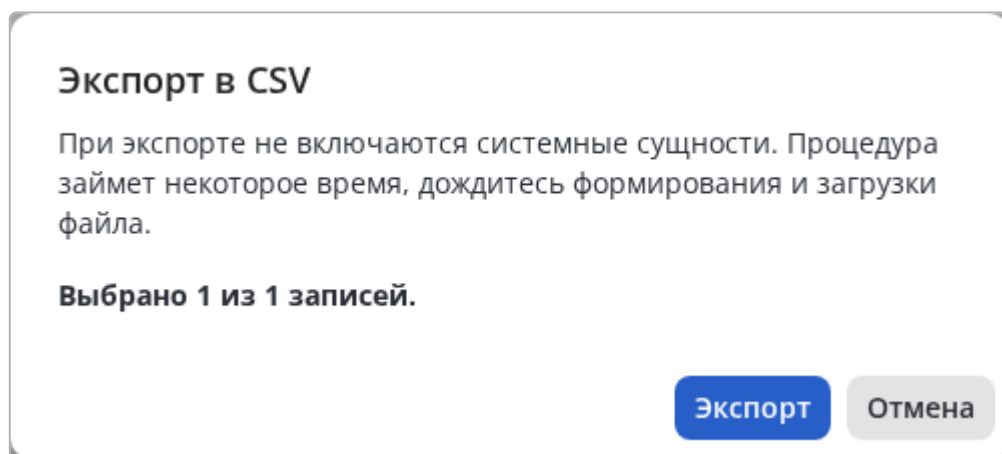


Рисунок 140. Экспорт выбранных

После нажатия кнопки "Экспорт" на устройство выгрузится файл, содержащий только отмеченные записи.



При **открытии** CSV-файлов в качестве разделителя полей **всегда** используйте **запятую (,)**, разделителем строк/текста могут быть **двойные кавычки (")** или **пустое значение**.

При **сохранении** CSV-файлов в качестве разделителя полей **всегда** используйте **запятую (,)**, а разделитель строк/текста - **пустое значение**.



Если при открытии файла использовался разделитель строк — двойная кавычка (") , то значения, содержащие символы двойной кавычки (") или слэша (/) , экранированные как \ , могут при сохранении получить лишнюю кавычку (") после (\) . Проверьте файл в текстовом редакторе и удалите лишние кавычки, если они появились.

Шаблон

Если в таблице отсутствуют записи (либо присутствуют только системные), при выборе режима **"Экспорт всего"** будет сформирован CSV-файл, содержащий исключительно заголовки столбцов. Данный файл может быть использован в качестве **шаблона** для подготовки данных перед импортом.

Особенности экспорта групп устройств



Имя группы будет прописано в формате полного пути через разделитель - # .

Структура CSV-файла для групп устройств описана в разделе ["Особенности импорта групп устройств"](#).

Профили устройств



Некоторые функции, описанные на данной странице, доступны только при наличии расширенной лицензии. Такие функции помечены специальными метками в виде цветных значков рядом с наименованием.

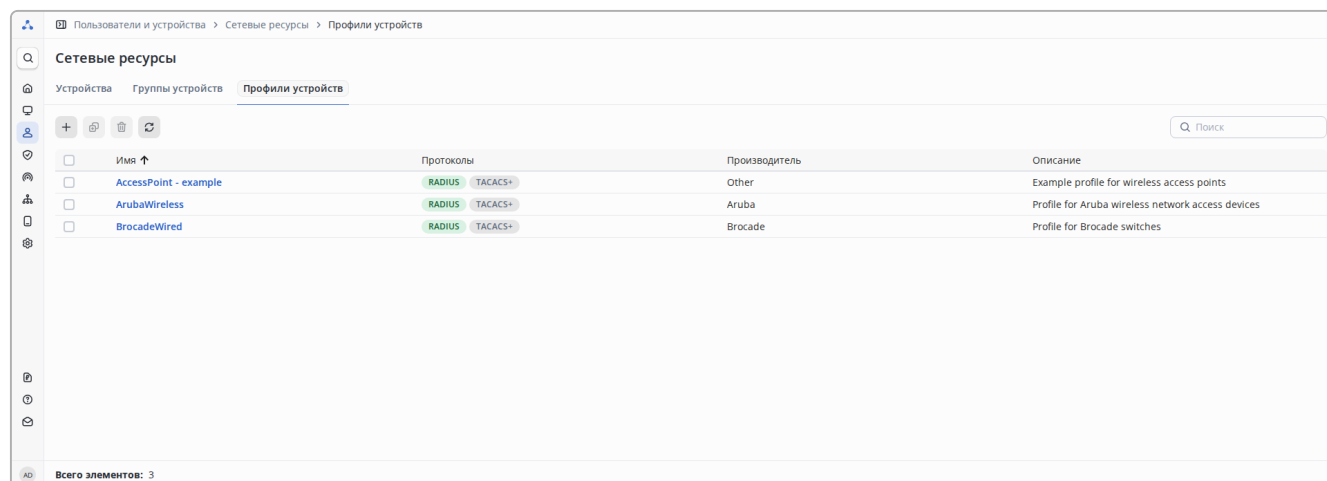
Описание

Профили устройств предназначены для обобщения настроек похожих [сетевых устройств](#). Как правило похожие настройки имеют устройства одного производителя и/или одного семейства.

Основными настройками в профилях устройств являются:

- *условия определения типа подключения* - при получении каких RADIUS-атрибутов подключение пользователя будет определено, например, как проводное MAB или беспроводной 802.1x. На основании типа подключения можно настраивать политики доступа. Например, для пользователя, подключающегося проводным способом, можно выдавать один VLAN, а для того же пользователя, подключающегося беспроводным способом - другой.
- *настройка MAB* - возможность авторизации подключенных к этому устройству клиентов по MAB и настройка особенностей этого подключения.
- *разрешения* - настройка возможности и RADIUS-атрибутов для выдачи VLAN и/или ACL для подключенных к этому устройству клиентов.
- *настройки RADIUS CoA* - актуально при поддержке устройством RADIUS CoA.
- **ADVANCED** *настройки перенаправления на портал*.

Просмотр списка профилей устройств



Сетевые ресурсы			
Устройства Группы устройств Профили устройств			
☐	Имя ↑	Протоколы	Описание
☐	AccessPoint - example	RADIUS TACACS+	Example profile for wireless access points
☐	ArubaWireless	RADIUS TACACS+	Profile for Aruba wireless network access devices
☐	BrocadeWired	RADIUS TACACS+	Profile for Brocade switches

Рисунок 141. Таблица с перечнем профилей сетевых устройств

На данной странице содержится таблица со списком профилей устройств.

Таблица содержит колонки:

- Имя - наименование профиля;
- Протоколы — показывает статус настройки протоколов RADIUS и TACACS.
 - Серый статус - протокол в профиле выключен;
 - Зеленый статус - протокол в профиле включен.
- Производитель - наименование вендора устройств;
- Описание - произвольное описание профиля.



При наведении на строку с интересующим профилем появляется подсказка ⓘ при нажатии на которую можно посмотреть настройки для данного профиля.

Доступна сортировка по колонкам Имя , Производитель .

Элементы управления:

- + — Добавить новый элемент.
-  — Дублировать выбранный чекбоксом элемент. Становится активным, если выбран только один элемент в списке.
-  — Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
-  — Обновить данные таблицы.
- ☐ — Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).
- ↑ — Изменить текущий порядок сортировки.
-

Поиск — Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.

Добавление профиля устройства

Страница добавления сетевого профиля устройств

Для добавления профиля устройства нажмите **+**.

Рисунок 142. Страница добавления профиля устройства. Таб Аутентификация/Авторизация

В открывшемся окне необходимо заполнить следующие параметры:

- **Имя *** - наименование профиля устройства. Максимальная длина - 100 символов.
- **Производитель *** - наименование производителя сетевого устройства. Максимальная длина - 100 символов.
- **Описание** - произвольное описание. Максимальная длина - 200 символов.
- **Поддерживаемые протоколы** - протоколы, которые используются для взаимодействия с сетевым устройством. По умолчанию включены протоколы RADIUS и TACACS+ (последний доступен только при наличии опции TACACS+ в лицензии).

Аутентификация/Авторизация - блок настройки, отвечающий за определение типа подключения клиентского устройства.

- Wired 802.1x / Wireless 802.1x / Wired MAB / Wireless MAB будет обнаружен при следующих условиях - включение настройки определения одного из типов подключения.



ADVANCED Для работы портальной авторизации необходимо включение определения типа подключения Wireless MAB!

- **Атрибут** - RADIUS-атрибут, используемый в условии.
- **=** означает что условие будет выполнено при равенстве атрибута указанному значению. При клике на иконку можно сменить условие на неравенство.
- **Значение атрибута** - значение RADIUS-атрибута, используемое в условии.
- - удалить условие.
- **+** - добавить условие.



При включении определения какого-либо типа подключения атрибуты заполнятся стандартными значениями. Их можно отредактировать или оставить без изменений.



Если используется несколько RADIUS-атрибутов в условии - они объединяются логическим "И". Если тип подключения не включен или не был определен - пользователь продолжает авторизацию, его тип подключения считается неопределенным.



Политики доступа можно настроить в зависимости от типа подключения. Например, пользователю может быть назначена одна сеть VLAN, если он подключается по проводному каналу, и другая сеть VLAN - если он подключается по беспроводному каналу.

MAB - блок настройки, отвечающий за разрешение и конфигурацию особенностей MAB авторизации.



ADVANCED Для работы портальной авторизации необходимо включение и настройка MAB!

- **Настроить MAB** - включение разрешения MAB авторизации на устройстве.
- **PAP / EAP_MD5** - включение разрешения MAB авторизации по указанным протоколам.
- **Проверять совпадение Calling-Station-Id и MAC адреса** - включение разрешения авторизации только тех устройств, в запросе которых RADIUS-атрибут Calling-Station-Id совпадает с MAC адресом в имени пользователя. Требуется, чтобы указанный атрибут присутствовал в RADIUS запросе от устройства.
- **Условие пароля** - условие, при котором пароль будет считаться корректным. По умолчанию задано условие равенства пароля логину пользователя.

Пользователи и устройства > Сетевые ресурсы > Профили устройств > Добавление

← **Добавление**

Имя *
Введите имя

Производитель *
Введите производителя

Описание
Введите описание
0 / 200

Поддерживаемые протоколы
☒ RADIUS
☒ TACACS+

Аутентификация/Авторизация **Разрешения** Настройки RADIUS CoA Настройки перенаправления на портал

☐ Настроить VLAN
☐ Настроить ACL

Имя *
Выберите атрибут

Отмена **Добавить**

Рисунок 143. Страница добавления профиля устройства. Таб Разрешения

Разрешения - блок настройки, определяющий возможность упрощенной выдачи пользователю дополнительных атрибутов после авторизации.

- **Настроить VLAN** - включить возможность упрощенной выдачи VLAN в RADIUS-атрибутах.
 - **Атрибуты по умолчанию** - использовать стандартные IETF RADIUS-атрибуты для выдачи VLAN.
 - **Уникальные атрибуты** - использовать vendor-specific RADIUS-атрибуты для выдачи VLAN.
 - **ID *** - vendor-specific RADIUS-атрибут для выдачи VLAN в формате числа от 1-4094.
 - **Имя** - vendor-specific RADIUS-атрибут для выдачи VLAN в формате строки.
- **Настроить ACL** - включить возможность упрощенной выдачи имени статической ACL в RADIUS-атрибутах.
 - **Имя *** - vendor-specific RADIUS-атрибут для выдачи имени ACL в формате строки.

Пользователи и устройства > Сетевые ресурсы > Профили устройств > Добавление

← **Добавление**

Имя *
Введите имя

Производитель *
Введите производителя

Описание
Введите описание
0 / 200

Поддерживаемые протоколы
☒ RADIUS
☒ TACACS+

Аутентификация/Авторизация Разрешения **Настройки RADIUS CoA** Настройки перенаправления на портал

☐ Устройство поддерживает RADIUS CoA

Порт RADIUS CoA *
Введите порт

Интервал ожидания, с *
Введите интервал

Количество повторных попыток *
Введите количество

☐ Отправка атрибута Message-Authenticator ⓘ

Реаутентификация

Атрибут	Значение атрибута
Выберите атрибут ⓘ	= Укажите значения атрибута +

Отмена **Добавить**

Рисунок 144. Страница добавления профиля устройства. Таб Настройка RADIUS CoA

Настройка RADIUS CoA - блок настройки, позволяющий настроить RADIUS CoA для динамического управления сессиями пользователей через RADIUS-сервер.

- **Устройство поддерживает RADIUS CoA** - включает настройку RADIUS CoA.
 - **Порт RADIUS CoA *** - Порт для отправки RADIUS CoA. Должен совпадать с портом, настроенным на сетевом устройстве (значение, устанавливаемое производителем может быть 1700 или 3799). Если настройка CoA включена, значение по умолчанию в NAICE будет 1700.
 - **Интервал ожидания, с *** - Количество секунд, в течение которых ожидается ответа после отправки CoA.
 - **Количество повторных попыток *** - Количество попыток отправки запроса при отсутствии ответа.
- **Отправка атрибута Message-Authenticator** - Опция добавляет атрибут для проверки подлинности и целостности пакетов CoA и Disconnect.



Значение атрибута Message-Authenticator формируется на основе секретного ключа RADIUS, указанного в настройках устройства. Получатель пакета проверяет данное значение, используя известный ему секретный ключ. В случае несовпадения значений пакет отбрасывается, предотвращая обработку поддельных пакетов.

- **Реаутентификация** - настройки, отвечающие за повторную проверку учетных данных пользователя без разрыва соединения.
 - **Атрибут** - RADIUS-атрибут, используемый в условии.
 - **Значение атрибута** - значение RADIUS-атрибута, используемое в условии.

Рисунок 145. Страница добавления профиля устройства. Таб Настройки перенаправления на портал

ADVANCED

Настройки перенаправления на портал - блок настроек, отвечающий за автоматическое перенаправление пользователей на веб-портал.



Для работы порталной авторизации необходимо включение определения типа подключения Wireless MAB!

- **Настроить перенаправление** - включает настройку параметров ссылки перенаправления на веб-портал.
 - **URL** - параметры для передачи в RADIUS-пакете ссылки перенаправления на страницу авторизации гостевого портала.
 - **Атрибут *** - RADIUS-атрибут, используемый в условии.
 - **Значение атрибута *** - значение RADIUS-атрибута, используемое в условии.
 - **ACL** - параметры для передачи в RADIUS-пакете ACL, которая будет назначена при перенаправлении на портал.
 - **Атрибут *** - RADIUS-атрибут, используемый в условии.
 - **Значение атрибута *** - значение RADIUS-атрибута, используемое в условии.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

После ввода необходимых данных нажмите кнопку **Добавить**.

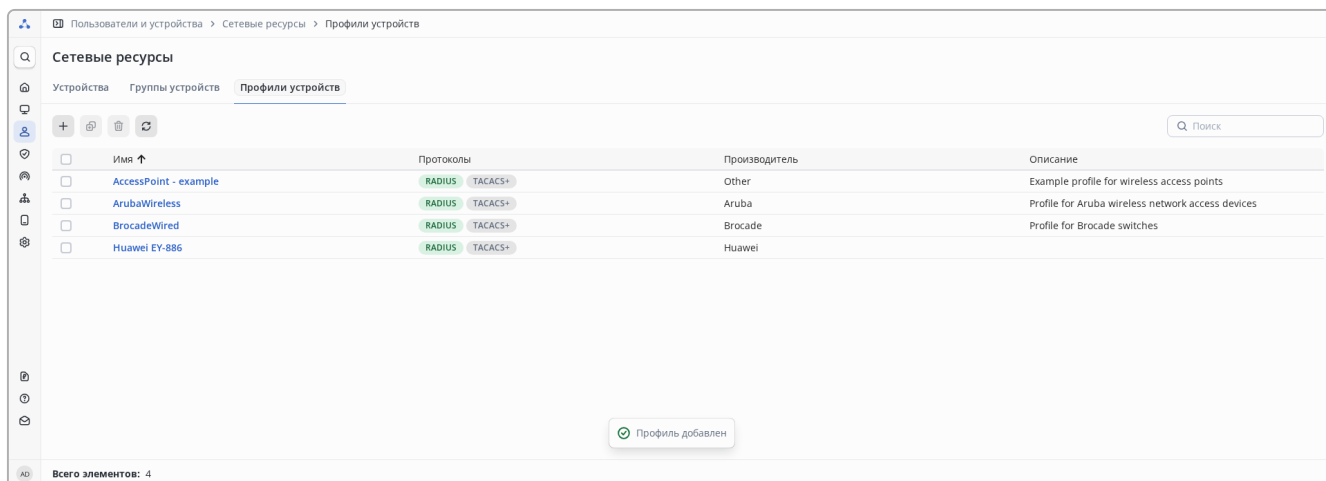


Рисунок 146. Страница успешного создания профиля устройства

Редактирование профиля устройства

Для редактирования профиля устройства необходимо на странице со списком нажать на его имя, после чего откроется окно редактирования, аналогичное окну добавления.

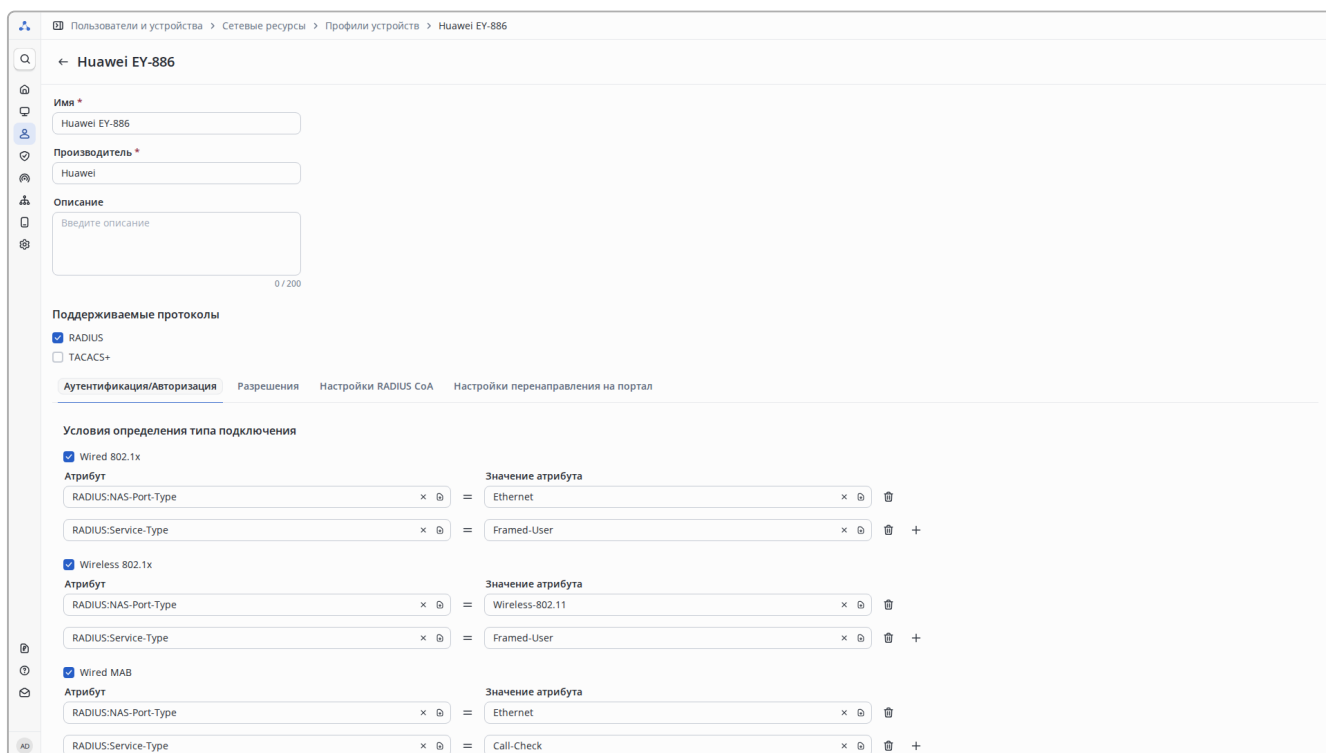


Рисунок 147. Страница редактирования профиля сетевых устройств

После редактирования необходимо нажать на кнопку **"Сохранить"**. Кнопка скрыта, пока не будет внесено хотя бы одно изменение.

Кнопка **"Отмена"** осуществляет сброс внесенных изменений до исходного состояния.

Удаление профиля устройства

Для удаления профиля выберите его чекбоксом и нажмите кнопку  в левой части панели над таблицей.

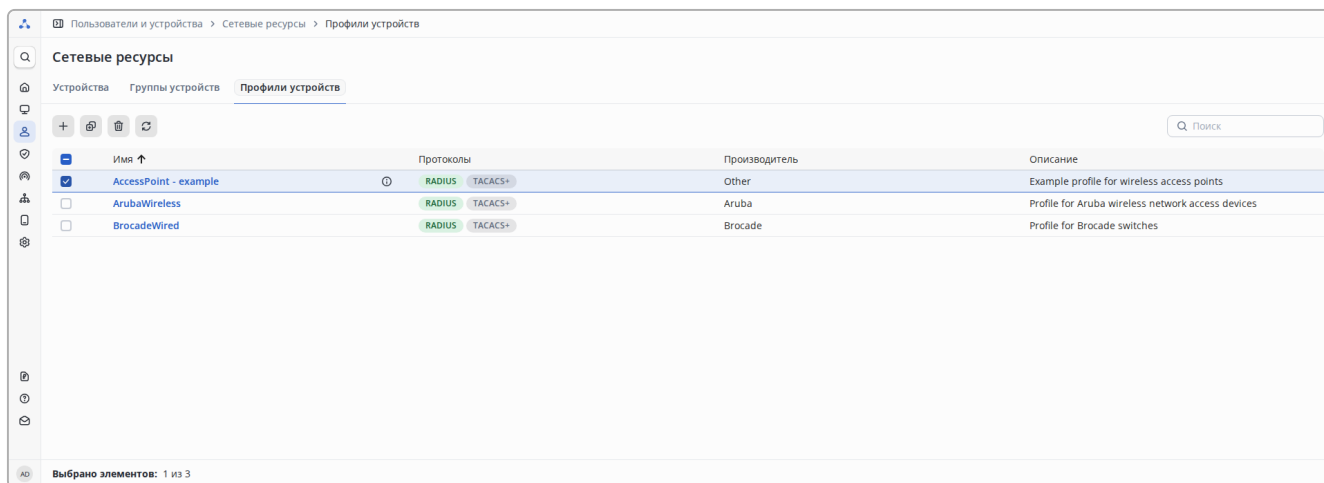


Рисунок 148. Страница с выбранным для удаления профилем устройств



Удаление элементов требует подтверждения в модальном окне. Выбранные элементы будут удалены только после явного подтверждения операции.

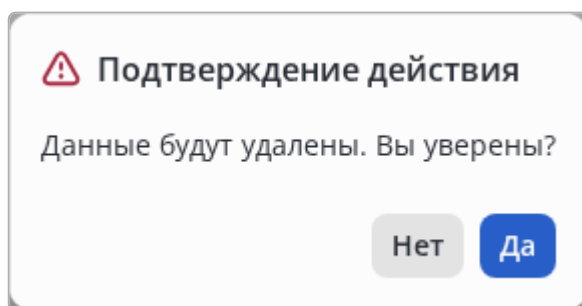


Рисунок 149. Диалоговое окно подтверждения действия

После удаления произойдет переход на страницу просмотра списка профилей устройств.

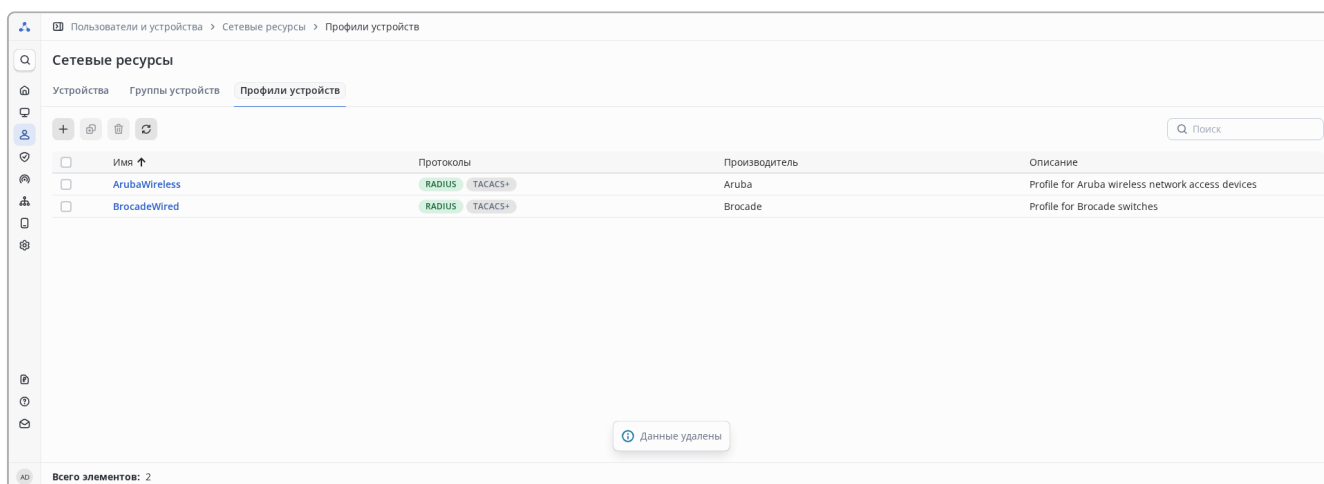


Рисунок 150. Страница просмотра списка профилей устройств после удаления



Ограничения:

- нельзя удалить профиль, который уже назначен какому-то [устройству](#).
- нельзя удалить профиль, который используется в каком-либо [профиле авторизации](#).

Управление идентификацией

Управление пользователями (суппликантами) выполняется в меню "Пользователи и устройства" → "Управление идентификацией".

В качестве источника данных, используемого для аутентификации пользователей может использоваться внутренний список клиентов (их настройка рассматривается в [Пользователи сети](#)) и подключение к внешнему источнику идентификации данных о клиентах Active Directory или LDAP. Здесь же осуществляется работа с конечными устройствами (эндпоинтами).

Меню содержит разделы:

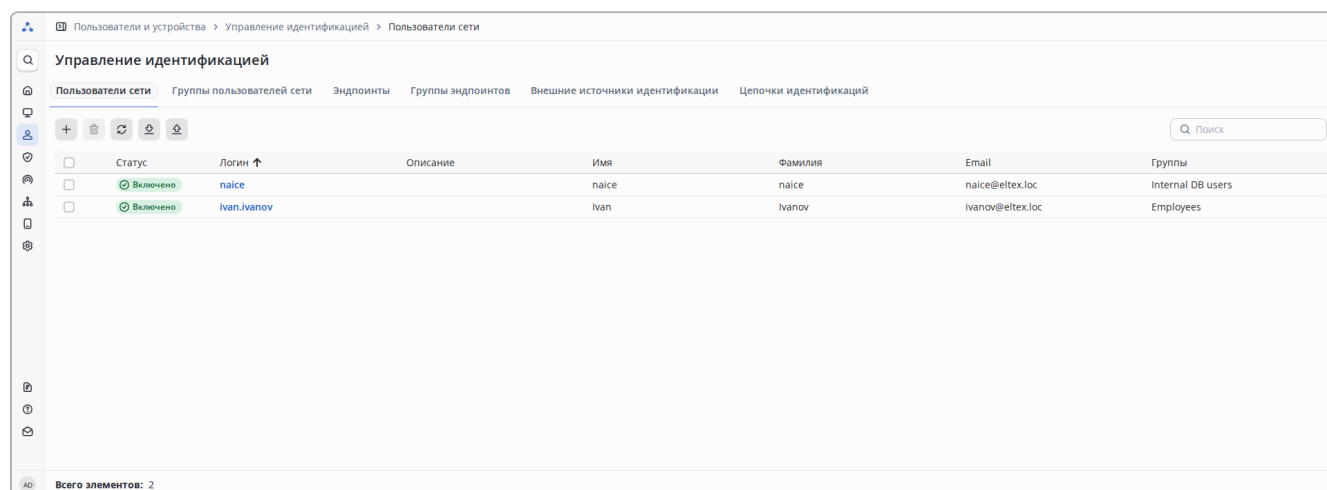
- [Пользователи сети](#) - раздел управления учетными данными пользователей, с которыми производится авторизация на устройствах.
- [Группы пользователей сети](#) - раздел настроек, позволяющий создать записи для группировки пользователей.
- [Эндпоинты](#) - раздел для работы со списком конечных устройств, которые подключаются к сетевой инфраструктуре.
- [Группы эндпоинтов](#) - раздел для работы с группами конечных устройств.
- [Внешние источники идентификации](#) - раздел управления внешними источниками идентификации.
- [Цепочки идентификаций](#) - раздел настроек, позволяющий составить списки источников учетных данных пользователей.

Пользователи сети

Описание

Раздел *Пользователи сети* предназначен для управления локальными учётными данными пользователей, с которыми производится авторизация на устройствах. Такие пользователи объединяются в источник *Internal DB*.

Просмотр пользователей сети



Управление идентификацией							
Пользователи сети							
Пользователи сети Группы пользователей сети Эндпоинты Группы эндпоинтов Внешние источники идентификации Цепочки идентификаций							
	Статус	Логин ↑	Описание	Имя	Фамилия	Email	Группы
☐	Включено	naice		naice	naice	naice@eltex.loc	Internal DB users
☐	Включено	Ivan.Ivanov		Ivan	Ivanov	Ivanov@eltex.loc	Employees

Рисунок 151. Таблица с перечнем пользователей сети на странице просмотра

На данной странице содержится таблица со списком учетных данных пользователей.

Таблица содержит колонки:

- **Статус** - статус пользователя (выключено или включено);
- **Логин** - логин пользователя (должен быть уникальным);
- **Описание** - произвольное описание пользователя;
- **Имя** - имя пользователя;
- **Фамилия** - фамилия пользователя;
- **Email** - адрес электронной почты пользователя;
- **Группы** - группы, в которых состоит пользователь.

Возможна сортировка в прямом и обратном порядке по колонкам "Статус", "Логин", "Описание", "Имя", "Фамилия", "Email" (по всем колонкам, кроме "Группы"). По умолчанию сортировка выполняется в прямом (алфавитном) порядке по полю "Логин".

Элементы управления:

-  — Добавить новый элемент.
-  — Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
-  — Обновить данные таблицы.
-  — Позволяет загрузить данные из csv-файла.
-  — Позволяет выгрузить данные в csv-файл.
- ☐ — Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).
-  — Изменить текущий порядок сортировки.
-  **Поиск** — Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.

Добавление пользователя

Для добавления пользователя нажмите  в левой части поля над таблицей.

Рисунок 152. Страница добавления пользователя

В открывшейся странице представлены следующие параметры:

- - переключатель статуса пользователя, может принимать значения "Включено" или "Выключено". Аутентификация по выключенным учетным данным запрещена.
- **Логин *** - логин пользователя. Максимальная длина логина - 100 символов.
- **Пароль *** - пароль пользователя. Минимальная длина пароля - 8 символов, максимальная - 100 символов. По нажатию на можно включить отображение вводимого пароля, по умолчанию текст скрыт. Пароль можно скопировать по клику на .
- **Имя** - имя пользователя. Максимальная длина - 100 символов.
- **Фамилия** - фамилия пользователя. Максимальная длина - 100 символов.
- **Email** - адрес электронной почты пользователя. Должно соответствовать определенному формату (например, `naice@eltex.loc`) и не превышать 100 символов.
- **Описание** - произвольное описание пользователя. Максимальная длина - 200 символов.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

Также на данной странице находится таблица **Группы пользователя**, в которые входит данный пользователь.

Элементы управления:

- **Поиск** - регистронезависимая фильтрация по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
- - добавить пользователя в группы.

 - удалить пользователя из выбранных чекбоксом групп (неактивно, пока не выбрана хоть одна группа).

-  - изменить текущий порядок сортировки.
- ☐ - чекбокс, который отвечает за выбор групп для выполнения дальнейших действий (например, удаления пользователя из группы).

По нажатию  появляется окно **Добавление пользователя в группы**, в котором необходимо выбрать группы, куда нужно добавить пользователей.

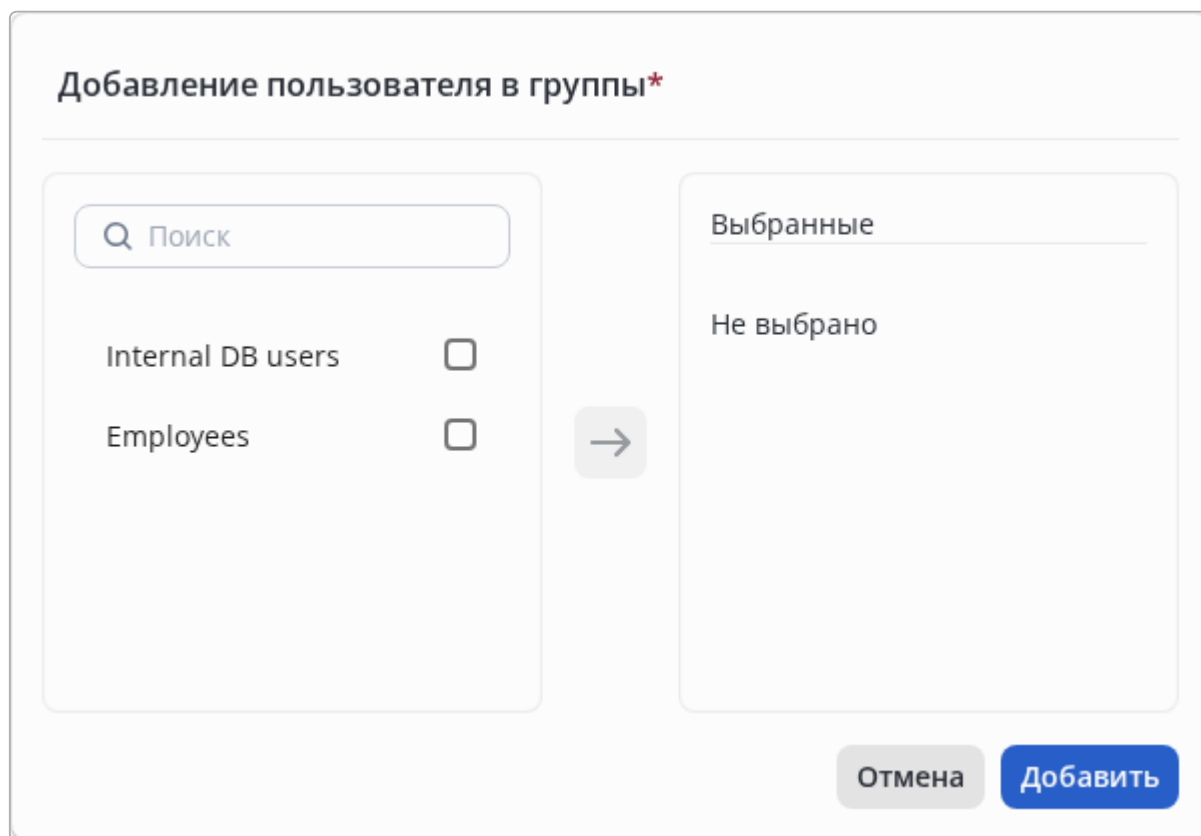


Рисунок 153. Страница добавления пользователя в группы

Элементы управления:

-  Поиск - регистронезависимый поиск среди пользовательских групп: отображаются только группы, удовлетворяющие условию фильтрации.
- ☐ - чекбокс, который отвечает за выбор групп, для назначения пользователю (отображается только для доступных групп).
-  - назначить выбранные группы пользователю.
-  - удалить группу из списка выбранных для назначения (отображается только для выбранных групп).
- **Добавить** - применить изменения (активна только если что-либо было изменено).
- **Отмена** - отменить изменения.

Для добавления пользователя в список не забудьте нажать **Добавить**. Для сброса изменений и возврата на страницу просмотра нажмите на **Отменить**.

Редактирование пользователя

Для редактирования ранее добавленного пользователя на странице просмотра нажмите на логин в таблице.

☐	Статус	Логин ↑
☐	✓ Включено	naice
☐	✓ Включено	ivan.ivanov

Рисунок 154. Гиперссылка на страницу редактирования пользователя

Откроется страница редактирования.

The screenshot shows a web interface for editing a user. The breadcrumb trail at the top is: Пользователи и устройства > Управление идентификацией > Пользователи сети > ivan.ivanov. The page title is '← ivan.ivanov'. On the left, there is a sidebar with icons for various actions. The main content area includes a toggle switch for 'Включено' (On), a 'Логин *' field with 'ivan.ivanov', a 'Сменить пароль' (Change password) toggle, and fields for 'Имя' (Ivan), 'Фамилия' (Ivanov), 'Email' (ivanov@eltext.loc), and 'Описание' (Description). Below these fields is a section for 'Группы пользователя' (User groups) with a search bar and a table showing 'Имя ↑' and 'Employees'.

Рисунок 155. Страница редактирования пользователя



Старый пароль пользователя не отображается на странице редактирования! Для изменения пароля необходимо включить переключатель **"Сменить пароль"**, после чего ввести желаемый пароль в соответствующие поля.

После редактирования нажмите на **Сохранить**. Кнопка будет неактивной пока не изменено хотя бы одно поле.

Удаление пользователя

Для удаления пользователей необходимо на странице просмотра, используя чекбокс ☐, выбрать необходимых пользователей и в левом верхнем углу над таблицей нажать на .

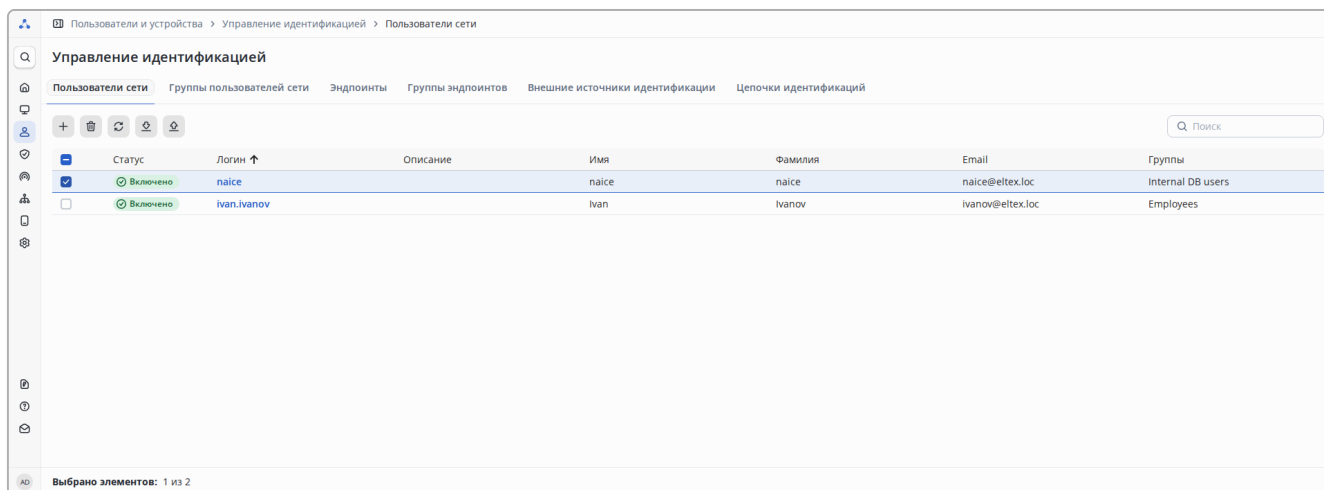


Рисунок 156. Выбор пользователей в таблице для удаления



Удаление элементов требует подтверждения в модальном окне. Выбранные элементы будут удалены только после явного подтверждения операции.

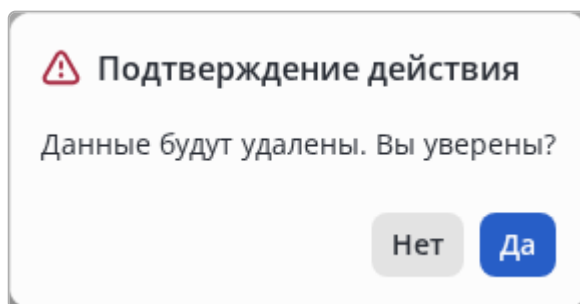


Рисунок 157. Диалоговое окно подтверждения действия

Импорт

NAICE поддерживает импорт данных из CSV-файлов.

Предварительная подготовка перед импортом

1. Создайте или проверьте наличие необходимых связанных сущностей (например, профиль устройства).
2. Ознакомьтесь с требованиями к CSV-файлу:
 - Файл должен быть в кодировке UTF-8;
 - Разделитель полей: запятая (,)
 - Разделитель строк/текста: двойная кавычка (")
 - Заголовки и значения должны быть взяты в двойные кавычки (")
 - Максимальный размер файла 2МБ.
3. Проверьте содержимое файла на наличие лишних кавычек перед импортом;
4. Проверьте то что значения, содержащие двойную кавычку (") или слэш (/) правильно экранированы.

Значения, содержащие двойную кавычку (") экранируются с помощью \

- Значения, содержащие слэш (/) экранируются с помощью \

Правильное написание значений (с экранированием при помощи \) на примере содержания файла для импорта набора команд TACACS:

"name:Required"	"description"	"permit_unmatched(true/false)"	"commands(Grant/command/arguments/enabled;...)"
"command_set"	"\"Test command set\""	"false"	"PERMIT/\"show/vlan 1 2 \"/true"

Некорректное написание значений (без экранирования) на примере содержания файла для импорта набора команд TACACS:

"name:Required"	"description"	"permit_unmatched(true/false)"	"commands(Grant/command/arguments/enabled;...)"
"command_set"	"Test command set"	"false"	"PERMIT/show/vlan 1 2 /true"



Игнорирование экранирования приведёт к некорректному распознаванию данных.

Порядок выполнения импорта

Для импорта данных из CSV-файла нажмите  на панели действий, расположенной над таблицей. После чего откроется окно:

Импорт

При импорте дублирующиеся данные не будут перезаписаны или отредактированы - система пропустит их. Если вы хотите изменить старые данные, удалите их из системы вручную перед импортом.

Внимательно ознакомьтесь с [Документацией](#) , чтобы импорт прошёл без ошибок.

Выберите файл*
Максимальный размер файла 2МБ

 **Загрузите** или перетащите сюда

Поле обязательно для заполнения

Источник данных *

NAICE

☐

Игнорировать существующие данные 

☐

Остановить импорт при первой ошибке

☐

Автоматически создать недостающие записи 

Отмена

Импорт

Рисунок 158. Окно импорта

Импорт данных из CSV-файла выполняется в несколько шагов:

1. Выберите необходимый CSV-файл, перетащив его в поле загрузки или выбрав через проводник, нажав кнопку "Загрузите";



Измененный CSV-файл нужно загрузить повторно, чтобы применить правки.

2. Выберите источник данных, если он заранее не определён;
3. При необходимости активируйте флаги импорта:

Игнорировать существующие данные

- Если переключатель включен — дубликаты записей считаются предупреждением.
- Если переключатель выключен — дубликаты расцениваются как ошибка.

Остановить импорт при первой ошибке

-

Если переключатель включен — импорт останавливается при первой же ошибке. Будут импортированы только записи, которые были успешно обработаны до её возникновения.

- Если переключатель выключен — ошибочные строки пропускаются, импорт продолжается до конца. Будут импортированы только валидные записи.

Автоматически создать недостающие записи

- Если переключатель включен — при выполнении импорта недостающие записи будут заполнены автоматически. Перечень автозаполняемых записей можно узнать при наведении на подсказку справа от переключателя.
- Если переключатель выключен — все требуемые поля необходимо заполнить вручную.

4. Для того чтобы импорт начался, нажмите кнопку **"Импорт"**.



При импорте дублирующиеся данные перезаписаны или отредактированы не будут - система пропустит их. Если вы хотите изменить старые данные, удалите их из системы вручную перед импортом.

Просмотр отчета по импорту

Сразу после завершения обработки файла откроется окно отчёта по импорту.

Если все записи в файле были обработаны корректно, вы увидите окно:

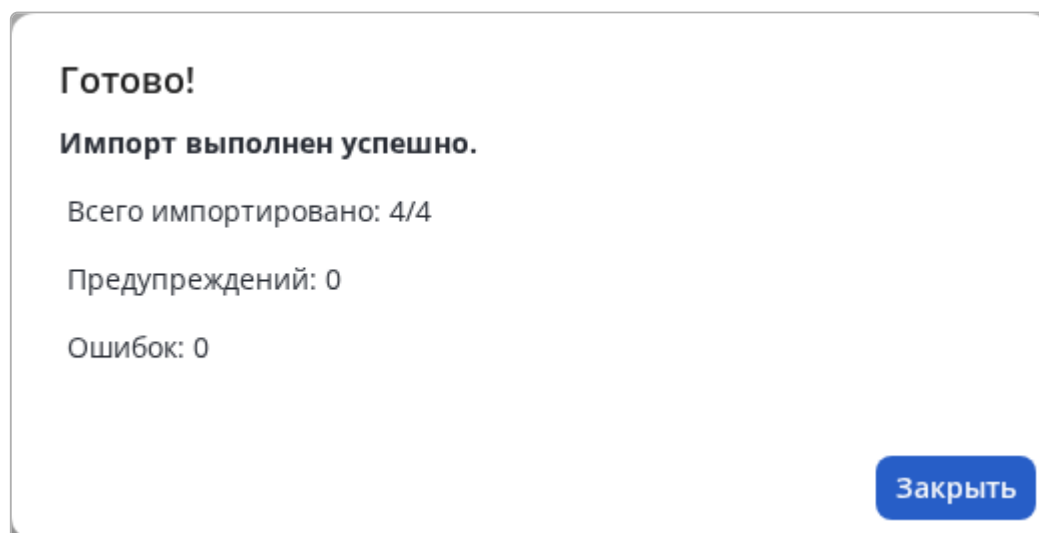


Рисунок 159. Отчет импорта (все записи обработаны корректно)

Блок с общей информацией содержит:

- **Всего импортировано** - Счётчик того, сколько записей было импортировано из общего импортируемого количества строк;
- **Предупреждений** - Количество возникших предупреждений;
- **Ошибок** - Количество возникших ошибок.

Если не все записи были обработаны корректно, вы увидите окно:

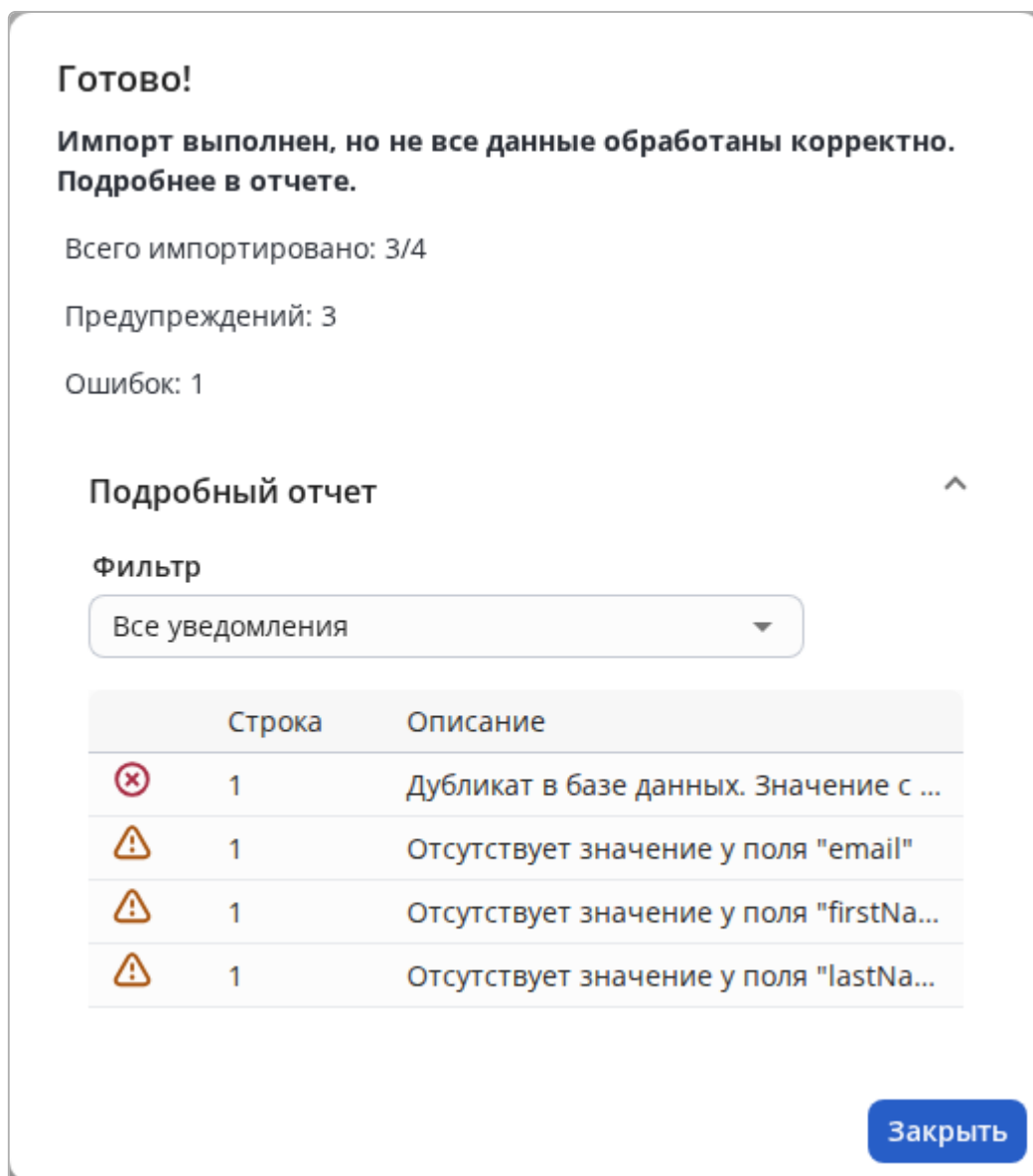


Рисунок 160. Отчет импорта (записи обработаны с ошибками/предупреждениями)

Подробный отчет содержит следующую информацию:

- **Фильтр** - Выпадающий список, в котором можно выбрать отображаемые уведомления (Все уведомления, Только ошибки или Только предупреждения)

Таблица уведомлений содержит колонки:

- **Строка** - Номер строки в CSV-файле, где обнаружена ошибка или предупреждение;
- **Описание** - Детальное текстовое объяснение ошибки или предупреждения.



Для просмотра полного текста описания наведите курсор мыши на соответствующую строку - во всплывающей подсказке отобразится полный текст сообщения об ошибке или предупреждении.

Особенности импорта пользователей



Для импорта пользователей в качестве источника данных поддержан только NAICE

В таблице ниже приведен список полей, их обязательность, описание и требования:

Поле	Описание	Требования
login:Required	Логин пользователя	Обязательное поле Максимальная длина - 100 символов Должен быть уникальным Нельзя использовать пробелы
password:Required	Пароль пользователя. Может быть импортирован как в захешированом, так и в открытом виде	Обязательное поле Длина: 8-100 символов Нельзя использовать пробелы Нельзя использовать символ №
isEncrypted:Required	Флаг хэширования пароля. Показывает в каком виде передается пароль	Обязательное поле Возможные значения: - true - передаваемый пароль захеширован - false - пароль передается в открытом виде и будет захеширован во время импорта
enabled:Required	Возможность авторизации	Обязательное поле Возможные значения: - true - статус "Включено" - false - статус "Выключено"
firstName	Имя пользователя	Максимальная длина - 100 символов
lastName	Фамилия пользователя	Максимальная длина - 100 символов
email	Адрес электронной почты	Максимальная длина - 200 символов Формат: admin123@gmail.com Недопустимые символы: • кириллические буквы (а-я) (А-Я) • пробел • двойные кавычки " • символ номера № • точка с запятой ; • двоеточие : • запятая , • круглые скобки () • квадратные скобки [] • знаки больше/меньше < > • обратный слеш \
description	Произвольное описание	Максимальная длина - 200 символов
groups	Группы пользователей сети	Группы должны существовать в системе Разделитель между группами: ;

Пример корректного содержания файла:

"login:Required"	"password:Required"	"isEncrypted:Required"	"enabled:Required"	"firstName"	"lastName"	"email"	"description"	"groups"
"user_1"	"password"	"false"	"true"	"Иван"	"Иванов"	"ivan@t est.ru"	""	"Internal DB;Users"

Получение CSV-файла шаблона описано далее в разделе "Экспорт".

Экспорт

NAICE поддерживает экспорт данных в формате CSV. Значения и заголовки обрамляются двойными кавычками, разделитель полей: запятая (,).

Процедура экспорта

Доступны два режима экспорта данных:

- **Экспорт всего** - Выгрузка всех записей текущего раздела. Системные записи исключаются из экспорта;
- **Экспорт выбранного** - Выгрузка только отмеченных чекбоксом записей.

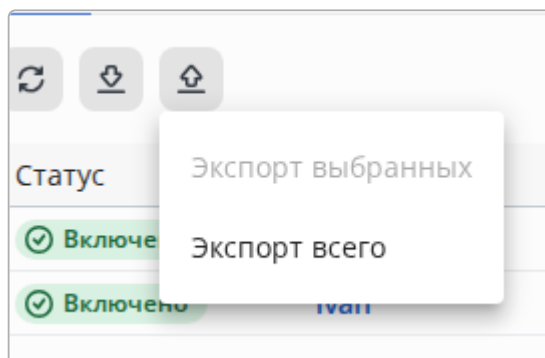


Рисунок 161. Окно выбора режима экспорта



Значения содержащие двойную кавычку (") или слэш (/) будут экранированы с помощью \".

Экспорт всех записей

На панели действий над таблицей нажмите  и выберите режим "Экспорт всего". В открывшемся окне подтвердите действие кнопкой "Экспорт":

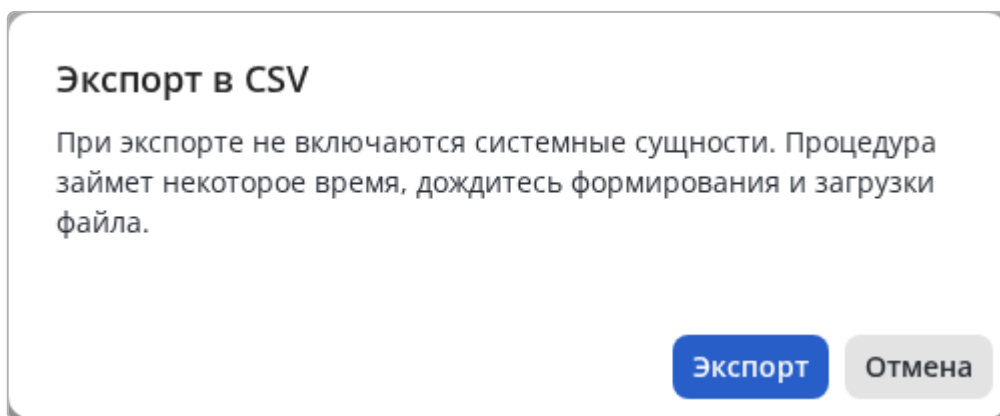


Рисунок 162. Экспорт всего

После нажатия кнопки **"Экспорт"** на устройство выгрузится файл, содержащий все записи из текущего раздела.

Экспорт выбранных записей

На панели действий над таблицей нажмите  и выберите режим **"Экспорт выбранных"**. В открывшемся окне подтвердите действие кнопкой **"Экспорт"**:

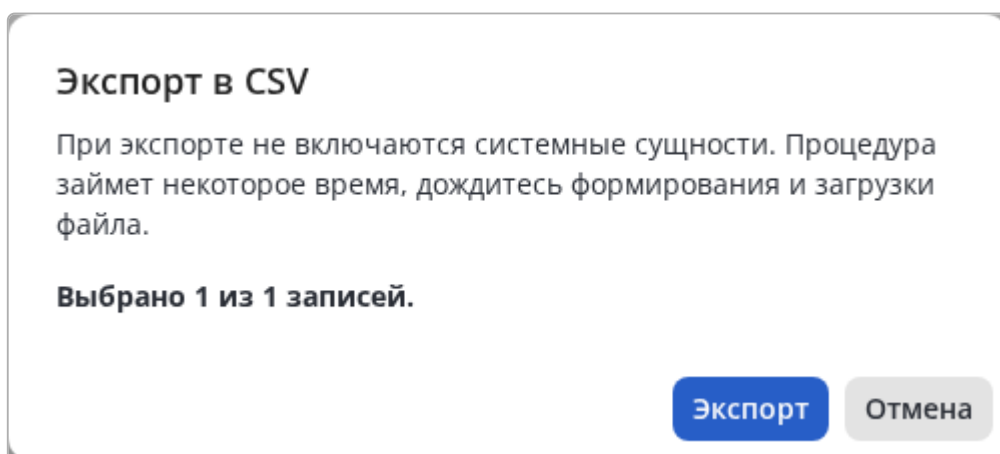


Рисунок 163. Экспорт выбранных

После нажатия кнопки **"Экспорт"** на устройство выгрузится файл, содержащий только отмеченные записи.



При **открытии** CSV-файлов в качестве разделителя полей **всегда** используйте **запятую (,)**, разделителем строк/текста могут быть **двойные кавычки (")** или **пустое значение**.

При **сохранении** CSV-файлов в качестве разделителя полей **всегда** используйте **запятую (,)**, а разделитель строк/текста - **пустое значение**.



Если при открытии файла использовался разделитель строк — двойная кавычка (**"**), то значения, содержащие символы двойной кавычки (**"**) или слэша (**/**), экранированные как ****, могут при сохранении получить лишнюю кавычку (**"**) после (****). Проверьте файл в текстовом редакторе и удалите лишние кавычки, если они появились.

Шаблон

Если в таблице отсутствуют записи (либо присутствуют только системные), при выборе режима **"Экспорт всего"** будет сформирован CSV-файл, содержащий исключительно заголовки столбцов. Данный файл может быть использован в качестве **шаблона** для подготовки данных перед импортом.

Особенности экспорта пользователей



Пароли пользователей будут выгружены из базы данных в зашифрованном с помощью ntHash виде.

Структура CSV-файла для пользователей описана в разделе ["Особенности импорта пользователей"](#).

Группы пользователей сети

Описание

Существует возможность объединять [пользователей сети](#) в *группы* и использовать в дальнейшем признак принадлежности пользователя к группе при настройке [Политики RADIUS](#) или [Политики TACACS+](#).

Раздел "Группы пользователей сети" отвечает за создание, редактирование, удаление и просмотр данных групп.

Просмотр групп пользователей сети

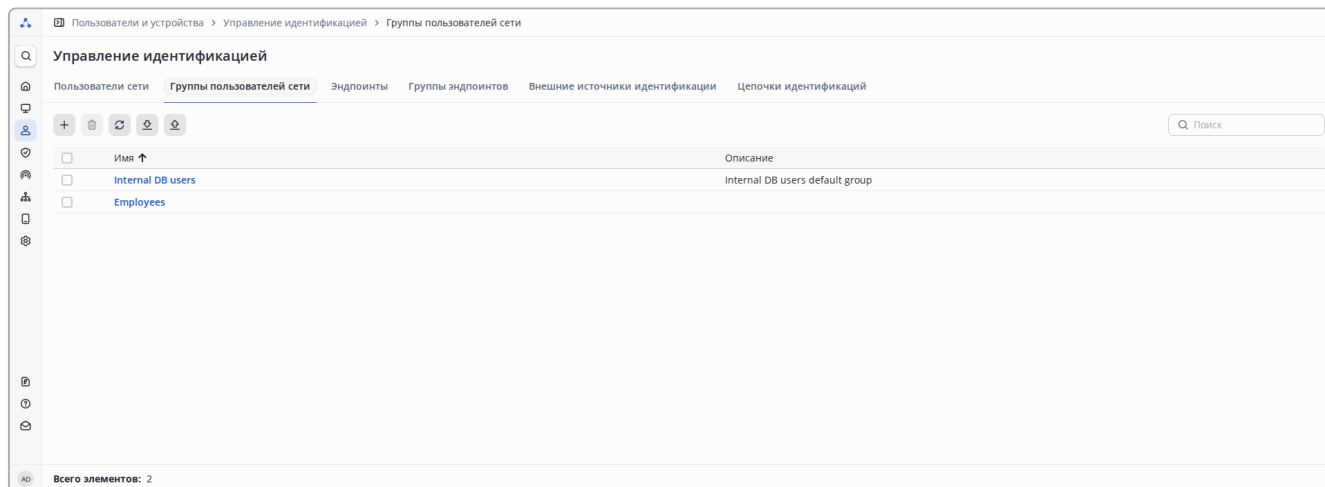


Рисунок 164. Таблица с перечнем групп пользователей сети на странице просмотра

На данной странице содержится таблица со списком всех групп пользователей сети.

Таблица содержит колонки:

- **Имя** - название группы.
- **Описание** - произвольное описание группы.

Возможна сортировка в прямом и обратном порядке по всем колонкам. По умолчанию сортировка выполняется в прямом (алфавитном) порядке по полю "Имя".

Элементы управления:

-  — Добавить новый элемент.
-  — Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
-  — Обновить данные таблицы.
-  — Позволяет загрузить данные из csv-файла.
-  — Позволяет выгрузить данные в csv-файл.
- ☐ — Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).
-  — Изменить текущий порядок сортировки.
-  Поиск — Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.

Добавление группы пользователей

Для добавления группы пользователей нажмите  в левой части поля над таблицей, откроется страница **Добавление**:

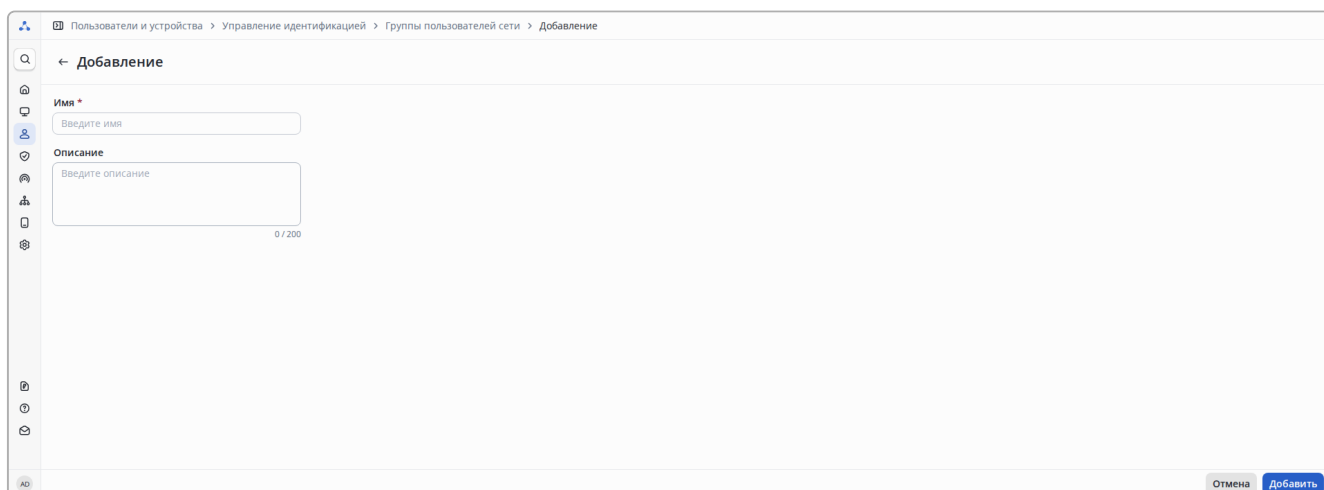


Рисунок 165. Страница добавления группы пользователей

Для заполнения доступны следующие параметры:

- **Имя *** - название группы. Максимальная длина - 100 символов.
- **Описание** - произвольное описание группы. Максимальная длина - 200 символов.

Параметры, отмеченные звездочкой *, обязательны для заполнения.



Добавление пользователей в группу доступно на странице редактирования ранее добавленной группы.
На этапе создания группы добавить в нее пользователей нельзя.

Для добавления группы в список групп пользователей не забудьте нажать **Добавить**. Для сброса изменений и выхода на страницу просмотра нажмите на **Отменить**.

Редактирование группы пользователей

Для редактирования ранее добавленной группы на странице просмотра групп пользователей нажмите на имя группы в таблице.

☐	Имя ↑
☐	Internal DB users
☐	Employees

Рисунок 166. Гиперссылка на страницу редактирования группы пользователей

Откроется страница редактирования с возможностью добавления пользователей в группу.

Рисунок 167. Страница изменения группы пользователей

Элементы управления в таблице **Пользователи группы**:

- Поиск - регистронезависимая фильтрация по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
- - удалить выбранных чекбоксом пользователей из группы (неактивно, пока не выбран хоть один пользователь).
- - изменить текущий порядок сортировки.
- ☐ - чекбокс, который отвечает за выбор пользователей для выполнения дальнейших действий (например, удаления пользователя из группы).
- - добавить пользователей в группу.

По нажатию появляется окно **Добавление пользователей в группу**, в котором необходимо выбрать пользователей для добавления в группу.

Рисунок 168. Окно добавления пользователей в группу

Элементы управления:

- Поиск - регистронезависимый поиск среди пользователей: отображаются только пользователи, удовлетворяющие условию фильтрации.
- ☐ - чекбокс, который отвечает за выбор пользователя для добавления (отображается только в левой колонке).
- - переместить пользователей, выбранных чекбоксом из доступных, в список выбранных.
- - удалить пользователя из списка выбранных (отображается только в правой колонке).
- **Добавить** - применить изменения (активна только если есть изменения).
- **Отменить** - отменить изменения.



Если при редактировании группы изменены только пользователи (имя и описание группы остались прежними), то кнопка **Сохранить** останется неактивной, так как изменения в списке пользователей группы сохраняются автоматически.

Просто выйдете из режима редактирования по кнопке **Отменить**.

Удаление группы пользователей

Для удаления групп необходимо на странице просмотра, используя чекбокс ☐, выбрать необходимые группы и в левом верхнем углу над таблицей нажать на .

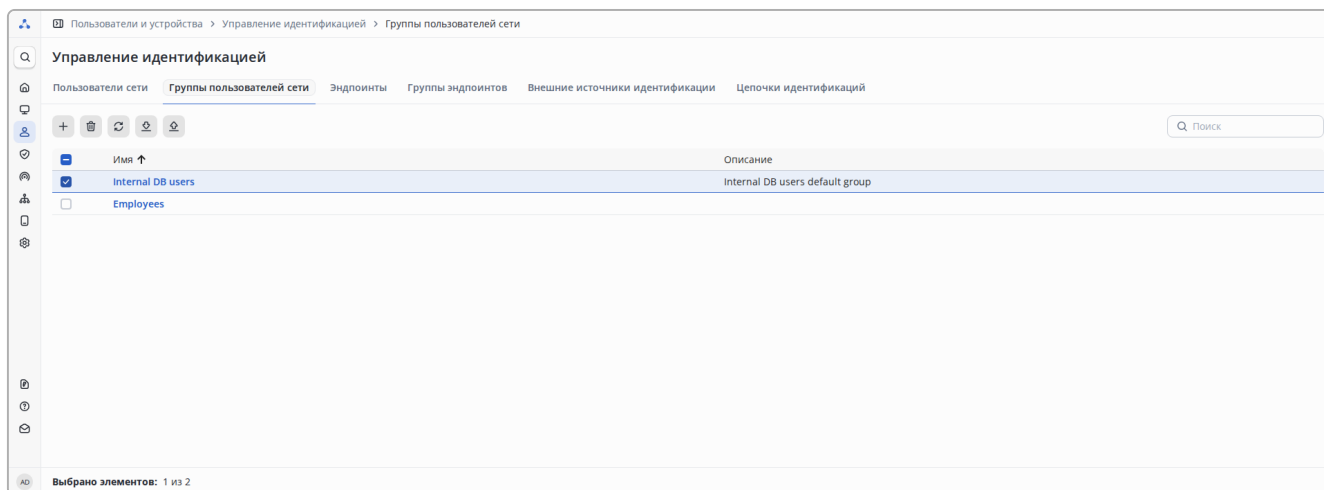


Рисунок 169. Выбор групп пользователей в таблице для удаления



Удаление элементов требует подтверждения в модальном окне. Выбранные элементы будут удалены только после явного подтверждения операции.

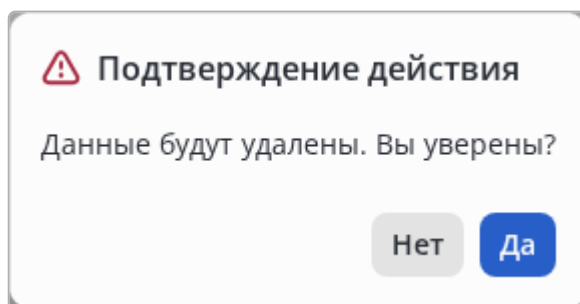


Рисунок 170. Диалоговое окно подтверждения действия



Ограничения:

- нельзя удалить группу, в которой состоят пользователи. В этом случае необходимо сначала удалить из группы всех пользователей, затем удалить пустую группу.
- нельзя удалить группу, которая используется в каком-либо логическом условии.

Импорт

NAICE поддерживает импорт данных из CSV-файлов.

Предварительная подготовка перед импортом

1. Создайте или проверьте наличие необходимых связанных записей (например, профиль устройства).
2. Ознакомьтесь с требованиями к CSV-файлу:
 - Файл должен быть в кодировке UTF-8;
 - Разделитель полей: запятая (,)
 - Разделитель строк/текста: двойная кавычка (")

- Заголовки и значения должны быть взяты в двойные кавычки (")
 - Максимальный размер файла 2МБ.
3. Проверьте содержимое файла на наличие лишних кавычек перед импортом;
 4. Проверьте то что значения, содержащие двойную кавычку (") или слэш (/) правильно экранированы.
 - Значения, содержащие двойную кавычку (") экранируются с помощью \
 - Значения, содержащие слэш (/) экранируются с помощью \

Правильное написание значений (с экранированием помощью \) на примере содержания файла для импорта набора команд TACACS:

"name:Required"	"description"	"permit_unmatch ed(true/false)"	"commands(Grant/command/argume nts/enabled;...)"
"command_set"	"\"Test command set\""	"false"	"PERMIT/\"show/vlan 1 2 \"/true"

Некорректное написание значений (без экранирования) на примере содержания файла для импорта набора команд TACACS:

"name:Required"	"description"	"permit_unmatch ed(true/false)"	"commands(Grant/command/argume nts/enabled;...)"
"command_set"	"Test command set"	"false"	"PERMIT/show/vlan 1 2 /true"



Игнорирование экранирования приведёт к некорректному распознаванию данных.

Порядок выполнения импорта

Для импорта данных из CSV-файла нажмите  на панели действий, расположенной над таблицей. После чего откроется окно:

Импорт

При импорте дублирующиеся данные не будут перезаписаны или отредактированы - система пропустит их. Если вы хотите изменить старые данные, удалите их из системы вручную перед импортом.

Внимательно ознакомьтесь с [Документацией](#) , чтобы импорт прошёл без ошибок.

Выберите файл*
Максимальный размер файла 2МБ

 **Загрузите** или перетащите сюда

Поле обязательно для заполнения

Источник данных *

NAICE

☐ Игнорировать существующие данные 

☐ Остановить импорт при первой ошибке

Отмена

Импорт

Рисунок 171. Окно Импорта

Импорт данных из CSV-файла выполняется в несколько шагов:

1. Выберите необходимый CSV-файл, перетащив его в поле загрузки или выбрав через проводник, нажав кнопку "Загрузите";



Измененный CSV-файл нужно загрузить повторно, чтобы применить правки.

2. Выберите источник данных, если он заранее не определён;
3. При необходимости активируйте флаги импорта:

Игнорировать существующие данные

- Если переключатель включен — дубликаты записей считаются предупреждением.
- Если переключатель выключен — дубликаты расцениваются как ошибка.

Остановить импорт при первой ошибке

- Если переключатель включен — импорт останавливается при первой же ошибке. Будут импортированы только записи, которые были успешно обработаны до её возникновения.

Если переключатель выключен — ошибочные строки пропускаются, импорт продолжается до конца. Будут импортированы только валидные записи.

4. Для того чтобы импорт начался, нажмите кнопку **"Импорт"**.



При импорте дублирующиеся данные перезаписаны или отредактированы не будут - система пропустит их. Если вы хотите изменить старые данные, удалите их из системы вручную перед импортом.

Просмотр отчета по импорту

Сразу после завершения обработки файла откроется окно отчёта по импорту.

Если все записи в файле были обработаны корректно, вы увидите окно:

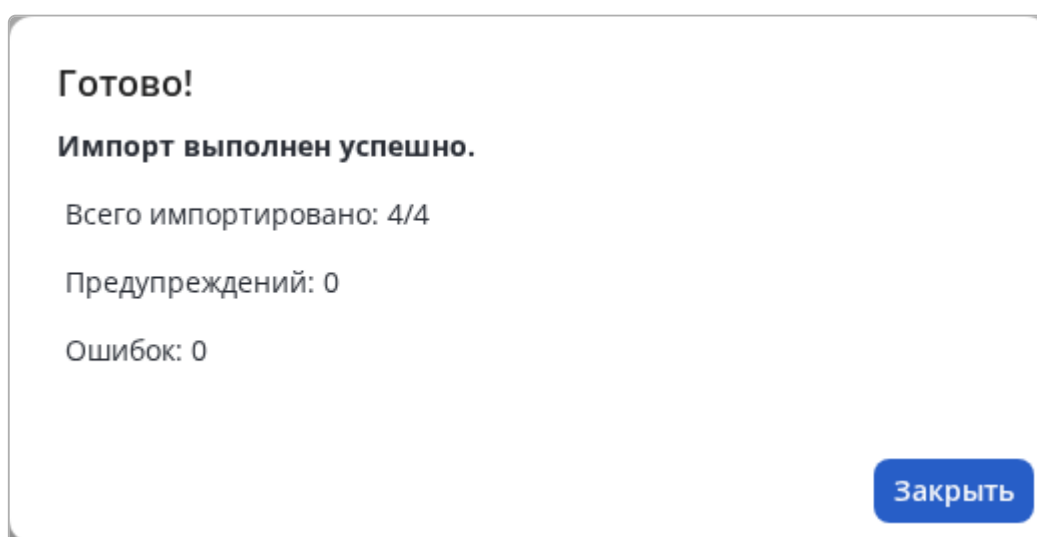


Рисунок 172. Отчет импорта (все записи обработаны корректно)

Блок с общей информацией содержит:

- **Всего импортировано** - Счётчик того, сколько записей было импортировано из общего импортируемого количества строк;
- **Предупреждений** - Количество возникших предупреждений;
- **Ошибок** - Количество возникших ошибок.

Если не все записи были обработаны корректно, вы увидите окно:

Готово!

Импорт выполнен, но не все данные обработаны корректно. Подробнее в отчете.

Всего импортировано: 3/4

Предупреждений: 3

Ошибок: 1

Подробный отчет

Фильтр

Все уведомления

	Строка	Описание
	1	Дубликат в базе данных. Значение с ...
	1	Отсутствует значение у поля "email"
	1	Отсутствует значение у поля "firstNa..."
	1	Отсутствует значение у поля "lastNa..."

Заккрыть

Рисунок 173. Отчет импорта (записи обработаны с ошибками/предупреждениями)

Подробный отчет содержит следующую информацию:

- **Фильтр** - Выпадающий список, в котором можно выбрать отображаемые уведомления (Все уведомления , Только ошибки или Только предупреждения)

Таблица уведомлений содержит колонки:

- **Строка** - Номер строки в CSV-файле, где обнаружена ошибка или предупреждение;
- **Описание** - Детальное текстовое объяснение ошибки или предупреждения.



Для просмотра полного текста описания наведите курсор мыши на соответствующую строку - во всплывающей подсказке отобразится полный текст сообщения об ошибке или предупреждении.

Особенности импорта групп пользователей



Для групп пользователей в качестве источника данных поддерживан только NAICE

В таблице ниже приведен список полей, их обязательность, описание и требования:

Поле	Описание	Требования
name:Required	Имя группы	Обязательное поле Максимальная длина - 100 символов
description	Произвольное описание группы	Максимальная длина - 200 символов

Пример корректного содержания файла:

"name:Required"	"description"
"Internal DB users"	"Internal DB users"

Получение CSV-файла шаблона описано далее в разделе "Экспорт".

Экспорт

NAICE поддерживает экспорт данных в формате CSV. Значения и заголовки обрамляются **двойными кавычками** , разделитель полей: **запятая (,)** .

Процедура экспорта

Доступны два режима экспорта данных:

- **Экспорт всего** - Выгрузка всех записей текущего раздела. Системные записи исключаются из экспорта;
- **Экспорт выбранного** - Выгрузка только отмеченных чекбоксом записей.

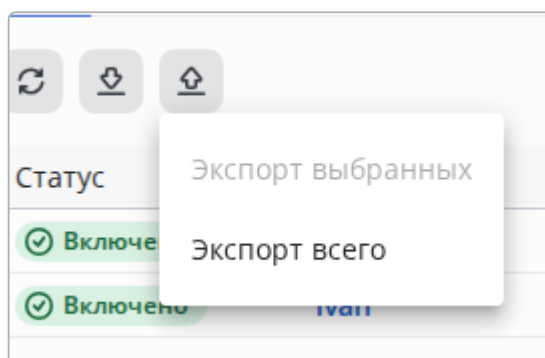


Рисунок 174. Окно выбора режима экспорта



Значения содержащие двойную кавычку (") или слэш (/) будут экранированы с помощью \ " .

Экспорт всех записей

На панели действий над таблицей нажмите  и выберите режим **"Экспорт всего"**. В открывшемся окне подтвердите действие кнопкой **"Экспорт"**:

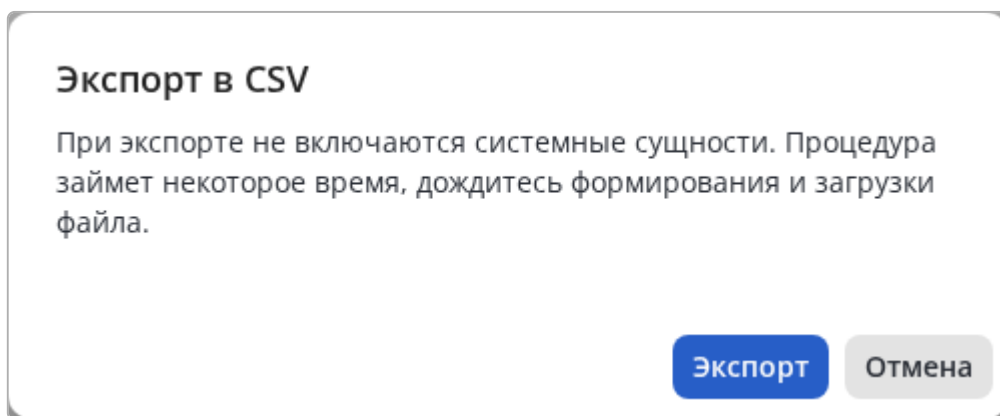


Рисунок 175. Экспорт всего

После нажатия кнопки **"Экспорт"** на устройство выгрузится файл, содержащий все записи из текущего раздела.

Экспорт выбранных записей

На панели действий над таблицей нажмите  и выберите режим **"Экспорт выбранных"**. В открывшемся окне подтвердите действие кнопкой **"Экспорт"**:

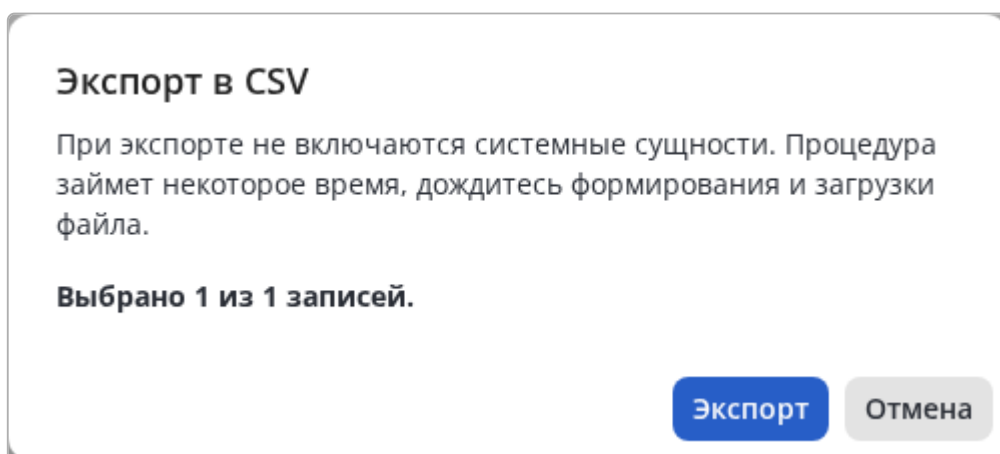


Рисунок 176. Экспорт выбранных

После нажатия кнопки **"Экспорт"** на устройство выгрузится файл, содержащий только отмеченные записи.



При **открытии** CSV-файлов в качестве разделителя полей **всегда** используйте **запятую (,)**, разделителем строк/текста могут быть **двойные кавычки (")** или **пустое значение**.

При **сохранении** CSV-файлов в качестве разделителя полей **всегда** используйте **запятую (,)**, а разделитель строк/текста - **пустое значение**.



Если при открытии файла использовался разделитель строк — двойная кавычка (**"**), то значения, содержащие символы двойной кавычки (**"**) или слэша (**/**), экранированные как ****, могут при сохранении получить лишнюю кавычку (**"**) после (****). Проверьте файл в текстовом редакторе и удалите лишние кавычки, если они появились.

Шаблон

Если в таблице отсутствуют записи (либо присутствуют только системные), при выборе режима **"Экспорт всего"** будет сформирован CSV-файл, содержащий исключительно заголовки столбцов. Данный файл может быть использован в качестве **шаблона** для подготовки данных перед импортом.

Особенности экспорта групп пользователей

Структура CSV-файла для групп пользователей описана в разделе ["Особенности импорта групп пользователей"](#).

Эндпоинты

Описание

Эндпоинты - это любые конечные устройства, которые подключаются к сетевой инфраструктуре через устройства-аутентификаторы (такие, как коммутаторы или точки доступа с аутентификацией по протоколу 802.1x или MAB), например - персональные компьютеры, мобильные и IP-телефоны, принтеры, IoT-устройства и другие.

Система NAICE позволяет отслеживать эндпоинты в сети, группировать их по определенным признакам автоматически или вручную, и на основе получаемых в процессе [профилирования](#) параметров и [Политики RADIUS](#) разрешать или запрещать доступ к сети.

Заполнение таблицы эндпоинтов

Заполнение таблицы эндпоинтов происходит в автоматическом и ручном режиме.

- *в ручном режиме:* добавление эндпоинтов выполняется пользователем системы по аналогии с добавлением других записей.
- *в автоматическом режиме:* добавление эндпоинтов происходит при получении RADIUS-запросов от аутентификаторов в ходе подключения клиентов.



Для определения MAC-адреса добавляемого эндпоинта используется значение атрибута "Calling-Station-Id" RADIUS-запроса. В случае отсутствия атрибута в RADIUS запросе или если он не содержит MAC адрес - эндпоинт не будет отображаться в таблице, но будет учитываться в лимите лицензии.



Случайно сгенерированные MAC-адреса (randomized MAC address) не будут добавлены в качестве эндпоинтов автоматически. При необходимости добавьте такие эндпоинты в ручном режиме.

Просмотр списка эндпоинтов

Пользователи и устройства > Управление идентификацией > Эндпоинты

Управление идентификацией

Пользователи сетиГруппы пользователей сетиЭндпоинтыГруппы эндпоинтовВнешние источники идентификацииЦепочки идентификаций

+↺⌵🔍🗑️📄🔒

Фильтры

	MAC адрес	Статус	Подробнее	Описание	Производитель	IP адрес эндпоинта	Имя пользователя	Имя хоста
	74:56:3C:E7:3D:9C	Подключено		Discovered Endpoint	GIGA-BYTE TECHNOLOGY CO.,L...	192.168.118.179	74563ce73d9c	PC-16489
	B8:2A:5E:C4:5F	Отключено		Discovered Endpoint	Apple, Inc.	192.168.130.58	b82aa95ec45f	
	44:E4:D9:3B:54:1A	Отключено		Discovered Endpoint	Cisco Systems, Inc	192.168.87.192	44e4d93b541a	
	A8:F9:4B:26:C0:16	Подключено		Discovered Endpoint	Eltex Enterprise Ltd	192.168.30.198	a8f94b26c016	NV-501-Wav-reva
	7C:C2:C6:4B:0D:C9	Подключено		Discovered Endpoint	TP-Link Systems Inc	192.168.50.25	7cc2c64bd0c9	LAPTOP-JRU6IBE
	40:86:CB:44:C1:8A	Отключено		Discovered Endpoint	D-Link Corporation	192.168.240.155	4086cb44c18a	
	A4:3B:0E:00:8C:39	Подключено		Discovered Endpoint	Huawei Device Co., Ltd.	192.168.23.150	a43be0e08c39	MNA-LX9
	50:EB:F6:DB:65:FA	Подключено		Компьютер	ASUSTek COMPUTER INC.	192.168.151.144	50ebf6db65fa	PC-16488
	14:58:D0:C5:2A:36	Подключено		Discovered Endpoint	Hewlett Packard	192.168.126.51	1458d0c52a36	user-HP-ProBook-450-G2
	CC:9D:A2:C7:C6:50	Подключено		Discovered Endpoint	Eltex Enterprise Ltd.	192.168.179.242	cc9da2c7c650	WEP-3ax
	68:13:E2:09:7A:77	Подключено		Discovered Endpoint	Eltex Enterprise LTD	192.168.113.111	6813e2097a77	VP-12P
	74:56:3C:26:B4:5F	Подключено		Discovered Endpoint	GIGA-BYTE TECHNOLOGY CO.,L...	192.168.106.231	74563c26b45f	DESKTOP-NUBAQBS
	00:ED:4C:68:30:FF	Подключено		Discovered Endpoint	REALTEK SEMICONDUCTOR CO...	192.168.96.151	00ed4c6830ff	azurecloud-o-pc
	A4:BADB:D4:CD:EF	Подключено		Discovered Endpoint	Dell Inc.	192.168.35.90	a4badbd4cdcf	vostro
	E8:F7:91:DF:B2:36	Подключено		Discovered Endpoint	Xiaomi Communications Co Ltd	192.168.50.137	e8f791dfb236	Redmi 11N

Всего элементов: 15

Рисунок 177. Просмотр списка эндпоинтов

На данной странице содержится таблица со списком всех вручную или автоматически добавленных эндпоинтов.

Таблица по умолчанию содержит колонки:

- **MAC адрес** - MAC адрес эндпоинта в формате "XX:XX:XX:XX:XX:XX".
- **Статус** - текущее состояние подключения эндпоинта. Статус отображается после первой попытки аутентификации эндпоинта и может принимать следующие значения:
 -  **Подключено** - устройство успешно прошло аутентификацию и авторизацию и получило доступ к сети;
 -  **Отклонено** - устройство не прошло аутентификацию и не получило доступ к сети;
 -  **Отключено** - устройство отключено от сети.
- **Подробнее** - переход на страницу детальной информации об атрибутах эндпоинта и его последних событий аутентификации.
- **Описание** - произвольное описание.
- **Производитель** - производитель конечного устройства, определенный по первым трем октетам MAC-адреса (MAC OUI).
- **IP адрес эндпоинта** - IP-адрес эндпоинта, информация о котором была получена в ходе профилирования. Для получения данных требуются настройки профилирования.
- **Имя пользователя** - имя пользователя, с которым эндпоинт проходил аутентификацию в последний раз.
- **Имя хоста** - имя хоста эндпоинта, информация о котором была получена в ходе профилирования. Для получения данных требуются настройки профилирования.
- **Профиль эндпоинта** - результат профилирования эндпоинта.

Дополнительно при нажатии на  возможно настроить отображение следующих колонок:

Причина ошибки аутентификации - причина ошибки в ходе подключения клиента.

- Политика аутентификации - название правила политики аутентификации, которое было применено в рамках данной сессии;
- Политика авторизации - название правила политики авторизации, которое было применено в рамках данной сессии;
- Протокол аутентификации - протокол, по которому проходила аутентификация (например, PAP).
- Тип подключения - тип подключения, который был определен исходя из настроек [профиля сетевого устройства](#).
- Тип эндпоинта - логический профиль, которому принадлежит устройство в результате профилирования.
- Дата последней активности - дата, когда последний раз была предпринята попытка подключения клиента (успешная или неуспешная).
- Группа эндпоинта - группа, в которую автоматически или вручную был помещен эндпоинт.
- Имя NAS - имя устройства-аутентификатора.

Возможна сортировка в прямом и обратном порядке по колонкам MAC адрес, Статус, Описание, Производитель, IP адрес эндпоинта, Имя пользователя, Профиль эндпоинта, Дата последней активности (по умолчанию), Группа эндпоинта.

Страница содержит следующие элементы управления:

-  - Добавить новый элемент.
-  - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
-  - Запустить процесс перепрофилирования выбранных эндпоинтов (неактивно, пока не выбран хоть один элемент).
-  - Обновить данные таблицы.
-  - Позволяет загрузить данные из csv-файла.
-  - Позволяет выгрузить данные в csv-файл.
-  - Настроить отображение колонок таблицы.
- ☐ - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).
-  - Изменить текущий порядок сортировки.
-  **Фильтры** - Открыть окно настройки фильтрации данных по таблице.

Фильтрация данных в таблице настраивается в следующем окне:

Рисунок 178. Настройка фильтрации данных в таблице

Фильтрация доступна по параметрам **Профиль эндпоинта**, **MAC адрес**, **Статус**, **Описание** и **Имя пользователя**.

В настройках таблицы можно сменить состав отображаемых колонок.

Кнопка **Сбросить все** предназначена для сброса настроенных колонок к состоянию по умолчанию (неактивно, пока состоянию по умолчанию не изменено).

Добавление эндпоинта

Эндпоинты добавляются в систему автоматически в ходе попыток аутентификации. При необходимости можно добавить эндпоинт вручную. Для добавления эндпоинта нажмите в левой части поля над таблицей.

Рисунок 179. Добавление эндпоинта

На открывшейся странице представлены следующие параметры:

- **MAC адрес *** - MAC адрес эндпоинта.
- **Описание** - произвольное описание длиной до 200 символов.
- **Ручное назначение политики** - назначить для данного эндпоинта [политику профилирования](#) вручную. Данное значение не будет перезаписано в результате профилирования.

Ручное назначение группы - назначить для данного эндпоинта **группу** вручную. Данное значение не будет перезаписано в результате профилирования.

Параметры, отмеченные символом *, обязательны для заполнения.

Для добавления эндпоинта в список эндпоинтов не забудьте нажать **Добавить**. Для сброса изменений и возврата на страницу просмотра нажмите на **Отменить**.

Редактирование эндпоинта

Для редактирования ранее добавленного эндпоинта на странице просмотра нажмите на MAC адрес эндпоинта в таблице.

☐	MAC адрес	Статус
☐	74:56:3C:E7:3D:9C	 Подключено
☐	B8:2A:A9:5E:C4:5F	 Отклонено
☐	44:E4:D9:3B:54:1A	 Отклонено
☐	A8:F9:4B:26:C0:16	 Подключено
☐	7C:C2:C6:4B:0D:C9	 Подключено
☐	40:86:CB:44:C1:8A	 Отклонено
☐	A4:3B:0E:00:8C:39	 Подключено
☐	50:EB:F6:DB:65:FA	 Подключено
☐	14:58:D0:C5:2A:36	 Подключено
☐	CC:9D:A2:C7:C6:50	 Подключено
☐	68:13:E2:09:7A:77	 Подключено
☐	74:56:3C:26:B4:5F	 Подключено
☐	00:E0:4C:68:30:FF	 Подключено
☐	A4:BA:DB:D4:CD:EF	 Подключено
☐	E8:F7:91:DF:B2:36	 Подключено

Рисунок 180. Гиперссылка на страницу редактирования эндпоинта

Откроется страница редактирования, аналогичная странице добавления.

Рисунок 181. Редактирование эндпоинта



Редактирование MAC адреса эндпоинта недоступно.
Если необходимо отредактировать адрес, то удалите и создайте эндпоинт заново.

После редактирования нажмите на **Сохранить**. Кнопка останется неактивной пока не будет изменено хотя бы одно поле.

Просмотр детальной информации об эндпоинте

Для просмотра детальной информации об эндпоинте нажмите на  в колонке **Подробнее** в таблице. В браузере будет открыта новая вкладка с нужной страницей.

Атрибуты	Аутентификация	Пробы
Manual Policy Assignment	false	
Endpoint Policy	Unknown	
Manual Group Assignment	false	
Endpoint Identity Group	Unknown	
MAC Address	97:74:B5:AD:AD:0E	

Рисунок 182. Просмотр детальной информации об эндпоинте

Информация на странице разделена на 4 блока:

- Краткая и наиболее важная информация об эндпоинте;
- **Атрибуты** - атрибуты эндпоинта, которые были получены в результате профилирования или заданы пользователем системы;
- **Аутентификация** - данные о последней аутентификации эндпоинта:
 - **Общая информация** - краткая информация о результатах последнего подключения эндпоинта, отображается только если были попытки подключения;

Детали аутентификации - детальная информация, которая может быть полезна для отладки;

- Прочие атрибуты - содержание пакета, полученного NAICE от RADIUS-сервера;
- Результат - список атрибутов, которыми был обогащен ответ клиенту в результате авторизации (например, атрибуты для выдачи VLAN или ACL). Если выдача дополнительных атрибутов не настроена в профиле авторизации, то список будет пуст.

- Пробы - данные, которые могут быть использованы в настройках условий профилирования.



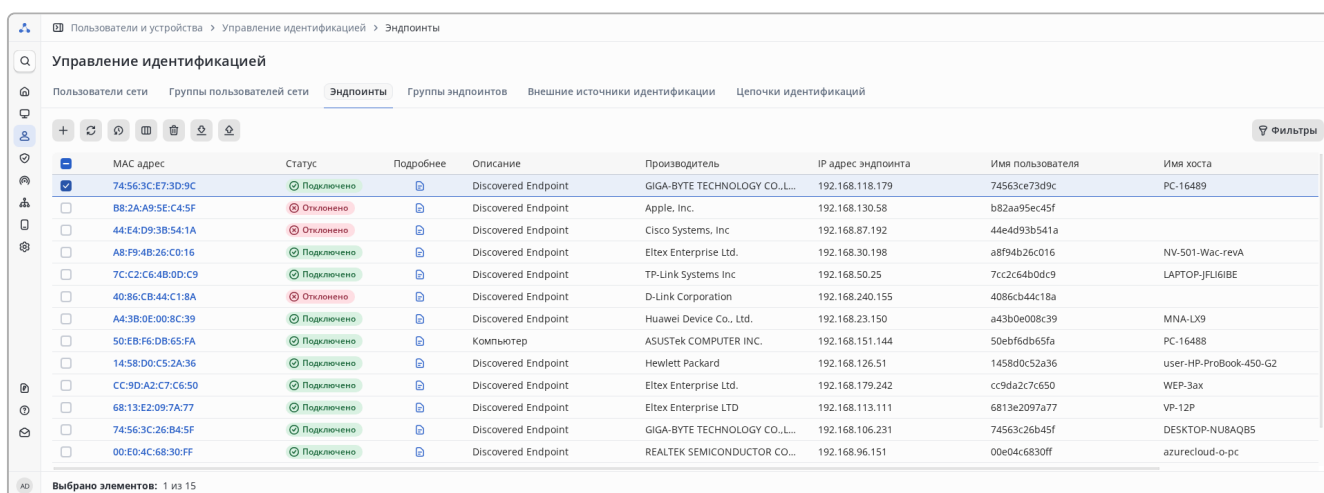
До окончания профилирования и до первой аутентификации страница может быть практически пуста. В таком случае вернитесь на страницу через некоторое время.

Удаление эндпоинта



Таблица эндпоинтов заполняется автоматически в процессе нормальной работы NAICE в ходе попыток подключения эндпоинтов. При удалении эндпоинта он будет повторно изучен при следующей попытке подключения. Отключить автоизучение эндпоинтов нельзя.

Для удаления эндпоинта необходимо на странице просмотра, используя чекбокс ☐, выбрать необходимые эндпоинты и в левом верхнем углу над таблицей нажать на .



	MAC адрес	Статус	Подробнее	Описание	Производитель	IP адрес эндпоинта	Имя пользователя	Имя хоста
☒	74:56:3C:E7:3D:9C	Подключено		Discovered Endpoint	GIGA-BYTE TECHNOLOGY CO.,L...	192.168.118.179	74563ce73d9c	PC-16489
☐	B8:2A:A9:5E:C4:5F	Отключено		Discovered Endpoint	Apple, Inc.	192.168.130.58	b82aa95ec45f	
☐	44:E4:D9:3B:54:1A	Отключено		Discovered Endpoint	Cisco Systems, Inc	192.168.87.192	44e4d93b541a	
☐	A8:F9:4B:26:C0:16	Подключено		Discovered Endpoint	Eltex Enterprise Ltd.	192.168.30.198	a8f94b26c016	NV-501-Wac-revA
☐	7C:C2:C6:4B:0D:C9	Подключено		Discovered Endpoint	TP-Link Systems Inc	192.168.50.25	7cc2c64b0dc9	LAPTOP-JFLI6IBE
☐	40:86:CB:44:C1:8A	Отключено		Discovered Endpoint	D-Link Corporation	192.168.240.155	4086cb44c18a	
☐	A4:3B:0E:00:8C:39	Подключено		Discovered Endpoint	Huawei Device Co., Ltd.	192.168.23.150	a43b0e008c39	MNA-LX9
☐	50:E8:F6:DB:65:FA	Подключено		Компьютер	ASUSTek COMPUTER INC.	192.168.151.144	50ebf6db65fa	PC-16488
☐	14:58:D0:C5:2A:36	Подключено		Discovered Endpoint	Hewlett Packard	192.168.126.51	1458d0c52a36	user-HP-ProBook-450-G2
☐	CC:9D:A2:C7:C6:50	Подключено		Discovered Endpoint	Eltex Enterprise Ltd.	192.168.179.242	cc9da2c7c650	WEP-3ax
☐	68:13:E2:09:7A:77	Подключено		Discovered Endpoint	Eltex Enterprise LTD	192.168.113.111	6813e2097a77	VP-12P
☐	74:56:3C:26:B4:5F	Подключено		Discovered Endpoint	GIGA-BYTE TECHNOLOGY CO.,L...	192.168.106.231	74563c26b45f	DESKTOP-NUBAQBS
☐	00:E0:4C:68:30:FF	Подключено		Discovered Endpoint	REALTEK SEMICONDUCTOR CO...	192.168.96.151	00e04c6830ff	azurecloud-o-pc

Рисунок 183. Выбор эндпоинтов в таблице для удаления



Удаление элементов требует подтверждения в модальном окне. Выбранные элементы будут удалены только после явного подтверждения операции.

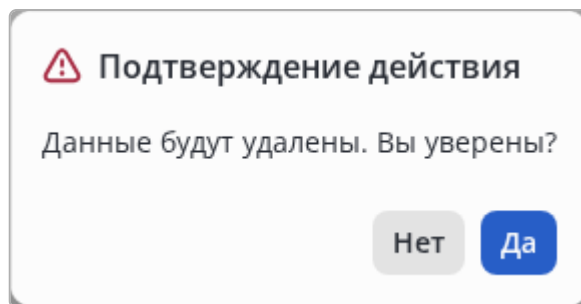


Рисунок 184. Диалоговое окно подтверждения действия

Импорт

NAICE поддерживает импорт данных из CSV-файлов.

Предварительная подготовка перед импортом

1. Создайте или проверьте наличие необходимых связанных сущностей (например, профиль устройства).
2. Ознакомьтесь с требованиями к CSV-файлу:
 - Файл должен быть в кодировке UTF-8;
 - Разделитель полей: запятая (,)
 - Разделитель строк/текста: двойная кавычка (")
 - Заголовки и значения должны быть взяты в двойные кавычки (")
 - Максимальный размер файла 2МБ.
3. Проверьте содержимое файла на наличие лишних кавычек перед импортом;
4. Проверьте то что значения, содержащие двойную кавычку (") или слэш (/) правильно экранированы.
 - Значения, содержащие двойную кавычку (") экранируются с помощью \
 - Значения, содержащие слэш (/) экранируются с помощью \

Правильное написание значений (с экранированием при помощи `\`) на примере содержания файла для импорта набора команд TACACS:

"name:Required"	"description"	"permit_unmatched(true/false)"	"commands(Grant/command/arguments/enabled;...)"
"command_set"	"\"Test command set\""	"false"	"PERMIT/\"show/vlan 1 2 \"/true"

Некорректное написание значений (без экранирования) на примере содержания файла для импорта набора команд TACACS:

"name:Required"	"description"	"permit_unmatched(true/false)"	"commands(Grant/command/arguments/enabled;...)"
"command_set"	"Test command set"	"false"	"PERMIT/show/vlan 1 2 /true"



Игнорирование экранирования приведёт к некорректному распознаванию данных.

Порядок выполнения импорта

Для импорта данных из CSV-файла нажмите  на панели действий, расположенной над таблицей. После чего откроется окно:

Импорт

При импорте дублирующиеся данные не будут перезаписаны или отредактированы - система пропустит их. Если вы хотите изменить старые данные, удалите их из системы вручную перед импортом.

Внимательно ознакомьтесь с [Документацией](#) , чтобы импорт прошёл без ошибок.

Выберите файл*
Максимальный размер файла 2МБ

 **Загрузите** или перетащите сюда

Поле обязательно для заполнения

Источник данных *

NAICE

☐ Игнорировать существующие данные 

☐ Остановить импорт при первой ошибке

☐ Автоматически создать недостающие записи 

Отмена

Импорт

Рисунок 185. Окно импорта

Импорт данных из CSV-файла выполняется в несколько шагов:

1. Выберите необходимый CSV-файл, перетащив его в поле загрузки или выбрав через проводник, нажав кнопку "Загрузите";



Измененный CSV-файл нужно загрузить повторно, чтобы применить правки.

2. Выберите источник данных, если он заранее не определён;
3. При необходимости активируйте флаги импорта:

Игнорировать существующие данные

- Если переключатель включен — дубликаты записей считаются предупреждением.
- Если переключатель выключен — дубликаты расцениваются как ошибка.

Остановить импорт при первой ошибке

-

Если переключатель включен — импорт останавливается при первой же ошибке. Будут импортированы только записи, которые были успешно обработаны до её возникновения.

- Если переключатель выключен — ошибочные строки пропускаются, импорт продолжается до конца. Будут импортированы только валидные записи.

Автоматически создать недостающие записи

- Если переключатель включен — при выполнении импорта недостающие записи будут заполнены автоматически. Перечень автозаполняемых записей можно узнать при наведении на подсказку справа от переключателя.
- Если переключатель выключен — все требуемые поля необходимо заполнить вручную.

4. Для того чтобы импорт начался, нажмите кнопку **"Импорт"**.



При импорте дублирующиеся данные перезаписаны или отредактированы не будут - система пропустит их. Если вы хотите изменить старые данные, удалите их из системы вручную перед импортом.

Просмотр отчета по импорту

Сразу после завершения обработки файла откроется окно отчёта по импорту.

Если все записи в файле были обработаны корректно, вы увидите окно:

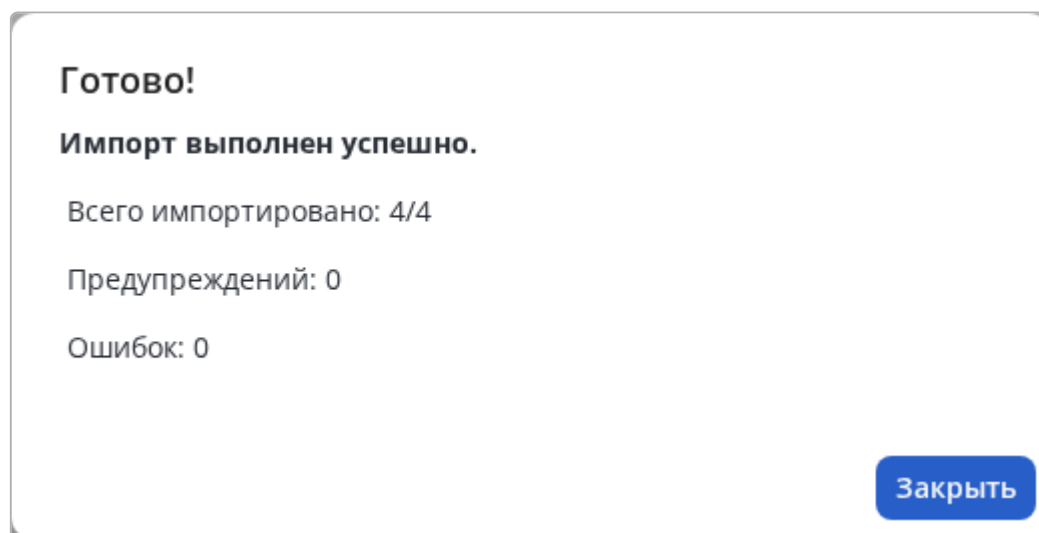


Рисунок 186. Отчет импорта (все записи обработаны корректно)

Блок с общей информацией содержит:

- **Всего импортировано** - Счётчик того, сколько записей было импортировано из общего импортируемого количества строк;
- **Предупреждений** - Количество возникших предупреждений;
- **Ошибок** - Количество возникших ошибок.

Если не все записи были обработаны корректно, вы увидите окно:

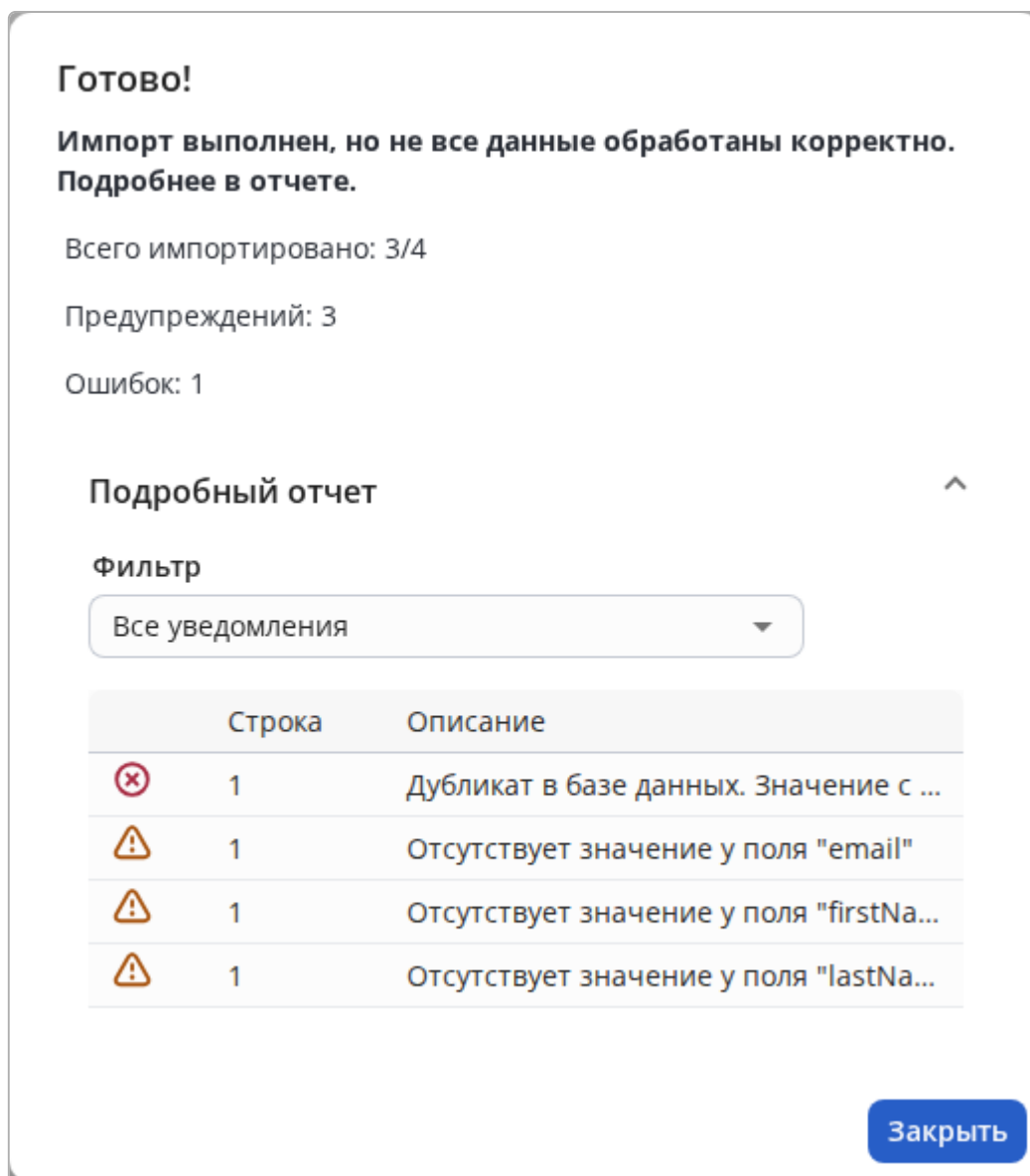


Рисунок 187. Отчет импорта (записи обработаны с ошибками/предупреждениями)

Подробный отчет содержит следующую информацию:

- **Фильтр** - Выпадающий список, в котором можно выбрать отображаемые уведомления (Все уведомления, Только ошибки или Только предупреждения)

Таблица уведомлений содержит колонки:

- **Строка** - Номер строки в CSV-файле, где обнаружена ошибка или предупреждение;
- **Описание** - Детальное текстовое объяснение ошибки или предупреждения.



Для просмотра полного текста описания наведите курсор мыши на соответствующую строку - во всплывающей подсказке отобразится полный текст сообщения об ошибке или предупреждении.

Особенности импорта эндпоинтов



Для эндпоинтов в качестве источника данных поддержан только **NAICE**

В таблице ниже приведен список полей, их обязательность, описание и требования:

Поле	Описание	Требования
mac_address:Required	MAC-адрес эндпоинта	Обязательное поле Допустимыми считаются форматы: - XX:XX:XX:XX:XX:XX - XX-XX-XX-XX-XX-XX - XXXX.XXXX.XXXX - XXXXXXXXXXXX
vendor	Производитель конечного устройства	При импорте поле игнорируется
description	Произвольное описание	Максимальная длина - 200 символов
profiler_policy	Политика профилирования, которая будет присвоена эндпоинту (указывается полный путь)	Должна существовать в системе NAICE Формат: родительская_политика#политика
endpoint_group	Группа, которая будет назначена эндпоинту (указывается полный путь)	Должна существовать в системе NAICE Формат: группа#подгруппа
hostname	Имя хоста эндпоинта	Максимальная длина - 100 символов
username	Имя пользователя	Максимальная длина - 100 символов
current_ip_addresses	IP-адрес эндпоинта	Формат: четыре числа 0-255, разделенные точками



Логика обработки полей profiler_policy и endpoint_group:

- Если значение найдено в системе — политика/группа считается **назначенной вручную** и не будет перезаписана в результате будущего **профилирования**.
- Если значение отсутствует/не найдено — автоматически назначается значение **Unknown**, которое может быть перезаписано в результате будущего **профилирования**.

Пример корректного содержания файла:

"mac_address:Required"	"vendor"	"description"	"profiler_policy"	"endpoint_group"	"hostname"	"username"	"current_ip_address"
"85:BF:DA:B7:87:66"	""	""	"test#test_policy"	"test_group"	"test"	"tester"	"10.25.95.105"

Получение CSV-файла шаблона описано далее в разделе "Экспорт".

Экспорт

NAICE поддерживает экспорт данных в формате CSV. Значения и заголовки обрамляются двойными кавычками, разделитель полей: запятая (,).

Процедура экспорта

Доступны два режима экспорта данных:

- Экспорт всего - Выгрузка всех записей текущего раздела. Системные записи исключаются из экспорта;
- Экспорт выбранного - Выгрузка только отмеченных чекбоксом записей.

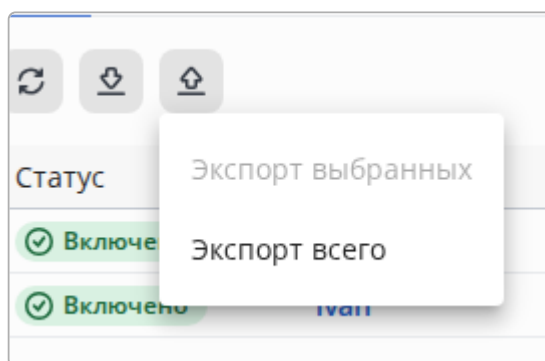


Рисунок 188. Окно выбора режима экспорта



Значения содержащие двойную кавычку (") или слэш (/) будут экранированы с помощью \".

Экспорт всех записей

На панели действий над таблицей нажмите  и выберите режим "Экспорт всего". В открывшемся окне подтвердите действие кнопкой "Экспорт":

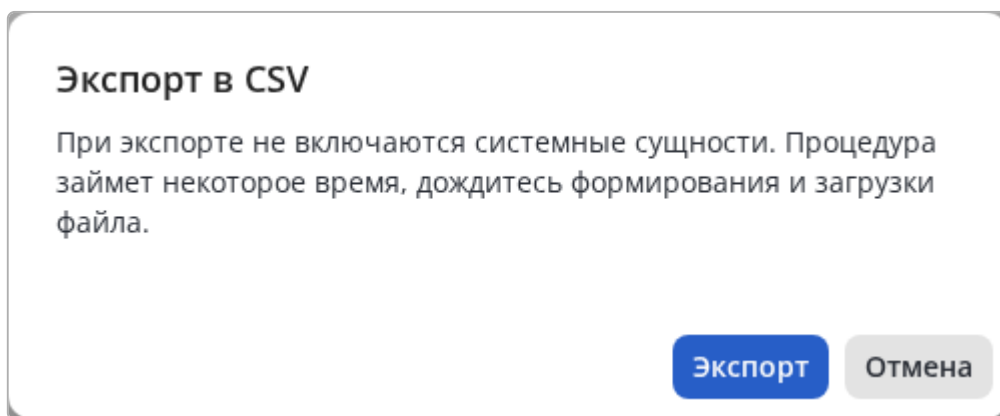


Рисунок 189. Экспорт всего

После нажатия кнопки **"Экспорт"** на устройство выгрузится файл, содержащий все записи из текущего раздела.

Экспорт выбранных записей

На панели действий над таблицей нажмите  и выберите режим **"Экспорт выбранных"**. В открывшемся окне подтвердите действие кнопкой **"Экспорт"**:

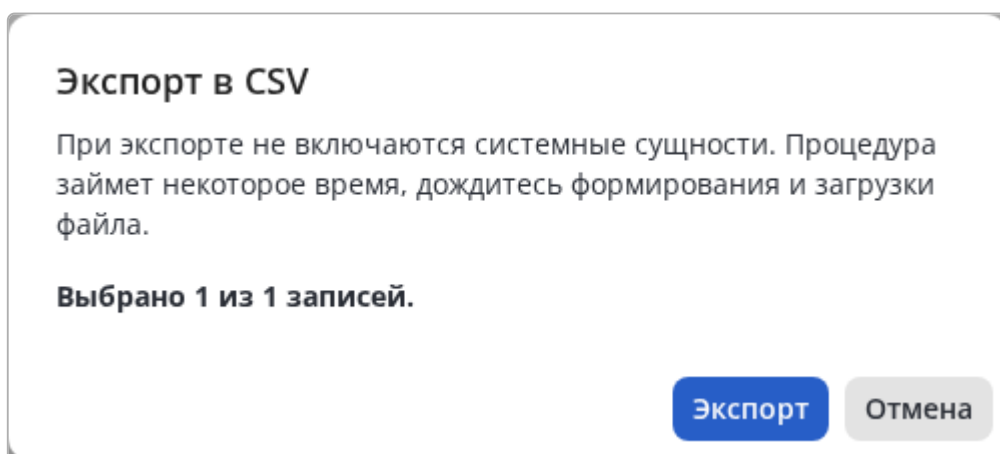


Рисунок 190. Экспорт выбранных

После нажатия кнопки **"Экспорт"** на устройство выгрузится файл, содержащий только отмеченные записи.



При **открытии** CSV-файлов в качестве разделителя полей **всегда** используйте **запятую (,)**, разделителем строк/текста могут быть **двойные кавычки (")** или **пустое значение**.

При **сохранении** CSV-файлов в качестве разделителя полей **всегда** используйте **запятую (,)**, а разделитель строк/текста - **пустое значение**.



Если при открытии файла использовался разделитель строк — двойная кавычка (**"**), то значения, содержащие символы двойной кавычки (**"**) или слэша (**/**), экранированные как ****, могут при сохранении получить лишнюю кавычку (**"**) после (****). Проверьте файл в текстовом редакторе и удалите лишние кавычки, если они появились.

Шаблон

Если в таблице отсутствуют записи (либо присутствуют только системные), при выборе режима "Экспорт всего" будет сформирован CSV-файл, содержащий исключительно заголовки столбцов. Данный файл может быть использован в качестве **шаблона** для подготовки данных перед импортом.

Особенности экспорта эндпоинтов



В экспортированном файле будет присутствовать поле `vendor` - производитель конечного устройства, определенный по первым трем октетам MAC-адреса (MAC OUI).



Политика/группа эндпоинтов будет прописана в формате полного пути через разделитель - `#`.

Структура CSV-файла для эндпоинтов описана в разделе "[Особенности импорта эндпоинтов](#)".

Группы эндпоинтов

Описание

Группы эндпоинтов - это совокупность эндпоинтов, объединенных в группы по логическому признаку.

Система NAICE позволяет отслеживать [эндпоинты](#) в сети, группировать их вручную или автоматически, на основе получаемых в процессе [профилирования](#) параметров.

Просмотр всех групп

При переходе на вкладку "Группы эндпоинтов", открывается панель просмотра всех групп.

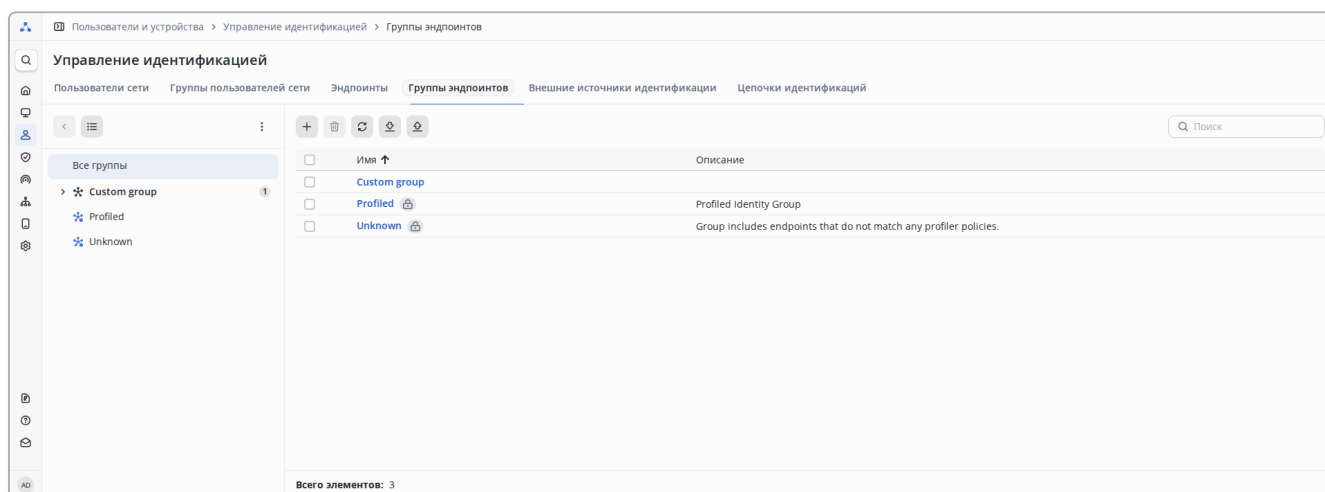


Рисунок 191. Просмотр списка групп эндпоинтов

Таблица содержит колонки:

- **Имя** - Имя группы
 - - Данная запись является системной и недоступна для удаления или редактирования.
- **Описание** - Полное описание группы

Элементы управления:

-  — Добавить новый элемент.
-  — Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
-  — Обновить данные таблицы.
-  — Позволяет загрузить данные из csv-файла.
-  — Позволяет выгрузить данные в csv-файл.
- ☐ — Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).
-  — Изменить текущий порядок сортировки.
-  Поиск — Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.

В левой стороне располагается панель быстрого просмотра в виде дерева или списка

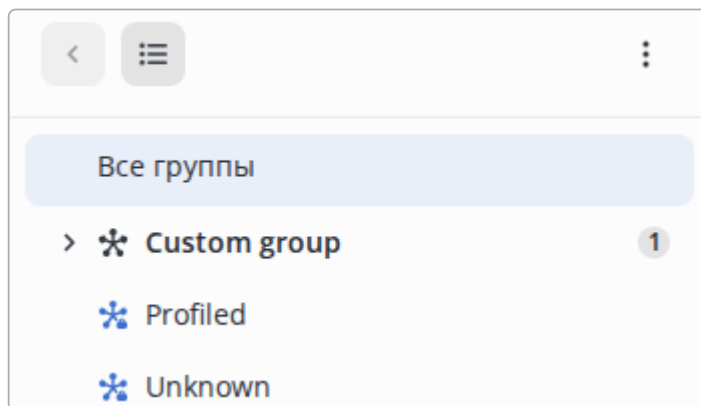


Рисунок 192. Меню навигации по дереву групп эндпоинтов

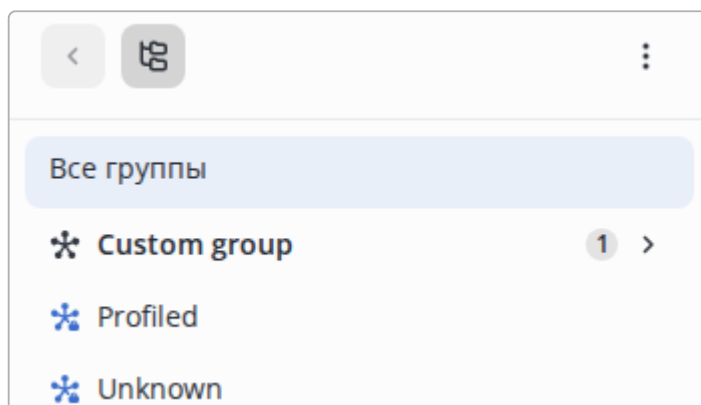


Рисунок 193. Вид Меню навигации в режиме списка

Содержит следующие элементы управления:

- Все группы - открыть таблицу с просмотром и администрированием всех групп
-  - Выбор доступных действий (зависит от выбранного элемента в дереве):
 - Добавить корневую группу

- Добавить дочернюю группу
- Удалить группу
-  - включен режим отображения в виде дерева
-  - включен режим отображения в виде списка
-  - переход на уровень выше (активно только в режиме списка).
-  - в режиме дерева отображается слева от наименования групп, имеющих дочерние элементы, если список закрыт. В режиме списка отображается справа от наименования групп, имеющих дочерние элементы.

Добавление группы

Для добавления группы нажмите  в левой части поля над таблицей, откроется страница **Добавление:**

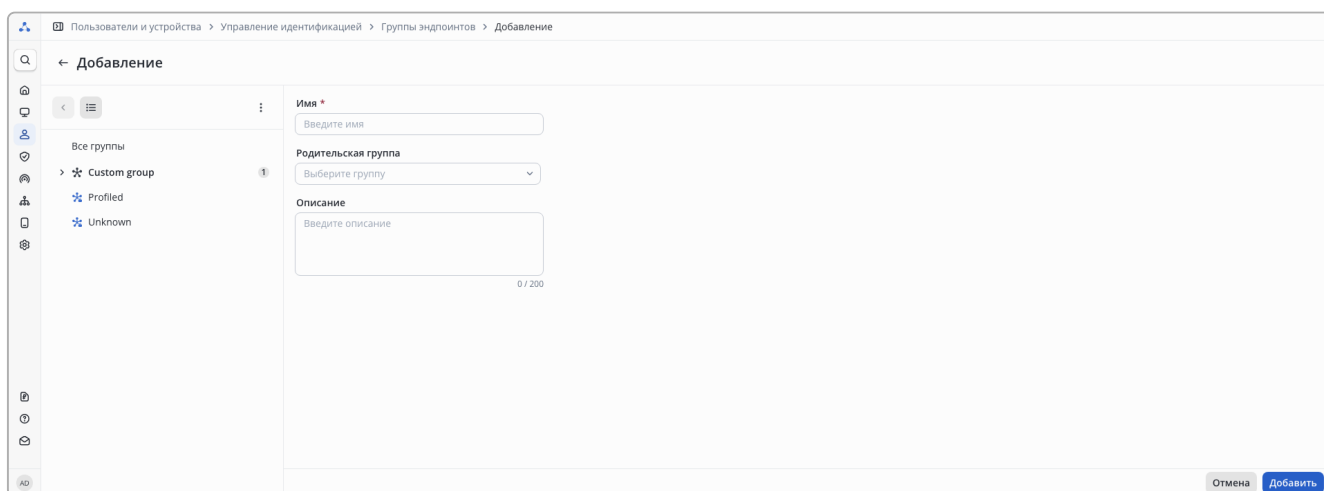


Рисунок 194. Форма добавления группы эндпоинтов

Для заполнения доступны следующие параметры:

- **Имя *** - название группы. Максимальная длина - 100 символов.
- **Родительская группа** - выбор родительской группы из списка. Настройка родительской группы доступна только в момент создания группы по кнопке .
- **Описание** - произвольное описание группы. Максимальная длина - 200 символов.

Параметры, отмеченные звездочкой *, обязательны для заполнения.



Также создать группу можно по кнопке  на панели навигации по дереву групп - **Добавить корневую группу**, **Добавить дочернюю группу**



Перемещение групп (смена родительской группы) после создания не предусмотрены.

Редактирование группы

Для редактирования ранее добавленной группы на странице просмотра нажмите на имя группы в таблице или дереве.

Рисунок 195. Форма редактирование группы эндпоинтов

Для изменения доступны:

- **Имя *** - название группы. Максимальная длина - 100 символов.
- **Описание** - произвольное описание группы. Максимальная длина - 200 символов.

После редактирования нажмите на **Сохранить**. Кнопка останется неактивной пока не будет изменено хотя бы одно поле.

Добавление эндпоинтов в группу

На странице редактирования группы в нижней части располагается таблица **Эндпоинты**.

Таблица содержит колонки:

- **MAC адрес** - MAC-адрес эндпоинта;
- **Назначено вручную** - признак добавления эндпоинта в группу вручную;
- **Профиль эндпоинта** - профиль, назначенный эндпоинту.

Элементы управления:

- **+** — Добавить новый элемент.
- **🗑** — Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- **🔄** — Обновить данные таблицы.
- **☐** — Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).
- **↑** — Изменить текущий порядок сортировки.
-

 **Поиск** — Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.



При удалении **эндпоинта** из группы ему автоматически назначается группа "Unknown".

Для добавления эндпоинта в группу нажмите на . Откроется всплывающее окно, в котором необходимо выбрать эндпоинты для добавления в группу с помощью чекбоксов ☐ и перенести в список "Выбранные" по кнопке .

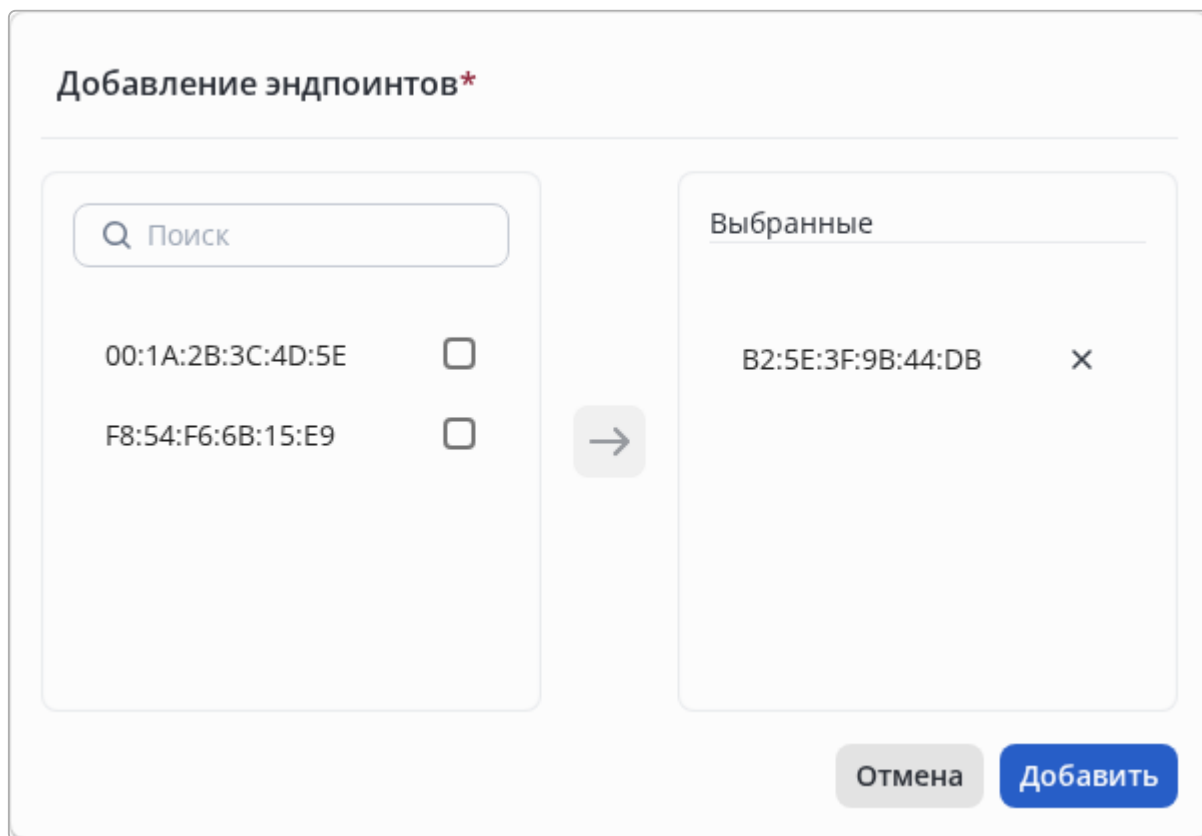


Рисунок 196. Модальный диалог добавления эндпоинтов

После выбора всех необходимых эндпоинтов нажмите на **Добавить**. Кнопка останется неактивной пока не будет выбран хотя бы один эндпоинт.



Все изменения в таблице **Эндпоинты** применяются автоматически и не требуют нажатия кнопки **Сохранить**. Действие кнопки сохранения распространяется на параметры группы.

Удаление группы

Для удаления групп необходимо на странице просмотра, используя чекбокс ☐, выбрать необходимые группы и в верхней левой части таблицы нажать на .

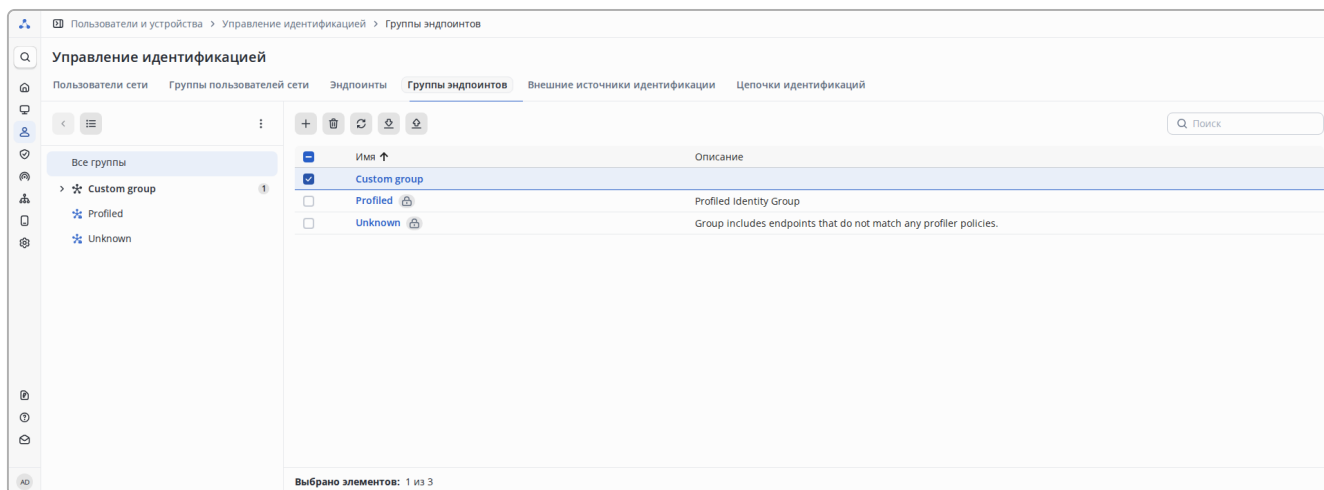


Рисунок 197. Выбор групп для удаления



Удаление элементов требует подтверждения в модальном окне. Выбранные элементы будут удалены только после явного подтверждения операции.

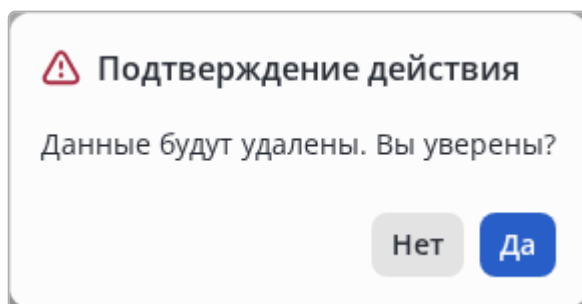


Рисунок 198. Диалоговое окно подтверждения действия



Ограничения:

- нельзя удалить группу, которая имеет дочернюю группу;
- нельзя удалить группу в которой есть эндпоинты;
- нельзя удалить системные группы Profiled и Unknown.

Импорт

NAICE поддерживает импорт данных из CSV-файлов.

Предварительная подготовка перед импортом

1. Создайте или проверьте наличие необходимых связанных записей (например, профиль устройства).
2. Ознакомьтесь с требованиями к CSV-файлу:
 - Файл должен быть в кодировке UTF-8;
 - Разделитель полей: запятая (,)
 - Разделитель строк/текста: двойная кавычка (")
 - Заголовки и значения должны быть взяты в двойные кавычки (")

- Максимальный размер файла 2МБ.
3. Проверьте содержимое файла на наличие лишних кавычек перед импортом;
 4. Проверьте то что значения, содержащие двойную кавычку (") или слэш (/) правильно экранированы.
 - Значения, содержащие двойную кавычку (") экранируются с помощью \"
 - Значения, содержащие слэш (/) экранируются с помощью \

Правильное написание значений (с экранированием помощью \) на примере содержания файла для импорта набора команд TACACS:

"name:Required"	"description"	"permit_unmatch ed(true/false)"	"commands(Grant/command/argume nts/enabled;...)"
"command_set"	"\"Test command set\""	"false"	"PERMIT/\"show/vlan 1 2 \"/true"

Некорректное написание значений (без экранирования) на примере содержания файла для импорта набора команд TACACS:

"name:Required"	"description"	"permit_unmatch ed(true/false)"	"commands(Grant/command/argume nts/enabled;...)"
"command_set"	"Test command set"	"false"	"PERMIT/show/vlan 1 2 /true"



Игнорирование экранирования приведёт к некорректному распознаванию данных.

Порядок выполнения импорта

Для импорта данных из CSV-файла нажмите  на панели действий, расположенной над таблицей. После чего откроется окно:

Импорт

При импорте дублирующиеся данные не будут перезаписаны или отредактированы - система пропустит их. Если вы хотите изменить старые данные, удалите их из системы вручную перед импортом.

Внимательно ознакомьтесь с [Документацией](#) , чтобы импорт прошёл без ошибок.

Выберите файл*
Максимальный размер файла 2МБ

 **Загрузите** или перетащите сюда

Поле обязательно для заполнения

Источник данных *

NAICE

☐ Игнорировать существующие данные 

☐ Остановить импорт при первой ошибке

Отмена

Импорт

Рисунок 199. Окно Импорта

Импорт данных из CSV-файла выполняется в несколько шагов:

1. Выберите необходимый CSV-файл, перетащив его в поле загрузки или выбрав через проводник, нажав кнопку "**Загрузите**";



Измененный CSV-файл нужно загрузить повторно, чтобы применить правки.

2. Выберите источник данных, если он заранее не определён;
3. При необходимости активируйте флаги импорта:

Игнорировать существующие данные

- Если переключатель включен — дубликаты записей считаются предупреждением.
- Если переключатель выключен — дубликаты расцениваются как ошибка.

Остановить импорт при первой ошибке

- Если переключатель включен — импорт останавливается при первой же ошибке. Будут импортированы только записи, которые были успешно обработаны до её возникновения.

Если переключатель выключен — ошибочные строки пропускаются, импорт продолжается до конца. Будут импортированы только валидные записи.

4. Для того чтобы импорт начался, нажмите кнопку **"Импорт"**.



При импорте дублирующиеся данные перезаписаны или отредактированы не будут - система пропустит их. Если вы хотите изменить старые данные, удалите их из системы вручную перед импортом.

Просмотр отчета по импорту

Сразу после завершения обработки файла откроется окно отчёта по импорту.

Если все записи в файле были обработаны корректно, вы увидите окно:

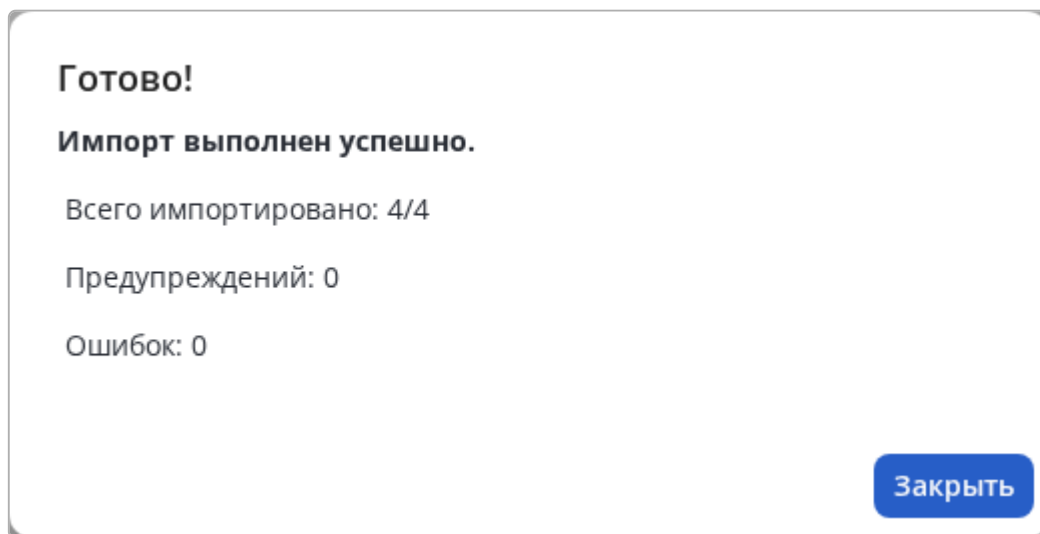


Рисунок 200. Отчет импорта (все записи обработаны корректно)

Блок с общей информацией содержит:

- **Всего импортировано** - Счётчик того, сколько записей было импортировано из общего импортируемого количества строк;
- **Предупреждений** - Количество возникших предупреждений;
- **Ошибок** - Количество возникших ошибок.

Если не все записи были обработаны корректно, вы увидите окно:

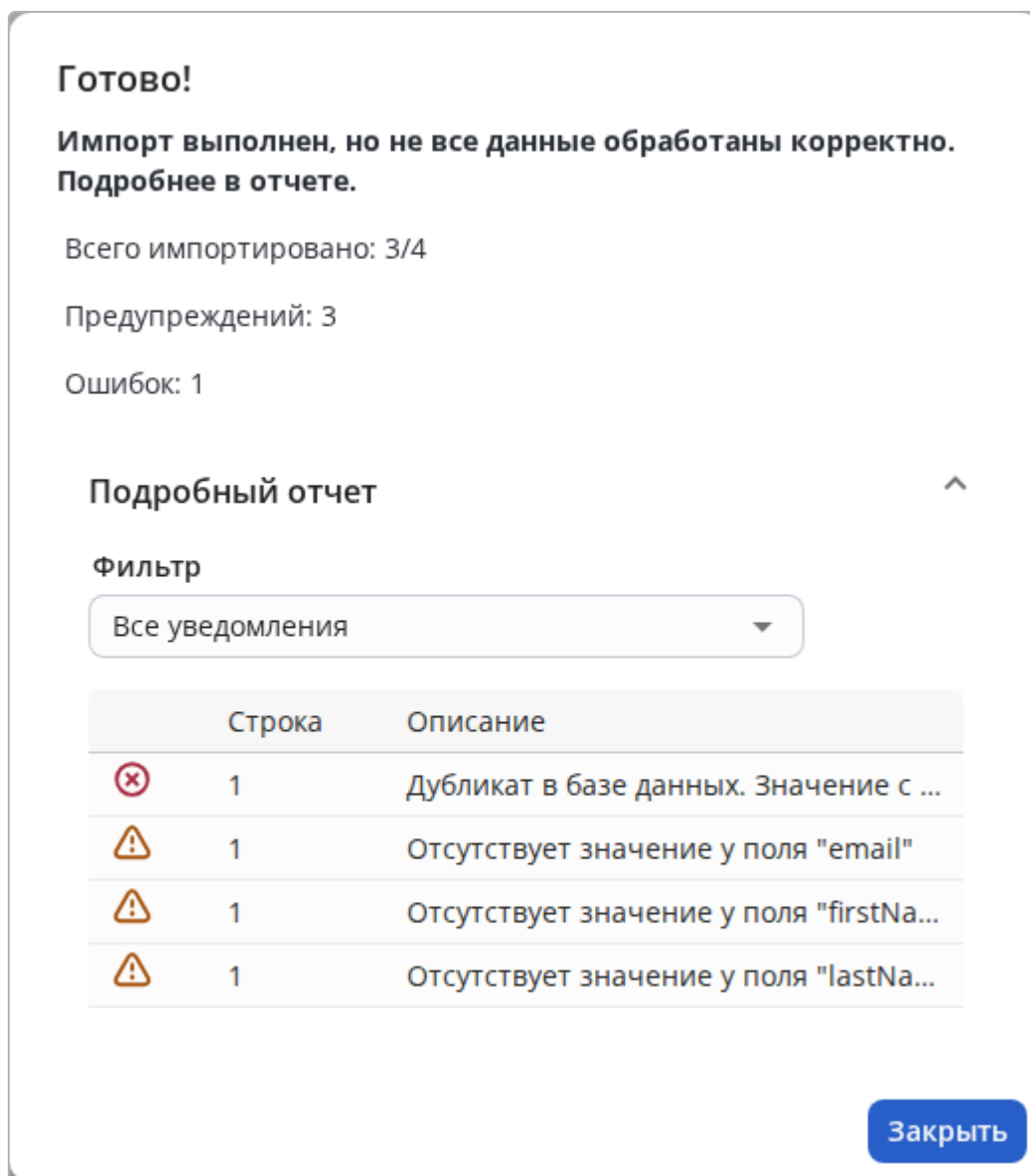


Рисунок 201. Отчет импорта (записи обработаны с ошибками/предупреждениями)

Подробный отчет содержит следующую информацию:

- **Фильтр** - Выпадающий список, в котором можно выбрать отображаемые уведомления (Все уведомления, Только ошибки или Только предупреждения)

Таблица уведомлений содержит колонки:

- **Строка** - Номер строки в CSV-файле, где обнаружена ошибка или предупреждение;
- **Описание** - Детальное текстовое объяснение ошибки или предупреждения.



Для просмотра полного текста описания наведите курсор мыши на соответствующую строку - во всплывающей подсказке отобразится полный текст сообщения об ошибке или предупреждении.

Особенности импорта групп эндпоинтов



Для групп эндпоинтов в качестве источника данных поддерживан только **NAICE**

В таблице ниже приведен список полей, их обязательность, описание и требования:

Поле	Описание	Требования
name:Required	Имя группы в формате полного пути до нее	Обязательное поле Формат: группа#подгруппа
description	Произвольное описание группы	Максимальная длина - 200 символов



Если в системе нет промежуточной корневой/дочерней группы, она создается автоматически

Пример корректного содержания файла:

"name:Required"	"description"
"test#test_1"	""

Получение CSV-файла шаблона описано далее в разделе "Экспорт".

Экспорт

NAICE поддерживает экспорт данных в формате CSV. Значения и заголовки обрамляются двойными кавычками, разделитель полей: запятая (,).

Процедура экспорта

Доступны два режима экспорта данных:

- **Экспорт всего** - Выгрузка всех записей текущего раздела. Системные записи исключаются из экспорта;
- **Экспорт выбранного** - Выгрузка только отмеченных чекбоксом записей.

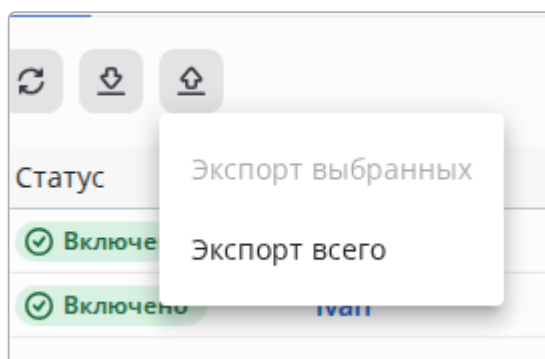


Рисунок 202. Окно выбора режима экспорта



Значения содержащие двойную кавычку (") или слэш (/) будут экранированы с помощью \".

Экспорт всех записей

На панели действий над таблицей нажмите  и выберите режим "Экспорт всего". В открывшемся окне подтвердите действие кнопкой "Экспорт":

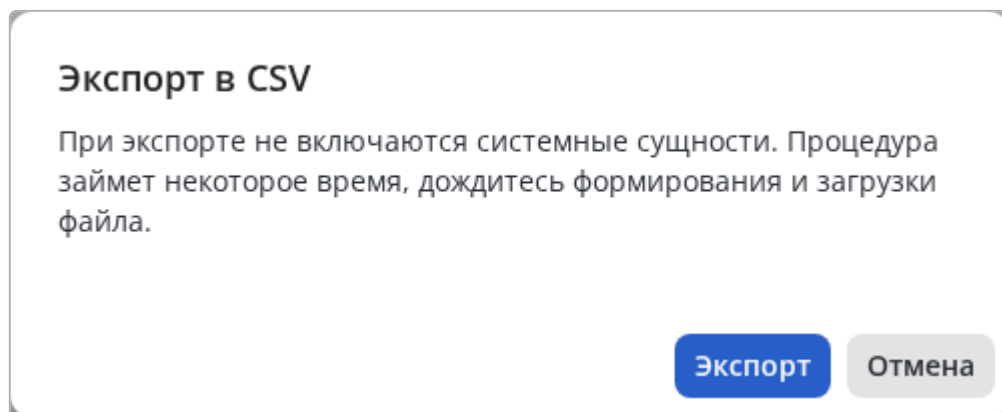


Рисунок 203. Экспорт всего

После нажатия кнопки "Экспорт" на устройство выгрузится файл, содержащий все записи из текущего раздела.

Экспорт выбранных записей

На панели действий над таблицей нажмите  и выберите режим "Экспорт выбранных". В открывшемся окне подтвердите действие кнопкой "Экспорт":

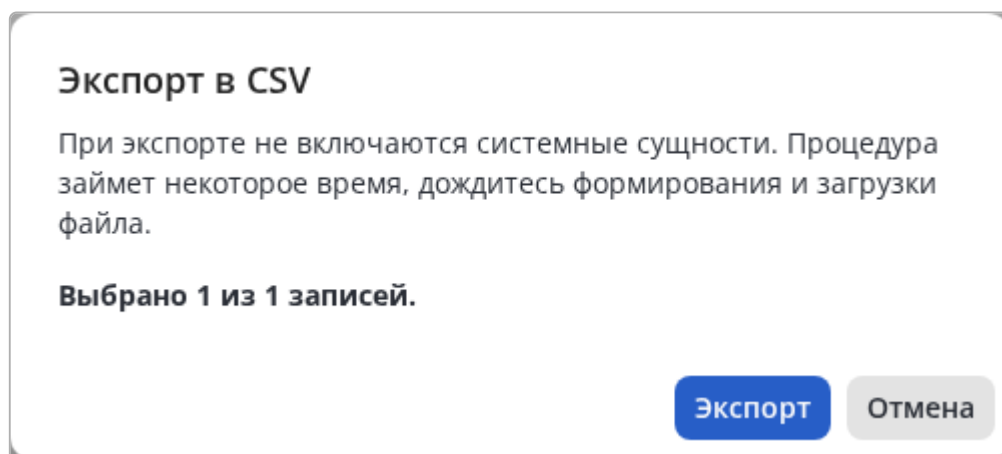


Рисунок 204. Экспорт выбранных

После нажатия кнопки "Экспорт" на устройство выгрузится файл, содержащий только отмеченные записи.



При **открытии** CSV-файлов в качестве разделителя полей **всегда** используйте **запятую (,)**, разделителем строк/текста могут быть **двойные кавычки (")** или **пустое значение**.

При **сохранении** CSV-файлов в качестве разделителя полей **всегда** используйте **запятую (,)**, а разделитель строк/текста - **пустое значение**.



Если при открытии файла использовался разделитель строк — двойная кавычка ("), то значения, содержащие символы двойной кавычки (") или слэша (/), экранированные как \", могут при сохранении получить лишнюю кавычку (") после (\"). Проверьте файл в текстовом редакторе и удалите лишние кавычки, если они появились.

Шаблон

Если в таблице отсутствуют записи (либо присутствуют только системные), при выборе режима **"Экспорт всего"** будет сформирован CSV-файл, содержащий исключительно заголовки столбцов. Данный файл может быть использован в качестве **шаблона** для подготовки данных перед импортом.

Особенности экспорта групп эндпоинтов



Имя группы эндпоинтов будет прописано в формате полного пути через разделитель - #.

Структура CSV-файла для групп устройств описана в разделе ["Особенности импорта групп эндпоинтов"](#).

Внешние источники идентификации

Описание

В качестве источника данных, используемого для аутентификации пользователей, помимо внутренней базы пользователей могут использоваться внешние источники идентификации данных о клиентах, такие как MS Active Directory, OpenLDAP и т.п.

Внешние источники идентификации могут использоваться в NAICE:

- **Для аутентификации пользователей системы (администраторов)** — внешний источник идентификации можно настроить **в качестве основного источника аутентификации на странице «Вход в систему»**. Пользователи системы смогут входить в веб-интерфейс NAICE под своими корпоративными учетными записями, а их данные (имя, фамилия, email) будут автоматически подтягиваться из атрибутов каталога.
- **Для аутентификации пользователей сети** — внешний источник используется при настройке [политик доступа](#). Пользователи проходят авторизацию на сетевом оборудовании через внешний каталог, а их атрибуты и группы могут применяться в условиях и профилях авторизации.

В данном разделе производится настройка подключения к внешним источникам и добавление групп пользователей и/или атрибутов, которые в дальнейшем могут быть использованы при настройке [Политики RADIUS](#), [Политики TACACS+](#) и при настройке [внешних ролей](#).

Просмотр внешних источников идентификации

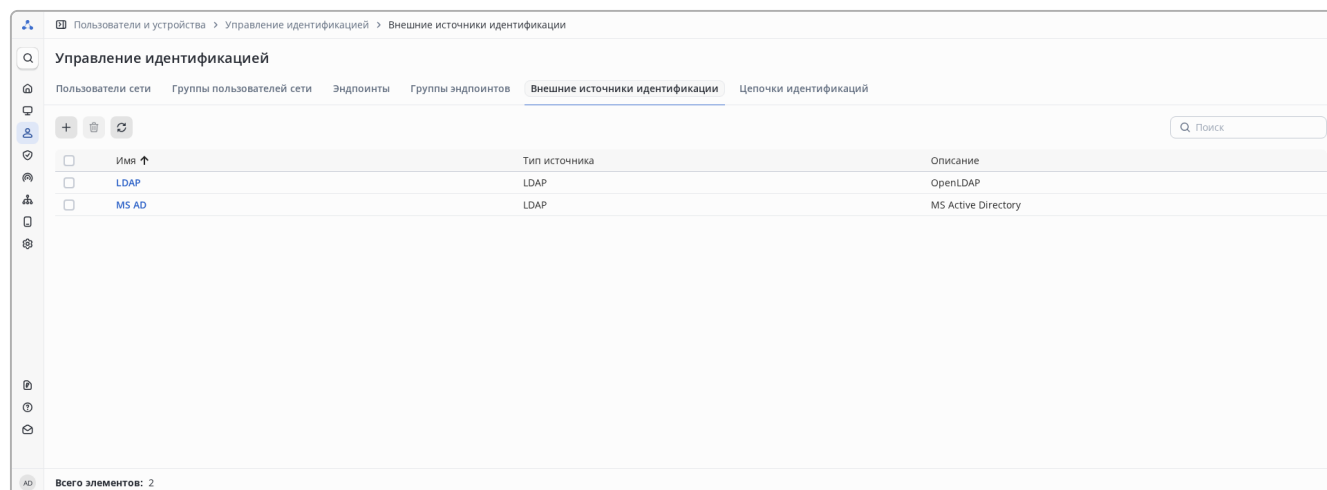


Рисунок 205. Просмотр внешних источников идентификации

На данной странице отображается таблица со списком внешних источников идентификации.

Таблица содержит колонки:

- **Имя** - наименование источника.
- **Тип источника** - тип источника.
- **Описание** - произвольное описание источника.

Возможна сортировка в прямом и обратном порядке по колонкам **Имя**, **Описание**. По умолчанию сортировка выполняется в прямом (алфавитном) порядке по полю **Имя**.

Элементы управления:

- **+** — Добавить новый элемент.
- **🗑️** — Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- **🔄** — Обновить данные таблицы.
- ☐ — Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).
- **↑** — Изменить текущий порядок сортировки.
- **🔍 Поиск** — Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.



Поддержано взаимодействие с источниками идентификации типа "Microsoft Active Directory" и "OpenLDAP".
Для каждого источника идентификации существуют определенные условия настройки и ограничения.

Настройка взаимодействия с каждым типом источника идентификации далее рассматривается отдельно.

Добавление источника идентификации типа Active Directory

Требования

При интеграции с источником типа MS Active Directory необходимо обеспечить выполнение следующих требований:

- DNS-сервер, который будет использоваться хостом с установленным NAICE, должен обеспечивать:
 - разрешение полного имени домена (например: EXAMPLE.ORG), в котором будет работать NAICE;
 - разрешение полного имени контроллеров AD (например: SRV1.EXAMPLE.ORG) обслуживающих домен;
 - возвращать ответ на DNS-запрос типа SRV со списком контроллеров обслуживающих домен.
- Минимальная версия контроллера Active Directory: Windows Server 2008 R2.
- Использование протокола NTLM контроллером Active Directory, на котором выполняется авторизация пользователей должна быть разрешена.
- В домене MS AD, с которым выполняется интеграция, необходимо добавить учетные записи компьютера и сервисного пользователя для взаимодействия с NAICE.
- Учетные записи пользователя и компьютера должны иметь пароль.



Если используется установка с резервированием, для корректного взаимодействия с Active Directory необходимо добавить отдельную учетную запись компьютера для каждой ноды NAICE. Сервисная учетная запись пользователя будет использоваться одинаковая для всех нод NAICE.



Задать пароль компьютера на сервере с MS Active Directory можно командой в оболочке PowerShell, входящей в состав Active Directory, запущенной с правами администратора:

```
Set-ADAccountPassword -Identity Computer-Name$ -Reset
```

- После выполнения команды необходимо два раза ввести пароль в окне терминала.

Если требуется указать пароль явно в команде:

```
Set-ADAccountPassword -Identity Computer-name$ -Reset -NewPassword  
(ConvertTo-SecureString -AsPlainText "password" -Force)
```



Имя компьютера необходимо указывать без доменной части, с окончанием на "\$".

Пароль должен отвечать требованиям сложности, настроенным в MS AD.

Учетная запись пользователя должна иметь права:

- Выполнять поиск в Active Directory
- Получать информацию о всех пользователях и группах домена



Права на запись информации в Active Directory не требуются.



В настройках пользователя необходимо отключить опцию "требовать смену пароля при первом подключении" (включена по умолчанию)

Обращение Eltex-NAICE к Active Directory выполняется по портам:

Протокол	Порт	Назначение	Примечание
UDP	53	DNS	Сервер, отвечающий за разрешение доменных имен может быть отдельным от сервера Active Directory
TCP/UDP	389	LDAP	Не используется шифрование передаваемых данных, поиск выполняется в рамках указанного локального домена
TCP/UDP	636	LDAPS	Используется для защищенного подключения с шифрованием передаваемых данных, поиск выполняется в рамках указанного локального домена
TCP/UDP	3268	LDAP GC	Не используется шифрование передаваемых данных, поиск выполняется по всему лесу доменов Active Directory
TCP/UDP	3269	LDAPS GC	Используется для защищенного подключения с шифрованием передаваемых данных, поиск выполняется по всему лесу доменов Active Directory
TCP/UDP	49152-65535	RPC Dynamic Port Range	Используется для проверки пароля пользователя при аутентификации в Active Directory, используется шифрование передаваемых данных

Ограничения реализации

Есть следующие ограничения реализации взаимодействия с Active Directory:

- Поиск пользователей, их атрибутов и групп возможен только в рамках одного глобального каталога Active Directory.
- В рамках указанного в настройках локального домена имя пользователя на клиентском устройстве допускается вводить в форматах:

<пользователь> без указания домена (при обращении в Active Directory домен будет добавлен автоматически).

- UPN: <пользователь>@<FQDN домен> или в формате пред-Windows 2000: <ИМЯ ДОМЕНА>\<пользователь>.
- Если пользователь принадлежит к другому домену глобального каталога Active Directory (отличному от указанного в настройках локального домена) - имя пользователя необходимо задавать на клиентском устройстве в формате UPN: <пользователь>@<FQDN домен>.
- Если у пользователя используется префикс, отличный от домена Active Directory, необходимо использовать только UPN формат: <пользователь>@<префикс домена>.
- В именах пользователей и их паролях допускаются только латинские символы, цифры, знаки препинания.
- Допускается использование групп пользователей, которые содержат пользователя не напрямую, а через включение другой группы, содержащей пользователя.
- Группа пользователя, которая указана в Active Directory как **Основная группа**, не может использоваться, так как не возвращается в списке групп пользователя при выполнении их поиска в Active Directory.

Добавление источника идентификации

Для добавления источника идентификации необходимо нажать  на панели действий над таблицей:

Пользователи и устройства > Управление идентификацией > Внешние источники идентификации > Добавление

← Добавление

1 Основные настройки 2 Группы Опционально 3 Атрибуты Опционально

Имя *
Введите имя

Описание
Введите описание
0 / 200

☐ Включить LDAPS ⓘ

Схема
Выберите схему
ACTIVE_DIRECTORY

Subject object class *
Person

Subject name attribute *
userPrincipalName

Group name attribute *
cn

Group object class *
group

Group map attribute *
memberOf

Subject in group attribute *
DISTINGUISHED_NAME

☐ Группы содержат пользователей
☒ Пользователи содержат группы

Сопоставление информации о пользователях системы ⓘ
Для схемы "ACTIVE_DIRECTORY" поля атрибутов заполняются автоматически

Атрибут имени
givenName

Атрибут фамилии
sn

Атрибут email
mail

Подключение
Имя домена * ⓘ
Введите текст

Admin dn * ⓘ
Введите текст

Admin password *
Введите текст

FQDN * ⓘ
Введите текст

Port *
Введите порт

Структура каталога
Subject search base * ⓘ
Введите текст

Group search base * ⓘ
Введите текст

Учетные записи компьютеров ⓘ
Hostname
Выберите hostname

Имя компьютера ⓘ
Введите имя компьютера

Пароль
Введите пароль

Список учетных записей *

Hostname	Компьютер	Действия
Данные отсутствуют		

Рисунок 206. Окно добавления источника идентификации

В данной форме представлены следующие параметры:

- Блок **Основные настройки**:
 - **Имя *** - наименование источника идентификации. Максимальная длина поля 63 знака.
 - **Описание** - описание. Максимальная длина поля 200 знаков.
 - **Включить LDAPS** - Включить использование защищённого соединения со службой каталогов по протоколу LDAPS (LDAP over TLS), обеспечивающего шифрование передаваемых данных и проверку сертификата сервера. Потребуется загрузка сертификатов сервиса в хранилище **доверенных сертификатов**. При включении данной опции становится доступна дополнительная опция **Доверять неизвестным источникам**.
 - **Доверять неизвестным источникам** - Доступно только при активации **Включить LDAPS**. Позволяет разрешить подключение к службе каталогов по протоколу LDAPS, с **недоверенным** или **неизвестным** сертификатом.



Рисунок 207. Включение опции "Включить LDAPS"

- Блок **Схема**:

- Выберите схему * - схема атрибутов источника идентификации. По умолчанию выбрана "ACTIVE_DIRECTORY", для данной схемы значение атрибутов предустановлено и не может быть изменено.

- Блок **Подключение**:

- Имя домена * - имя домена Active Directory, в котором будет выполняться авторизация пользователей. Необходимо указывать только короткое имя домена, в котором будет выполняться авторизация пользователей. Поле доступно только для схемы "ACTIVE_DIRECTORY". Максимальная длина поля 63 знака.
- Admin dn * - данные административного пользователя для взаимодействия с Active Directory. Имя пользователя необходимо указывать в формате UPN: <пользователь>@<домен> или в формате пред-Windows 2000: <ИМЯ ДОМЕНА>\<пользователь>. Максимальная длина поля 200 знаков.
- Admin password * - пароль административного пользователя. По умолчанию не отображается, для просмотра требуется нажать . Максимальная длина поля 200 знаков.
- FQDN * - полное имя домена или полное имя предпочтительного для обращений контроллера домена Active Directory. Максимальная длина поля 255 знаков. Если указан предпочтительный для выполнения обращений контроллер домена - обращения к нему будут выполняться пока он доступен. В случае его недоступности обращения будут выполняться на следующий сервер из списка обслуживающих доменов, полученный из DNS-запроса типа SRV.
- Port * - порт подключения к контроллеру(ам) домена (как правило используется TCP:389).

- Блок **Структура каталога**:

- Subject search base * - контекст для поиска атрибутов записей службы каталогов. Максимальная длина поля 200 знаков.
- Group search base * - контекст для поиска групп службы каталогов. Максимальная длина поля 200 знаков.



Оба поля имеют формат вида перечисления через запятую атрибут=значение, например "dc=example,dc=org". Если требуется ограничить поиск определенным подразделением (ou) необходимо указать его, например "ou=naice,dc=example,dc=org". Если есть несколько вложенных подразделений, то необходимо указать их все, начиная с самого дальнего от корня домена, например "ou=test,ou=naice,dc=example,dc=org" - это будет соответствовать структуре:

```
(dc)org
  \-(dc)example
    \-(ou)naice
      \-(ou)test
```

Подробнее о формате вводимых в этом поле данных можно узнать при наведении на  или по подсказке ниже.

Допустимые символы при вводе параметров Subject search base и Group search base:

- пробел,
- двойные кавычки (""),
- знак равенства (=),
- запятая (,),
- дефис (-),
- латинские буквы (a-z)(A-Z),
- кириллические буквы (а-я)(А-Я),
- цифры (0-9).

Ввод других элементов запрещен.

Система при сохранении автоматически удаляет пробелы возле знака равенства (=) и запятой (,), значение с пробелом берется в двойные кавычки. Значение атрибута, введенное слева от знака равенства (=), переводится в нижний регистр.

Пример:

Введённое значение	Сохранённое значение
ou=naice test, dc = example ,dc = org	ou="naice test",dc=example,dc=org
ou="naice test",dc = example,dc=org	ou="naice test",dc=example,dc=org

- Блок **Учетные записи компьютеров** - доступен только для схемы "ACTIVE_DIRECTORY". В этом блоке настраиваются учетные записи компьютеров для взаимодействия с Active Directory индивидуально для каждого узла NAICE. Имена компьютеров в списке не должны повторяться.
 - **Hostname** - выпадающий список с доступными узлами NAICE. Выберите узел, для которого настраивается учетная запись компьютера.
 - **Имя компьютера** - имя компьютера, который будет использоваться NAICE для подключения к Active Directory. Допустимые символы: латинские буквы, цифры, дефис. Максимальная длина: 63 символа. Имя должно быть уникальным в пределах списка.
 -

Пароль - пароль учетной записи компьютера. По умолчанию не отображается, для просмотра требуется нажать . Максимальная длина поля 200 знаков.

Для добавления записи заполните поля **Hostname**, **Имя компьютера**, **Пароль** и нажмите кнопку **Добавить**. Запись появится в таблице **Список учетных записей**.

Таблица **Список учетных записей** содержит колонки:

- **Hostname** - наименование узла NAICE.
- **Компьютер** - имя учетной записи компьютера.
- **Действия** - меню действий с записью, которое открывается нажатием на :
 - **Редактировать** - открыть диалог редактирования учетной записи. В диалоге доступна смена наименования узла, имени и пароля учетной записи компьютера.
 - **Удалить** - удалить учетную запись из списка.



Для схемы "ACTIVE_DIRECTORY" необходимо добавить хотя бы одну учетную запись компьютера.

- **Проверить связь с сервером** - проверить корректность настроек и связь с сервером Active Directory.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

- Блок **Сопоставление информации о пользователях системы** — настройка соответствия атрибутов из внешнего источника полям учетной записи пользователя системы в NAICE:
 - **Атрибут имени** — атрибут, значение которого будет подставляться в поле **Имя** внешней учетной записи.
 - **Атрибут фамилии** — атрибут, значение которого будет подставляться в поле **Фамилия**.
 - **Атрибут email** — атрибут, значение которого будет подставляться в поле **Email**.



Для схемы "ACTIVE_DIRECTORY" поля атрибутов заполняются автоматически:

- Атрибут имени — атрибут givenName.
- Атрибут фамилии — атрибут sn.
- Атрибут email — атрибут mail.



Если атрибуты в каталоге для пользователя не заполнены, соответствующие поля учетной записи останутся пустыми.

Если в каталоге атрибуты отсутствуют у конкретного пользователя, при проверке связи с сервером, даже если подключение к серверу успешно будет возвращена ошибка вида: Не удалось найти у пользователей поле "mail".

После заполнения всех необходимых данных станет активна кнопка **"Проверить связь с сервером"**.

При успешной проверки связи с сервером появится сообщение вида:

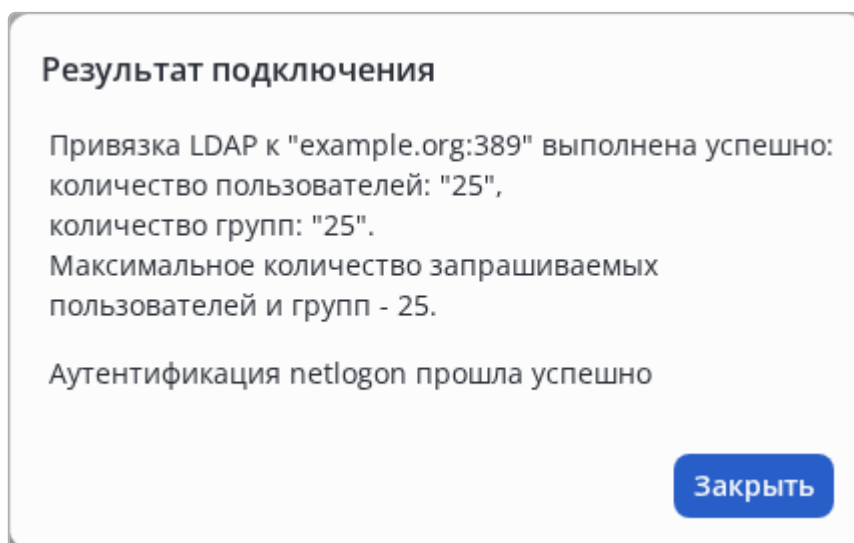


Рисунок 208. Привязка к LDAP выполнена успешно



Сообщение вида "Аутентификация netlogon прошла успешно" подтверждает возможность авторизации пользователей.



При проверке соединения запрашивается не более 25 предметов и групп, чтобы не вызывать лишнюю нагрузку на сервер, поэтому если реальных пользователей или групп больше все равно будет показано число "25" - это не свидетельствует о проблеме.

Добавление групп пользователей



Для возможности аутентификации пользователей сети через внешний источник идентификации добавление групп не является обязательным.

Группы можно использовать в политиках авторизации пользователей.



Для использования внешнего источника для аутентификации пользователей системы (администраторов) на странице **«Вход в систему»** **добавление групп обязательно**.

Без групп невозможно настроить внешние роли. При отсутствии внешних ролей вход в систему невозможен — будет возвращаться ошибка «У вас недостаточно прав».

После добавления источника идентификации кнопка **"Добавить"** примет значение **"Далее"**. Так же можно выполнить переход нажав на надпись **(2) Группы**, откроется страница:

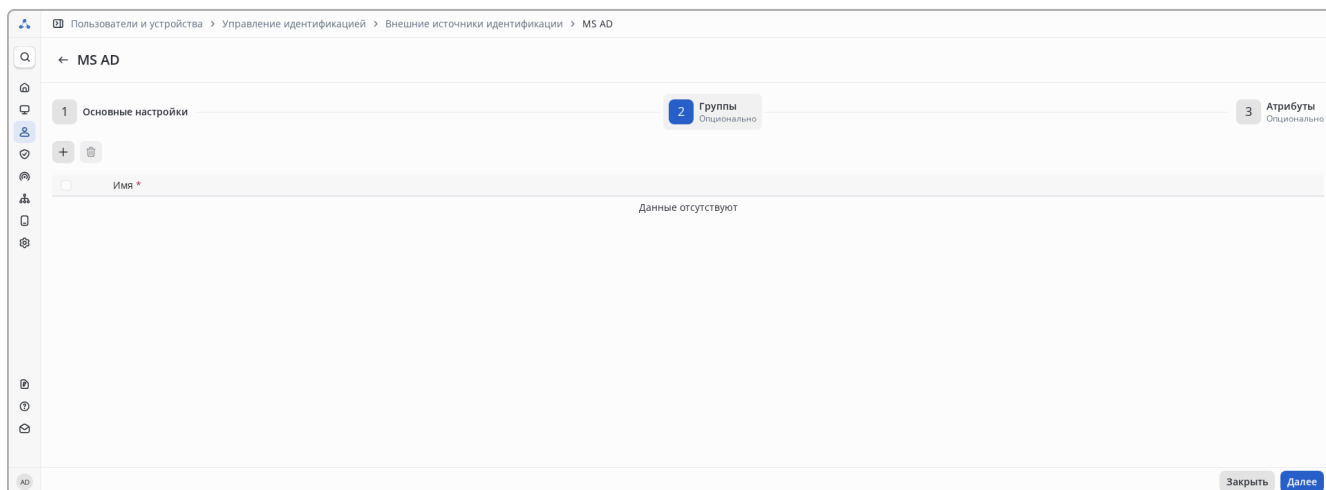


Рисунок 209. Пустая таблица групп

Таблица содержит колонки:

- **Имя *** - имя группы.

Элементы управления:

- **+** - добавить группу.
- **🗑️** - удалить выбранные чекбоксом группы (неактивно, пока не выбран хоть бы одна группа).
- **✎** - редактировать группу (не отображается, пока не добавлена хотя бы одна группа).
- **💾** - сохранить группу после редактирования (не отображается, пока не начато редактирование группы).

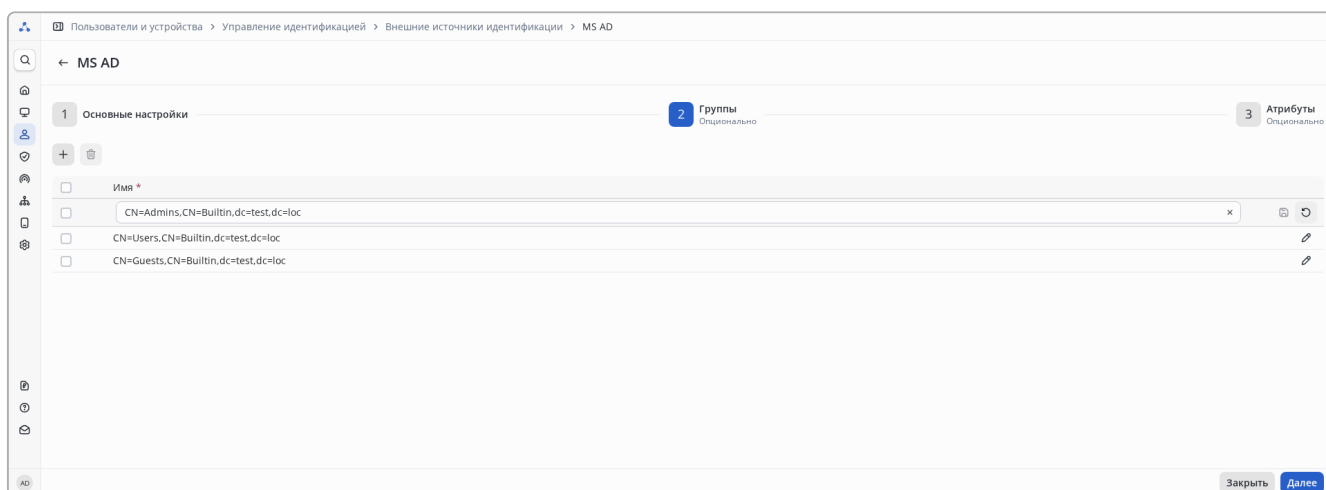


Рисунок 210. Таблица групп в режиме редактирования

После нажатия кнопку **+** откроется меню:

- **Добавить новую группу** - создать произвольную новую группу.
- **Выбрать группы из службы каталогов** - добавить группы из источника идентификации.

Добавить новую группу

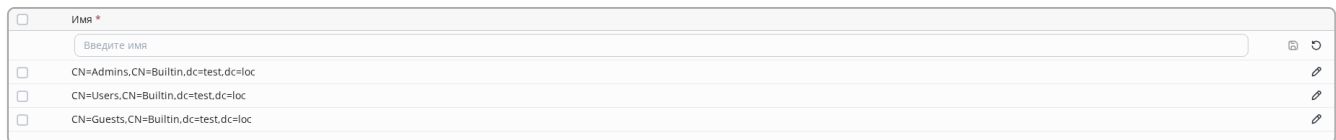


Рисунок 211. Добавить новую группу

В появившейся строке требуется указать произвольное имя группы. После заполнения имени группы станет активна кнопка сохранения. Требуется нажать её для добавления группы.

Выбрать группы из службы каталогов

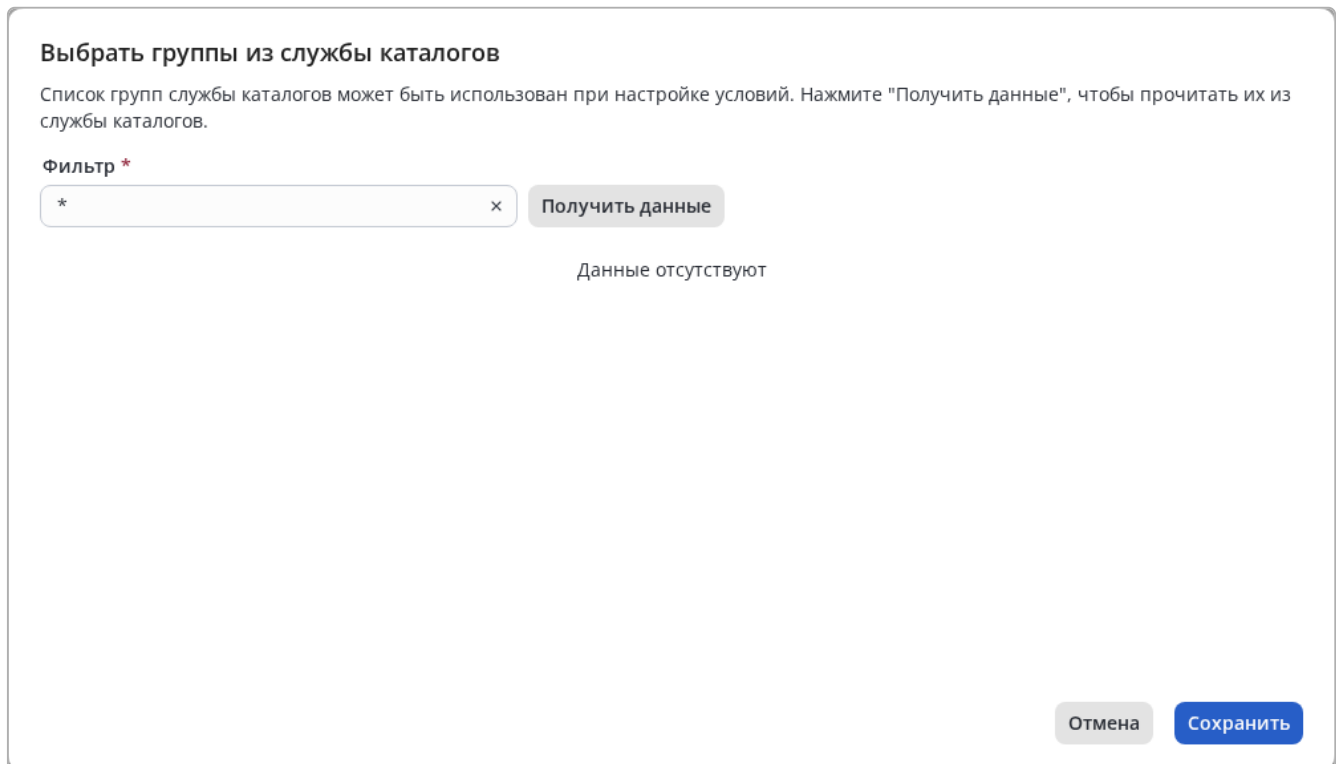


Рисунок 212. Окно выбора групп

В данном окне представлены следующие параметры:

- **Фильтр *** - фильтр для поиска групп, по умолчанию *, можно ввести название группы.
- **Получить данные** - получить данные с учетом фильтра

Выбрать группы из службы каталогов

Список групп службы каталогов может быть использован при настройке условий. Нажмите "Получить данные", чтобы прочитать их из службы каталогов.

Фильтр *

×
Получить данные

	Имя
☒	cn=admin1,ou=roles,dc=test,dc=loc
☐	cn=admin2,ou=roles,dc=test,dc=loc

Отмена
Сохранить

Рисунок 213. Окно выбора групп после получения данных

Требуется выбрать чекбоксом ☐ слева требуемые группы и нажать кнопку "Сохранить".



Ранее сохранённые группы, которые не были повторно выбраны в списке поиска, будут удалены при повторном сохранении других выбранных групп!

Добавление атрибутов



Для возможности аутентификации через внешний источник идентификации добавление атрибутов не является обязательным. Атрибуты можно использовать в политиках и профилях авторизации пользователей.

После добавления групп можно нажать кнопку "Далее" внизу справа экрана. Так же можно выполнить переход нажав на надпись (3) **Атрибуты**, откроется страница:

Пользователи и устройства > Управление идентификацией > Внешние источники идентификации > MS AD

← MS AD

1 Основные настройки

2 Группы Опционально

3 Атрибуты Опционально

Имя *	Тип *	Внутреннее имя *	Значение по умолчанию
Данные отсутствуют			

Закреть

Рисунок 214. Добавление атрибутов

Таблица содержит колонки:

- **Имя *** - имя атрибута, которое будет отображаться в словаре LDAP и использоваться при настройке логических условий и профилей авторизации. Можно указать произвольное, для удобства использования.
- **Тип *** - тип атрибута, возможные значения:
 - **INTEGER** - числовой,
 - **IP_4_ADDR** - адрес IPv4,
 - **STRING** - строковый.
- **Внутреннее имя *** - наименование атрибута в схеме Active Directory.
- **Значение по умолчанию** - значение атрибута, которое будет использоваться, если оно не получено от Active Directory.

Элементы управления:

- **+** - добавить атрибуты.
- **🗑** - удалить выбранные чекбоксом атрибуты (неактивно, пока не выбран хоть бы один атрибут).
- **✎** - редактировать атрибуты (не отображается, пока не добавлен хотя бы один).
- **💾** - сохранить атрибут после редактирования (не отображается, пока не начато редактирование).

The screenshot shows the 'MS AD' configuration page in a web application. The page has a breadcrumb trail: 'Пользователи и устройства > Управление идентификацией > Внешние источники идентификации > MS AD'. The main content area is divided into three tabs: '1 Основные настройки', '2 Группы (Опционально)', and '3 Атрибуты (Опционально)'. The '3 Атрибуты' tab is active. Below the tabs, there is a table with four columns: 'Имя *', 'Тип *', 'Внутреннее имя *', and 'Значение по умолчанию'. The table contains three rows of attributes: 'countryCode' (STRING), 'description' (STRING), and 'name' (STRING). Each row has a checkbox in the first column and an edit icon in the last column. At the bottom right of the table, there is a 'Закрыть' button.

Имя *	Тип *	Внутреннее имя *	Значение по умолчанию
☐ countryCode	STRING	countryCode	Введите текст
☐ description	STRING	description	
☐ name	STRING	name	

Рисунок 215. Таблица атрибутов в режиме редактирования

После нажатия кнопку **+** откроется меню:

- **Добавить новый атрибут** - создать произвольный новый атрибут.
- **Выбрать атрибут из службы каталогов** - добавить атрибут из источника идентификации.

Добавить новый атрибут

☐	Имя *	Тип *	Внутреннее имя *	Значение по умолчанию	
☐	Введите имя	STRING	Введите внутреннее имя	Введите текст	
☐	countryCode	STRING	countryCode		
☐	description	STRING	description		
☐	name	STRING	name		

Рисунок 216. Добавить новый атрибут

В появившейся строке добавления атрибута представлены следующие параметры:

- **Имя *** - произвольное имя атрибута, которое будет отображаться в словаре.
- **Тип *** - тип атрибута. Возможные значения:
 - **INTEGER** - числовой,
 - **IP_4_ADDR** - адрес IPv4,
 - **STRING** - строковый (по умолчанию).
- **Внутреннее имя *** - имя атрибута из источника идентификации.
- **Значение по умолчанию** - значение атрибута, которое будет использоваться, если оно не получено от Active Directory.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

После заполнения необходимых параметров станет активна кнопка сохранения. Требуется нажать её для добавления атрибута.

Выбрать атрибут из службы каталогов

Выбрать атрибуты из службы каталогов

Атрибуты записей службы каталогов могут быть использованы в условиях политик. Данные атрибуты задаются на текущей странице. Для извлечения атрибутов из службы каталогов необходимо выполнить их поиск, задав условие для поиска в фильтре. Например: "sp=*" или "objectClass=person" и т.д. По нажатию кнопки "Получить данные" будет получен список атрибутов и их значений. Полученные атрибуты можно выбрать и добавить в словарь для данного источника идентификации. Помните, что значения для выбранных атрибутов будут видны в логах сессии при обработке связанных запросов. Помните, что дефолтные значения атрибутов будут использоваться только если в ответе службы каталогов не указано значение для данного атрибута. Рекомендуется указывать определенное имя пользователя, который содержит искомые атрибуты и их значения, т.к. в противном случае атрибуты могут не показываться в результатах поиска.

Фильтр *

sp=*

Получить данные

Данные отсутствуют

Отмена

Сохранить

Рисунок 217. Выбор атрибутов из службы каталогов

В данном окне представлены следующие параметры:

- **Фильтр *** - фильтр для поиска атрибутов, по умолчанию `sp=*`. В качестве фильтра можно использовать выражения `<Атрибут>=<значение>`, если значение не важно надо указать `*`. Если у атрибута есть несколько значений - отображается только первое найденное.
- **Получить данные** - получить данные с учетом фильтра.



Как правило, дополнительные атрибуты пользователя добавляются после того, как им будут заданы значения, и до этого их вычитать нельзя.



Для выбора атрибутов из источника типа Active Directory рекомендуется использовать атрибут `userPrincipalName` или `sAMAccountName` с указанием определенной УЗ, которая точно содержит импортируемые записи. Например:

```
userPrincipalName=ivan.ivanov@example.org
```

```
sAMAccountName=ivan.ivanov
```



Для выбора атрибутов из источника типа LDAP рекомендуется использовать атрибут, который указан в настройке схемы `Subject name attribute`.

После получения данных по атрибутам:

Выбрать атрибуты из службы каталогов

Атрибуты записей службы каталогов могут быть использованы в условиях политик. Данные атрибуты задаются на текущей странице. Для извлечения атрибутов из службы каталогов необходимо выполнить их поиск, задав условие для поиска в фильтре. Например: "cn=*" или "objectClass=person" и т.д. По нажатию кнопки "Получить данные" будет получен список атрибутов и их значений. Полученные атрибуты можно выбрать и добавить в словарь для данного источника идентификации. Помните, что значения для выбранных атрибутов будут видны в логах сессии при обработке связанных запросов. Помните, что дефолтные значения атрибутов будут использоваться только если в ответе службы каталогов не указано значение для данного атрибута. Рекомендуется указывать определенное имя пользователя, который содержит искомые атрибуты и их значения, т.к. в противном случае атрибуты могут не показываться в результатах поиска.

Фильтр *

cn=*

Получить данные

☒	Имя	Тип	Значение
☒	isCriticalSystemObject	STRING	TRUE
☒	uSNCreated	INTEGER	56123

Отмена

Сохранить

Рисунок 218. Окно выбора атрибутов после получения данных

Требуется выбрать чекбоксом слева требуемые атрибуты и нажать кнопку "Сохранить".



Ранее сохранённые атрибуты, которые не были повторно выбраны в списке поиска, будут удалены при повторном сохранении других выбранных атрибутов!

Добавление источника идентификации типа Custom

Данный тип источника идентификации предназначен для интеграции с LDAP сервером, который может иметь произвольную схему.

Ограничения реализации

Есть следующие ограничения реализации взаимодействия с LDAP:

- Пароль пользователя должен храниться в ClearText.
- В именах пользователей и их паролях допускаются только латинские символы, цифры, знаки препинания.

Добавление источника идентификации

Для добавления источника идентификации необходимо нажать  на панели действий над таблицей, после чего откроется следующая страница, на которой надо будет выбрать схему **CUSTOM**:

Пользователи и устройства > Управление идентификацией > Внешние источники идентификации > Добавление

← Добавление

1 Основные настройки

2 Группы
Опционально

3 Атрибуты
Опционально

Имя *

Введите имя

Описание

Введите описание

0 / 200

☐ Включить LDAPS ⓘ

Схема

Выберите схему

CUSTOM

Subject object class *

InetOrgPerson

Subject name attribute *

uid

Group name attribute *

cn

Group object class *

groupOfNames

Group map attribute *

gidNumber

Subject in group attribute *

DISTINGUISHED_NAME

☐ Группы содержат пользователей
☒ Пользователи содержат группы

Сопоставление информации о пользователях системы ⓘ

Для схемы "CUSTOM" поля атрибутов заполняются вручную

Атрибут имени

Введите атрибут имени

Атрибут фамилии

Введите атрибут фамилии

Атрибут email

Введите атрибут email

Проверить связь с сервером

Подключение

Admin dn *

Введите текст

Admin password *

Введите текст

Имя хоста (IP) *

Введите текст

Port *

Введите порт

Структура каталога

Subject search base *

Введите текст

Group search base *

Введите текст

Отмена

Добавить

Рисунок 219. Окно добавления источника идентификации

В данной форме представлены следующие параметры:

- Блок **Основные настройки**:

- Имя * - наименование источника идентификации. (Максимальная длина поля - 64 знаков)
- Описание - описание.

- Блок **Схема**:

- Выберите схему * - схема атрибутов источника идентификации. По умолчанию выбрана ACTIVE_DIRECTORY требуется сменить на CUSTOM, что бы выбор значений атрибутов схемы стал доступным.
- Subject object class * - атрибут, определяющий класс пользователей.
- Subject name attribute * - атрибут, определяющий имя пользователя, которое он будет использовать в качестве логина на клиентском устройстве.
- Group name attribute * - атрибут, определяющий имя группы пользователя.
- Group object class * - атрибут, определяющий класс групп.
- Group map attribute * - атрибут, определяющий принадлежность к группе:

■

При выборе **Группы содержат пользователей** — это атрибут группы, который содержит ссылки на её участников.

- При выборе **Пользователи содержат группы** — это атрибут пользователя, который содержит ссылки на группы, в которые он входит.
- **Subject in group attribute *** - задает формат (атрибут), в котором перечислены пользователи или группы в атрибуте **Group map attribute**.
- **Группы содержат пользователей *** - выберите, если атрибут принадлежности пользователя к группе находится в атрибутах группы.
- **Пользователи содержат группы *** - выберите, если атрибут принадлежности пользователя к группе находится в атрибутах пользователя.
- Блок **Подключение**:
 - **Admin dn *** - данные административного пользователя для взаимодействия с LDAP (в формате "cn=admin,dc=example,dc=org").
 - **Admin password *** - пароль административного пользователя. По умолчанию не отображается, для просмотра требуется нажать .
 - **Имя хоста (IP) *** - IP-адрес или доменное имя сервера LDAP.
 - **Port *** - порт подключения (по умолчанию используется порт 389 для незащищенного или 636 для защищенного подключения).
- Блок **Структура каталогов**:
 - **Subject search base *** - контекст для поиска пользователей (предметов) службы каталогов.
 - **Group search base *** - контекст для поиска групп службы каталогов.

Оба поля имеют формат вида перечисления через запятую атрибут=значение, например dc=example,dc=org или ou=naice test,dc=example,dc=org.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

Максимальная длина поля **Имя** - 64 знаков, поля **Имя хоста (IP)** - 255 знаков, остальных полей - 200 знаков.

Допустимые символы при вводе параметров Subject search base и Group search base:

- пробел,
- двойные кавычки (""),
- знак равенства (=),
- запятая (,),
- дефис (-),
- латинские буквы (a-z)(A-Z),
- кириллические буквы (а-я)(А-Я),
- цифры (0-9).



Ввод других элементов запрещен.

Система при сохранении автоматически удаляет пробелы возле знака равенства (=) и запятой (,), значение с пробелом берется в двойные кавычки. Значение атрибута, введенное слева от знака равенства (=), переводится в нижний регистр.

Пример:

Введённое значение	Сохранённое значение
ou=naice test, dc = example ,dc = org	ou="naice test",dc=example,dc=org
ou="naice test",dc = example,dc=org	ou="naice test",dc=example,dc=org

- Блок **Сопоставление информации о пользователях системы** — настройка соответствия атрибутов из внешнего источника полям учетной записи пользователя системы в NAICE:
 - Атрибут имени — атрибут, значение которого будет подставляться в поле **Имя** внешней учетной записи.
 - Атрибут фамилии — атрибут, значение которого будет подставляться в поле **Фамилия**.
 - Атрибут email — атрибут, значение которого будет подставляться в поле **Email**.



Поля являются **необязательными**. Если атрибуты не указаны или в каталоге для пользователя они не заполнены, соответствующие поля учетной записи останутся пустыми.

Если атрибуты указаны в настройках, но в каталоге у найденных пользователей они отсутствуют, то при проверке связи с сервером будет возвращено предупреждение вида: **Не удалось найти у пользователей поле "mail"**.

После заполнения всех необходимых данных станет активна кнопка **"Проверить связь с сервером"**.

При успешной проверки связи с сервером появится сообщение вида:

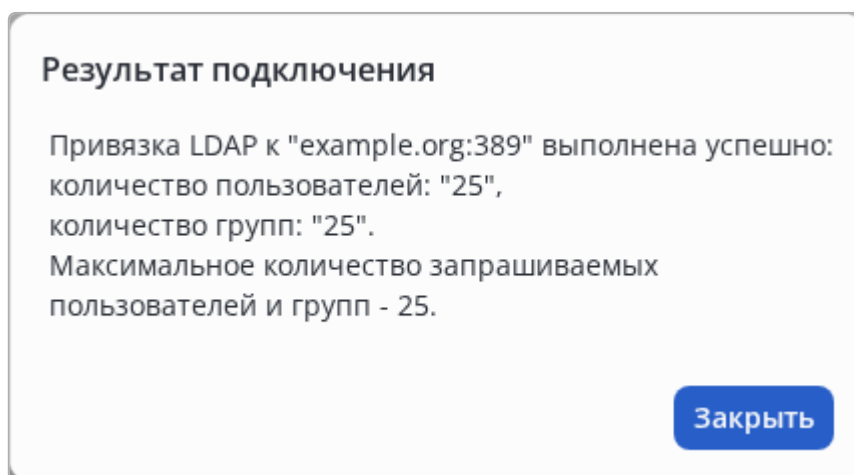


Рисунок 220. Привязка к LDAP выполнена успешно



При проверке соединения запрашивается не более 25 предметов и групп, что бы не вызывать лишнюю нагрузку на сервер, поэтому если реальных пользователей или групп больше будет показано число "25" - это не свидетельствует о проблеме.

Добавление групп пользователей



Для возможности аутентификации *пользователей сети* через внешний источник идентификации добавление групп не является обязательным.

Группы можно использовать в политиках авторизации пользователей.



При использовании внешнего источника для аутентификации *пользователей системы* (администраторов) на странице «Вход в систему» **добавление групп обязательно.**

Без групп невозможно настроить внешние роли. При отсутствии внешних ролей вход в систему невозможен — будет возвращаться ошибка «У вас недостаточно прав».

После добавления источника идентификации кнопка "Добавить" примет значение "Далее". Так же можно выполнить переход нажав на надпись **(2) Группы**, откроется страница:

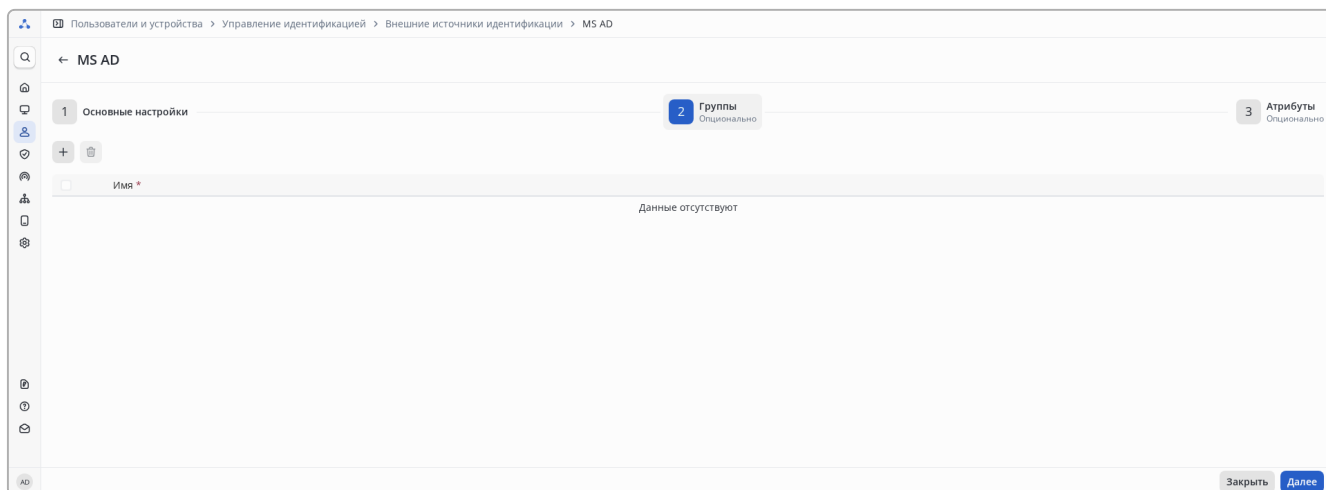


Рисунок 221. Пустая таблица групп

Элементы управления:

-  - добавить группу.
-  - удалить выбранные чекбоксом группы (неактивно, пока не выбрана хотя одна группа).

После нажатия кнопку  откроется меню:

- **Добавить новую группу** - создать произвольную новую группу.
- **Выбрать группы из службы каталогов** - добавить группы из источника идентификации.

Добавить новую группу

Рисунок 222. Добавить новую группу

В появившейся строке требуется указать произвольное имя группы. После заполнения имени группы станет активна кнопка сохранения. Требуется нажать её для добавления группы.

Выбрать группы из службы каталогов



Поиск групп осуществляется по атрибуту DN (Distinguished Name, уникальное имя) для дифференциации групп с одинаковым именем в разных ветках дерева службы каталогов. Если в схеме используется иной атрибут для **Group name attribute**, то запрос на поиск групп может быть выполнен некорректно. В таком случае добавление новой группы следует выполнять вручную.

Выбрать группы из службы каталогов

Список групп службы каталогов может быть использован при настройке условий. Нажмите "Получить данные", чтобы прочитать их из службы каталогов.

Фильтр *

*

×

Получить данные

Данные отсутствуют

Отмена

Сохранить

Рисунок 223. Окно выбора групп

В данном окне представлен следующие параметры:

- **Фильтр *** - фильтр для поиска групп, по умолчанию *, можно ввести название группы.
- **Получить данные** - получить данные с учетом фильтра.

Выбрать группы из службы каталогов

Список групп службы каталогов может быть использован при настройке условий. Нажмите "Получить данные", чтобы прочитать их из службы каталогов.

Фильтр *

*

×

Получить данные

Имя

☒

cn=admin1,ou=roles,dc=test,dc=loc

☐

cn=admin2,ou=roles,dc=test,dc=loc

Отмена

Сохранить

Рисунок 224. Окно выбора групп после получения данных

Требуется выбрать чекбоксом ☐ слева требуемые группы и нажать кнопку "Сохранить".



Ранее сохранённые группы, которые не были повторно выбраны в списке поиска, будут удалены при повторном сохранении других выбранных групп!

Добавление атрибутов



Для возможности аутентификации через внешний источник идентификации добавление атрибутов не является обязательным. Атрибуты можно использовать в политиках и профилях авторизации пользователей.

После добавления групп можно нажать кнопку **"Далее"** внизу справа экрана. Так же можно выполнить переход нажав на надпись **(3) Атрибуты**, откроется страница:

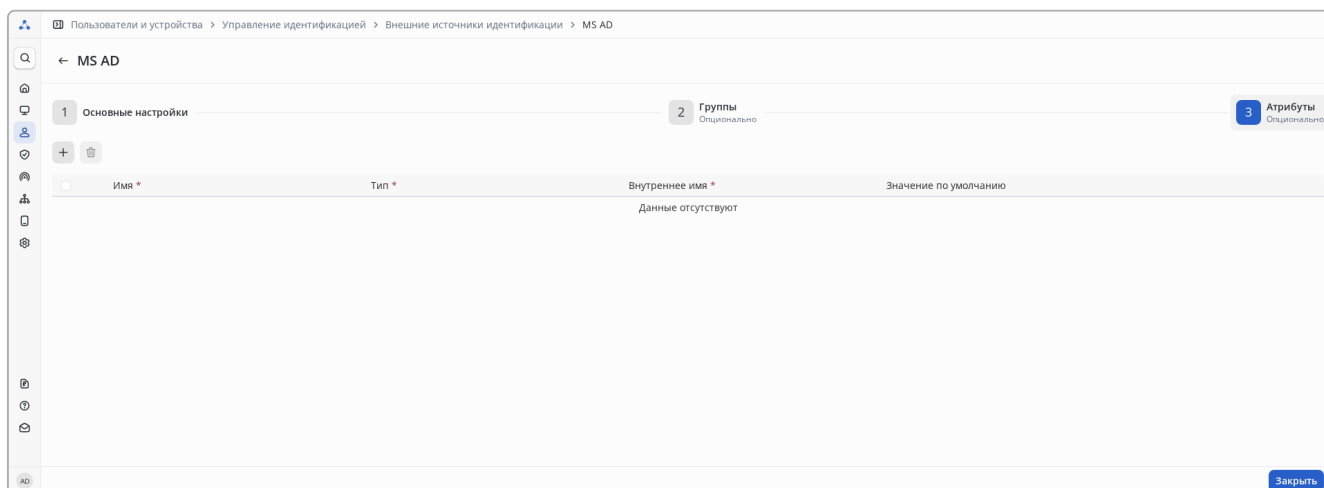


Рисунок 225. Добавление атрибутов

Элементы управления:

- - добавить атрибуты.
- - удалить выбранные чекбоксом атрибуты (неактивно, пока не выбран хоть один атрибут).

После нажатия кнопку откроется меню:

- **Добавить новый атрибут** - создать произвольный новый атрибут.
- **Выбрать атрибут из службы каталогов** - добавить атрибут из источника идентификации.

Добавить новый атрибут

☐	Имя *	Тип *	Внутреннее имя *	Значение по умолчанию	
☐	Введите имя	STRING	Введите внутреннее имя	Введите текст	
☐	countryCode	STRING	countryCode		
☐	description	STRING	description		
☐	name	STRING	name		

Рисунок 226. Добавить новый атрибут

В появившейся строке добавления атрибута представлены следующие параметры:

- **Имя *** - произвольное имя атрибута, которое будет отображаться в словаре.
- **Тип *** - тип атрибута. Возможные значения:
 - **INTEGER** - числовой,

- IP_4_ADDR - адрес IPv4,
- STRING - строковый (по умолчанию).
- Внутреннее имя * - имя атрибута из источника идентификации.
- Значение по умолчанию - значение атрибута, которое будет использоваться, если оно не получено от Active Directory.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

После заполнения необходимых параметров станет активна кнопка сохранения. Требуется нажать её для добавления атрибута.

Выбрать атрибут из службы каталогов

Выбрать атрибуты из службы каталогов

Атрибуты записей службы каталогов могут быть использованы в условиях политик. Данные атрибуты задаются на текущей странице. Для извлечения атрибутов из службы каталогов необходимо выполнить их поиск, задав условие для поиска в фильтре. Например: "sp=*" или "objectClass=person" и т.д. По нажатию кнопки "Получить данные" будет получен список атрибутов и их значений. Полученные атрибуты можно выбрать и добавить в словарь для данного источника идентификации. Помните, что значения для выбранных атрибутов будут видны в логах сессии при обработке связанных запросов. Помните, что дефолтные значения атрибутов будут использоваться только если в ответе службы каталогов не указано значение для данного атрибута. Рекомендуется указывать определенное имя пользователя, который содержит искомые атрибуты и их значения, т.к. в противном случае атрибуты могут не показываться в результатах поиска.

Фильтр *

Данные отсутствуют

Рисунок 227. Выбор атрибутов из службы каталогов

В данном окне представлен следующие параметры:

- Фильтр * - фильтр для поиска атрибутов, по умолчанию sp=*. В качестве фильтра можно использовать выражения <Атрибут>=<значение>, если значение не важно надо указать *. Если у атрибута есть несколько значений - отображается только первое найденное. При выполнении поиска в LDAP, как правило, можно указать uid=* или givenName=*.
- Получить данные - получить данные с учетом фильтра.

После получения данных по атрибутам:

Выбрать атрибуты из службы каталогов

Атрибуты записей службы каталогов могут быть использованы в условиях политик. Данные атрибуты задаются на текущей странице. Для извлечения атрибутов из службы каталогов необходимо выполнить их поиск, задав условие для поиска в фильтре. Например: "cn=*" или "objectClass=person" и т.д. По нажатию кнопки "Получить данные" будет получен список атрибутов и их значений. Полученные атрибуты можно выбрать и добавить в словарь для данного источника идентификации. Помните, что значения для выбранных атрибутов будут видны в логах сессии при обработке связанных запросов. Помните, что дефолтные значения атрибутов будут использоваться только если в ответе службы каталогов не указано значение для данного атрибута. Рекомендуется указывать определенное имя пользователя, который содержит искомые атрибуты и их значения, т.к. в противном случае атрибуты могут не показываться в результатах поиска.

Фильтр *

cn=*

Получить данные

☒	Имя	Тип	Значение
☒	isCriticalSystemObject	STRING	TRUE
☒	uSNCreated	INTEGER	56123

Отмена

Сохранить

Рисунок 228. Окно выбора атрибутов после получения данных

Требуется выбрать чекбоксом слева требуемые атрибуты и нажать кнопку **"Сохранить"**.



Ранее сохранённые атрибуты, которые не были повторно выбраны в списке поиска, будут удалены при повторном сохранении других выбранных атрибутов!

Редактирование источника идентификации

Для редактирования ранее добавленного источника идентификации на странице просмотра необходимо нажать на имя источника в таблице:

☐	Имя ↑
☐	LDAP
☐	MS AD

Рисунок 229. Гиперссылка на страницу редактирования внешнего источника идентификации

После этого откроется страница редактирования источника, аналогичная странице добавления:

Пользователи и устройства > Управление идентификацией > Внешние источники идентификации > MS AD

← MS AD

1 Основные настройки 2 Группы Опционально 3 Атрибуты Опционально

Имя *
MS AD

Описание
MS Active Directory
19 / 200

☐ Включить LDAPS ⓘ

Схема

Выберите схему
CUSTOM

Subject object class *
Person

Subject name attribute *
userPrincipalName

Group name attribute *
cn

Group object class *
group

Group map attribute *
memberOf

Subject in group attribute *
DISTINGUISHED_NAME

☐ Группы содержат пользователей
☒ Пользователи содержат группы

Сопоставление информации о пользователях системы ⓘ
Для схемы "CUSTOM" поля атрибутов заполняются вручную

Атрибут имени
Введите атрибут имени

Атрибут фамилии
Введите атрибут фамилии

Атрибут email
Введите атрибут email

Проверить связь с сервером

Подключение

Admin dn * ⓘ
uid=admin,ou=system

☐ Сменить Admin password

Имя хоста (IP) * ⓘ
216.133.112.166

Port *
389

Структура каталога

Subject search base * ⓘ
DC=test,DC=loc

Group search base * ⓘ
DC=test,DC=loc

Заккрыть Далее

Рисунок 230. Страница редактирования источника идентификации

Для смены Admin password необходимо активировать переключатель **"Сменить Admin password"**, после чего ввести желаемый пароль в соответствующее поле. Для смены пароля учетной записи компьютера нажмите **Редактировать** в колонке **Действия** таблицы **Список учетных записей**, активируйте переключатель **Сменить пароль** и введите новый пароль.

После внесения изменений нажмите кнопку **"Сохранить"**. Кнопка скрыта, пока не будет изменено хотя бы одно поле.

Кнопка **"Отмена"** осуществляет сброс внесенных изменений до исходного состояния.

Удаление источника идентификации

Для удаления одного или нескольких источников идентификации необходимо на странице просмотра через чекбокс ☐ выбрать необходимые источники и на панели действий над таблицей нажать на  .

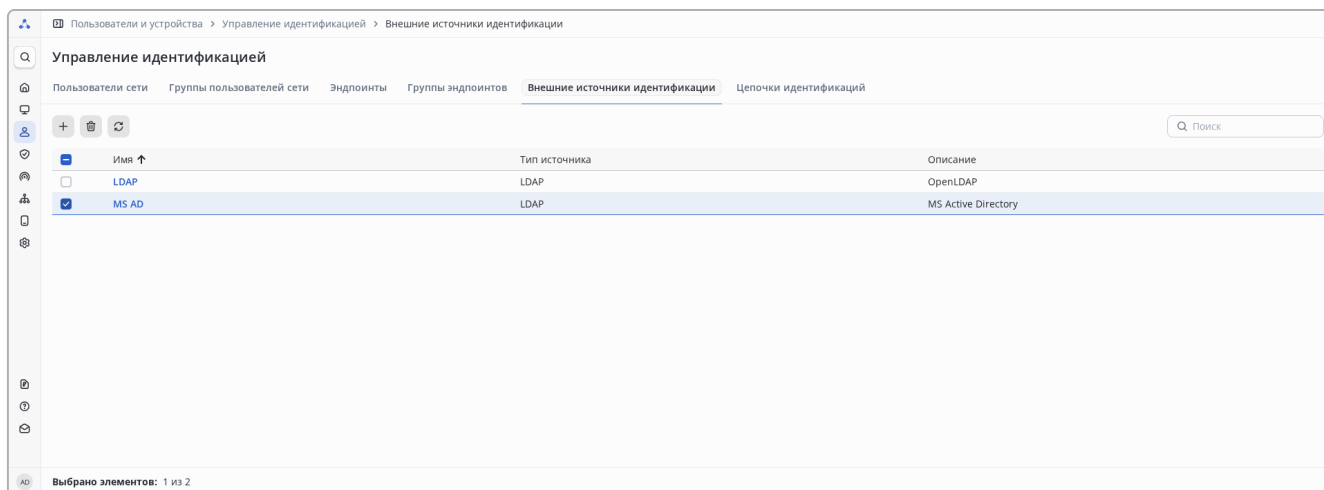


Рисунок 231. Выбор источников для удаления



При удалении внешнего источника также будут удалены все внешние учетные записи пользователей полученные из этого источника.

Удаление внешнего источника требует подтверждения:

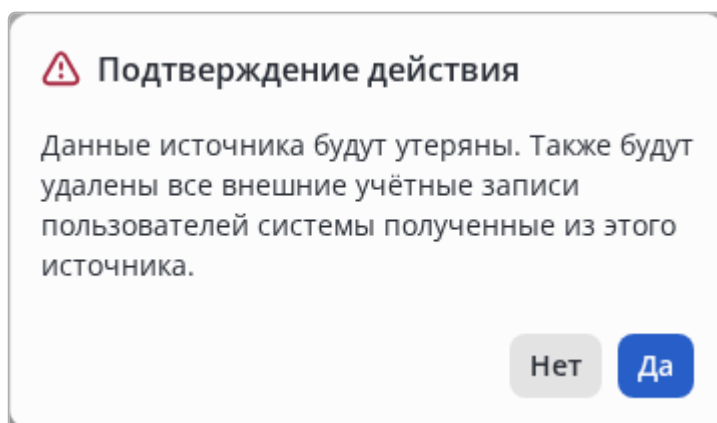


Рисунок 232. Подтверждение удаления внешнего источника

Цепочки идентификаций



Некоторые функции, описанные на данной странице, доступны только при наличии расширенной лицензии. Такие функции помечены специальными метками в виде цветных значков рядом с наименованием.

Описание

Цепочки идентификаций (цепочки источников идентификаций) используются в политиках аутентификации при настройке [Политики RADIUS](#) и [Политики TACACS+](#). Они определяют, в каких источниках и в каком их порядке искать пользователей при аутентификации.

В качестве источников пользователей поддерживаны [внутренняя база данных пользователей](#) и [внешние источники идентификации](#), такие как MS AD и OpenLDAP.

ADVANCED

Для portalной авторизации в качестве источников дополнительно используются источники [Пользователи портала](#) и [Гостевые эндпоинты](#).

Просмотр цепочек идентификаций

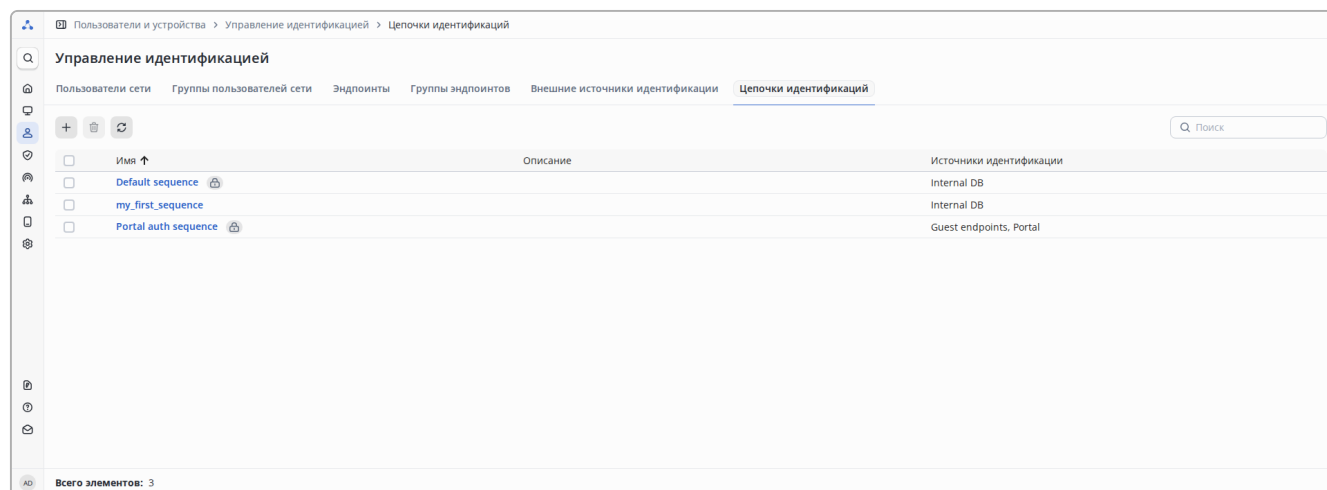


Рисунок 233. Просмотр цепочек идентификации

На данной странице содержится таблица со списком всех цепочек идентификаций.

Таблица содержит колонки:

- **Имя** - название цепочки.
 -  - Данная запись является системной и недоступна для удаления или редактирования.
- **Тип** - тип цепочки идентификации. Возможны значения "Создана администратором" или "Системная".
- **Описание** - произвольное описание цепочки.
- **Источники идентификации** - список источников учетных данных пользователей, которые настроены в данной цепочке.

Возможна сортировка в прямом и обратном порядке по колонкам **Имя** и **Описание**. По умолчанию сортировка выполняется в прямом (алфавитном) порядке по полю **Имя**.

Элементы управления:

-  — Добавить новый элемент.
-  — Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
-  — Обновить данные таблицы.
- ☐ — Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).
-  — Изменить текущий порядок сортировки.
-  **Поиск** — Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.



Нельзя переименовать или удалить системные цепочки идентификации: "[Default sequence, Portal auth sequence]"

Добавление цепочки идентификаций

Для добавления цепочки идентификаций  в левой части поля над таблицей страницы просмотра, откроется следующая страница:

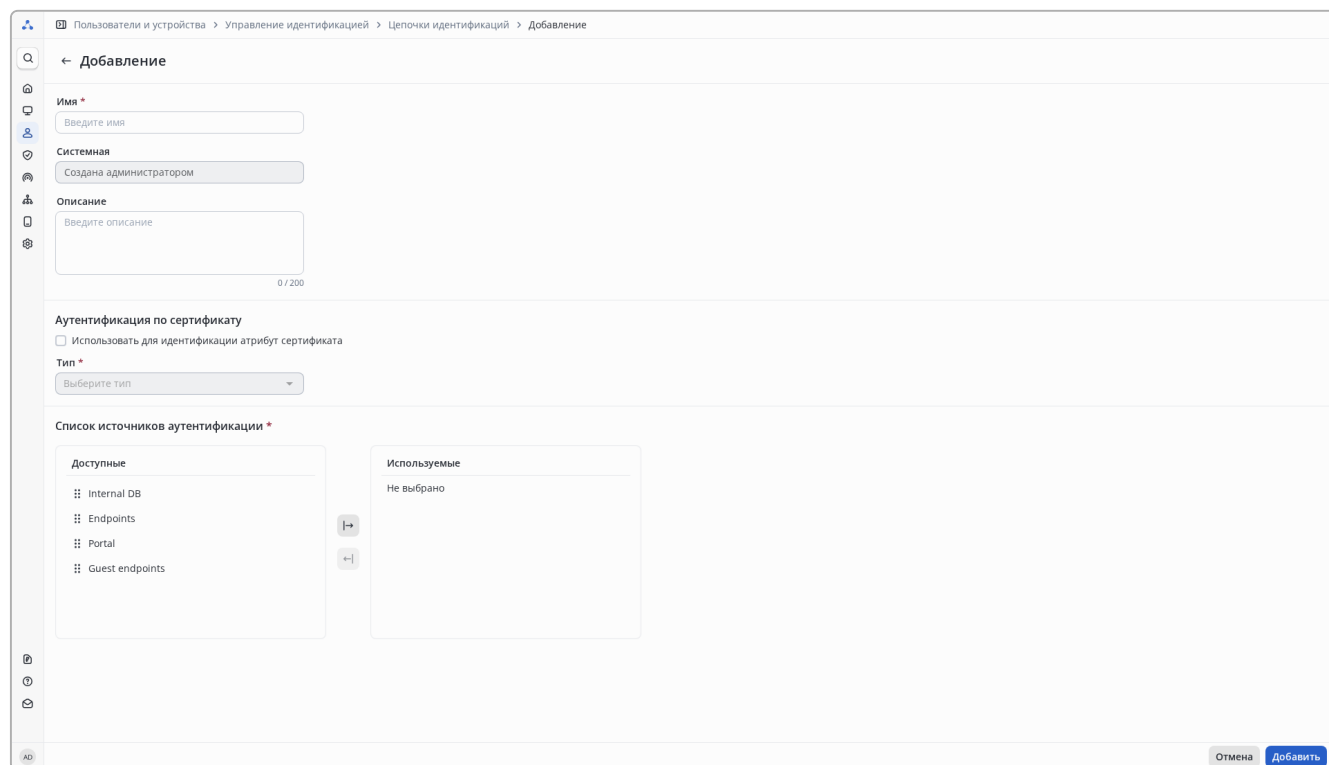


Рисунок 234. Страница добавления цепочки

Для заполнения доступны следующие параметры:

- **Имя *** - название цепочки. Максимальная длина - 100 символов.
- **Тип** - тип цепочки идентификации. Все вручную созданные цепочки идентификации имеют значение "Создана администратором", изменить его нельзя.
- **Описание** - произвольное описание цепочки. Максимальная длина - 200 символов.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

Аутентификация по сертификату



Данная настройка может быть использована только при аутентификации пользователя по протоколу EAP-TLS.

В данном разделе настраивается проверка соответствия выбранного поля сертификата пользователя атрибуту в источнике идентификации. Выбранное значение атрибута из сертификата пользователя сравнивается с атрибутом пользователя, указанным в поле "Subject Name Attribute" во внешнем источнике идентификации. В случае использования внутреннего источника идентификации (Internal DB) сравнение выполняется со значением указанным в поле "Логин" пользователя.

Использовать для идентификации атрибут сертификата - включает возможность выбора атрибута, который будет использоваться для проверки в качестве имени пользователя. При отключенной

настройке используется значение атрибута User-Name из RADIUS-запроса аутентификации пользователя.

После включения настройки станет доступным поле **Атрибут**.

- **Атрибут** - поле в сертификате, содержащее данные для идентификации пользователя.

Поле может принимать следующие значения:

- Subject - Common Name
- Subject - Serial Number
- Subject
- Subject Alternative Name - Email
- Subject Alternative Name - DNS
- Subject Alternative Name - UPN

Список источников идентификации

В этом разделе выбираются источники аутентификации, которые будут использоваться.



Доступность некоторых источников зависит от уровня текущей лицензии.

- **Доступные** - список всех источников, доступных для выбора.
- **Используемые** - список источников, которые будут применяться для аутентификации.

Для выбора источника учетных данных пользователей захватите его курсором мышки за поле  и переместите его из левой колонки "Доступные" в правую "Используемые".

Элементы управления:

-  - выбрать все доступные источники аутентификации.
-  - удалить все выбранные источники аутентификации.



Поиск пользователя по логину выполняется во всех доступных источниках, указанных в "Используемые". Поиск выполняется сверху вниз по списку. Поиск завершается как только совпадающий логин пользователя будет найден в источнике.

Редактирование цепочки идентификаций

Для редактирования нажмите на имя цепочки идентификаций в таблице.

☐	Имя ↑	
☐	Default sequence	
☐	my_first_sequence	
☐	Portal auth sequence	

Рисунок 235. Гиперссылка на страницу редактирования цепочки идентификации

Откроется страница редактирования.

Пользователи и устройства > Управление идентификацией > Цепочки идентификаций > my_first_sequence

← my_first_sequence

Имя *

my_first_sequence

Системная

Создана администратором

Описание

Введите описание

0 / 200

Аутентификация по сертификату

☐ Использовать для идентификации атрибут сертификата

Тип *

Выберите тип

Список источников аутентификации *

Доступные

- Endpoints
- Portal
- Guest endpoints

Используемые

- Internal DB

AD

Рисунок 236. Страница редактирования цепочки идентификации

После редактирования нажмите **Сохранить**. Кнопка будет неактивной пока не будет внесено хотя бы одно изменение.

Удаление цепочки идентификаций

Для удаления одной или нескольких цепочек идентификации необходимо выбрать их через чекбокс ☐ и в левом верхнем углу над таблицей нажать на .

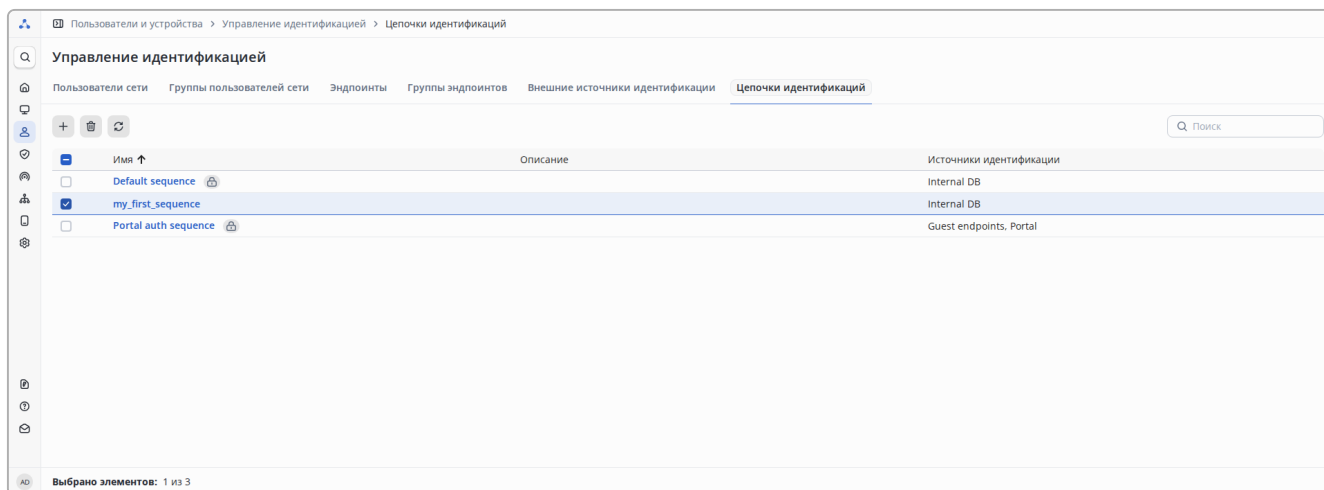


Рисунок 237. Выбор цепочек для удаления



Удаление элементов требует подтверждения в модальном окне. Выбранные элементы будут удалены только после явного подтверждения операции.

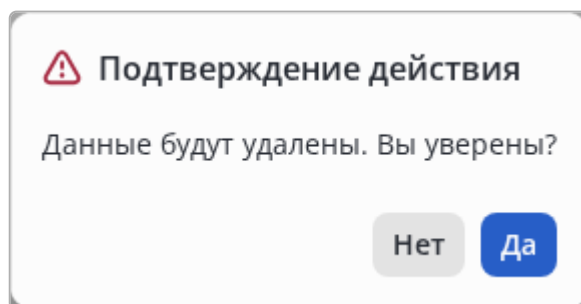


Рисунок 238. Диалоговое окно подтверждения действия



Вы не сможете удалить цепочку, которая используется в политиках аутентификации какого-либо набора политик. Для удаления цепочки необходимо сначала удалить ее из политики аутентификации, а затем удалить саму цепочку.

Доступ к сети

Элементы политик

Профили авторизации



Некоторые функции, описанные на данной странице, доступны только при наличии расширенной лицензии. Такие функции помечены специальными метками в виде цветных значков рядом с наименованием.

Описание

Профили авторизации позволяют определить действия, которые необходимо выполнить после аутентификации пользователя. Доступно как разрешение доступа (ACCESS-ACCEPT), так и его запрет (ACCESS_REJECT).

Поддержано добавление в ответ ACCESS-ACCEPT после аутентификации клиента атрибутов:

- Динамически назначаемый VLAN клиента, с использованием стандартных IETF атрибутов (Tunnel-Medium-Type: IEEE-802, Tunnel-Type: VLAN, Tunnel-Private-Group-Id: <VLAN ID>) или атрибутов, настроенных в профиле устройства.
- Имя ACL, которую необходимо назначить клиенту (ACL с данным именем должна быть настроена на сетевом оборудовании).
- Ссылка редиректа на портал и ACL, применяемая до аутентификации клиента ("pre-auth ACL").
- Любой другой RADIUS-атрибут через Расширенные настройки атрибутов.

Просмотр списка доступных профилей авторизации

Имя ↑	Профиль сетевого устройства	Описание
DenyAccess	DEFAULT	
MES auth	Elitex MES	
PermitAccess	DEFAULT	
Portal web redirect profile	Elitex WLC	

Рисунок 239. Таблица с перечнем профилей авторизации на странице просмотра

Снизу расположена таблица профилей авторизации, которая содержит колонки:

- **Имя** - название профиля авторизации.
- **Профиль сетевого устройства** - выбранный профиль сетевого устройства.

Описание - произвольное описание.

Возможна сортировка в прямом и обратном порядке по любой колонке. По умолчанию сортировка выполняется в прямом (алфавитном) порядке по колонке "Имя".

Элементы управления:

-  — Добавить новый элемент.
-  — Дублировать выбранный чекбоксом элемент. Становится активным, если выбран только один элемент в списке.
-  — Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
-  — Обновить данные таблицы.
- ☐ — Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).
-  — Изменить текущий порядок сортировки.
-  Поиск — Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.

Добавление профиля авторизации

Для добавления профиля авторизации нажмите , откроется окно добавления профиля авторизации.

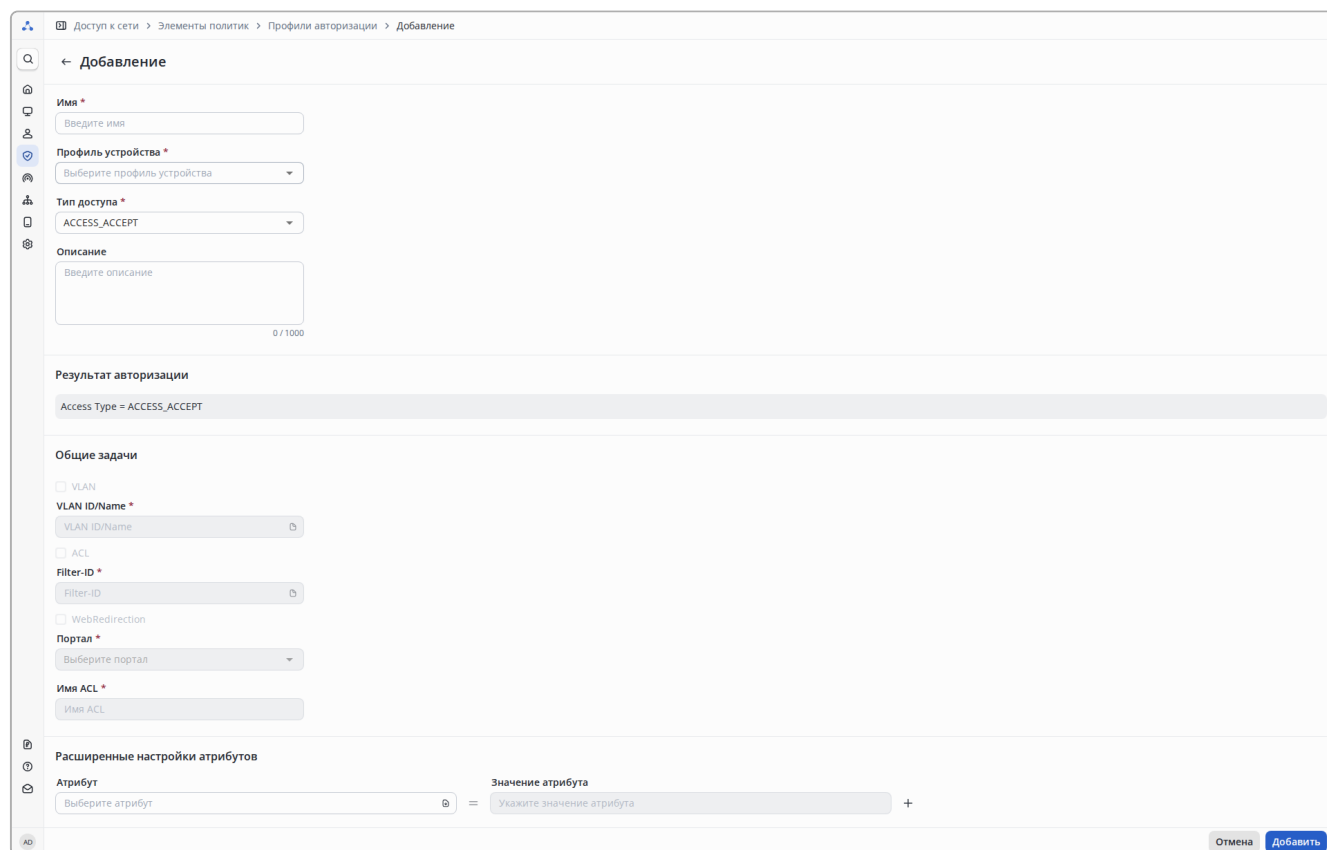


Рисунок 240. Окно добавления профиля авторизации

Имя * - название, должно быть уникально. Максимальная длина - 100 символов.

- Профиль * - [профиль сетевого устройства](#). В профиле сетевого устройства настраивается разрешение на выдачу клиентского VLAN и ACL, а также какие для этого использовать RADIUS-атрибуты.
- Тип доступа * - тип доступа, при котором будет применяться профиль авторизации. Выпадающий список из двух элементов: ACCESS_ACCEPT (по умолчанию) и ACCESS_REJECT.
- Описание - произвольное описание. Максимальная длина - 200 символов.
- Результат авторизации - визуализация атрибутов в результирующем RADIUS-пакете на основе настроек "Типа доступа", "Общих задач" и "Расширенных настроек атрибутов".
- Общие задачи - включение и настройка распространенных сценариев при авторизации пользователя. Сценарии объединяют под собой один или несколько атрибутов, настраиваемых в [профиле устройства](#). По умолчанию все сценарии отключены.



Для возможности настройки Общие задач необходимо, чтобы они были разрешены в [профиле сетевого устройства](#), который используется в профиле авторизации. В противном случае их настройка будет недоступна.

- VLAN - включить динамическое назначение VLAN пользователю.
 - VLAN ID/Name - номер или имя VLAN, выдаваемое в атрибуте "Tunnel-Private-Group-Id" или другом атрибуте, настроенном в профиле устройства.
- ACL - включить выдачу имени списка доступа пользователю.
 - Filter-ID - наименование списка доступа, назначаемое пользователю. Должно быть настроено с соответствующим наименованием на сетевом оборудовании, к которому подключается пользователь.
- **ADVANCED** WebRedirection - включить перенаправление пользователя на заданный портал.
 - Портал - [портал](#), на который пользователь будет перенаправлен при подключении к сети.
 - Имя ACL - имя списка контроля доступа, который должен быть назначен при перенаправлении на портал до момента аутентификации пользователя ("pre-auth ACL"). Сам ACL должен быть предварительно настроен на оборудовании.
- Расширенные настройки атрибутов - ручная настройка выдачи RADIUS-атрибутов. Рекомендуются только в том случае, когда для определенного результата авторизации не доступен сценарий из списка Общие задач.

* - поля, обязательные для заполнения.

После ввода необходимых данных и выбора доступных протоколов нажмите кнопку **Добавить**.

Редактирование профиля авторизации

Для редактирования профиля авторизации необходимо на странице со списком нажать на его наименование.

☐	Имя ↑
☐	DenyAccess
☐	MES auth
☐	PermitAccess
☐	Portal web redirect profile

Рисунок 241. Гиперссылка на страницу редактирования профиля авторизации

После этого откроется окно редактирования, аналогичное окну добавления.

The screenshot shows the 'Profile' editing interface. It includes a left sidebar with navigation icons. The main area contains the following sections:

- Profile:** Fields for 'Имя *' (Name), 'Профиль устройства *' (Device Profile), 'Тип доступа *' (Access Type), and 'Описание' (Description).
- Результат авторизации:** A section showing 'Access Type = ACCESS_ACCEPT'.
- Общие задачи:** A section with checkboxes for 'VLAN', 'ACL', and 'WebRedirection', each with associated input fields.
- Портал:** A dropdown menu for selecting a portal.
- Имя ACL:** An input field for the ACL name.
- Расширенные настройки атрибутов:** A section for defining attributes with a table-like structure for attribute name and value.

Рисунок 242. Окно редактирования профиля авторизации

После редактирования необходимо нажать на кнопку **"Сохранить"**. Кнопка скрыта, пока не будет внесено хотя бы одно изменение.

Кнопка **"Отмена"** осуществляет сброс внесенных изменений до исходного состояния.

Дублирование профиля

Новый профиль может быть создан на основе существующего. Для этого выберите копируемый профиль с помощью чекбокса, а затем нажмите на кнопку .

Откроется форма, аналогичная форме добавления, где все поля будут заполнены значениями из выбранного референса. По умолчанию к значению в поле **Имя** добавляется "_сору". Можно выбрать любое другое название, которое еще не используется в системе.

Удаление профиля авторизации

Для удаления в окне со списком необходимо выделить чекбокс слева от профилей авторизации, которые требуется удалить, и нажать кнопку  вверху слева.

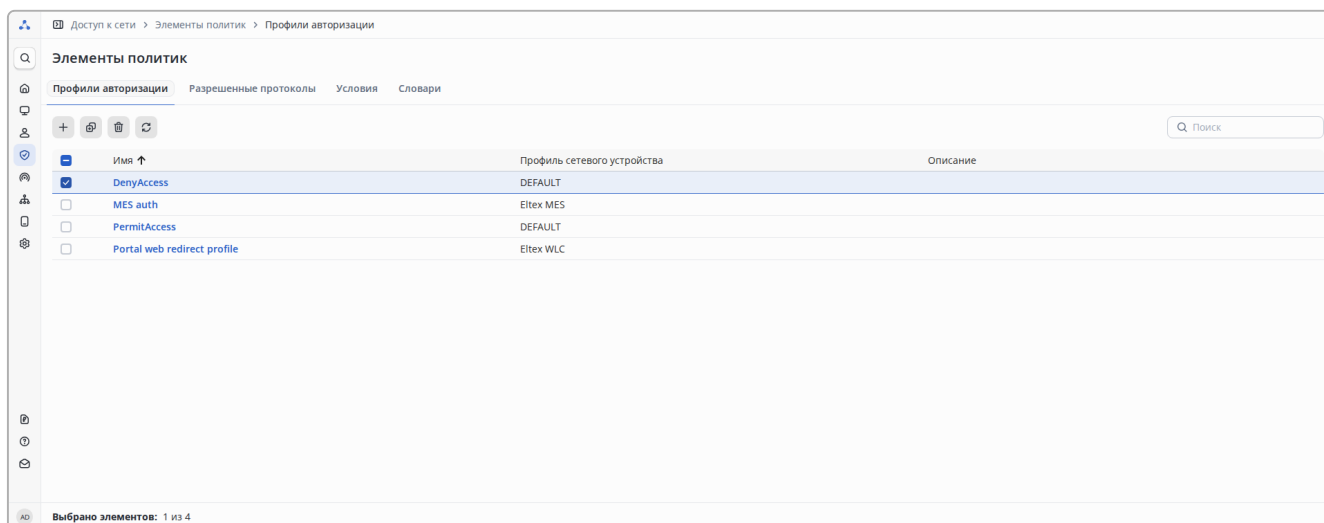


Рисунок 243. Выбор профиля авторизации в таблице для удаления



Удаление элементов требует подтверждения в модальном окне. Выбранные элементы будут удалены только после явного подтверждения операции.

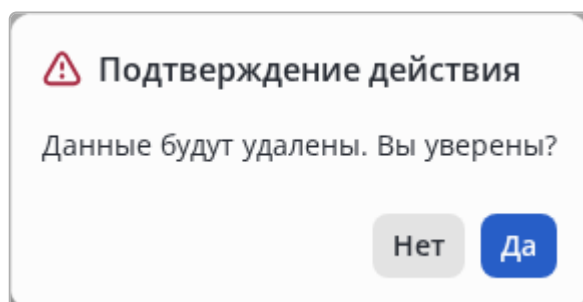


Рисунок 244. Диалоговое окно подтверждения действия



Ограничения:

- нельзя удалить профиль авторизации, который используется в какой-либо политике авторизации.

Разрешенные протоколы

Описание

Управление протоколами аутентификации позволяет разрешить или запретить использование определенных протоколов или методов при аутентификации клиентского устройства. Существует возможность настройки нескольких списков разрешенных протоколов, что позволяет гибко настраивать разрешенные протоколы в [наборах политик RADIUS](#) для каждого пользовательского сценария.

В данный момент поддерживаются следующие протоколы: PAP, MS-CHAPv2, EAP-PEAP, EAP-TLS, EAP-TTLS.

Доступна настройка разрешения или запрета MAB авторизации.

Просмотр списков разрешенных протоколов

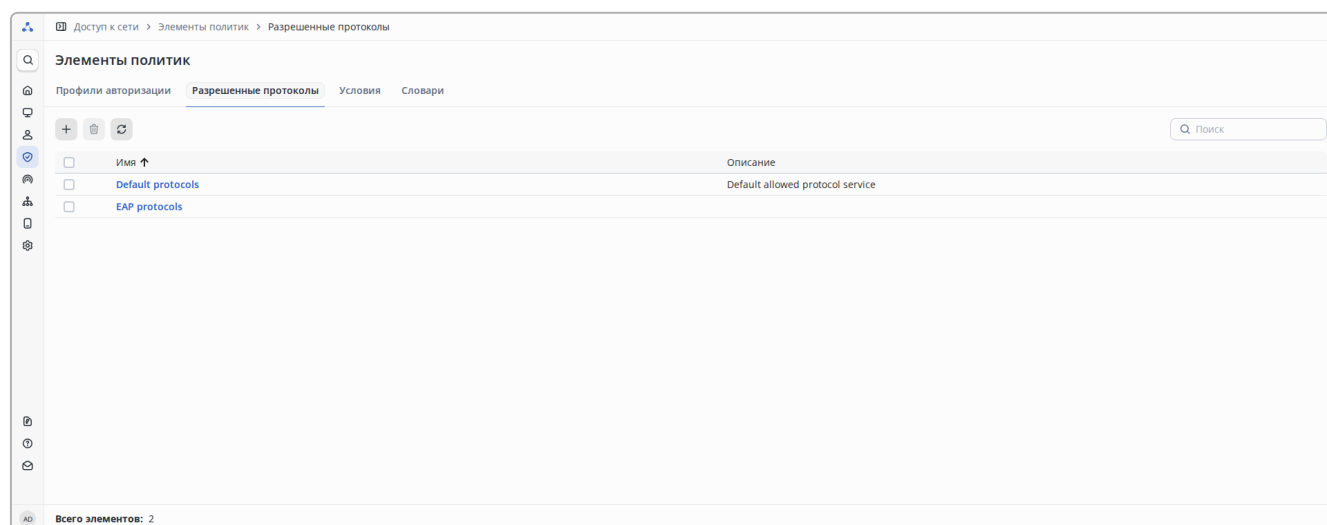


Рисунок 245. Таблица с перечнем списков разрешенных протоколов на странице просмотра

Снизу расположена таблица со списком, которая содержит колонки:

- **Имя** - название списка разрешенных протоколов.
- **Описание** - произвольное описание.

Возможна сортировка в прямом и обратном порядке по любой колонке. По умолчанию сортировка выполняется в прямом (алфавитном) порядке по колонке "Имя".

Элементы управления:

- **+** — Добавить новый элемент.
- **🗑️** — Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- **🔄** — Обновить данные таблицы.
- **☐** — Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).
- **↑** — Изменить текущий порядок сортировки.
- **🔍 Поиск** — Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.

Добавление списка разрешенных протоколов

Для добавления списка разрешенных протоколов нажмите **+**, после чего откроется окно:

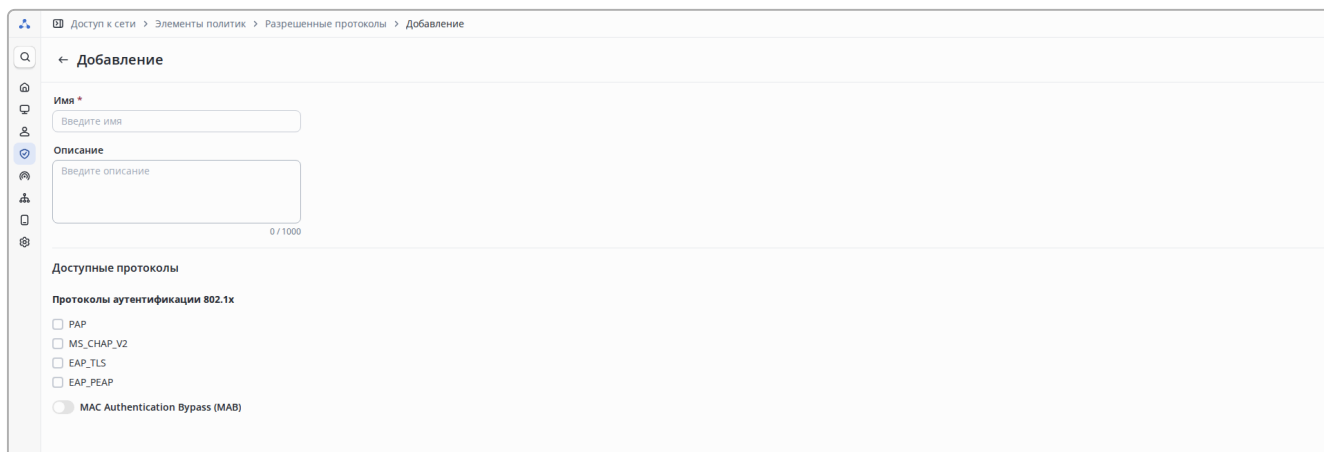


Рисунок 246. Окно добавления списка разрешенных протоколов

- **Имя *** - наименование, должно быть уникально. Максимальная длина - 100 символов.
- **Описание** - произвольное описание. Максимальная длина - 1000 символов.
- **Доступные протоколы** - выбор разрешенных протоколов аутентификации. По умолчанию все протоколы отключены.
 - **PAP** - выбрать протокол PAP (password authentication protocol), предусматривающий отправку логина и пароля на сервер аутентификации открытым текстом.
 - **MS_CHAP_V2** - выбрать протокол MS-CHAPv2 (Microsoft challenge handshake authentication protocol версии 2).
 - **EAP_TLS** - выбрать протокол EAP-TLS (Extensible Authentication Protocol Transport Layer Security).
 - **EAP_PEAP** - выбрать протокол EAP-PEAP (Protected Extensible Authentication Protocol), который инкапсулирует EAP (Extensible Authentication Protocol) внутри TLS-туннеля (Transport Layer Security).
 - **EAP_TTLS** - выбрать протокол EAP-TTLS (Tunneled TLS) - более гибкий аналог PEAP, который может нести внутри не только современные EAP-методы, но и старые протоколы проверки паролей.
 - **MAC Authentication Bypass (MAB)** - разрешить аутентификацию конечных устройств по MAC адресу.

* - поля, обязательные для заполнения.

После ввода необходимых данных и выбора разрешенных протоколов нажмите кнопку **"Добавить"**.

Редактирование списка разрешенных протоколов

Для редактирования списка разрешенных протоколов необходимо на странице со списком нажать на его наименование.

☐	Имя ↑
☐	Default protocols

Рисунок 247. Гиперссылка на страницу редактирования списка разрешенных протоколов

После этого откроется окно редактирования, аналогичное окну добавления.

Рисунок 248. Окно редактирования списка разрешенных протоколов

После редактирования необходимо нажать на кнопку **"Сохранить"**. Кнопка скрыта, пока не будет внесено хотя бы одно изменение.

Кнопка **"Отмена"** осуществляет сброс внесенных изменений до исходного состояния.

Удаление списка разрешенных протоколов

Для удаления в окне со списками необходимо выделить чекбокс слева от списка разрешенных протоколов, которые требуется удалить, и нажать кнопку  вверху слева.

Рисунок 249. Выбор списков разрешенных протоколов в таблице для удаления



Удаление элементов требует подтверждения в модальном окне. Выбранные элементы будут удалены только после явного подтверждения операции.

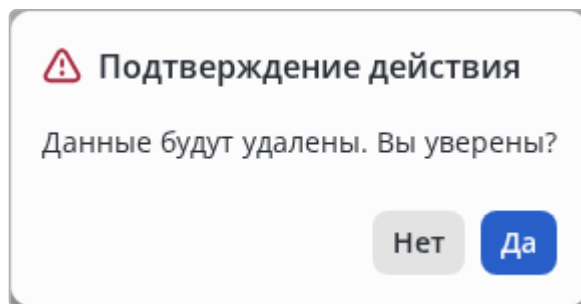


Рисунок 250. Диалоговое окно подтверждения действия



Ограничения:

- нельзя удалить список разрешенных протоколов, которая используется в каком-либо наборе политик.

Условия

Описание

Логические условия являются основным элементом политик аутентификации и авторизации, которые отвечают за формирование критериев, определяющих может ли пользователь пройти аутентификацию и какие действия должны быть к нему применены при выполнении авторизации.

В основе создания и обработки логического условия лежит алгебра логики. Результатом выполнения условия является "Истина" или "Ложь". Результат может быть инвертирован. Условие может быть простым и сложным. В простом условии в качестве критерия проверки выступает только один атрибут. В сложном условии можно использовать несколько различных атрибутов, объединив их логическими операциями "И" или "ИЛИ".

Просмотр списка логических условий

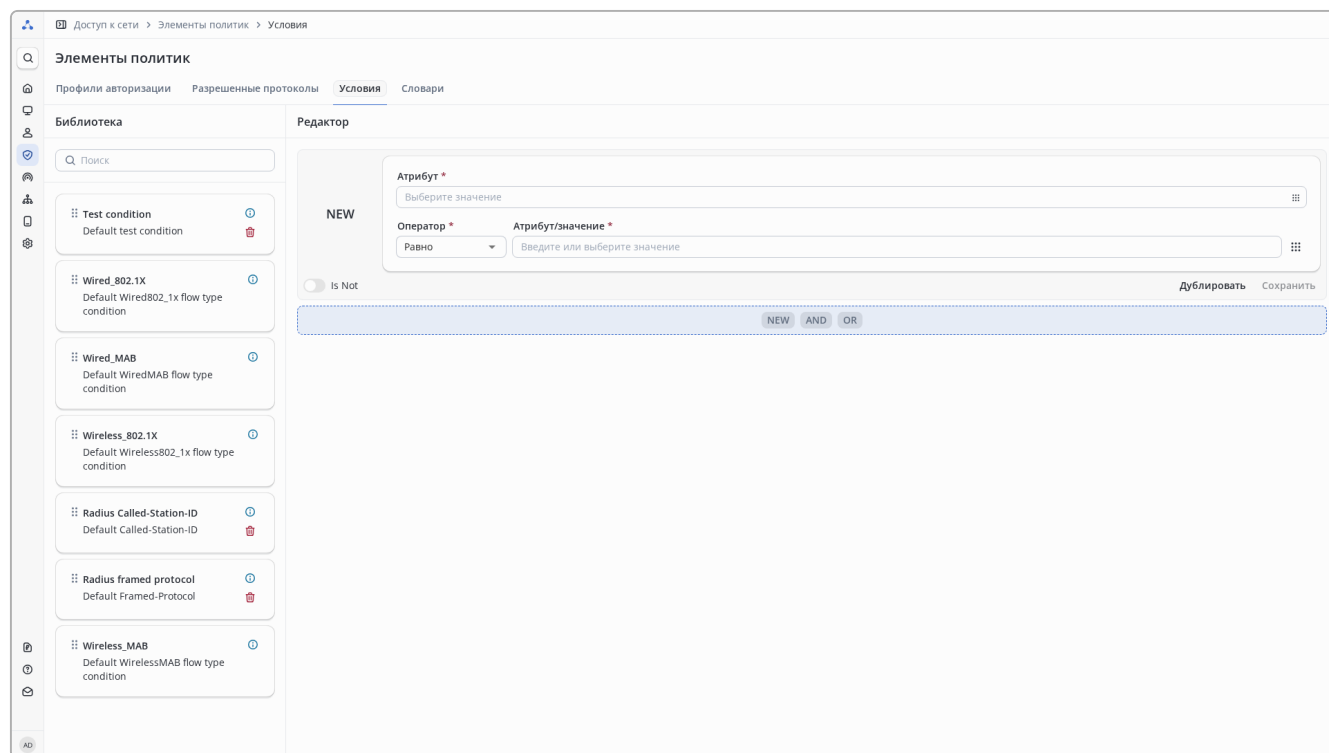


Рисунок 251. Библиотека логических условий

В левой части страницы расположена **Библиотека** логических условий.

Основной компонент страницы - **Редактор** логических условий:

- **Атрибут *** - атрибут логического условия.
- **Оператор *** - выбранный оператор логического условия. Может принимать значения (в зависимости от типа значения атрибута):
 - Больше или равно / Менее или равно
 - Больше чем / Менее чем
 - Равно / Не равно
 - Равно NULL / Не равно NULL
 - Начинается на / Не начинается на
 - Заканчивается на / Не заканчивается на
 - Содержит / Не содержит
 - Соответствует (полное соответствие строки с учетом регистра, так же есть поддержка [регулярных выражений](#))
 - Диапазон IP
 - Маска IP
 - Пустое значение
-

Атрибут/значение * - атрибут/значение, которые используются для сопоставления с атрибутом логического условия в соответствии с выбранным оператором. Для атрибута, предполагающего predetermined значения, выбор значения производится из списка.

- **Is Not** - выбор инвертирования результата выполнения условия (по умолчанию условие "Соблюдается", при включении настройки условие будет считаться "Не соблюдается")
- **NEW** - добавление нового логического условия в существующую иерархию на одном уровне с текущим.
- **AND** - добавление нового логического условия в качестве "дочернего" для существующего с логическим оператором "И".
- **OR** - добавление нового логического условия в качестве "дочернего" для существующего с логическим оператором "ИЛИ".

* - поля, обязательные для заполнения.

Элементы управления:

- **"Поиск"** - Выполняется регистронезависимая фильтрация по библиотеке логических условий по имени и описанию.
-  - Предпросмотр содержания логического условия.
-  - Удаление логического условия.
-  - Открыть словарь для добавления элемента.
-  - Удалить элемент из редактора. Действие зависит от расположения:
 - нажатие справа от поля "Атрибут" очистит соответствующее поле;
 - нажатие справа от поля "Атрибут/значение" очистит соответствующее поле;
 - нажатие справа от логического условия удалит данное условие.
- **"Сохранить"** - Сохранить соответствующее логическое условие.

Меню выбора атрибута

Для выбора атрибута, который будет использоваться в условии, необходимо нажать  - раскроется меню выбора атрибута.

Выбор атрибута для условия

Все

Device

Identity

Internal RADIUS

LDAP

Normalised RADIUS

RADIUS

Поиск

Словарь

ID

Выберите словарь

ID

Атрибут	Словарь	ID
3GPP-Allocate-IP-Type	3GPP	27
3GPP-Camel-Charging-Info	3GPP	24
3GPP-Charging-Characteristics	3GPP	13
3GPP-Charging-Gateway-Address	3GPP	4
3GPP-Charging-Gateway-IPv6-Ad...	3GPP	14
3GPP-Charging-ID	3GPP	2
3GPP-GGSN-Address	3GPP	7
3GPP-GGSN-IPv6-Address	3GPP	16

Рисунок 252. Меню выбора атрибута

Вверху находится список, позволяющий выполнить фильтрацию по типам словарей. Может быть выбран только один тип.

Типы словарей:

-  **RADIUS** - словари RADIUS-атрибутов, в том числе vendor-specific.
-  **NORMALISED_RADIUS** - системные атрибуты, формируемые на основе RADIUS-атрибутов, например - тип подключения.
-  **INTERNAL_RADIUS** - служебный словарь с системными атрибутами, как правило не используется.
-  **DEVICE** - атрибуты на основе параметров [устройства](#), например - тип устройства.
-  **IDENTITY** - атрибуты [пользователей](#) и [эндпоинтов](#).
-  **LDAP** - атрибуты из [внешних источников идентификации](#).

Ниже находятся колонки для фильтрации атрибутов.

- "Атрибут" - регистронезависимая фильтрация по наименованию атрибута.
- "Словарь" - меню выбора словаря. Для использования должен быть выбран тип словаря.
- "ID" - фильтрация по номеру атрибута.

Создание логических условий

Создание простого логического условия

Создание логического условия выполняется в **Редакторе**.

NEW

Атрибут *

Выберите значение

Оператор *

Атрибут/значение *

Равно

Введите или выберите значение

Is Not

Дублировать

Сохранить

NEW

AND

OR

Рисунок 253. Исходное состояние редактора условия

После нажатия на  в правой части поля "Атрибут" раскроется [меню выбора атрибута](#). Для поиска нужного атрибута можно воспользоваться фильтрацией по наименованию атрибута. Либо выбрать тип словаря и в нем, выбрав необходимый словарь путем прокрутки выпадающего списка, определить необходимый атрибут.

Редактор

NEW

Атрибут *

Выберите значение

Оператор *

Атрибут/значение *

Равно

Введите или выберите значение

Is Not

Выбор атрибута для условия

Все

Device

Identity

Internal RADIUS

LDAP

Normalised RADIUS

RADIUS

Поиск

Выберите словарь

ID

Атрибут	Словарь	ID
3GPP-Allocate-IP-Type	3GPP	27
3GPP-Camel-Charging-Info	3GPP	24
3GPP-Charging-Characteristics	3GPP	13
3GPP-Charging-Gateway-Address	3GPP	4
3GPP-Charging-Gateway-IPv6-Ad...	3GPP	14
3GPP-Charging-ID	3GPP	2
3GPP-GGSN-Address	3GPP	7
3GPP-GGSN-IPv6-Address	3GPP	16

Рисунок 254. Выбор атрибута

После выбора атрибута необходимо кликнуть на него и он попадет в поле "Атрибут". Далее необходимо выбрать оператор для сравнения значения атрибута (по умолчанию подставляется "Равно"). Список операторов зависит от типа данных используемых в значении выбранного атрибута.

Тип данных атрибута	Поддерживаемые операторы
Строка	Соответствует, Оканчивается на, Не оканчивается на, Начинается с, Не начинается с, Содержит, Не содержит, Равно, Не равно, Равно NULL, Не равно NULL, Пустое значение
Число	Больше или равно, Больше чем, Меньше или равно, Меньше чем, Равно, Не равно, Равно NULL, Не равно NULL, Пустое значение
IPv4 адрес	Равно, Не равно, Равно NULL, Не равно NULL, Диапазон IP, Маска IP, Пустое значение

Тип данных атрибута	Поддерживаемые операторы
MAC адрес	Равно, Не равно, Равно NULL, Не равно NULL, Начинается на, Не начинается на, Заканчивается на, Не заканчивается на, Содержит, Не содержит, Пустое значение
Имя	Равно, Не равно, Равно NULL, Не равно NULL
Последовательность байт	Равно NULL, Не равно NULL

Затем в поле *Атрибут/значение* выбирается атрибут или вводится его значение.

Рисунок 255. Условие, в котором заполнены все параметры

Для сохранения условия в библиотеку условий нужно нажать кнопку **"Сохранить"**. Можно заменить существующее условие в библиотеке или сохранить новое.

По умолчанию действие предполагает сохранение нового условия:

- **Имя *** - наименование условия. Максимальная длина - 100 символов.
- **Описание** - произвольное описание. Максимальная длина - 200 символов.

* - поля, обязательные для заполнения.

После нажать кнопку "Сохранить".

Для сохранения с заменой существующего условия в библиотеке необходимо выбрать "Заменить существующее условие в библиотеке" и выбрать условие в выпадающем списке. При необходимости можно выполнить фильтрацию по наименованию, введя соответствующий текст в поле перед списком.

После нажать кнопку "Сохранить".



Кнопка "Сохранить" всегда активна, чтобы иметь возможность сохранить существующее условие под другим именем.

Создание сложного логического условия

Для создания сложного логического условия из простого используется панель под логическим условием.

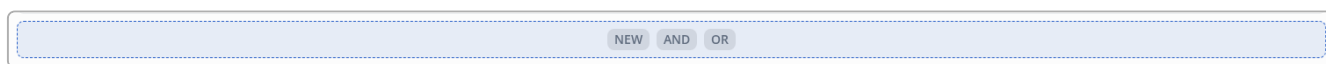


Рисунок 257. Панель для добавления дополнительного условия

- **New** - добавить логическое условие на одном уровне с существующим.
- **AND** - добавить дочернее условие с логическим "И".
- **OR** - добавить дочернее условие с логическим "ИЛИ".

При нажатии "New" в редакторе появится дополнительное правило на одном уровне с существующим, объединенные логическим "И".

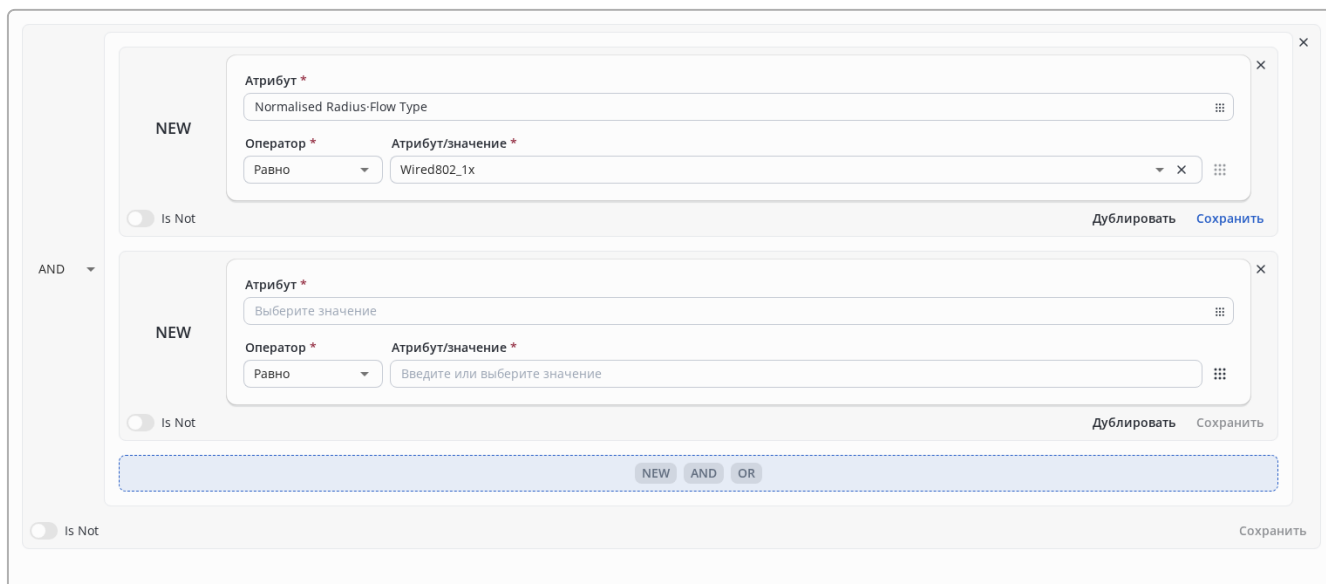


Рисунок 258. Условие, состоящее из двух условий, объединенные логическим "И"

- Логическое "И", объединяющее правила, можно изменить на "ИЛИ".
- Есть возможность сохранить каждое условие отдельно кнопкой "Сохранить" в его окне или все вместе, кнопкой "Сохранить" внизу.
- Для удаления условия надо нажать на  справа вверху в окне условия.
- Для полной очистки всех условий в редакторе надо нажать  вверху справа редактора, расположенный за окнами отдельных условий.

При нажатии "AND" или "OR" появится новое окно, в котором можно будет доступно новое меню, далее можно добавить условия на новом уровне или создать дочерние условия. Ограничение на вложенность условий нет.

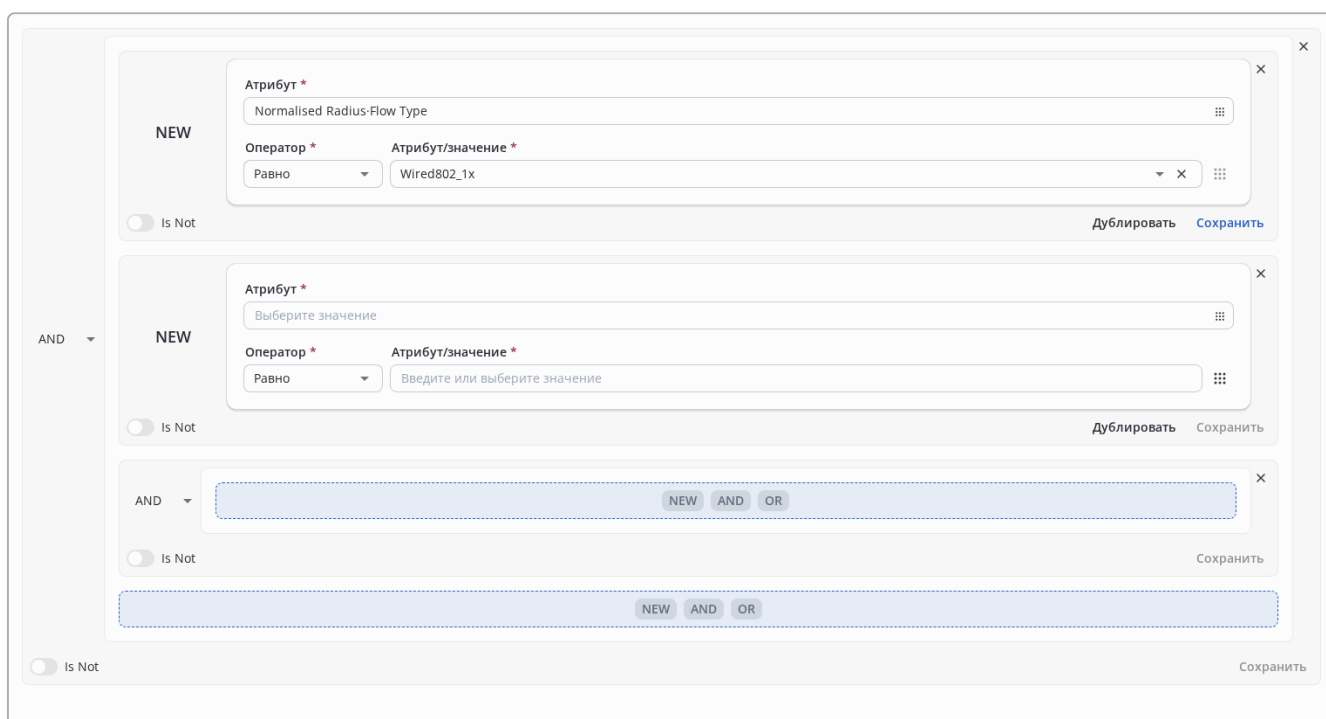


Рисунок 259. Условие, содержащее вложенные правила

Для сохранения всех условий надо нажать кнопку "Сохранить" в нижнем правом углу.

Использование регулярных выражений

При добавлении условия в набор политик для атрибутов с оператором `соответствует` могут использоваться регулярные выражения. Это позволяет указать "шаблон", под который может подходить несколько значений, с помощью всего одной строки.

Пример 1. Использование регулярных выражений в логических условиях

Задача: Необходимо применить набор политик ко всем подключениям с устройств, имя которых начинается с префикса `MES`.

Возможное решение:

Для того, чтобы выделить только подключения с определенных устройств, в условии можно использовать атрибут `RADIUS·NAS-Identifier`. Обратите внимание, что как правило требуется настройка его отправки на NAS-устройстве.

Чтобы не создавать отдельные условия `RADIUS·NAS-Identifier равно MES1` и т.п. для каждого устройства, можно создать одно условие `RADIUS·NAS-Identifier соответствует MES.*`.

Конструкция `.*` означает "любое количество любых символов" после `MES`.

Также можно использовать более строгое выражение, если, например, предполагается, что после `MES` всегда идут 4 цифры и одна буква: `MES\d{4}[A-Z]`.

Здесь:

`\d{4}` — четыре цифры;

`[A-Z]` — одна заглавная буква.

Краткий список часто используемых метасимволов

- СИМВОЛЫ:
 - `.` - любой символ
 - `\d` - любая цифра
 - `\w` - любая буква в любом регистре
 - `\s` - пробельный символ
 - `\` - экранирование любого спецсимвола
- группировка:
 - `[abc]` - один из перечисленных в скобках символов (или a, или b, или c)
 - `[a-z]` - один из перечисленных в диапазоне символов
 - `(abc)` - объединение символов в указанном порядке в одну группу
- квантификаторы:
 - `a?` - 0 или 1 вхождение символа
 - `a*` - 0 и больше вхождений символа
 - `a+` - 1 и больше вхождений символа
 - `a{n}` - вхождение символа n раз
 - `a{n,}` - вхождение символа n или больше раз
 - `a{n,m}` - вхождение символа от n до m раз
- логические операции:
 - `^a` - отрицание
 - `a|b` - один из двух указанных символов (ИЛИ)
- полезные комбинации:
 - `.*` - любой символ любое количество раз
 - `\w+` - любое слово
 - `(word1)|(word2)` - одно из указанных слов



Редактирование логического условия

Для редактирования логического условия необходимо его захватить курсором в библиотеке и перенести в поле редактора.

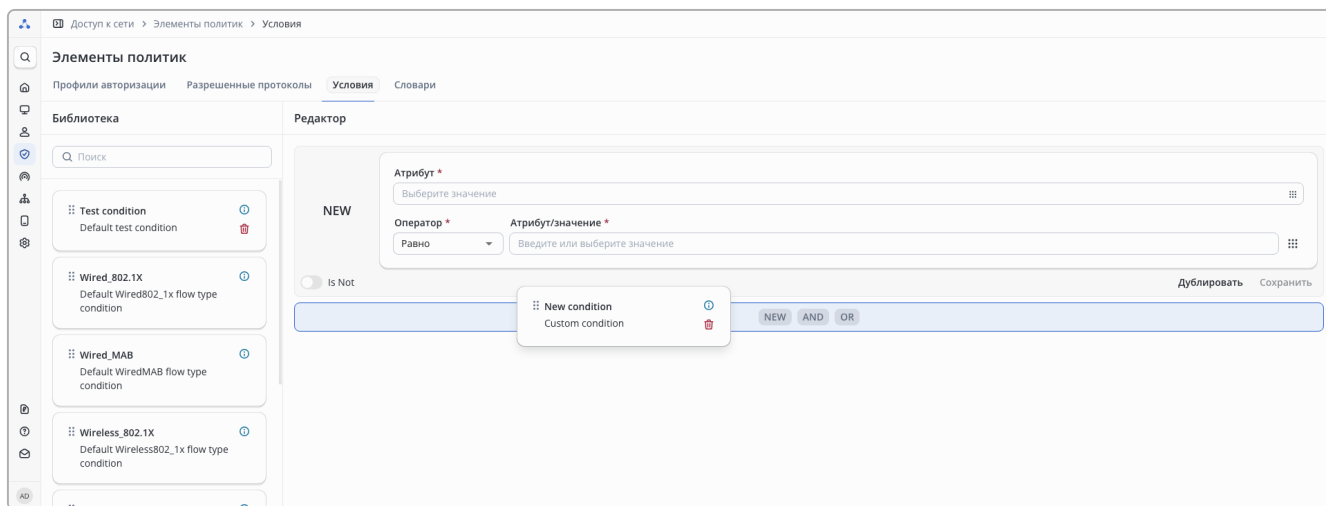


Рисунок 260. Выбор логического условия

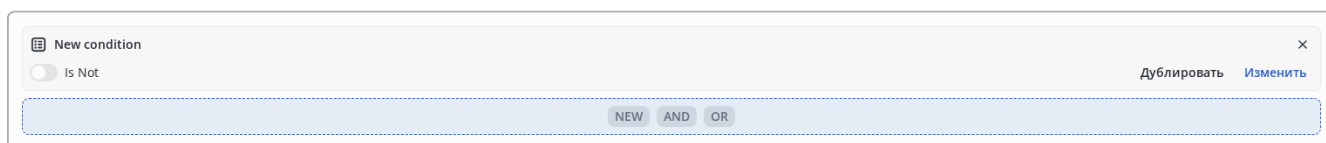


Рисунок 261. Редактирование логического условия

Для редактирования условия нажать кнопку "Изменить". После редактирования нажать кнопку "Сохранить". Так как условие ранее было сохранено в библиотеке - по умолчанию будет предложено сохранить его с тем же названием. При необходимости можно выбрать другое условие, которое будет перезаписано или выбрать "Сохранить в библиотеку как новое условие". Нажать кнопку "Сохранить".

Так же в ходе редактирования можно перетаскивать условия из библиотеки в поле редактора дочернего условия.

Удаление логического условия

Для удаления логического условия надо найти его в библиотеке и нажать кнопку  справа от имени условия.

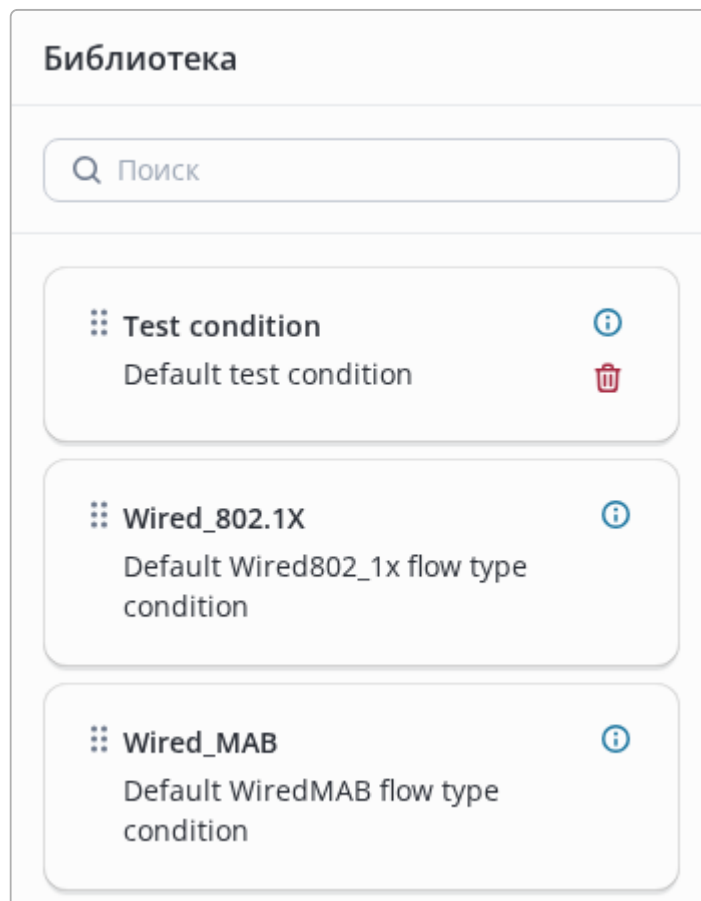


Рисунок 262. Выбор условия для удаления



Удаление элементов требует подтверждения в модальном окне. Выбранные элементы будут удалены только после явного подтверждения операции.

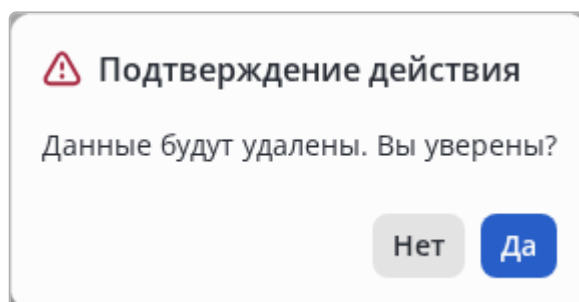


Рисунок 263. Диалоговое окно подтверждения действия

Ограничения:



- нельзя удалить или отредактировать некоторые системные логические условия;
- нельзя удалить логические условия, которые используются в других сложных логических условиях;
- нельзя удалить логические условия, которые используются в каком-либо наборе политик.

Словари

Описание

Базовым элементом при настройке [логического условия](#) являются атрибуты, сгруппированные по словарям. Помимо базовых и vendor-specific атрибутов RADIUS в NAICE доступно использование Не-RADIUS атрибутов, таких как параметры сетевого устройства (словарь DEVICE) или пользователя (словарь IDENTITY).

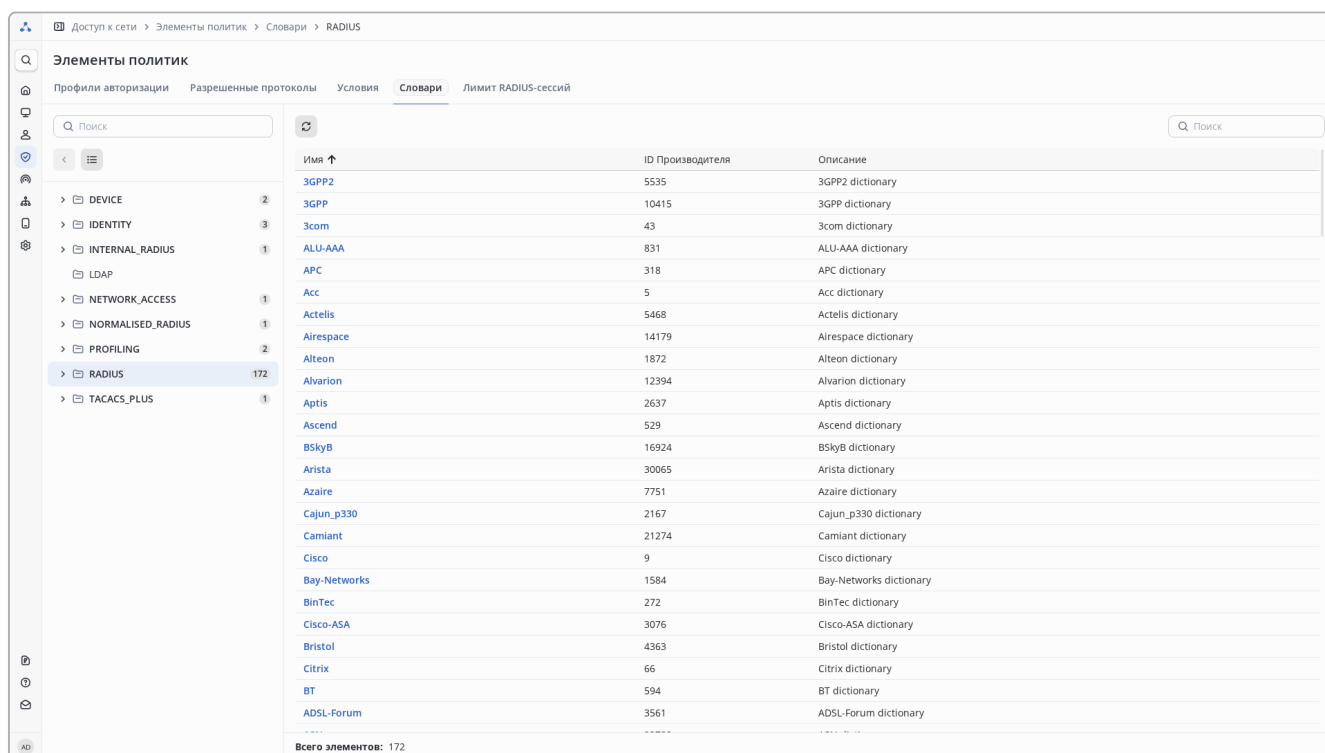
Словари и атрибуты доступны для просмотра на отдельной странице. Добавление новых словарей или редактирование существующих недоступно.



Если необходимый Вам словарь не добавлен в систему, обратитесь к нам при помощи кнопки "Оставить пожелание", доступной из навигационного меню или меню  в нижней левой части меню навигации.

Просмотр словарей

В левой части окна (с заголовком "Словари") находится список доступных словарей, в правой части - содержание выбранного словаря (по умолчанию - содержание словаря RADIUS).



Имя	ID Производителя	Описание
3GPP2	5535	3GPP2 dictionary
3GPP	10415	3GPP dictionary
3com	43	3com dictionary
ALU-AAA	831	ALU-AAA dictionary
APC	318	APC dictionary
Acc	5	Acc dictionary
Actelis	5468	Actelis dictionary
Airespace	14179	Airespace dictionary
Altheon	1872	Altheon dictionary
Alvarion	12394	Alvarion dictionary
Aptis	2637	Aptis dictionary
Ascend	529	Ascend dictionary
BSkyB	16924	BSkyB dictionary
Arista	30065	Arista dictionary
Azaire	7751	Azaire dictionary
Cajun_p330	2167	Cajun_p330 dictionary
Camiant	21274	Camiant dictionary
Cisco	9	Cisco dictionary
Bay-Networks	1584	Bay-Networks dictionary
BinTec	272	BinTec dictionary
Cisco-ASA	3076	Cisco-ASA dictionary
Bristol	4363	Bristol dictionary
Citrix	66	Citrix dictionary
BT	594	BT dictionary
ADSL-Forum	3561	ADSL-Forum dictionary

Рисунок 264. Просмотр словарей

Элементы управления:

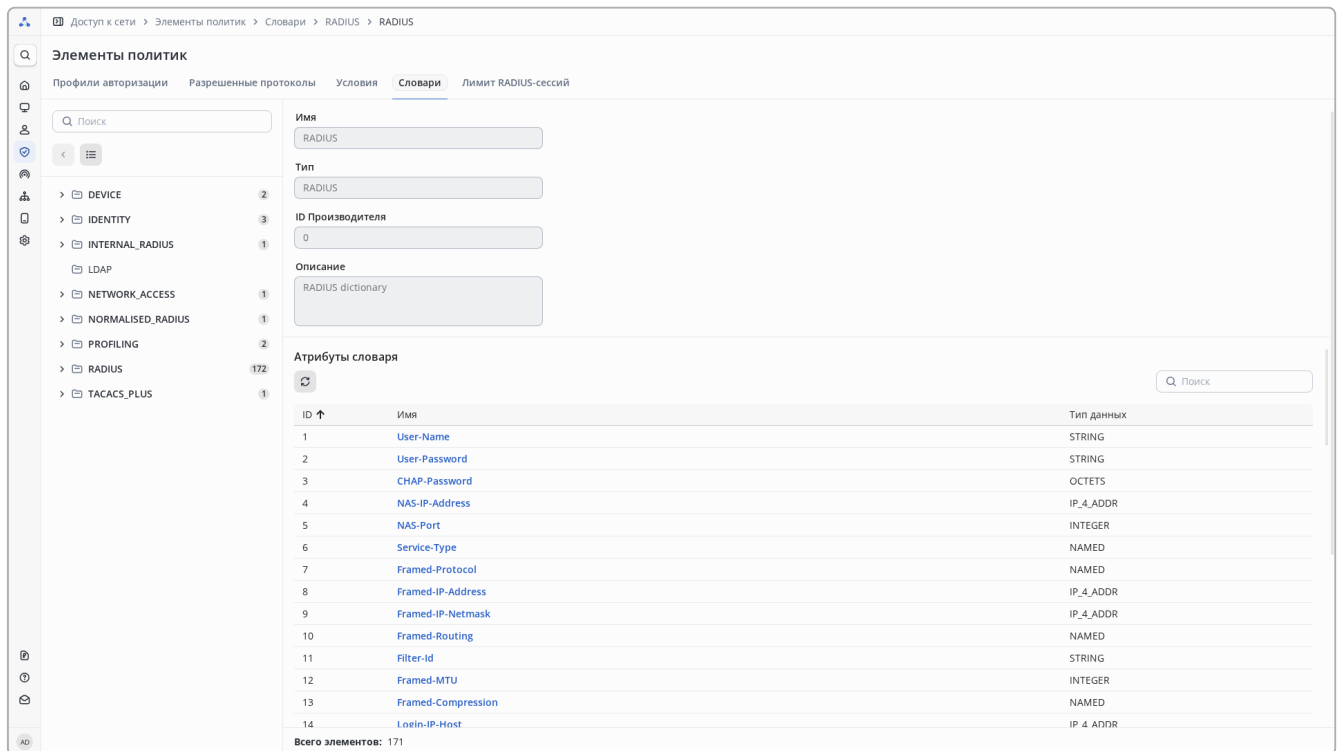
-  - раскрыть список вложенных словарей.
- "Словари. Поиск" - фильтрация по имени словаря.
- "RADIUS. Поиск" - фильтрация по вложенным словарям и атрибутам.
-  - обновить данные.

Переключение варианта отображения меню навигации по словарям:

-  - меню навигации в виде дерева.
-  - меню навигации в виде списка.

Просмотр вложенных словарей и атрибутов

Для просмотра атрибутов словаря требуется выбрать необходимый словарь в списке и нажать на его имя:



The screenshot shows a web interface for managing network policies. The breadcrumb trail is: **Доступ к сети** > **Элементы политик** > **Словари** > **RADIUS** > **RADIUS**. The main section is titled **Элементы политик** and has tabs for **Профили авторизации**, **Разрешенные протоколы**, **Условия**, **Словари** (selected), and **Лимит RADIUS-сессий**. On the left is a tree view of policy elements. The main content area shows the details for the **RADIUS** dictionary. It includes fields for **Имя** (RADIUS), **Тип** (RADIUS), **ID Производителя** (0), and **Описание** (RADIUS dictionary). Below this is a table of **Атрибуты словаря** (Dictionary Attributes).

ID ↑	Имя	Тип данных
1	User-Name	STRING
2	User-Password	STRING
3	CHAP-Password	OCTETS
4	NAS-IP-Address	IP_4_ADDR
5	NAS-Port	INTEGER
6	Service-Type	NAMED
7	Framed-Protocol	NAMED
8	Framed-IP-Address	IP_4_ADDR
9	Framed-IP-Netmask	IP_4_ADDR
10	Framed-Routing	NAMED
11	Filter-Id	STRING
12	Framed-MTU	INTEGER
13	Framed-Compression	NAMED
14	Login-IP-Host	IP_4_ADDR

At the bottom, it says **Всего элементов: 171**.

Рисунок 265. Просмотр атрибутов словаря

Для просмотра информации об атрибуте требуется нажать на имя атрибута в списке атрибутов:

RADIUS

✕

Имя

Service-Type

Тип данных

NAMED

ID Производителя

0

ID Атрибута

6

Допустимые значения

Ключ	Значение
Login-User	1
Framed-User	2
Callback-Login-User	3
Callback-Framed-User	4
Outbound-User	5
Administrative-User	6
NAS-Prompt-User	7
Authenticate-Only	8
Callback-NAS-Prompt	9
Call-Check	10
Callback-Administrative	11

Всего элементов: 11

Рисунок 266. Просмотр информации об атрибуте

Для атрибутов, предполагающих конечный список допустимых значений, на данной странице будет перечислен список этих значений.

Лимит RADIUS-сессий

Описание

Функциональность ограничения одновременных RADIUS-сессий позволяет контролировать использование учетных записей пользователей при подключении к сети. Механизм ограничивает

количество одновременно активных пользовательских сессий и предотвращает несанкционированное совместное использование учетных данных.

Ограничение применяется ко всем источникам идентификации, кроме гостевых эндпоинтов. Сессии редиректа на портал не учитываются в ограничении. Ограничение не применяется к MAB-аутентификации.



Данный раздел доступен только при включенной обработке RADIUS Accounting ([Настройки системы](#) → [Сервисы](#) → [RADIUS](#)).

Настройка лимита RADIUS-сессий

Источник идентификации	Лимит активных сессий	Лимит времени сессии (чч:мм)
Source 1	100	☐ Глобальный 48:00
Source 2	200	☒ Глобальный 00:00
Source 3	50	☐ Глобальный 12:00

Рисунок 267. Страница настройки ограничений активных RADIUS-сессий

В верхней части страницы расположен глобальный параметр:

- **Время жизни активной сессии *** - максимальный период жизни активной сессии с момента ее последнего обновления. Если в течение заданного периода по сессии не поступают события, подтверждающие ее актуальность, система считает сессию зависшей и автоматически завершает ее. Автоматическое завершение освобождает установленную для источника квоту для новых подключений.



Значение указывается в формате **часы:минуты** и должно быть больше **00:00**.

Глобальное время жизни сессии применяется к тем источникам идентификации, для которых включен переключатель **Глобальный** в настройках времени.

Под глобальной настройкой расположена таблица источников идентификации. В таблице для каждого источника можно настроить следующие параметры:

- **Лимит активных сессий** - максимальное количество одновременно активных сессий одного пользователя в рамках данного источника.
 - **0** - ограничение отключено. Система не выполняет проверку количества активных сессий.
 - **N > 0** - при достижении лимита система возвращает ответ **Access-Reject**, и пользователь не получает сетевой доступ.

Лимит времени сессии - время жизни активной сессии для данного источника, заданное в формате часы:минуты.

- Глобальный - переключатель применения глобального времени жизни сессии.
 - Включен - к сессиям данного источника применяется глобальная настройка времени жизни.
 - Выключен - для данного источника указывается собственное значение времени жизни, независимое от глобальной настройки.



При выключенном переключателе *Глобальный* указание лимита времени сессии является обязательным.

Принцип работы ограничения одновременных RADIUS-сессий

Подсчет активных сессий

Система NAICE ведет учет сессий на основе RADIUS Accounting атрибутов. Определение количества активных сессий для конкретного пользователя выполняется последовательно, с использованием следующих комбинаций атрибутов:

1. **Class-25** - определение уникальности подключения на основе атрибута, содержащего уникальный идентификатор подключения.
2. **NAS IP + Session-ID** - определение уникальности подключения по комбинации IP-адреса сетевого устройства и идентификатора сессии.
3. **Источник идентификации + NAS IP + MAC-адрес + Имя пользователя** - определение уникальности подключения в случаях, когда известен источник авторизации. MAC-адрес не является обязательным атрибутом, так как при MAB-аутентификации он может отсутствовать.
4. **NAS IP + MAC-адрес** - определение уникальности подключения для порталных пользователей.
5. **NAS IP + MAC-адрес + Имя пользователя** - определение уникальности подключений в случае, если ни одна из вышеперечисленных комбинаций атрибутов не была отправлена сетевым устройством. MAC-адрес не является обязательным атрибутом.



В системе NAICE используется первый подходящий по комбинации атрибутов вариант из перечисленных.

Проверка при аутентификации

При аутентификации пользователя система определяет его по комбинации "*Источник идентификации + Имя пользователя*" и проверяет количество активных RADIUS-сессий:

- Если число активных сессий меньше установленного лимита - доступ разрешается.
- Если число активных сессий превышает установленный лимит - система возвращает Access-Reject. В [журнале событий](#) фиксируется причина отказа: превышение лимита одновременных сессий.



Сессия считается активной, пока не получен пакет *RADIUS Accounting Stop* или сессия не завершена по таймауту. Ручное закрытие сессии администратором также освобождает квоту активных RADIUS-сессий.

Политики RADIUS

Описание

Политики аутентификации и авторизации определяют действия, которые необходимо выполнить при получении запросов на аутентификацию пользователей от сетевых устройств по протоколу RADIUS и действия при авторизации пользователей.

Порядок обработки запросов

Порядок обработки запросов аутентификации/авторизации от пользователей, передаваемых сетевыми устройствами, следующий:

1. Первоначальная проверка данных сетевого устройства:

- Входящий RADIUS-запрос анализируется на наличие атрибута **NAS-IP-Address** - в случае отсутствия пакет отбрасывается, никакой ответ не возвращается.
- Полученный **NAS-IP-Address** ищется среди записей о **сетевых устройствах** - в случае отсутствия пакет отбрасывается, никакой ответ не возвращается.
- Проверяется корректность **secret** в RADIUS-запросе - если секретный ключ неверен возвращается **ACCESS-REJECT**.

2. Обработка в таблице набора политик.

- Выполняется проверка соответствия RADIUS-пакета **логическим условиям**, используемым в наборах политик.
- Проверка выполняется последовательно сверху вниз.
- Политики RADIUS для которых установлен Статус **Выключено** не участвуют в проверке, счетчик в колонке **Количество срабатываний** не увеличивается.
- Политики RADIUS для которых установлен Статус **Проверка условия** не участвуют в проверке, но счетчик в колонке **Количество срабатываний** при соответствии политики увеличивается.
- При обнаружении подходящего набора политик дальнейший их перебор прекращается и продолжается проверка в рамках этого набора.
- Если набор политик с подходящим условием не будет найден - сетевому устройству будет отправлен ответ в рамках политики **Default**. По умолчанию в данном наборе политик в политике авторизации настроен профиль авторизации **DenyAccess**, согласно которому сетевому устройству будет отправлен **ACCESS-REJECT**. Данное поведение можно изменить, отредактировав политики в **Default**.

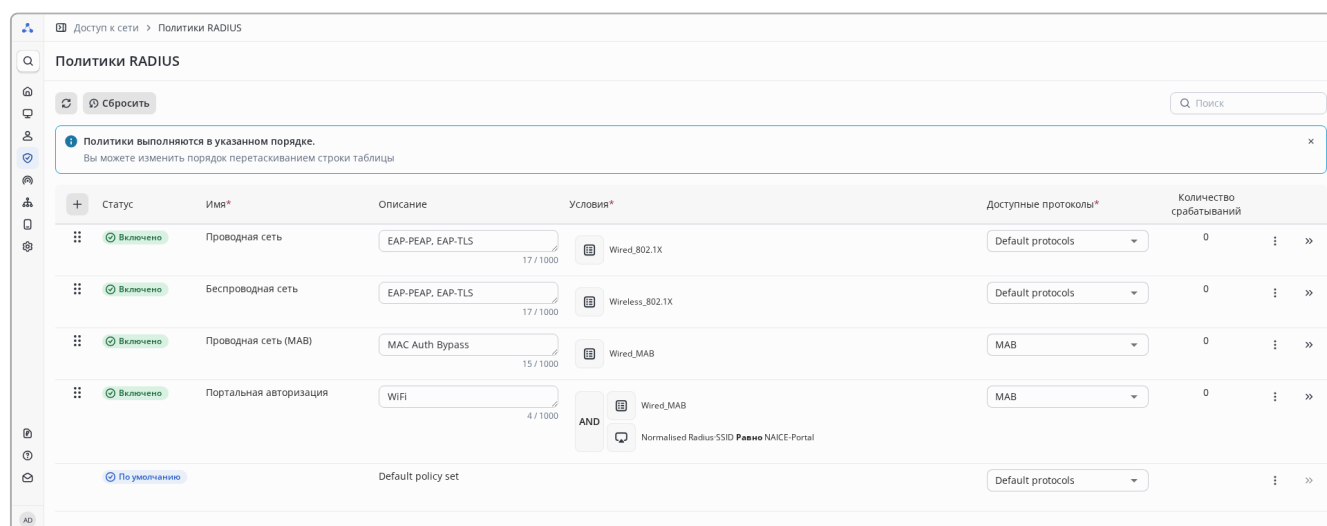
3. Обработка в рамках найденного набора политик:

- Проверяется используемый протокол аутентификации и сравнивается с доступными в выбранном **списке протоколов**. Если совпадений не обнаружено - сетевому устройству будет отправлен **ACCESS-REJECT**.
- В правилах политики аутентификации выполняется проверка сверху вниз, пока не будет найдено совпадающее условие. Если не будет найдено ни одного правила с совпадающим

условием, то будет применено правило **Default** - по умолчанию сетевому устройству будет отправлен **ACCESS-REJECT**.

- Выполняется поиск пользователя в выбранной **цепочки источников идентификации**. Если пользователь найден, то продолжается авторизация, если не найден - будет отправлен **ACCESS-REJECT**.
- В политиках авторизации выполняется проверка правил сверху вниз, пока не будет найдено совпадающее условие. Если не будет найдено ни одного правила с совпадающим условием - сетевому устройству будет отправлен **ACCESS-REJECT** по правилу **Default**. Дефолтное поведение может быть перенастроено.
- После определения правила политики авторизации выполняется проверка пароля пользователя. Если он не совпадает - сетевому устройству будет отправлен **ACCESS-REJECT**.
- После успешной проверки логина/пароля пользователя выполняются добавление в ответ атрибутов, предполагаемых по используемому **профилю авторизации**, и отправка ответа сетевому устройству. В профиле авторизации может быть настроен как **ACCESS-ACCEPT**, так и **ACCESS-REJECT** ответ.

Просмотр списка наборов политик



Статус	Имя*	Описание	Условия*	Доступные протоколы*	Количество срабатываний
Включено	Проводная сеть	EAP-PEAP, EAP-TLS 17 / 1000	Wired_802.1X	Default protocols	0
Включено	Беспроводная сеть	EAP-PEAP, EAP-TLS 17 / 1000	Wireless_802.1X	Default protocols	0
Включено	Проводная сеть (MAB)	MAC Auth Bypass 15 / 1000	Wired_MAB	MAB	0
Включено	Портальная авторизация	WIFI 4 / 1000	Wired_MAB AND Normalised Radius SSID Равно NAICE-Portal	MAB	0
По умолчанию	Default policy set			Default protocols	

Рисунок 268. Просмотр всех наборов политик

В таблице отображаются политики RADIUS, в соответствии с которыми проводится обработка запросов на аутентификацию/авторизацию.



Последний набор политик с именем **Default** не может быть удален, у него нельзя изменить имя или условие. Он всегда будет последним в списке, ниже которого расположить другие политики нельзя.

Описание колонок таблицы:

- **Статус** - статус набора политик.
- **Имя *** - наименование набора политик. Максимальная длина - 200 символов.
- **Описание** - произвольное описание. Максимальная длина - 1000 символов.

Условия * - используемые логические условия. Если используется библиотечное условие - отображается его имя. Если используется не библиотечное условие - отображается его структура.

- Доступные протоколы * - выбранный [список доступных протоколов](#).
- Количество срабатываний - количество попыток авторизации, подпадающих под указанные Условия.
- Действия - действия по добавлению/удалению набора политик.
- Настройка - переход к просмотру и редактированию политик аутентификации/авторизации выбранного набора политик.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

Элементы управления:

- Поиск - регистронезависимый поиск по имени набора политик (найденные совпадения будут подсвечены).
-  - обновить данные.
-  Сбросить - сбросить счетчики количества срабатываний всех наборов политик.
- + - добавить политику (политика будет добавлена первой в списке).
- Количество срабатываний - количество попыток авторизации, подпадающих под указанные Условия. При нажатии на число срабатываний счетчик можно **Сбросить**.
- ⋮ - действия:
 - Добавить сверху - добавить набор политик *До* выбранного;
 - Добавить снизу - добавить набор политик *После* выбранного;
 - Удалить - удалить выбранный набор политик.
- >> - перейти к управлению политиками аутентификации/авторизации текущего набора политик.
- Сохранить - сохранить изменения.
- Отменить - отменить изменения.

Все включенные политики RADIUS проверяются по порядку, как на экране - сверху вниз. Политики RADIUS отображаются на странице всегда полностью: Поиск не скрывает записи из списка, а только подсвечивает их.

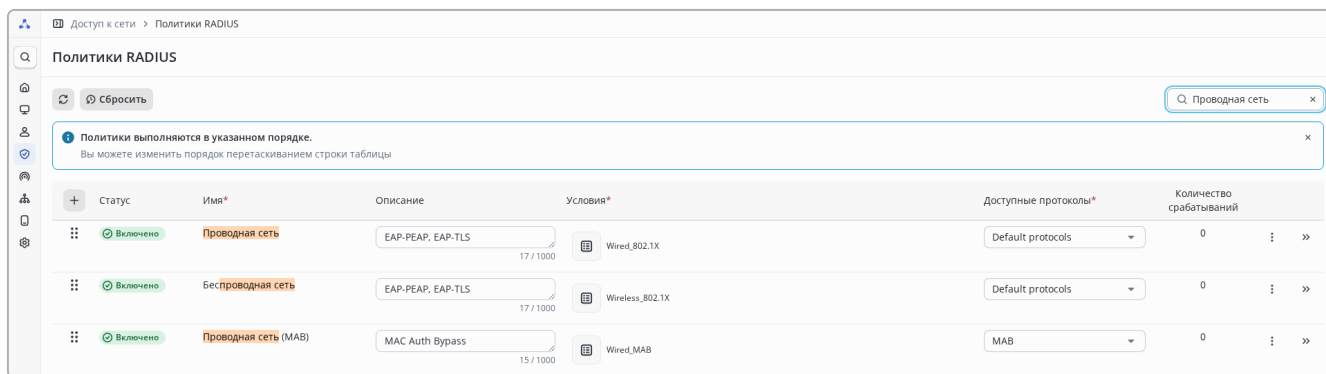


Рисунок 269. Поиск набора политик

Для изменения порядка перетащите политику за элемент  в колонке .

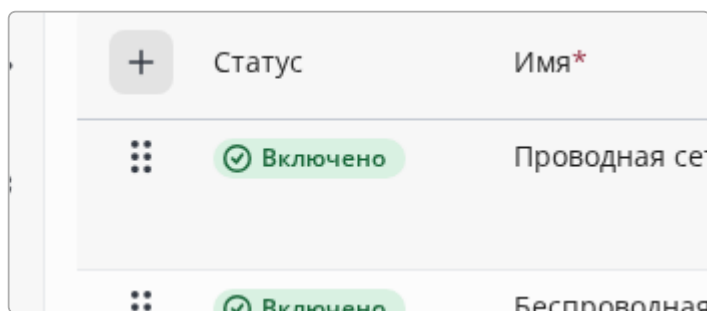


Рисунок 270. Иконка перетаскивания набора политик



После изменения порядка политик не забывайте нажать кнопку **Сохранить**, иначе изменения не вступят в силу.

Для просмотра списка [политик аутентификации и авторизации](#) необходимо в колонке **Настройка** нажать  справа от выбранного набора политик.

Редактирование набора политик

Для добавления набора политик в окне списка наборов политик можно нажать вверху слева кнопку  - новый набор будет добавлен первый в списке.

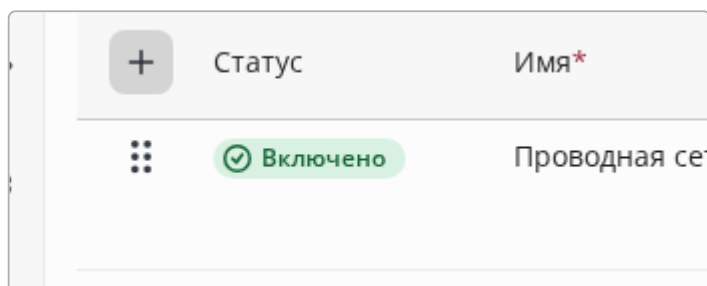


Рисунок 271. Иконка добавления набора политик

При необходимости добавить набор политик в произвольное место необходимо нажать на кнопку  справа от выбранного набора политик и в выпадающем меню выбрать **Добавить сверху** или **Добавить снизу**.

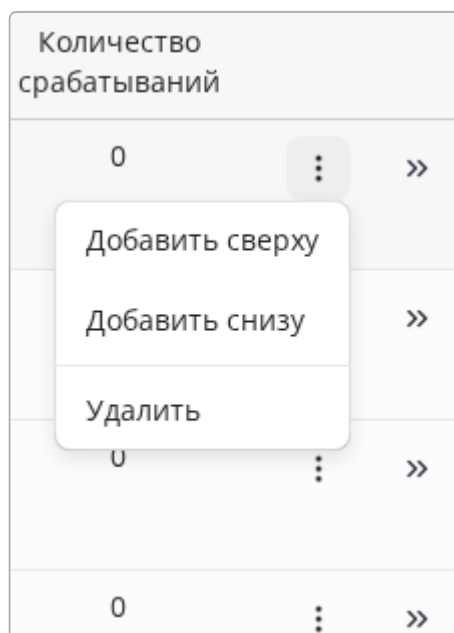


Рисунок 272. Отображение политики. Выпадающее меню с действиями.

Информация по Статусу:

- **✓ Включено** - разрешается обрабатывать запросы;
- **✗ Выключено** - исключить из обработки, не проверять Условие, не обрабатывать запросы;
- **🕒 Проверка условий** - разрешается проверять Условие (и инкрементировать счётчик срабатываний), обрабатывать запросы - нет;
- **✓ По умолчанию** - используется только для политики по умолчанию Default.

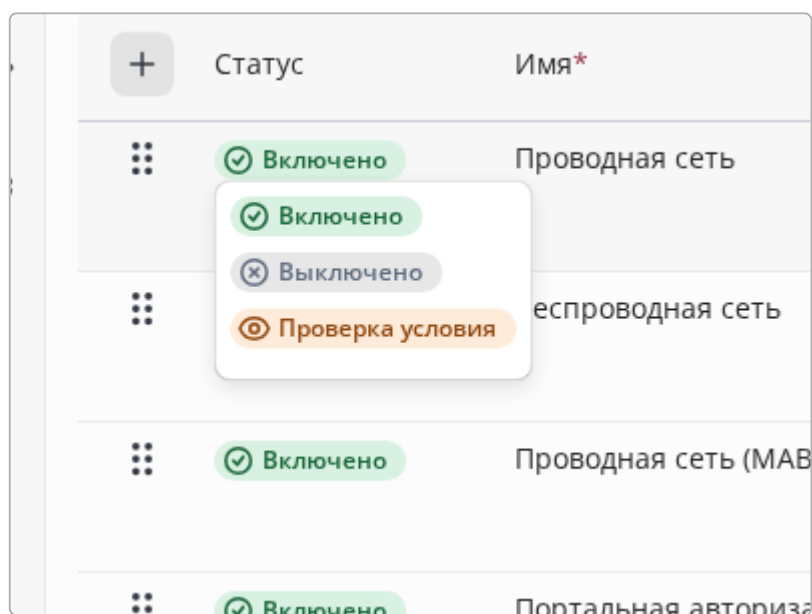


Рисунок 273. Изменение статуса политики

Во вновь созданном наборе политик в поле **Имя** ввести наименование набора политик или оставить неизменным автоматически сформированное имя.

Статус	Имя*	Описание	Условия*	Доступные протоколы*	Количество срабатываний
Включено	New Policy Set 1	Введите описание	+ Добавить	Выберите протокол	0 / 1000
Включено	Проводная сеть	EAP-PEAP, EAP-TLS	Wired_802.1X	Default protocols	0

Рисунок 274. Отображение записи новой политики. Элементы обязательные для заполнения

Для редактирования условия необходимо нажать **+ Добавить** и откроется редактор условий.

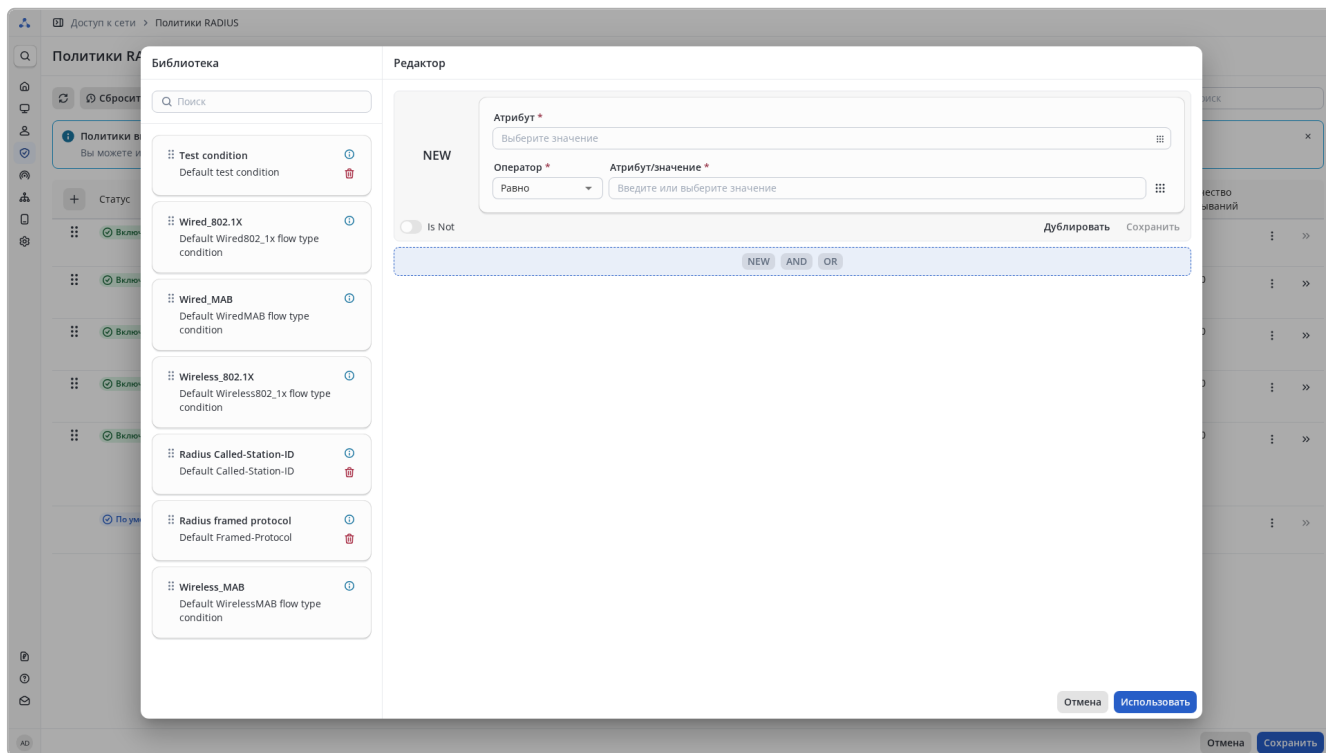


Рисунок 275. Редактор условий

Редактирование условий выполняется способом, аналогичным описанному в [условиях](#).



При настройке условия набора политик есть ограничение по используемым типам словарей. Можно использовать словари: **DEVICE**, **RADIUS**, **NORMALISED_RADIUS**, **INTERNAL_RADIUS**. Это связано с тем, какая информация о клиентском подключении может быть получена к моменту проверки набора политик, а какая еще нет.

При редактировании условий непосредственно в политике добавляется возможность использовать настроенное условие без сохранения его в **Библиотеке**. Для этого надо после настройки, не сохраняя условие, нажать кнопку **Использовать**.

После этого в колонке **Доступные протоколы** выбрать необходимый список.

По нажатию кнопки **Сохранить** изменения будут сохранены.



После создания новой политики необходимо настроить для нее политики аутентификации и авторизации, без этого все попытки подключения пользователей, попавшие под логическое условие данной политики, будут отклонены по правилам по умолчанию **Default**!

Для настройки перейти в [Политики аутентификации и авторизации](#).

Удаление набора политик

Удаление набора политик доступно в меню Действия. Доступно удаление только одного набора политик за раз.

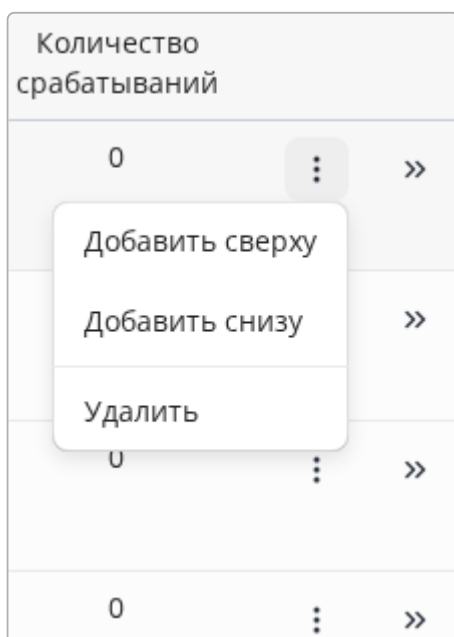


Рисунок 276. Выпадающее меню для удаления набора политик



Удаление элементов требует подтверждения в модальном окне. Выбранные элементы будут удалены только после явного подтверждения операции.

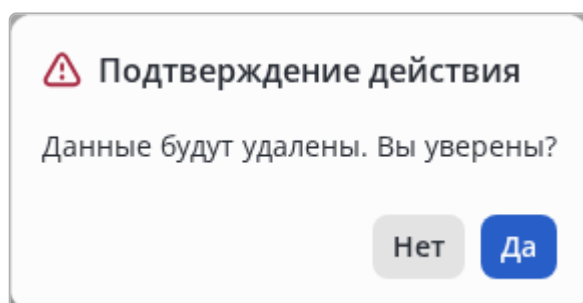


Рисунок 277. Диалоговое окно подтверждения действия

Количество срабатываний политики

Счётчики в колонке Количество срабатываний показывают, сколько попыток подключения было обработано с использованием этой политики. Изменения значений свидетельствует, что Условие срабатывает.



Используя статус **Проверка условий** и наблюдая за счётчиками срабатывания, можно сначала подобрать и отладить условие, а лишь потом включать политику в работу, переводя её в статус **Включено**.

Счетчики срабатывания всех наборов политик можно сбросить по клику на **Сбросить**. Для сброса счетчика конкретного набора нажмите на число в колонке Количество срабатываний,

нажмите на кнопку **Сбросить** и подтвердите действие.

Политики аутентификации и авторизации

Просмотр списка политик аутентификации и авторизации в выбранном наборе политик

Для просмотра списка политик аутентификации и авторизации необходимо в колонке **Просмотр** нажать **>>** справа от выбранного **набора политик**. Откроется детальная страница по изменению правил политик аутентификации и авторизации.

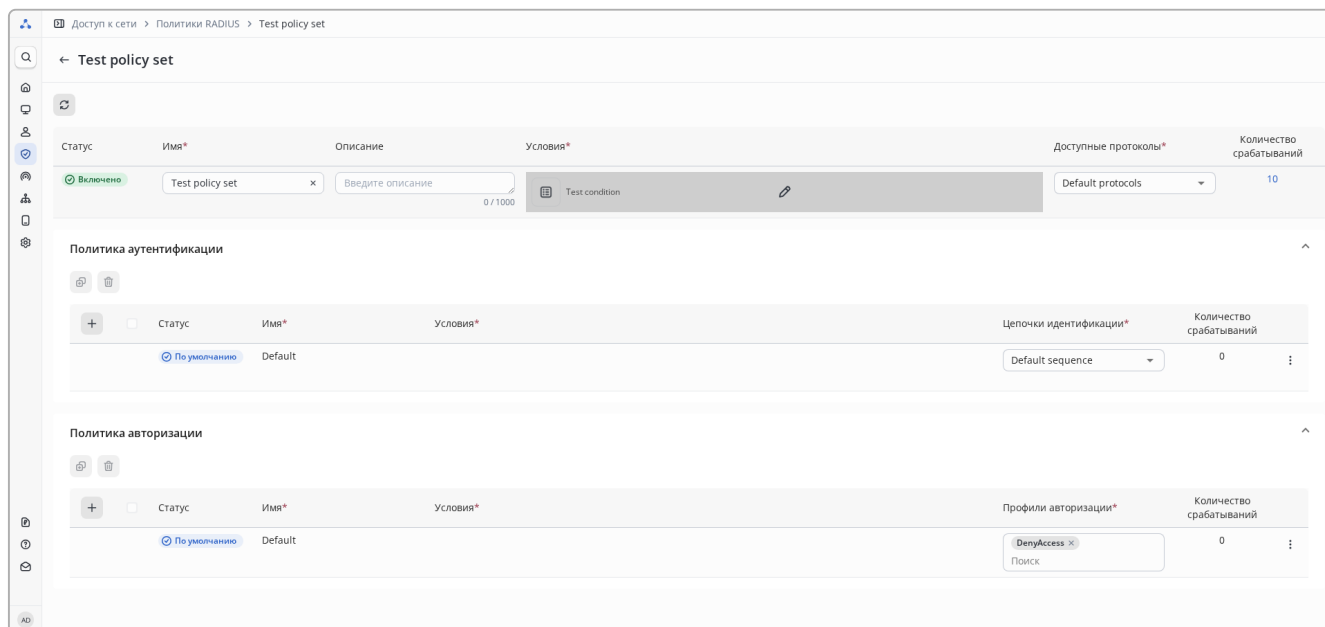


Рисунок 278. Страница просмотра и редактирования набора политик



Последние правила политик аутентификации и авторизации с именем **Default** нельзя переименовать или изменить им условие срабатывания. Они всегда будут последние в списке, ниже расположить другие правила нельзя. Данные правила предназначены для определения поведения по умолчанию, когда другие правила не подходят.

Форма просмотра отдельного набора политик разбита на блоки:

- Блок, отвечающий за управление набором политик, который отображает содержимое выбранного набора политик в формате аналогичном используемому на странице **Политики RADIUS**.
- **Политика аутентификации** - управление аутентификацией пользователей.
- **Политика авторизации** - управление авторизацией пользователей.

Элементы управления:

-  - запрос актуального количества срабатываний всех политик.
- **Статус** - включить/выключить/поставить на мониторинг соответствующую политику.
- **Имя *** - наименование политики.

Описание - произвольное описание.

- Условия * - используемые логические условия. Если используется библиотечное условие - отображается его имя. Если используется не библиотечное условие - отображается его структура.
- Доступные протоколы * - выбранный [список доступных протоколов](#).
- Цепочки идентификации * - выбранная [цепочка источников идентификации](#).
- Профили авторизации * - выбор доступных [профилей авторизации](#).
- Количество срабатываний - количество попыток авторизации, подпадающих под указанные Условия. При нажатии на число срабатываний счетчик можно **Сбросить**.
- ⋮ - действия:
 - Добавить сверху - добавить новое правило политики ДО выбранного;
 - Добавить снизу - добавить новое правило политики ПОСЛЕ выбранного;
 - Дублировать - добавить новое правило политики, аналогичное выбранному, перед дублируемым правилом;
 - Удалить - удалить выбранное правило.
- Сохранить - сохранить изменения.
- Отмена - отменить изменения.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

Для изменения порядка Политик Аутентификации и Авторизации перетащите политику за элемент ⋮ в колонке + аналогично разделу [Политики RADIUS](#).

Редактирование политик аутентификации и авторизации

Для редактирования необходимо нажать >> справа от выбранного набора политик.



Требуется настроить как минимум одну политику аутентификации и одну политику авторизации для возможности успешного подключения клиента с использованием данного набора политик, или перенастроить запрещающее правило по умолчанию Default.



Политику по умолчанию Default можно отредактировать, настроив другое поведение, однако для безопасности рекомендуется настраивать собственные правила с более узкой областью действия, а поведение по умолчанию оставить запрещающим.

Политика аутентификации

Статус	Имя*	Условия*	Цепочки идентификации*	Количество срабатываний
По умолчанию	Default		Default sequence	0

Рисунок 279. Панель политики аутентификации

Для настройки политики аутентификации в блоке **Политика аутентификации** необходимо нажать кнопку **+**. Появится новое правило.

Статус	Имя*	Условия*	Цепочки идентификации*	Количество срабатываний
☒	Authentication rule 1	+ Добавить	Выберите значение	
☒	Default		Default sequence	0

Рисунок 280. Новое правило политики аутентификации

В поле **Имя** ввести наименование правила политики.

Для редактирования условия необходимо нажать **+ Добавить** - откроется редактор условий. Редактирование условий выполняется аналогично описанному в [Условия](#).



При настройке условия для политики аутентификации есть ограничение по используемым типам словарей. Можно использовать словари: DEVICE, RADIUS, NORMALISED_RADIUS, INTERNAL_RADIUS.

При редактировании условий непосредственно в политике есть возможность использовать настроенное условие без сохранения его в Библиотеке условий. Для этого необходимо после настройки, не сохраняя условие, нажать кнопку **Использовать**.

Выбрать в выпадающем меню **Цепочки идентификации** [цепочку идентификаций](#).

Новое правило политики также можно создать из существующего, дублировав его. Для этого необходимо выбрать желаемое правило/правила через ☐, а затем нажать  над таблицей. Будет создано новое правило выше выбранного с аналогичными настройками и именем, оканчивающимся на "_сору".

Кнопкой  справа от политики можно добавить новое правило выше или ниже, дублировать либо удалить текущее.

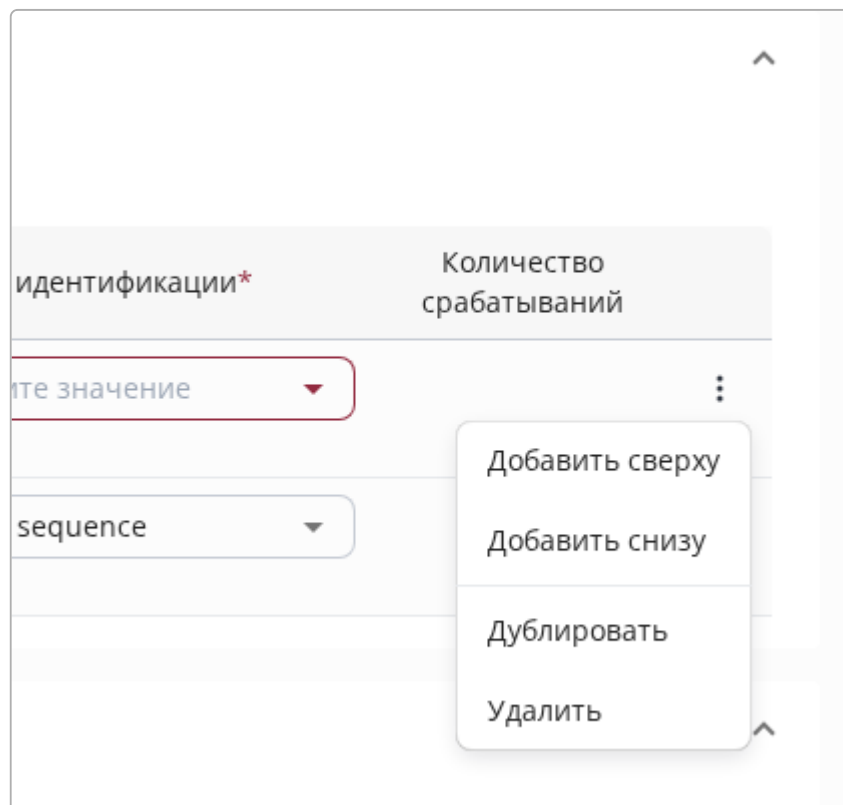


Рисунок 281. Политика аутентификации. Выпадающие меню. Действия

Также можно изменить статус политики аналогично статусам в наборах политик.

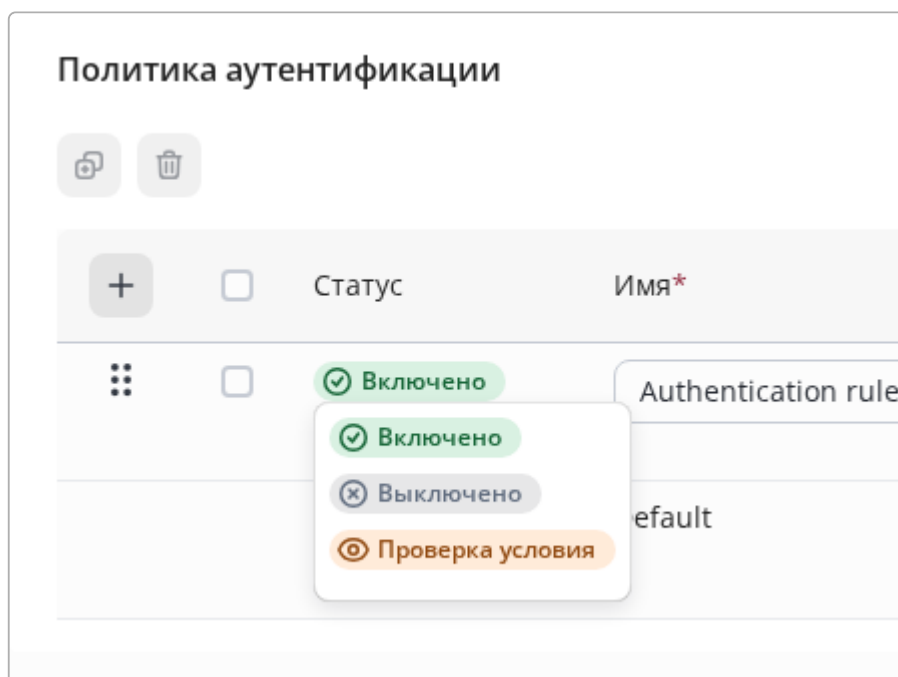


Рисунок 282. Политика аутентификации. Изменение статуса политики

Политика авторизации

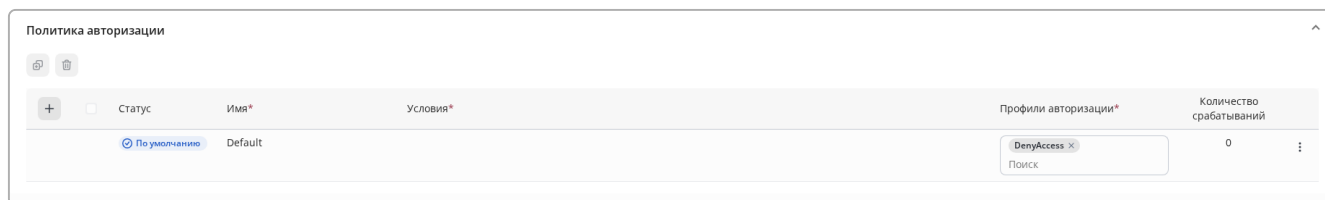


Рисунок 283. Панель политики авторизации

Для настройки правила политики авторизации в блоке **Политики авторизации** нажать **+**. Появится новое правило.

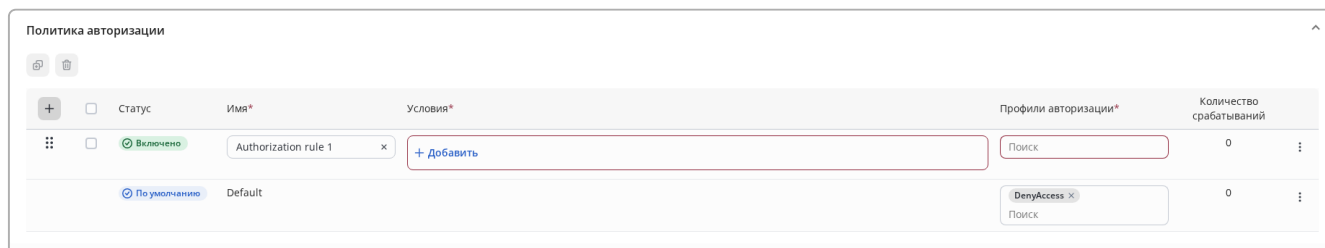


Рисунок 284. Новое правило политики авторизации

В поле **Имя** ввести наименование правила политики.

Для редактирования условия необходимо нажать **+ Добавить** - откроется редактор условий. Редактирование условий выполняется аналогично описанному в [Условия](#). При настройке политики авторизации можно использовать все типы словарей без ограничений.

При редактировании условий непосредственно в политике добавляется возможность использовать настроенное условие без сохранения его в Библиотеке. Для этого надо после настройки не сохраняя условие нажать кнопку **Использовать**.

Выбрать в выпадающем меню **Профили авторизации** необходимый [профиль авторизации](#). Можно при необходимости добавить несколько профилей, их не конфликтующие настройки будут просуммированы.



К одному правилу политики авторизации можно привязать несколько Профилей авторизации. Однако при обработке запроса будут учитываться только те, которые соответствуют текущему Профилю устройства.

Новое правило политики также можно создать из существующего, дублировав его. Для этого необходимо выбрать желаемое правило/правила через , а затем нажать  над таблицей. Будет создано новое правило выше выбранного с аналогичными настройками и именем, оканчивающимся на "_сору".

Кнопкой  справа от политики можно добавить новое правило выше или ниже, дублировать либо удалить текущее.

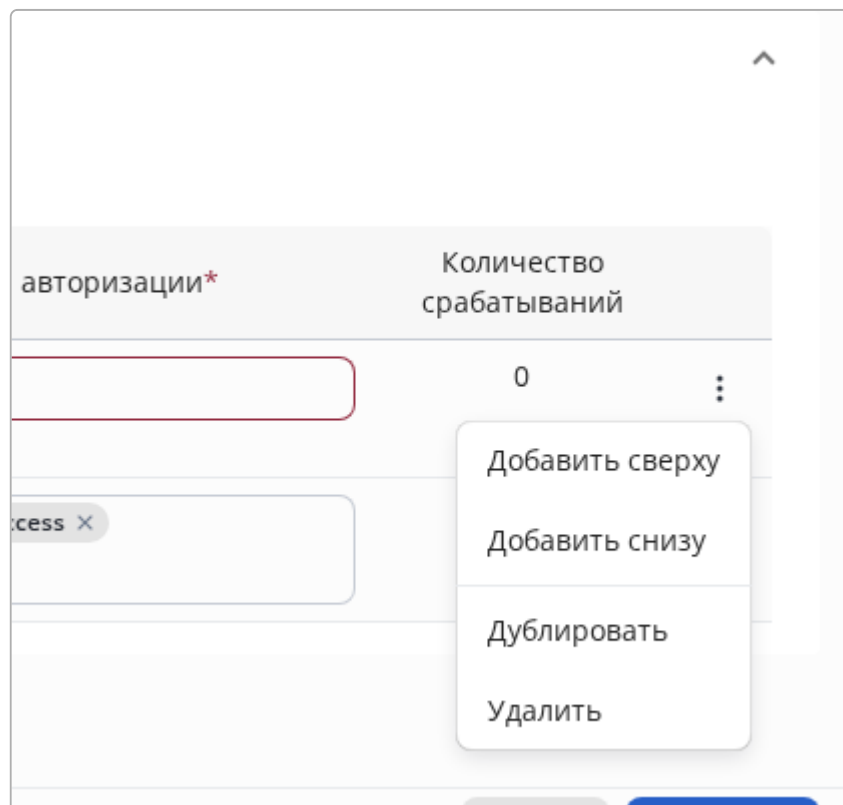


Рисунок 285. Политика авторизации. Выпадающие меню. Действия

Также можно изменить статус политики аналогично статусам в наборах политик.

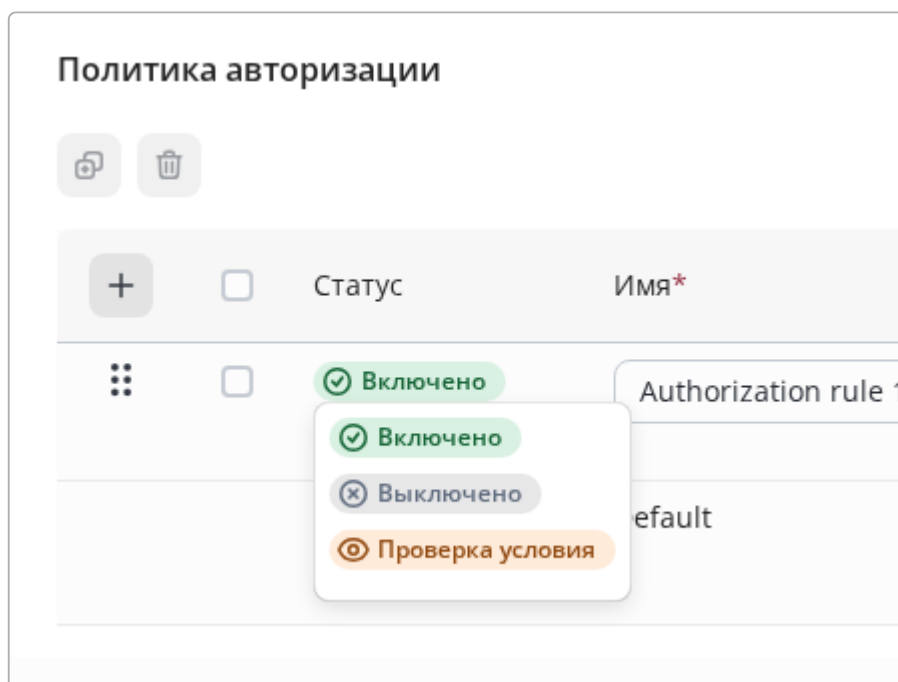


Рисунок 286. Политика авторизации. Изменение статуса политики

Кнопка **Сохранить** станет доступна только после добавления хотя бы одной, полностью настроенной, политики аутентификации и политики авторизации.

Нажать кнопку **Сохранить**.

Редактирование правил политик

Редактирование политик выполняется путем нажатия кнопкой мыши на поле соответствующей настройки.

После этого необходимо нажать кнопку **Сохранить**.

Удаление правил политик

Удаление единичного правила выполняется нажатием на кнопку  и выбором действия **Удалить**.

Для удаления нескольких правил необходимо выбрать их с помощью , а затем нажать  над таблицей с правилами.



Удаление элементов требует подтверждения в модальном окне. Выбранные элементы будут удалены только после явного подтверждения операции.

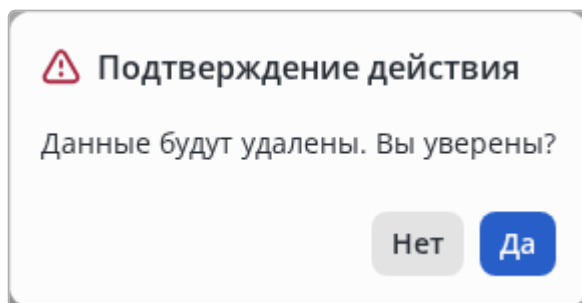


Рисунок 287. Диалоговое окно подтверждения действия

Профилирование

Профилирование - процесс динамического обнаружения и классификации эндпоинтов на основе атрибутов, получаемых из различных источников (проб). В ходе профилирования собранные атрибуты сопоставляются с заранее созданными или заданными пользователем условиями, которые затем сопоставляются с профилями для их присвоения эндпоинту.

Меню содержит разделы:

- [Условия профилирования](#) - условия, определяющие как собранные атрибуты должны быть интерпретированы для классификации эндпоинта;
- [Политики профилирования](#) - набор правил, которые используются для автоматической классификации и управления доступом эндпоинтов на основе результатов профилирования;
- [Логические профили](#) - объединение определенных политик профилирования в логическую группу для более удобного использования в политиках доступа.

Условия профилирования

Описание

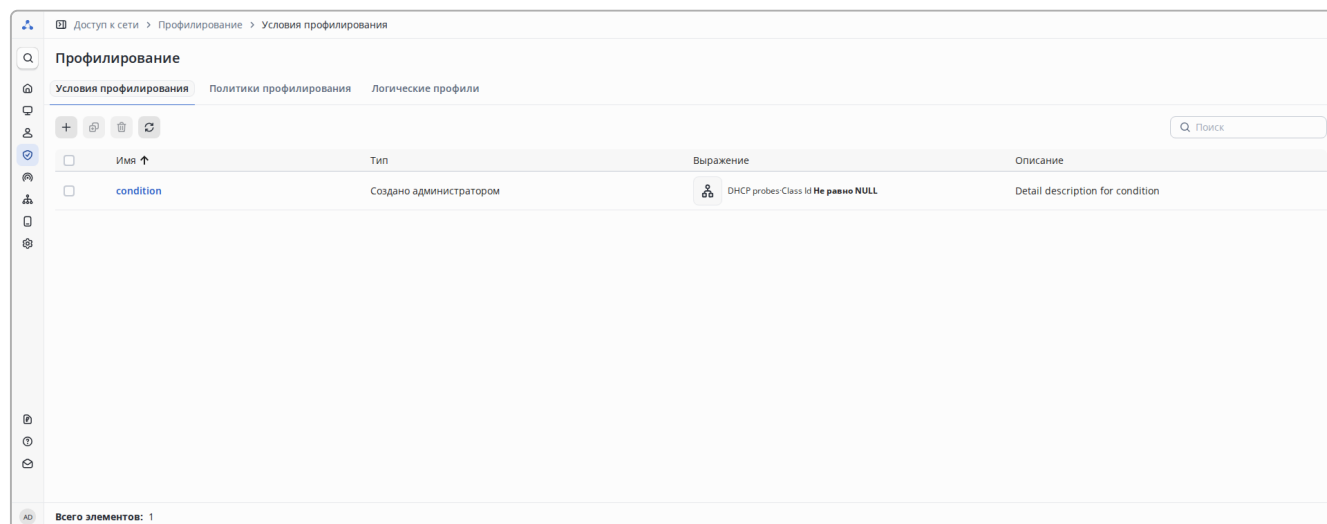
Условия профилирования являются основными элементами, используемыми в политиках профилирования. Они определяют, соответствует ли [эндпоинт](#) определенному признаку, на основе

которого можно сделать вывод о его типе, модели, производителе, операционной системе и другим атрибутам.

В основе создания и обработки логического условия профилирования лежит алгебра логики. Результатом выполнения условия является "Истина" или "Ложь". Каждое условие профилирования может содержать только один атрибут.

Просмотр списка условий профилирования

На данной странице содержится таблица со списком всех условий профилирования.



Имя	Тип	Выражение	Описание
condition	Создано администратором	DHCP probes Class Id Не равно NULL	Detail description for condition

Рисунок 288. Таблица условий профилирования

Таблица содержит колонки:

- Имя** - наименование условия профилирования.
- Тип** - тип условия профилирования. Может быть "Системное" или "Создано администратором". Системные условия предустановлены и не могут быть удалены или изменены.
- Выражение** - логическое условие, описывающее критерий по которому будет выполнено профилирование.
- Описание** - произвольное описание условия профилирования.

Сортировка возможна только по полю "Имя" в прямом и обратном порядке. По умолчанию сортировка выполняется в прямом (алфавитном) порядке.

Элементы управления:

-  — Добавить новый элемент.
-  — Дублировать выбранный чекбоксом элемент. Становится активным, если выбран только один элемент в списке.
-  — Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
-  — Обновить данные таблицы.
- ☐ — Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).

-  — Изменить текущий порядок сортировки.
-  Поиск — Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.

Добавление условия профилирования

Для добавления условия профилирования нажмите  в левой верхней части поля над таблицей.

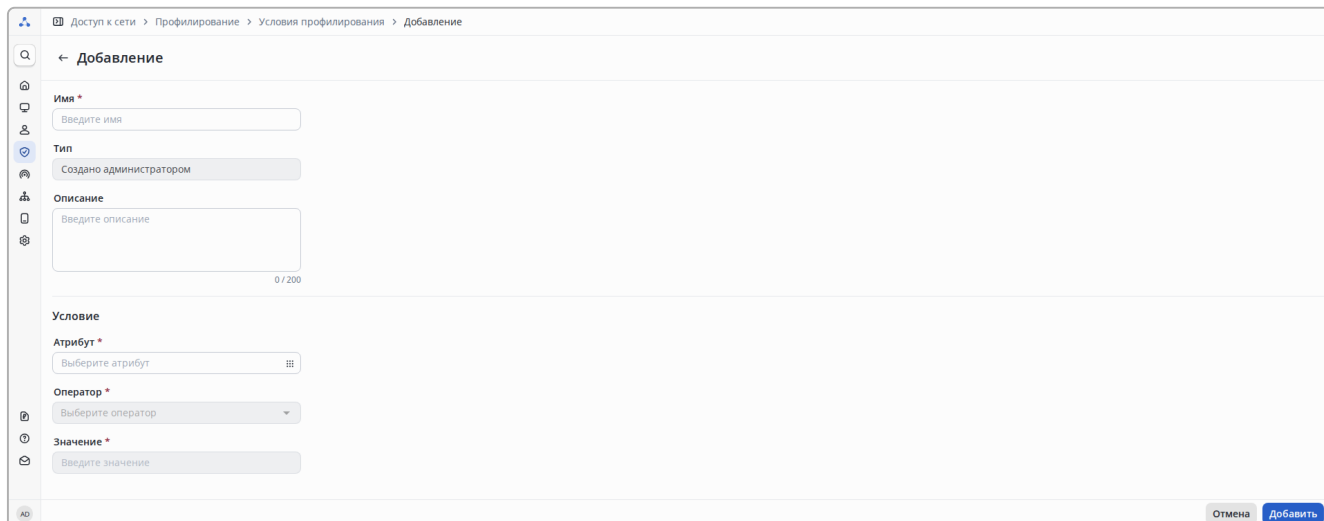


Рисунок 289. Форма добавления условия профилирования

В открывшейся странице представлены следующие параметры:

- **Имя *** - наименование условия профилирования. Максимальная длина - 100 символов.
- **Тип** - тип условия профилирования. Не может быть задано и всегда имеет значение "Создано администратором".
- **Описание** - произвольное описание условия профилирования. Максимальная длина - 200 СИМВОЛОВ.

Условие - блок, отвечающий за настройку условия профилирования.

- **Атрибут *** - по нажатию на кнопку  слева в поле откроется словарь для добавления атрибута.
- **Оператор *** - выбранный оператор логического условия. Может принимать значения (в зависимости от типа значения атрибута):
 - "Начинается с" / "Не начинается с"
 - "Оканчивается на" / "Не оканчивается на"
 - "Равно" / "Не равно"
 - "Равно NULL" / "Не равно NULL"
 - "Содержит" / "Не содержит"
 - "Соответствует" (полное соответствие строки с учетом регистра)
- **Значение *** - значение, которые используются для сопоставления с атрибутом логического условия в соответствии с выбранным оператором. Для атрибута, предполагающего

предопределенные значения, выбор значения производится из списка.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

Меню выбора атрибута

Для выбора атрибута, который будет использоваться в условии, необходимо нажать  - раскроется меню выбора атрибута.

Выбор атрибута для условия

Все  Profiling

Поиск

Словарь

Выберите словарь

ID

ID

Атрибут	Словарь	ID
Class Id	DHCP probes	60
Client Id	DHCP probes	61
Hostname	DHCP probes	12
Parameter List	DHCP probes	55
Requested address	DHCP probes	50
OUI	MAC	1

Рисунок 290. Меню выбора атрибута

Для выбора доступны только атрибуты словарей типа "PROFILING". Данный тип словарей обозначен иконкой .

Сверху находится список, позволяющий выполнить фильтрацию атрибутов:

- **Атрибут** - наименование атрибута.
- **Словарь** - наименование словаря, выполненное в форме выпадающего списка. Доступны для выбора словари "DHCP probes" и "MAC". Так же доступно для выбора "Не выбрано", если требуется отказаться от фильтрации.
- **ID** - идентификатор атрибута (числовое значение).

Редактирование условия профилирования

Для редактирования условия профилирования необходимо на странице со списком нажать на его имя.



Рисунок 291. Гиперссылка на страницу редактирования условия

После этого откроется окно редактирования.

A screenshot of a web application interface for editing a condition. The breadcrumb trail at the top reads: 'Доступ к сети > Профилирование > Условия профилирования > condition'. The main heading is '← condition'. The form contains several sections: 'Имя *' with a text input containing 'condition'; 'Тип' with a dropdown menu showing 'Создано администратором'; 'Описание' with a text area containing 'Detail description for condition' and a character count '32 / 200'; 'Условие' section with 'Атрибут *' (a dropdown showing 'DHCP probes-Class Id'), 'Оператор *' (a dropdown showing 'Не равно NULL'), and 'Значение *' (a text input with placeholder 'Введите значение'). A left sidebar contains various icons for navigation.

Рисунок 292. Форма редактирования условия профилирования

После редактирования необходимо нажать на кнопку **"Сохранить"**. Кнопка скрыта, пока не будет внесено хотя бы одно изменение.

Кнопка **"Отмена"** осуществляет сброс внесенных изменений до исходного состояния.

Копирование условия профилирования

Новое условие профилирования можно создать на основе уже существующего.

Для этого выберите одно из существующих условий с помощью чекбокса и нажмите на . В открывшемся окне добавления условия все поля заполнены значениями из выбранного условия. По умолчанию к значению в поле **Имя** добавляется "_сору". Можно задать любое другое имя, которое еще не используется в системе.

Рисунок 293. Форма копирования условия профилирования

После копирования условие не имеет никакой связи с исходным условием. Существуют и работают эти условия независимо друг от друга. Это всего лишь заполнение полей на момент добавления.

Имя	Тип	Выражение	Описание
condition	Создано администратором	DHCP probes-Class Id Не равно NULL	Detail description for condition
condition_copy	Создано администратором	DHCP probes-Class Id Не равно NULL	Detail description for condition

Рисунок 294. Таблица условий профилирования после копирования условия

Удаление условий профилирования

Для удаления в окне со списком надо выделить чекбокс слева от наименования условий профилирования, которые требуется удалить, и нажать кнопку  вверху слева.

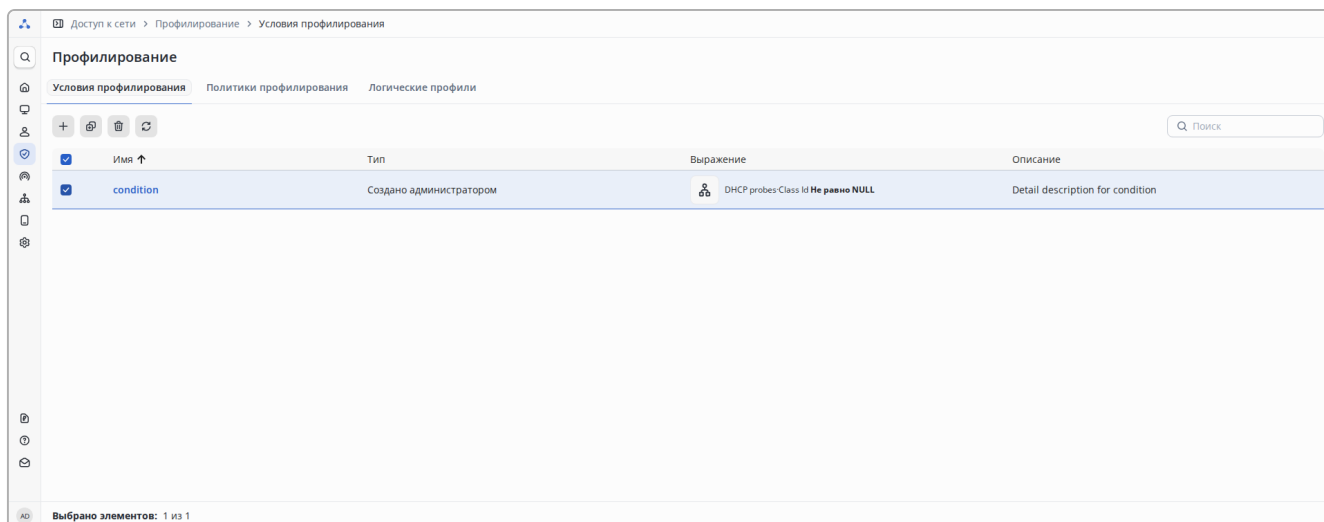


Рисунок 295. Выбор условий для удаления



Удаление элементов требует подтверждения в модальном окне. Выбранные элементы будут удалены только после явного подтверждения операции.

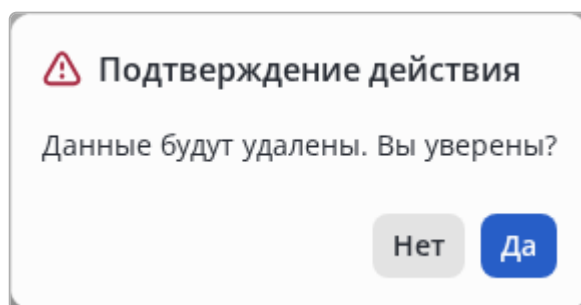


Рисунок 296. Диалоговое окно подтверждения действия

Ограничения:



Нельзя удалить условие профилирования, которое уже назначено какой-либо политике профилирования.

Политики профилирования

Описание

Политики профилирования предназначены для динамической классификации новых и существующих [эндпоинтов](#), подключенных к сети. Для классификации используются [условия профилирования](#), на основании которых выполняется определение и назначение эндпоинту политики профилирования. Она может использоваться в условиях политик авторизации для предоставления доступа в соответствии с определенной политикой. Также на основании политики профилирования эндпоинт помещается в выбранную [группу эндпоинтов](#).

Например, на основании условий профилирования можно определить эндпоинт как устройство определенного типа и производителя (например, IP-телефон Eltex), и настроить политику авторизации для выдачи этим устройствам определенных VLAN и ACL.

Процесс определения и назначения эндпоинту политики профилирования в соответствии с определенными для него в политике условиями называется "Профилирование эндпоинта".



Для эндпоинтов, имеющих вручную назначенные "Политику профилирования" или "Группу эндпоинта", эти параметры не могут быть изменены по результатам выполнения профилирования.

Просмотр политик профилирования

На данной странице доступен просмотр и управление политиками профилирования. Политики профилирования имеют иерархическую структуру, которая необходима для группировки эндпоинтов.

В левой части окна содержится дерево политик профилирования, в котором осуществляется выбор политики для просмотра или редактирования.

В правой части окна отображается форма создания/редактирования политики профилирования. Если в дереве выбран элемент **Все политики**, то в правой части окна отображается таблица со списком всех политик профилирования.

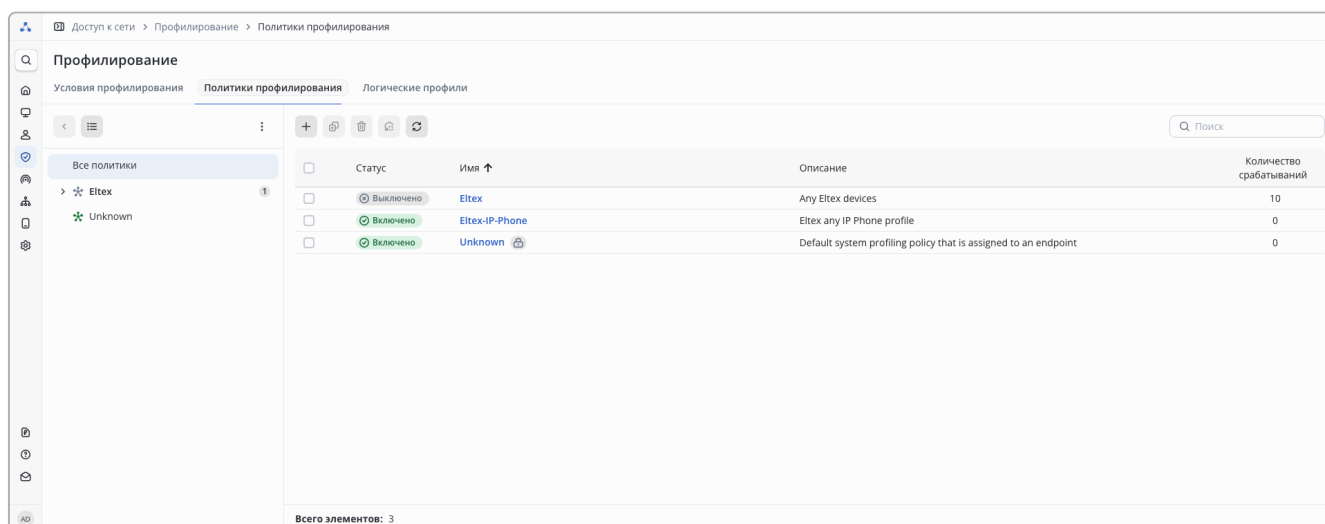


Рисунок 297. Просмотр политик профилирования

Просмотр дерева или списка политик профилирования

Дерево политик профилирования расположено в левой части и отображает список политик профилирования в виде древовидной структуры или в виде списка дочерних политики профилирования выбранного узла - способ отображения можно переключать, по умолчанию используется отображение в виде древовидной структуры.

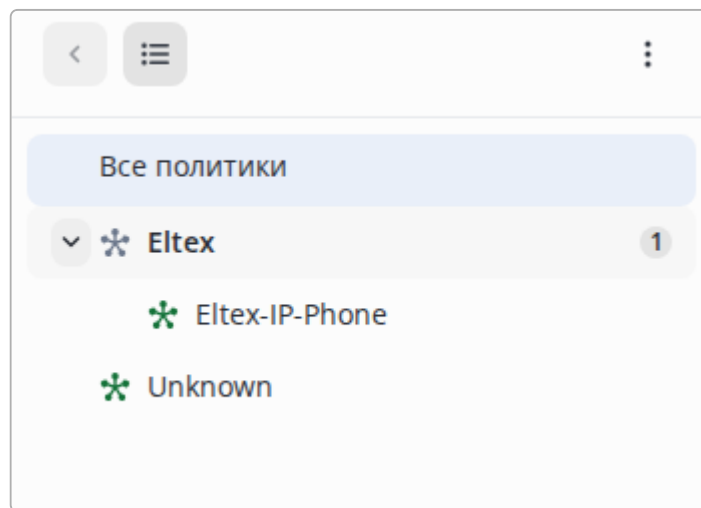


Рисунок 298. Дерево политик профилирования

Содержит следующие элементы управления:

-  - включен режим отображения в виде древовидной структуры политик профилирования (для переключения режима на противоположный необходимо нажать на иконку).
-  - включен режим отображения в виде списка дочерних политик профилирования (для переключения режима на противоположный необходимо нажать на иконку).
-  - добавление/дублирование/удаление политики. Выбор доступных действий зависит от выбранного элемента в дереве политик.
-  - переход на уровень выше от текущей политики (активно только в режиме списка дочерних политик, при нахождении в дочерней политике).
-  - в режиме древовидной структуры отображается слева от наименования политик профилирования, если список закрыт. Неактивна, если нет дочерних элементов. В режиме списка отображается справа наименования политик профилирования, имеющих дочерние элементы.
-  - в режиме древовидной структуры отображается слева от наименования политик профилирования имеющих дочерние элементы, если список раскрыт.
-  - элемент для обозначения политики профилирования.

Все политики - заголовок списка политик. При выборе данного элемента в правой части окна будет отображаться "плоский" список всех политик профилирования. Выбирается по умолчанию при переходе на страницу политик профилирования.

Unknown - системная политика профилирования, которая используется для профилирования эндпоинтов, не попавших под другие политики профилирования. Не может быть отредактирована. Так же для неё нельзя создать дочерние политики.

Просмотр списка политик профилирования

Список всех политик профилирования отображается в правой части страницы в виде таблицы, если в дереве политик профилирования выбран элемент Все политики.

☐	Статус	Имя ↑	Описание	Количество срабатываний
☐		Eltex	Any Eltex devices	10
☐		Eltex-IP-Phone	Eltex any IP Phone profile	0
☐		Unknown	Default system profiling policy that is assigned to an endpoint	0

Всего элементов: 3

Рисунок 299. Таблица со списком всех политик профилирования

Таблица содержит колонки:

- **Статус** - текущий статус политики профилирования: может принимать значения **Включено** или **Выключено**.
- **Имя** - наименование политики профилирования.
 - - Данная запись является системной и недоступна для удаления или редактирования.
- **Тип** - тип политики профилирования. Возможны значения "Создана администратором" или "Системная".
- **Описание** - описание политики профилирования.
- **Количество срабатываний** - количество проверок на соответствие эндпоинта политике профилирования.

Сортировка возможна по полям "Статус" и "Имя" в прямом и обратном порядке. По умолчанию сортировка выполняется в прямом (алфавитном) порядке по полю "Имя".

Элементы управления:

- — Добавить новый элемент.
- — Дублировать выбранный чекбоксом элемент. Становится активным, если выбран только один элемент в списке.
- — Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- — Обновить данные таблицы.
- ☐ — Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).
- — Изменить текущий порядок сортировки.
- **Поиск** — Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
-

 - Сбросить счётчик попаданий в политику профилирования. Становится активным, если выбран хотя бы один элемент в списке и количество срабатываний политики больше 0.

Добавление политики профилирования

Добавление политики профилирования возможно двумя способами:

- через дерево политик профилирования: нажать иконку  над деревом и выбрать "Добавить корневую политику", если выбран элемент "Все политики", или "Добавить дочернюю политику" если выбрана политика профилирования.

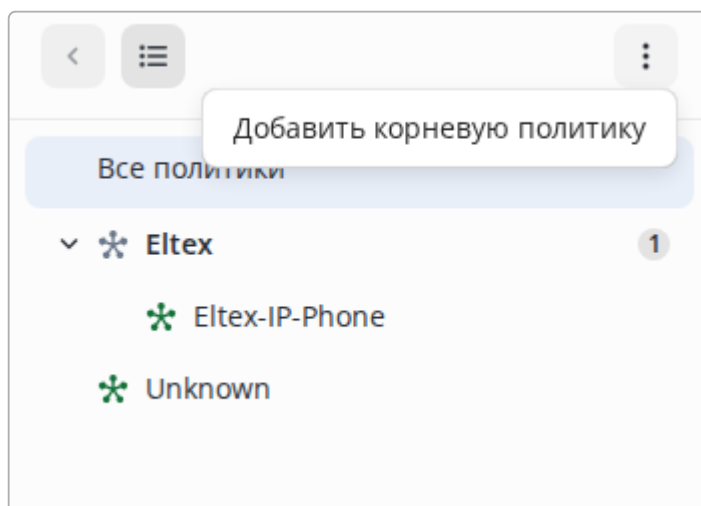


Рисунок 300. Добавление политики профилирования. Действия

- через таблицу политик профилирования: нажать иконку  в левой верхней части поля над таблицей. NOTE: Если выделить через чекбокс уже существующую политику, а после нажать иконку создания политики, то она станет родительской для новой политики.



Для системной политики профилирования "Unknown" добавление дочерних политик запрещено.

Доступ к сети > Профилирование > Политики профилирования > Добавление

← Добавление

Всё политики

> EteX

Unknown

Включено

Имя *

Введите имя

Родительская политика *

Выберите родительскую политику

Тип

Создана администратором

Минимальный уровень доверия *

10

Описание

Введите описание

0 / 200

Группировка эндпоинтов

☒ Использовать общую группу Profiled

☐ Создать группу эндпоинтов

Правила

Условие *	тогда	Действие	Значение *
Если	Выберите условие	Повышение уровня доверия	10

Рисунок 301. Добавление политики профилирования

В результате в правой части страницы откроется раздел добавления политик, содержащий следующие параметры:

- **Статус** - статус политик профилирования. Может принимать значения "Включено" и "Выключено". По умолчанию значение "Включено".
- **Тип** - тип политики профилирования. Все вручную созданные политики профилирования имеют значение "Создана администратором", изменить его нельзя.
- **Имя *** - наименование политики профилирования. Максимальная длина - 100 символов.
- **Родительская политика** - родительская политика профилирования. Можно выбрать родительскую политику профилирования в выпадающем списке или не выбирать ничего для создания корневой политики профилирования. При создании политики профилирования из дерева политик путем выбора меню "Добавить дочернюю политику" будет автоматически подставлена выбранная в дереве политика профилирования. При необходимости можно выбрать и другую Родительскую политику.
- **Минимальный уровень доверия *** - минимальное количество баллов, которое нужно получить в правилах, чтобы политика считалась подходящей для назначения эндпоинту. Не может быть больше, чем сумма значений всех уровней доверия, настроенных в разделе "Правила". Может принимать значения от 1 до 65535.
- **Описание** - произвольное описание условия политики профилирования. Максимальная длина - 200 символов.
- **Группировка эндпоинтов** - раздел, определяющий принцип группировки эндпоинтов. Доступен выбор следующих значений:
 - **Использовать общую группу Profiled** - данный выбор доступен и отображается только для корневой политики профилирования. Эндпоинты, классифицированные как принадлежащие данной политике профилирования, будут помещены в системную группу эндпоинтов "Profiled".

Использовать группу эндпоинтов родительской политики - данный выбор доступен и отображается только для дочерней политики профилирования. Эндпоинты, классифицированные как принадлежащие данной политике профилирования, будут помещены в указанную в родительской политике группу. Если для родительских политик не указаны группы - эндпоинты будут помещены в группу "Profiled".

- Создать группу эндпоинтов - автоматически создать группу эндпоинтов с использованием наименования политики профилирования. Эндпоинты, классифицированные как принадлежащие данной политике профилирования, будут помещены в эту группу.
- **Правила** - раздел правил, отвечающий за настройку классификации эндпоинтов с использованием условий профилирования. Содержит параметры:
 - **Условие *** - меню выбора условия профилирования.
 - **Значение *** - количество баллов, которое будет назначено эндпоинту в случае совпадения условия профилирования.
 - **+** - иконка расположена справа от условия профилирования. При нажатии данной иконки ниже будет добавлено новое условие профилирования.

Рисунок 302. Добавление правил в политику профилирования

Параметры, отмеченные звездочкой *, обязательны для заполнения.



Политика профилирования должна содержать минимум одно правило.



Для одной политики профилирования может быть добавлено несколько правил.



Запрещено добавлять одинаковое условие профилирования в политику несколько раз.

Для добавления политики нажмите кнопку **Добавить**. Кнопка станет активной после заполнения всех необходимых полей политики профилирования.

Редактирование политики профилирования

Редактирование политики профилирования возможно двумя способами:

- Выбрать политику профилирования в дереве политик слева и нажать на нее - в правой части откроется форма редактирования.
- В списке всех политик в колонке "Имя" нажать на наименование политики - произойдет переход на форму редактирования данной политики.

После добавления политики профилирования внутри ее детальной информации добавляется поле **Количество срабатываний политики** и элемент управления **Сбросить счётчик**.

- **Количество срабатываний политики** - количество проверок на соответствие эндпоинта политике профилирования.
-  - сбросить счётчик попаданий в политику профилирования. Становится активным, если количество срабатываний политики больше 0.

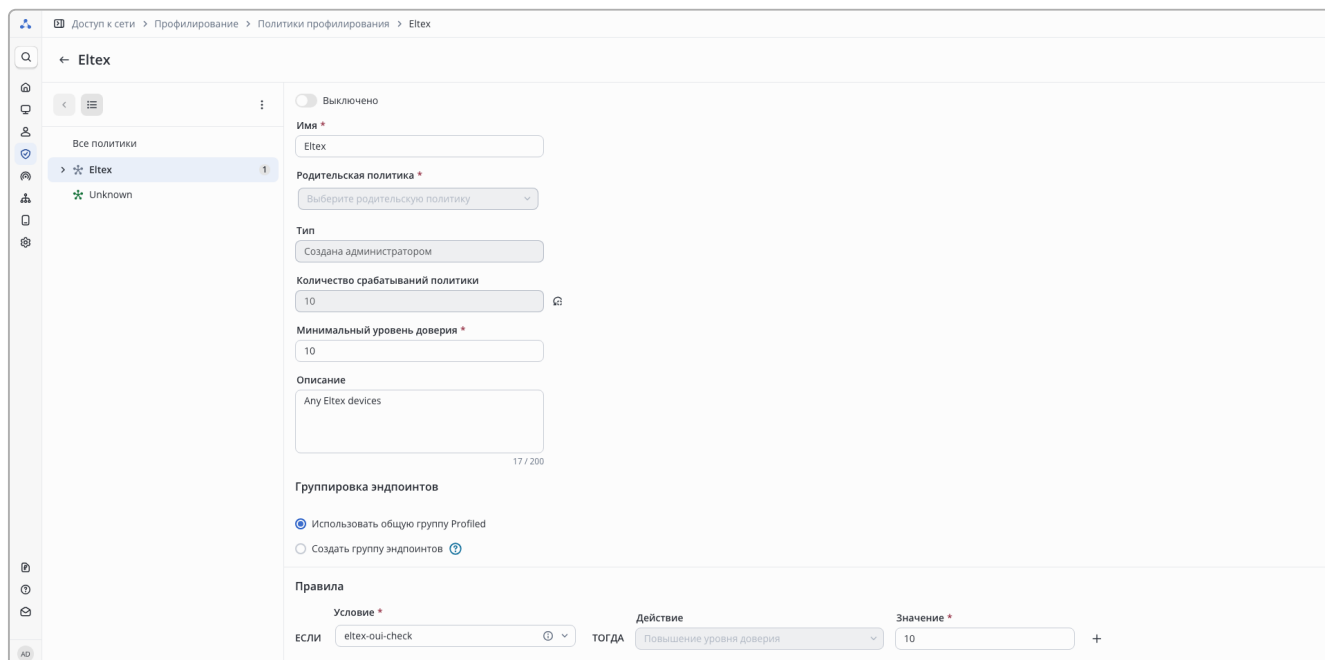


Рисунок 303. Редактирование политики профилирования



Редактирование системной политики профилирования "Unknown" недоступно.

После редактирования необходимо нажать на кнопку **"Сохранить"**. Кнопка скрыта, пока не будет внесено хотя бы одно изменение.

Кнопка **"Отмена"** осуществляет сброс внесенных изменений до исходного состояния.

Копирование политик профилирования

Новая политика профилирования может быть создана на основе существующей. Это можно сделать двумя способами:

- В дереве политик выбрать одну из существующих политик профилирования и нажать иконку . В списке доступных действий выбрать меню "Дублировать политику".
- В списке всех политик выбрать одну из существующих политик профилирования и нажать иконку .



Действие недоступно, если выбрано более одной политики или "Unknown".

Откроется форма, аналогичная форме добавления политик, где все поля будут заполнены значениями из выбранной политики. По умолчанию к значению в поле **Имя** добавляется "_copy". Можно задать любое другое имя, которое еще не используется в системе.

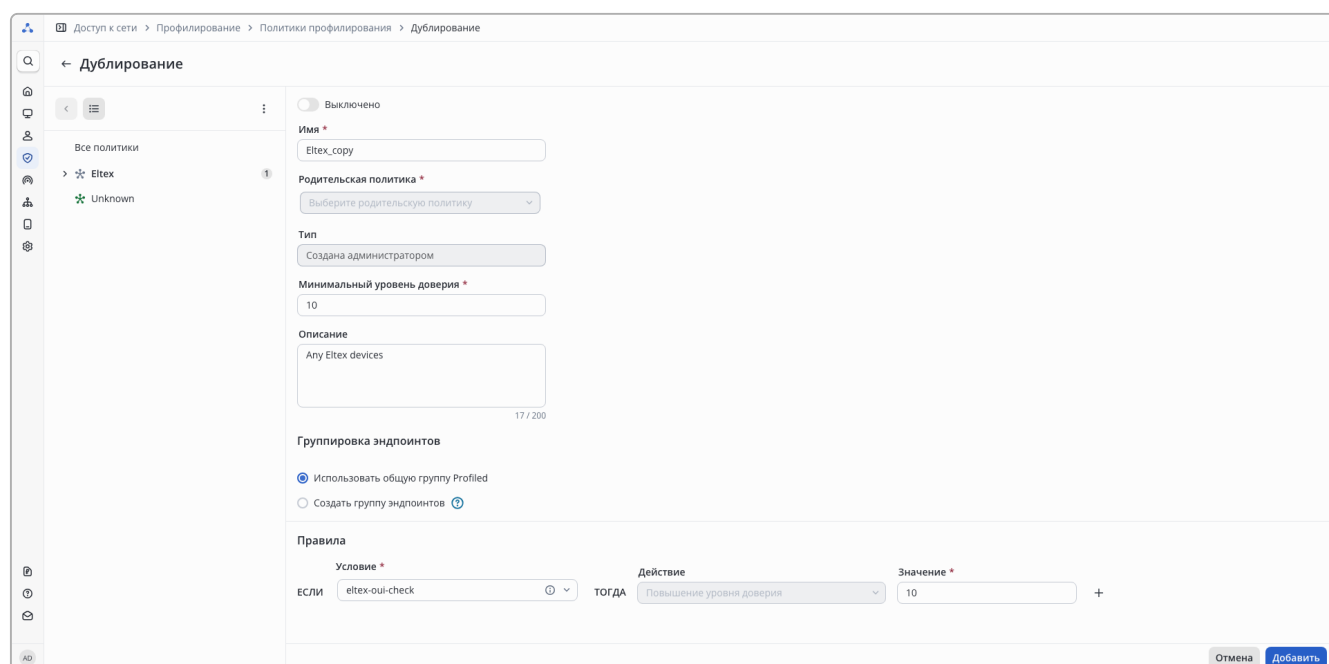


Рисунок 304. Дублирование политики профилирования

После копирования политика профилирования не имеет никакой связи с исходной. Существуют и работают эти политики профилирования независимо друг от друга - исходная используется для заполнения полей новой на момент добавления.

Удаление политик профилирования

Удаление политик профилирования возможно двумя способами:

- через дерево политик профилирования: необходимо выделить политику и нажать на иконку . В списке доступных действий выбрать меню "Удалить политику". В дереве политик можно выполнять удаление только по одной политике профилирования.
- через таблицу политик профилирования: необходимо выделить чекбокс слева от наименования политик профилирования, которые требуется удалить, и нажать кнопку  вверху слева. Можно выделить несколько политик профилирования для удаления.



Удаление элементов требует подтверждения в модальном окне. Выбранные элементы будут удалены только после явного подтверждения операции.

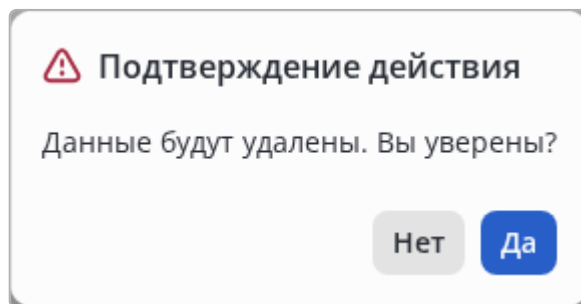


Рисунок 305. Диалоговое окно подтверждения действия



Ограничения:

- Нельзя удалить политику профилирования, которая используется в каком-либо [логическом профиле](#).
- Нельзя удалить политику профилирования, которая используется в каком-либо логическом условии или условии политики авторизации.
- Нельзя удалить системную политику профилирования "Unknown".

Описание работы профилирования

Принцип работы уровня доверия

В рамках политики профилирования выполняется проверка соответствия условиям, добавленным в раздел **Правила**, имеющихся данных по эндпоинту:

- Для условия профилирования по MAC OUI выполняется определение наименования вендора по MAC и указанному в настройках значению (в соответствии с выбранным оператором). В случае успешной проверки эндпоинт получает указанное в колонке **Значение** (по умолчанию 10).
- Для условий профилирования по DHCP проверяется наличие соответствующей пробы DHCP и соответствие ее указанному значению в условии профилирования. В случае успешной проверки значение уровня доверия к эндпоинту повышается на указанное в колонке **Значение** (по умолчанию 10).
- После выполнения проверки всех настроенных в политике профилирования правил, формируется значение уровня доверия эндпоинту. Данный уровень доверия представляет собой сумму всех значений, указанных в условиях профилирования, которым соответствуют имеющиеся пробы эндпоинта.
- Полученный уровень доверия эндпоинта сравнивается со значением, указанным в настройке **Минимальный уровень доверия** политики профилирования.
- Если минимальный уровень доверия политики профилирования меньше или равен уровню доверия, полученному в результате проверки эндпоинта, считается, что эндпоинт соответствует политике, и ему назначается данная политика профилирования и указанная в ее настройках группа эндпоинтов.



Уровень доверия считается только в рамках политики профилирования, для которой выполняется проверка соответствия эндпоинта. Никакие значения из других политик не учитываются!

Принцип проверки соответствия эндпоинта политикам профилирования

При профилировании эндпоинта выполняются следующие действия:

- На первом уровне политик профилирования выполняется поиск подходящей эндпоинту политики профилирования из добавленных пользователем системы.
- Если эндпоинт не попадает ни под одну добавленную пользователем систему политики профилирования или они не настроены: назначается политика профилирования по умолчанию **Unknown** и эндпоинт помещается в группу **Unknown**, процесс профилирования на этом заканчивается.
- Если найдена подходящая, добавленная пользователем система политики профилирования, - выполняется проверка наличия у нее дочерних политик профилирования - если их нет, эндпоинту назначается найденная политика профилирования и группа, указанная в её настройке Группировка эндпоинтов. Если в корневой политике выбрано Использовать общую группу Profiled - эндпоинт помещается в системную группу **Profiled**. Процесс профилирования на этом заканчивается.
- Если у политики профилирования есть дочерние политики - выполняется проверка соответствия эндпоинта среди дочерних политик. Если эндпоинт не соответствует ни одной из дочерних политик - проверка останавливается, эндпоинту назначается родительская политика и группа из настроек родительской политики.
- Если эндпоинт соответствует одной из дочерних политик - ему назначается эта политика профилирования и группа из настроек данной политики. Если в дочерней политике выбрана настройка Использовать группу эндпоинтов родительской политики - назначается группа в соответствии с настройками родительской политики.

Ограничения настроек политик профилирования

Существуют следующие ограничения, которые необходимо учитывать при настройке политик профилирования:

- На одном уровне корневых или дочерних политик профилирования не допускается настройка нескольких политик, которым может соответствовать эндпоинт! В случае возникновения такой ситуации необходимо изменить настройки политик профилирования, чтобы на одном уровне профилирование эндпоинтов проходило только по одной из них! Для более точного профилирования эндпоинтов следует настроить дочерние политики.
- В рамках одной политики профилирования минимальный уровень доверия не может быть больше (но может быть меньше или равен), чем сумма всех уровней доверия, указанных в ее правилах.
- При отключении политики профилирования также перестают использоваться для профилирования ее дочерние политики, даже если они включены.
- Политика по умолчанию **Unknown** не может быть удалена или изменена. Для нее не могут быть созданы дочерние политики.
- Если эндпоинт не удовлетворяет требованиям ни одной из настроенных политик, он считается соответствующим политике по умолчанию **Unknown**.
-

Если эндпоинту назначены вручную политика профилирования или группа эндпоинта, то соответствующая настройка не может быть изменена по результатам профилирования. Для возобновления автоматического профилирования потребуется отключить ручное назначение политики или ручное назначение группы.

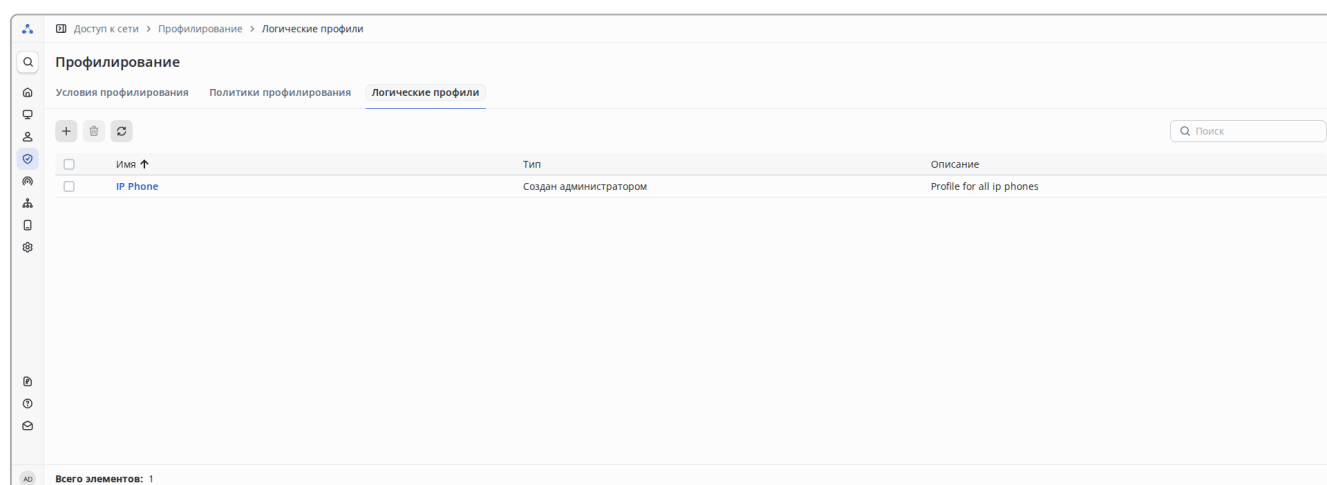
Логические профили

Описание

Логические профили предназначены для объединения определенных политик профилирования в логическую группу, которая может быть использована в настройках политик авторизации, что позволяет упростить структуру и уменьшить количество правил в политике. Например, логический профиль "Принтеры" может объединять в себе политики профилирования "Принтеры HP", "Принтеры Xerox", и "Принтеры Canon". Одна политика профилирования может быть членом нескольких различных логических профилей.

Просмотр логических профилей

На данной странице содержится таблица со списком всех логических профилей.



The screenshot shows a web interface for managing logical profiles. At the top, there's a breadcrumb trail: 'Доступ к сети > Профилирование > Логические профили'. Below this is a search bar and a tabbed interface with 'Логические профили' selected. The table has three columns: 'Имя' (Name), 'Тип' (Type), and 'Описание' (Description). One profile is listed: 'IP Phone' with type 'Создан администратором' and description 'Profile for all ip phones'. At the bottom left, it says 'Всего элементов: 1'.

Имя	Тип	Описание
IP Phone	Создан администратором	Profile for all ip phones

Рисунок 306. Таблица логических профилей

Таблица содержит колонки:

- Имя** - наименование логического профиля.
- Тип** - тип логического профиля. Может быть "Системное" или "Создано администратором". Системные условия предустановлены и не могут быть удалены или изменены.
- Описание** - произвольное описание логического профиля.

Сортировка возможна только по полю "Имя" в прямом и обратном порядке. По умолчанию сортировка выполняется в прямом (алфавитном) порядке.

Элементы управления:

-  — Добавить новый элемент.
-  — Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
-  — Обновить данные таблицы.

☐ — Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).

-  — Изменить текущий порядок сортировки.
-  Поиск — Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.

Добавление логического профиля

Для добавления логического профиля нажмите  в левой верхней части поля над таблицей.

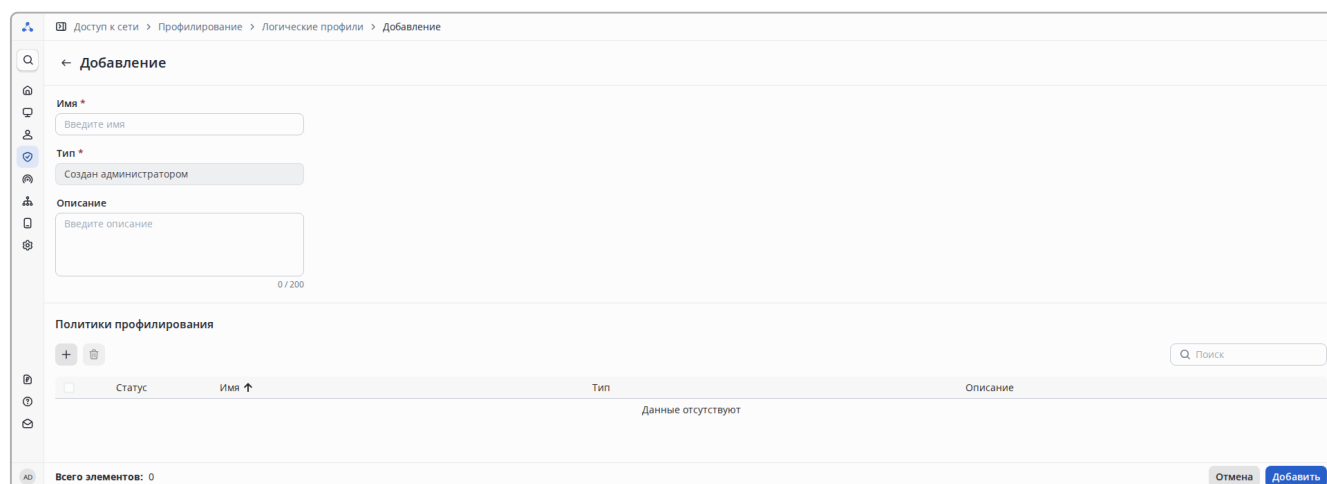


Рисунок 307. Форма добавления логического профиля

В открывшейся странице представлены следующие параметры:

- **Имя *** - наименование условия профилирования. Максимальная длина - 100 символов.
- **Тип** - тип условия профилирования. Не может быть задано и всегда имеет значение "Создано администратором".
- **Описание** - произвольное описание условия профилирования. Максимальная длина - 200 СИМВОЛОВ.

Политика профилирования - блок отвечающий за добавление/удаление политик профилирования. Для удобства конфигурирования ниже в табличной форме отображается список назначенных политик профилирования. Таблица содержит колонки:

- **Поиск** - Выполняет регистронезависимую фильтрацию по колонкам **Имя** и **Описание**: отображаются только записи, удовлетворяющие условию фильтрации.
-  - Добавить новый элемент.
-  - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
-  - Изменить текущий порядок сортировки.
- ☐ - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).

Параметры, отмеченные звездочкой *, обязательны для заполнения.

После добавления необходимых политик логический профиль необходимо сохранить.



Логический профиль должен содержать хотя бы одну политику профилирования. Кнопка "Сохранить" будет неактивна, пока список политик профилирования будет пустой, или не заполнены другие обязательные параметры.

Добавление политик профилирования в логический профиль

Для добавления политик профилирования в логический профиль требуется нажать на иконку  слева вверху над таблицей раздела **Политики профилирования**.

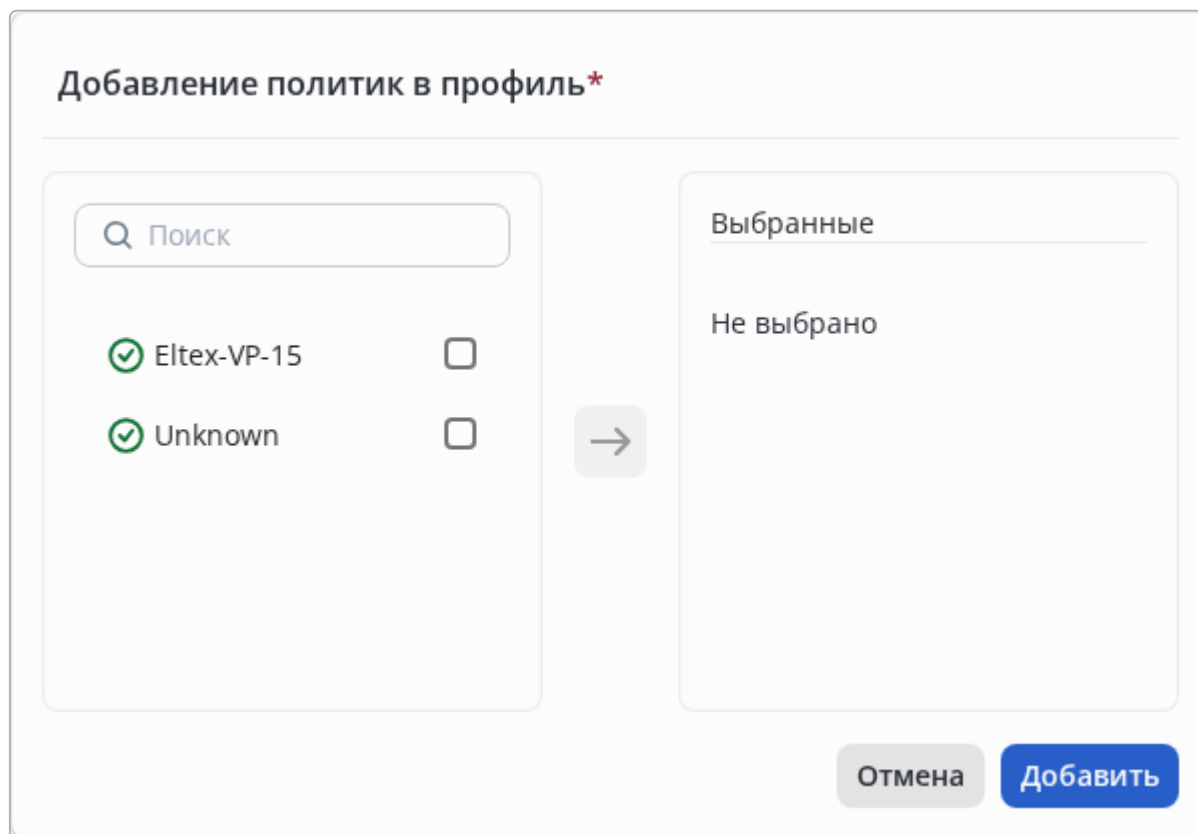


Рисунок 308. Модальный диалог добавления политик профилирования

В левой части открывшегося модального окне выбрать чекбокс ☐ для политик профилирования, которые необходимо добавить в профиль. Для поиска нужной политики можно ввести ее имя в строке **Поиск**.

После выбора нужных политик нажать иконку . Отмеченные чекбоксом политики профилирования переместятся в правую часть модального окна. При необходимости политики профилирования в правой части модального окна можно удалить, нажав на иконку  справа от наименования. Когда все нужные политики выбраны, нажать кнопку **Добавить**, чтобы применить изменения.

Добавленные политики профилирования начнут отображаться в таблице раздела **Политики профилирования**. Порядок следования политик никакого значения не имеет. Все они проверяются независимо друг от друга.



Системную политику профилирования **Unknown** нельзя использовать в логическом профиле.

Редактирование логического профиля

Для редактирования логического профиля необходимо на странице со списком нажать на его имя.

После этого откроется окно редактирования.

Доступ к сети > Профилирование > Логические профили > IP Phone

← IP Phone

Имя *

IP Phone

Тип *

Создан администратором

Описание

Profile for all ip phones

25 / 200

Политики профилирования

+ -

Статус Имя ↑ Тип Описание

☐ Включено Etetx-VP-15 Создана администратором

Поиск

Всего элементов: 1

Рисунок 309. Форма редактирования логического профиля

После редактирования необходимо нажать на кнопку **"Сохранить"**. Кнопка скрыта, пока не будет изменено хотя бы одно поле или изменен набор политик профилирования.

Кнопка **"Отмена"** осуществляет сброс внесенных изменений до исходного состояния.

Удаление логического профиля

Для удаления в окне со списком необходимо выделить чекбокс слева от наименования логических профилей, которые требуется удалить, и нажать кнопку  вверху слева.

Доступ к сети > Профилирование > Логические профили

Профилирование

Условия профилирования Политики профилирования Логические профили

+ -

Имя ↑ Тип Описание

☒ IP Phone Создан администратором Profile for all ip phones

Поиск

Выбрано элементов: 1 из 1

Рисунок 310. Выбор логических профилей для удаления



Удаление элементов требует подтверждения в модальном окне. Выбранные элементы будут удалены только после явного подтверждения операции.

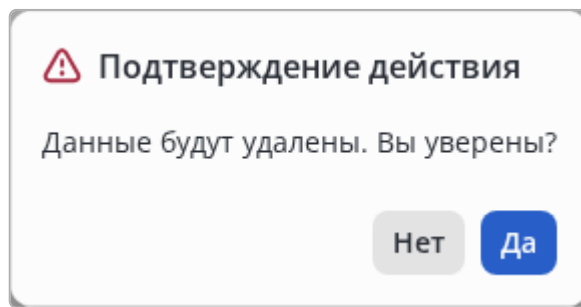


Рисунок 311. Диалоговое окно подтверждения действия



Ограничения:

- Нельзя удалить логический профиль, который используется в какой-либо политике авторизации.

Гостевые порталы

Гостевые эндпоинты



Данный раздел содержит информацию по настройке функционала, доступ к которому открывается с помощью лицензии уровня **ADVANCED**. По вопросам приобретения функционала обращайтесь к Вашему менеджеру или на электронную почту eltex@eltex-co.ru.

Описание

Гостевые эндпоинты - это **эндпоинты**, которые прошли порталную авторизацию в NAICE. Такие эндпоинты автоматически добавляются в систему и хранятся в ней в течение времени, указанном при настройке **портала**, через который подключился пользователь. Если эндпоинт находится в списке, то соответствующий пользователь сможет подключиться к сети без предварительной авторизации на портале (авторизация будет осуществляться по MAB).

Уникальность гостевого эндпоинта определяет комбинация MAC-адреса конечного устройства и SSID (идентификатор беспроводной сети), через которое устройство подключается. На практике это означает, что при подключении одного и того же пользователя с разных устройств создается несколько гостевых эндпоинтов по числу устройств. Аналогично, несколько гостевых эндпоинтов добавляется при подключении одного и того же устройства к нескольким разным беспроводным сетям.

В отличие от **обычных эндпоинтов**, гостевые эндпоинты со случайно сгенерированными MAC-адресами (randomized MAC address) автоматически добавляются в систему.

Ручное добавление или редактирование существующих гостевых эндпоинтов недоступно.

Просмотр списка эндпоинтов

Гостевые порталы > Управление порталами > Гостевые эндпоинты

Управление порталами

Гостевые эндпоинты Пользователи порталов Конструктор порталов

Фильтры

☐	Имя пользователя	Источник идентификации	Имя портала	MAC-адрес	SSID	Дата последнего подключения	Дата создания записи
☐	Maria_982	Maria_982 Device	Default Portal	27:ad:7e:b8:da:8d	CompanyWiFi	13.11.2025 03:47:54	10.11.2025 12:36:12
☐	Petr_820	Petr_820 Device	Default Portal	61:a7:2c:4b:13:f2	CompanyWiFi	12.11.2025 20:37:49	09.11.2025 23:01:42
☐	Pavel_160	Petr_820 Device	Default Portal	c4:e1:71:e4:27:fa	CompanyWiFi	14.11.2025 09:05:07	09.11.2025 06:03:59
☐	Petr_657	Petr_820 Device	Default Portal	5c:0e:93:cb:6c:7d	CompanyWiFi	13.11.2025 07:03:32	09.11.2025 15:04:56
☐	Artem_761	Petr_820 Device	Default Portal	ec:7c:bc:13:66:eb	CompanyWiFi	14.11.2025 02:53:10	13.11.2025 01:04:52

Всего элементов: 5

Рисунок 312. Просмотр списка эндпоинтов

На данной странице содержится таблица со списком всех гостевых эндпоинтов.

Таблица по умолчанию содержит колонки:

•

Имя пользователя - имя пользователя, с которым эндпоинт проходил аутентификацию в последний раз.

- **Источник идентификации** - источник, где был найден пользователь при аутентификации.
- **Имя портала** - портал, на котором пользователь прошел аутентификацию.
- **MAC-адрес** - MAC адрес эндпоинта в формате "XX:XX:XX:XX:XX:XX".
- **SSID** - имя беспроводной сети, к которой подключался пользователь при portalной авторизации.



Имя сети получается из RADIUS-атрибута Called-Station-Id, которое ожидается в формате <MAC-адрес ТД>:<имя SSID>, например - ec-b1-e0-2b-02-b0:naice-guest-portal-test.

- **Дата последнего подключения** - время последней авторизации или переавторизации эндпоинта.
- **Дата создания записи** - время первой portalной авторизации эндпоинта.

Возможна сортировка в прямом и обратном порядке по всем колонкам, кроме **MAC адрес**. По умолчанию сортировка выполняется в прямом порядке по колонке **Дата последнего подключения**.

Страница содержит следующие элементы управления:

-  - Обновить данные таблицы.
-  - Настроить отображение колонок таблицы.
-  - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
-  - Изменить текущий порядок сортировки.
- ☐ - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).
-  **Фильтры** - Открыть окно настройки фильтрации данных по таблице.

Фильтрация данных в таблице настраивается в следующем окне:

Фильтры

Имя пользователя ?
Введите имя

Источник идентификации
Введите источник идентификации

Имя портала
Введите имя портала

MAC-адрес ?
FF:FF:FF:00:00:00

Дата последнего подключения
ДД.ММ.ГГГГ - ДД.ММ.ГГГГ x 🗑

Дата создания записи
ДД.ММ.ГГГГ - ДД.ММ.ГГГГ x 🗑

SSID
Введите SSID

ЗаккрытьПрименить

Рисунок 313. Настройка фильтрации данных в таблице

Фильтрация доступна по всем параметрам гостевого эндпоинта.

В настройках таблицы  можно сменить состав отображаемых колонок.

Кнопка **Сбросить все** предназначена для сброса настроенных колонок к состоянию по умолчанию (неактивно, пока состоянию по умолчанию не изменено).

Настройки таблицы

☒ Показывать все колонки 

☒ Имя пользователя
☒ Источник идентификации
☒ Имя портала
☒ MAC-адрес
☒ SSID
☒ Дата последнего подключения
☒ Дата создания записи

ОтменаСохранить

Рисунок 314. Настройка отображаемых колонок в таблице

Удаление эндпоинта

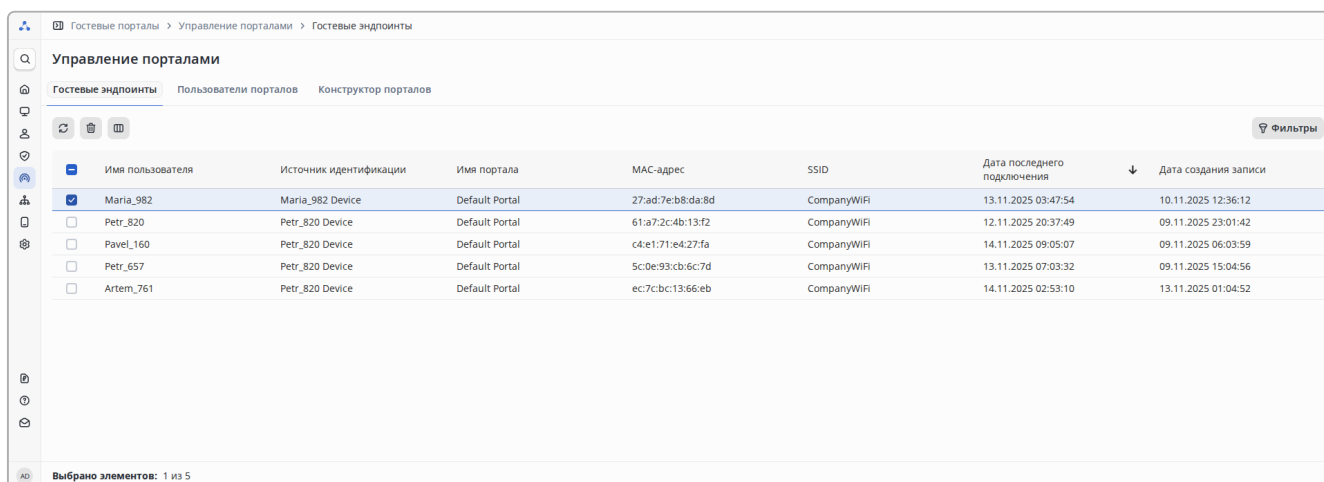


Таблица гостевых эндпоинтов заполняется автоматически в процессе нормальной работы NAICE в ходе порталных авторизаций эндпоинтов. При удалении эндпоинта он будет повторно изучен при следующей попытке подключения. Отключить автоизучение эндпоинтов нельзя.



Удаление гостевого эндпоинта приведет к необходимости повторной авторизации клиента на портале при следующем подключении к сети.

Для удаления эндпоинта необходимо на странице просмотра, используя чекбокс ☐, выбрать необходимые эндпоинты и в левом верхнем углу над таблицей нажать на .



	Имя пользователя	Источник идентификации	Имя портала	MAC-адрес	SSID	Дата последнего подключения	Дата создания записи
☒	Maria_982	Maria_982 Device	Default Portal	27:ad:7e:b8:da:8d	CompanyWiFi	13.11.2025 03:47:54	10.11.2025 12:36:12
☐	Petr_820	Petr_820 Device	Default Portal	61:a7:2c:4b:13:f2	CompanyWiFi	12.11.2025 20:37:49	09.11.2025 23:01:42
☐	Pavel_160	Petr_820 Device	Default Portal	c4:e1:71:e4:27:fa	CompanyWiFi	14.11.2025 09:05:07	09.11.2025 06:03:59
☐	Petr_657	Petr_820 Device	Default Portal	5c:0e:93:cb:6c:7d	CompanyWiFi	13.11.2025 07:03:32	09.11.2025 15:04:56
☐	Artem_761	Petr_820 Device	Default Portal	ec:7c:bc:13:66:eb	CompanyWiFi	14.11.2025 02:53:10	13.11.2025 01:04:52

Рисунок 315. Выбор эндпоинтов в таблице для удаления



Удаление элементов требует подтверждения в модальном окне. Выбранные элементы будут удалены только после явного подтверждения операции.

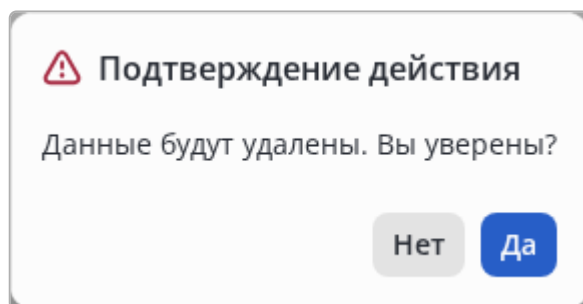


Рисунок 316. Диалоговое окно подтверждения действия

Пользователи портала



Данный раздел содержит информацию по настройке функционала, доступ к которому открывается с помощью лицензии уровня **ADVANCED**. По вопросам приобретения функционала обращайтесь к Вашему менеджеру или на электронную почту eltex@eltex-co.ru.

Описание

Пользователи порталов - внутренний источник пользователей, используемый при порталной авторизации. При настройке [цепочки источников](#) он отображается под именем *Portal*. Данный источник выполняет роль каталога всех гостевых пользователей вне зависимости от успешности подключения. Пользователь, присутствующий в данном каталоге, имеет возможность авторизоваться в сети через указанный [портал](#) по заданному имени и паролю.

Особенностью порталных пользователей является наличие механизма **саморегистрации** - пользователи, выполнившие вход по номеру телефона с помощью кода из СМС (при условии что данный способ разрешен в настройках портала), автоматически попадают в данный список. Для них автоматически заполняются все параметры учетной записи. Помимо саморегистрации, существует возможность вручную добавить порталного пользователя.

Портальные пользователи привязаны к [порталу](#), на котором они авторизовались или будут авторизовываться в последствии.



Для возможности авторизации на разных порталах требуется добавить пользователя с одинаковым именем и паролем для каждого портала.



Предполагается, что один портал используется для одной беспроводной сети ("**1 портал = 1 SSID**"). Если один и тот же портал будет использоваться в нескольких беспроводных сетях, то гостевой пользователь сможет авторизоваться на всех SSID с данным порталом, успешно авторизовавшись на одном из них. Для исключения подобной ситуации при настройке логического условия в [политиках доступа](#) используйте дополнительное условие: `Normalised Radius·SSID Equals <имя SSID>`.

Для пользователей системы предусмотрена возможность просмотра списка зарегистрированных пользователей портала, удаления отдельных записей, ручного добавления новых учетных записей либо редактирования существующих.

Просмотр пользователей

Гостевые порталы > Управление порталами > Пользователи порталов

Управление порталами

Гостевые эндпоинты Пользователи порталов Конструктор порталов

+

↺

↻

✖

Поиск

☐	Логин	Портал	СМС-шлюз	Описание	Дата создания записи ↓
☐	Hayley_1	Default portal	gateway_1	Test user	17.11.2025 12:00:00
☐	Zion_2	Default portal	gateway_2	Test user	16.11.2025 12:00:00
☐	Mina_3	Default portal	gateway_3	Test user	15.11.2025 12:00:00

Всего элементов: 3

Рисунок 317. Таблица с перечнем гостевых пользователей

На данной странице содержится таблица со списком учетных данных порталных пользователей.

Таблица содержит колонки:

- **Логин** - логин пользователя (должен быть уникальным для указанного портала);
- **Портал** - [портал](#), к которому привязан пользователь;
- **СМС-шлюз** - на каком [СМС-шлюзе](#) самозарегистрировался пользователь;
- **Описание** - произвольное описание пользователя;
- **Дата создания записи** - автоматически заполняемое поле с временем саморегистрации или ручного добавления пользователя.

Возможна сортировка в прямом и обратном порядке по колонке **Дата создания записи**. По умолчанию сортировка выполняется в обратном (нисходящем) порядке.

Элементы управления:

-  — Добавить новый элемент.
-  — Дублировать выбранный чекбоксом элемент. Становится активным, если выбран только один элемент в списке.
-  — Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
-  — Обновить данные таблицы.
- ☐ — Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).
-  — Изменить текущий порядок сортировки.
-  **Поиск** — Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.

Добавление пользователей

Если необходимо предварительно создать учетную запись для порталной авторизации по логину и паролю, то нажмите  в левой части поля над таблицей.

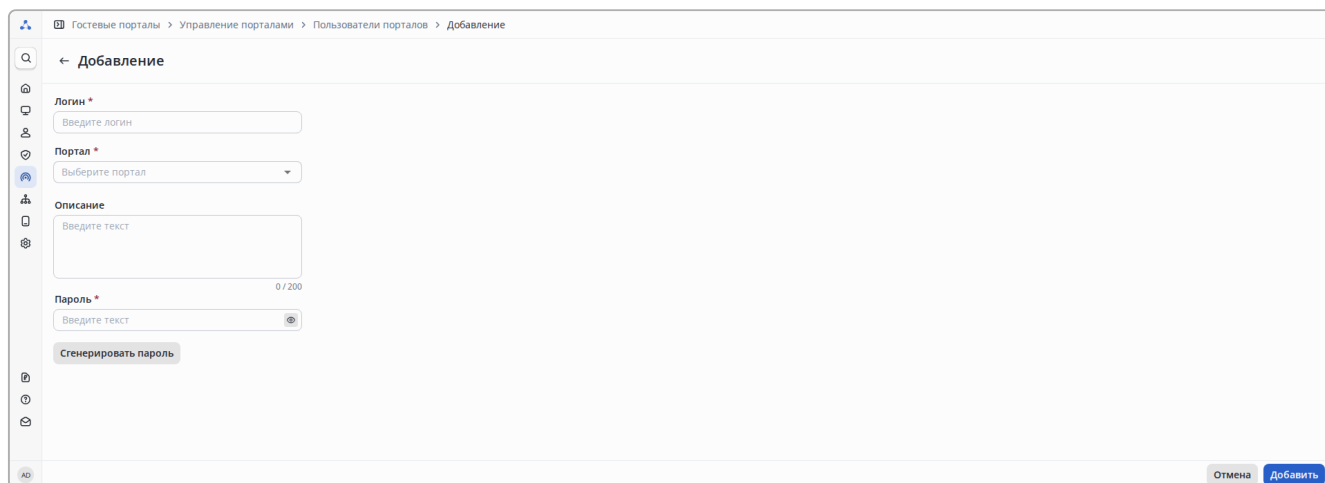


Рисунок 318. Страница добавления пользователя

На открывшейся странице представлены следующие параметры:

- **Логин *** - логин пользователя. Должен быть уникальным для одного портала. Максимальная длина логина - 100 символов.
- **Портал *** - [портал](#), к которому привязан пользователь. Учетные данные будут актуальны только при авторизации на беспроводной сети, использующей указанный портал.
- **Описание** - произвольное описание. Максимальная длина - 200 символов.
- **Пароль *** - пароль пользователя. Минимальная длина пароля - 4 символа, максимальная - 100 символов. По нажатию на  можно включить отображение вводимого пароля, по умолчанию текст скрыт. Доступна генерация случайного пароля по кнопке *Сгенерировать пароль* и его копирование в буфер обмена по кнопке .

Параметры, отмеченные звездочкой *, обязательны для заполнения.

Для добавления пользователя в список не забудьте нажать **Добавить**. Для сброса изменений и возврата на страницу просмотра нажмите на **Отменить**.

Редактирование пользователей

Для редактирования ранее добавленного пользователя на странице просмотра нажмите на логин пользователя в таблице.

Откроется страница редактирования, аналогичная странице добавления.

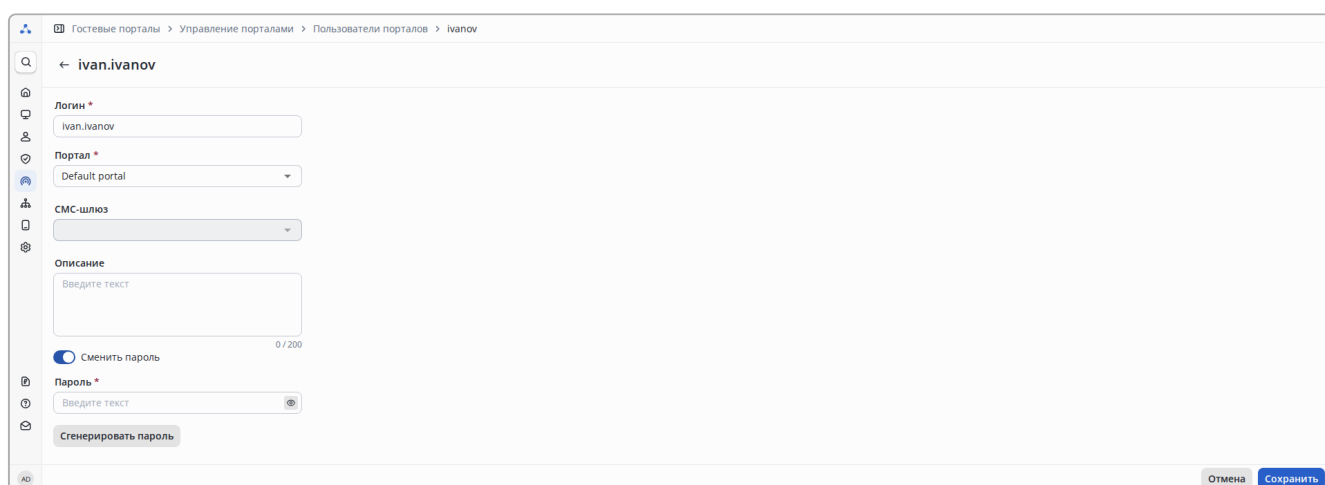


Рисунок 319. Страница редактирования пользователя

При редактировании гостевого пользователя для ознакомления доступен параметр СМС-шлюз - [шлюз](#), через который пользователь был зарегистрирован при входе по СМС. Редактирование шлюза недоступно.

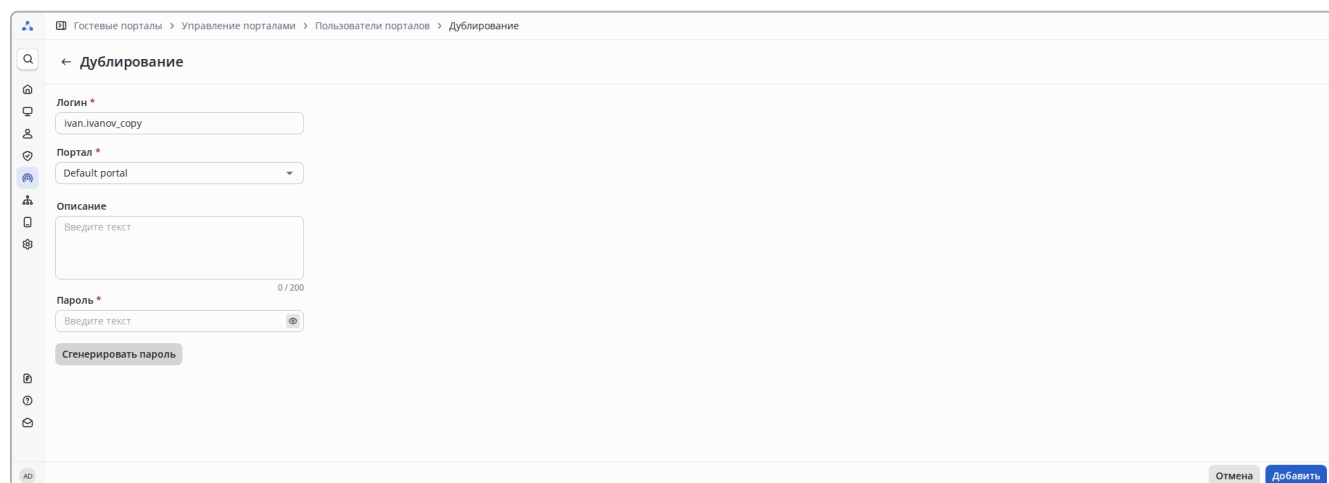
Для изменения пароля пользователя нажмите на переключатель *Сменить пароль*, после чего введите новый пароль пользователя в появившееся поле.

После редактирования необходимо нажать на кнопку **"Сохранить"**. Кнопка скрыта, пока не будет внесено хотя бы одно изменение.

Кнопка **"Отмена"** осуществляет сброс внесенных изменений до исходного состояния.

Дублирование пользователя

Новый порталный пользователь может быть создан на основе существующего. Для этого выберите копируемого пользователя с помощью чекбокса, а затем нажмите на кнопку .



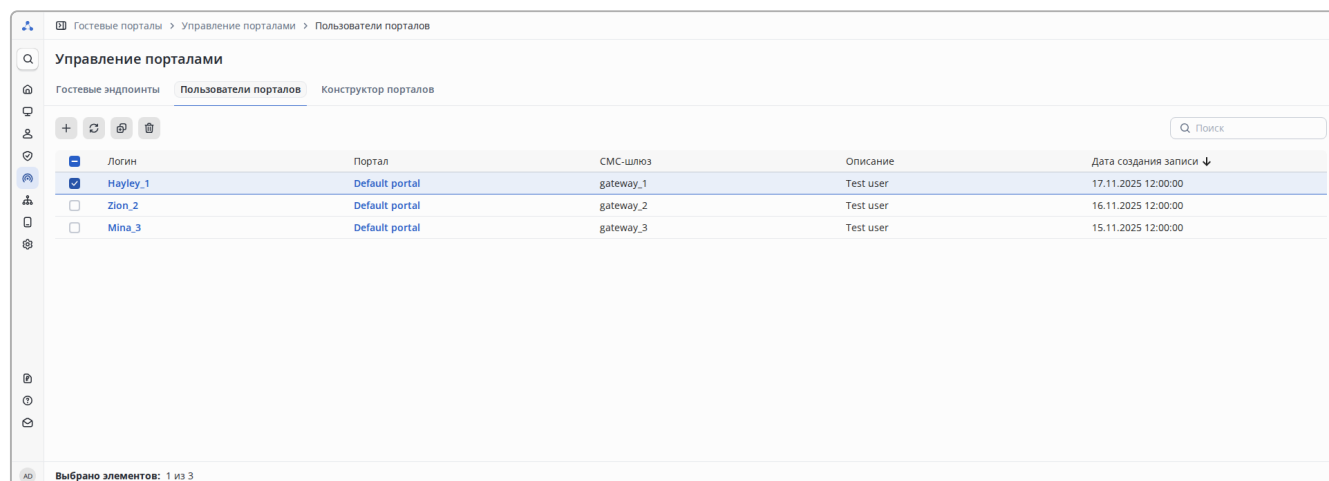
Скриншот интерфейса для дублирования пользователя. Вверху — хлебные крошки: «Гостевые порталы > Управление порталами > Пользователи порталов > Дублирование». Заголовок формы — «← Дублирование». Форма содержит следующие поля: «Логин *» с текстом «ivan.ivanov_copy», «Портал *» с выпадающим списком «Default portal», «Описание» с текстовым полем «Введите текст» и подсказкой «0 / 200», «Пароль *» с текстовым полем «Введите текст» и иконкой глаза. Под полем пароля — кнопка «Сгенерировать пароль». В нижнем правом углу — кнопки «Отмена» и «Добавить».

Рисунок 320. Дублирование пользователя

Откроется форма, аналогичная форме добавления пользователя, где все поля будут заполнены значениями из выбранного референса. По умолчанию к значению в поле Логин добавляется "_copy". Можно задать любое другое имя, которое еще не используется в системе. Также необходимо указать пароль пользователя.

Удаление пользователей

Для удаления пользователей необходимо на странице просмотра, используя чекбокс ☐, выбрать необходимых пользователей и в левом верхнем углу над таблицей нажать на .



Скриншот интерфейса «Управление порталами» с заголовком «Пользователи порталов». Вверху — панель действий с иконками: «+», «↺», «↻», «🗑️». В центре — таблица с 6 столбцами: «Логин», «Портал», «СМС-шлюз», «Описание», «Дата создания записи». В левом столбце «Логин» есть чекбоксы для выбора. В нижнем левом углу — статус «Выбрано элементов: 1 из 3».

Логин	Портал	СМС-шлюз	Описание	Дата создания записи
☒ Hayley_1	Default portal	gateway_1	Test user	17.11.2025 12:00:00
☐ Zion_2	Default portal	gateway_2	Test user	16.11.2025 12:00:00
☐ Mina_3	Default portal	gateway_3	Test user	15.11.2025 12:00:00

Рисунок 321. Выбор пользователей в таблице для удаления



Удаление элементов требует подтверждения в модальном окне. Выбранные элементы будут удалены только после явного подтверждения операции.

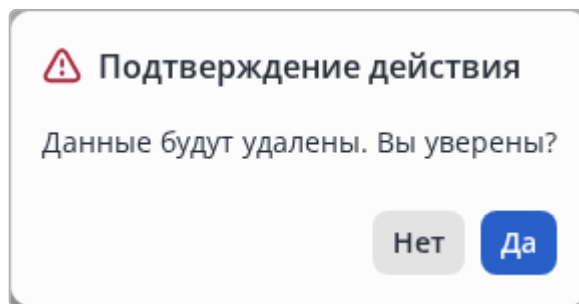


Рисунок 322. Диалоговое окно подтверждения действия



После удаления гостевого пользователя для ранее подключенного клиента сохраняется возможность переподключения по МАР до момента, пока не будет удален связанный **гостевой эндпоинт**. Гостевой эндпоинт удаляется автоматически после истечения настроенного в **портале** периода, а также может быть удален в любой момент вручную.

Конструктор порталов



Данный раздел содержит информацию по настройке функционала, доступ к которому открывается с помощью лицензии уровня **ADVANCED**. По вопросам приобретения функционала обращайтесь к Вашему менеджеру или на электронную почту eltex@eltex-co.ru.

Описание

В состав NAICE как один из компонентов включен WEB-портал, с помощью которого реализуется модель авторизации hotspot-клиентов. Неизвестный системе пользователь может свободно (без получения заранее логина и пароля) подключиться к точке доступа, но при попытке выйти в интернет через браузер пользователь перенаправляется на страницу WEB-портала, на которой может по выбору пройти процедуру авторизации или саморегистрации (например, с помощью СМС). В процессе выполнения процедур авторизации клиент перемещается по различным страницам портала, внешний вид которых может быть кастомизирован под нужды оператора беспроводной сети.

Для кастомизации используется *Конструктор порталов*, с помощью которого пользователи могут настраивать сценарии работы и внешний вид порталов. Пользователи могут создавать и удалять порталы, выбирать их фон и содержание (текст, изображения, цветовая схема), устанавливать различные способы авторизации для каждого из порталов и поведение после успешного входа.

Просмотр списка порталов

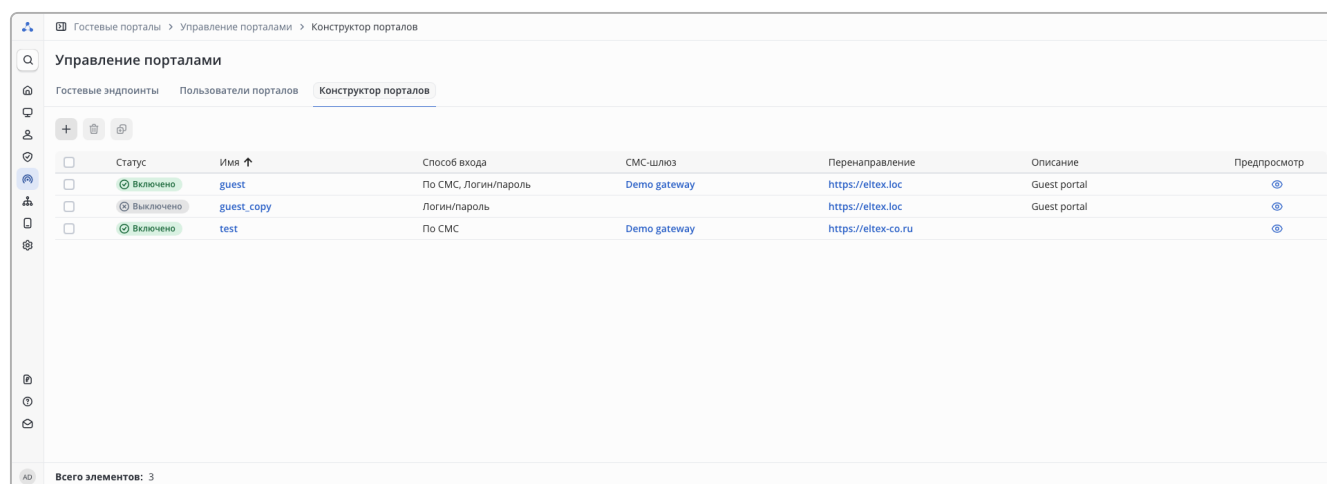


Рисунок 323. Просмотр списка порталов

На данной странице содержится таблица со списком всех порталов.

Таблица содержит колонки:

- **Статус** - текущее состояние активированности портала: Включено или Выключено .
- **Имя** - название портала.
- **Способ входа** - настроенные на портале способы авторизации пользователей.
- **СМС-шлюз** - используемый [СМС-шлюз](#) при включенном способе входа по СМС.
- **Перенаправление** - URL финального редиректа успешно подключившегося пользователя.
- **Описание** - произвольное описание портала.
- **Предпросмотр** - открытие в новой вкладке превью портала при клике на .

Возможна сортировка в прямом и обратном порядке по колонкам **Статус** и **Имя** . По умолчанию сортировка выполняется в прямом порядке по имени портала.

Страница содержит следующие элементы управления:

- - Добавить новый элемент.
- - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- - Дублировать выбранный чекбоксом элемент. Становится активным, если выбран только один элемент в списке.
- - Изменить текущий порядок сортировки.
- ☐ - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).

Добавление портала

Для добавления нового портала кликните на **+** в левой части поля над таблицей страницы просмотра. Откроется следующая страница:

Рисунок 324. Страница глобальных настроек портала

Настройка портала происходит в 3 этапа: глобальные настройки, настройки внешнего вида и настройка страниц. Обязательным для настройки является лишь 1 этап, оставшиеся два можно пропустить. В таком случае внешний вид и содержание портала останется исходя из настроек по умолчанию.

Глобальные настройки

Для настройки доступны следующие параметры:

- Общие параметры
 - **Статус** - текущее состояние активированности портала: **Включено** или **Выключено**. Авторизация на выключенном портале недоступна
 - **Имя *** - название портала.
 - **Описание** - произвольное описание портала.
- Аутентификация
 - **Основной способ входа *** - вариант аутентификации, который будет отображаться пользователю первым.
 - **Дополнительный способ входа** - запасной вариант аутентификации, альтернативный основному.
 - **СМС-шлюз *** - используемый **СМС-шлюз** при включенном способе входа по СМС.

- **Цепочка идентификации *** - список и порядок источников, среди которых будет производиться поиск учетных данных при использовании способа входа по логину и паролю.



Источниками учетных данных могут быть как и специальные **гостевые пользователи**, так и **обычные пользователи** или пользователи из **внешних источников идентификации**.

- **Дополнительные настройки**

- **Пользовательское соглашение на использование портала** - включение данной настройки добавляет страницу "Пользовательское соглашение".
- **Подтверждение пользовательского соглашения *** - включение требования от пользователя согласия с пользовательским соглашением.
- **Срок действия гостевых аккаунтов** - время, по истечении которого связанные с данным порталом **гостевые эндпоинты** будут автоматически удалены. После удаления гостевого эндпоинта пользователю придется заново проходить порталную авторизацию.
- **Адрес перехода после успешного входа** - URL финального редиректа успешно подключенного пользователя.



Для различных клиентских устройств может наблюдаться разное поведение после успешной авторизации. Некоторые устройства после успешного подключения и обнаружения наличия доступа в Интернет могут автоматически закрывать всплывающее окно, из-за чего пользователь может не успеть увидеть финальную страницу редиректа.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

После завершения настройки нажмите на кнопку **Далее** или выберите следующий этап настройки в верхней части страницы.

Внешний вид

Данный этап направлен на настройку параметров внешнего вида портала, таких как цветовая схема и отображаемые изображения.

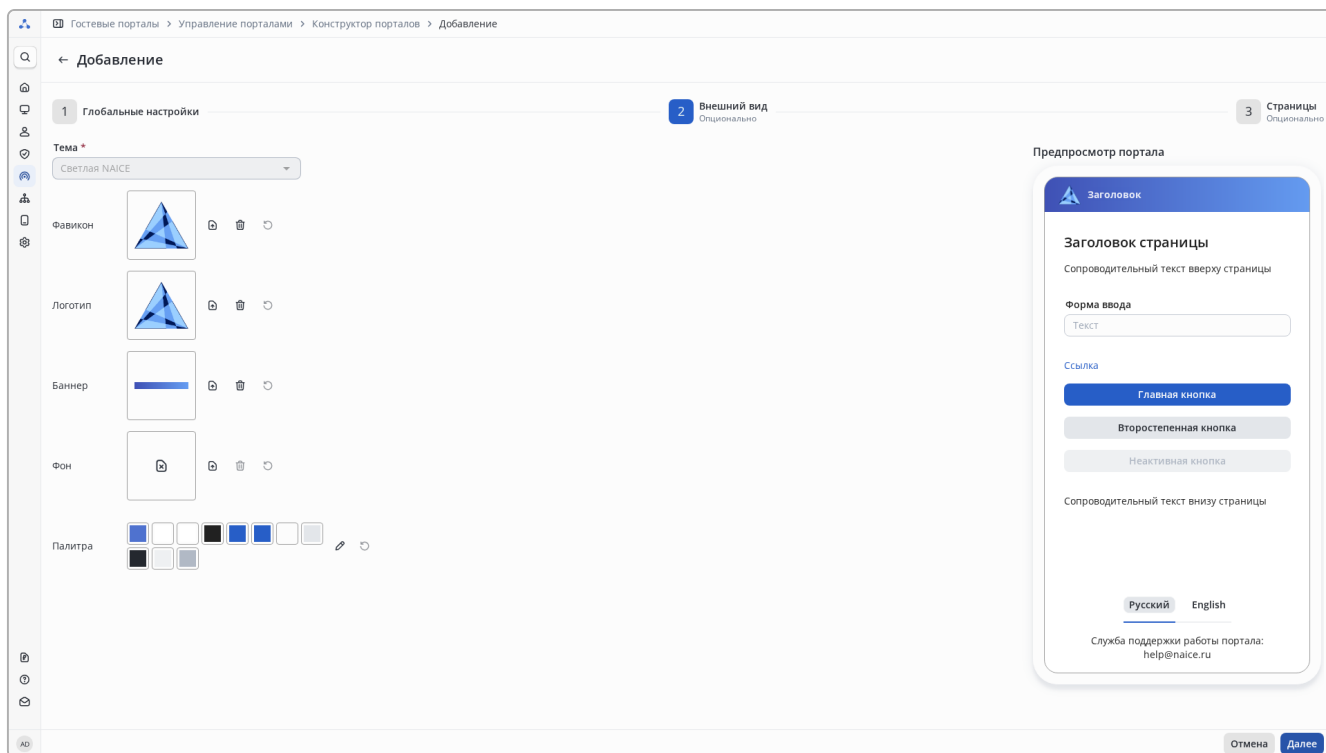


Рисунок 325. Страница настроек внешнего вида

Для настройки доступны следующие параметры:

- **Фавикон** - иконка, отображаемая во вкладке браузера рядом с названием страницы, а также в других местах, таких как закладки или поисковая выдача.
- **Логотип** - иконка, отображаемая в заголовке в верхней части страницы.
- **Баннер** - фон заголовка в верхней части страницы.
- **Фон** - изображение, которое будет подложено под всю страницу ниже заголовка.
- **Палитра** - настройка используемой цветовой схемы.

Палитра

Цвет баннера		#4F72CF
Цвет текста баннера		#FFFFFF
Цвет фона страницы		#FFFFFF
Цвет текста страницы		#212121
Цвет ссылок		#275EC7
Цвет главной кнопки		#275EC7
Цвет текста главной кнопки		#FCFCFC
Цвет второстепенной кнопки		#E3E6EA
Цвет текста второстепенной кнопки		#24282F
Цвет неактивной кнопки		#EEF0F2
Цвет текста неактивной кнопки		#B1B9C5

Отмена
Сохранить

Рисунок 326. Палитра



Изображения баннера и фона приоритетнее цветовых настроек и отображаются поверх.

При этом используются следующие элементы управления:

-  - загрузка файла изображения;
-  - удаление изображения, после чего оно перестанет отображаться;
-  - сбросить настройку к дефолтной;
-  - редактирование палитры.

По умолчанию выбрана тема "Светлая NAICE", редактирование параметров которой недоступно. Для того, чтобы настроить собственную тему, необходимо начать изменение одного из вышеперечисленных параметров.

В процессе можно отслеживать влияние изменений на итоговый внешний вид портала с помощью превью в правой части страницы.

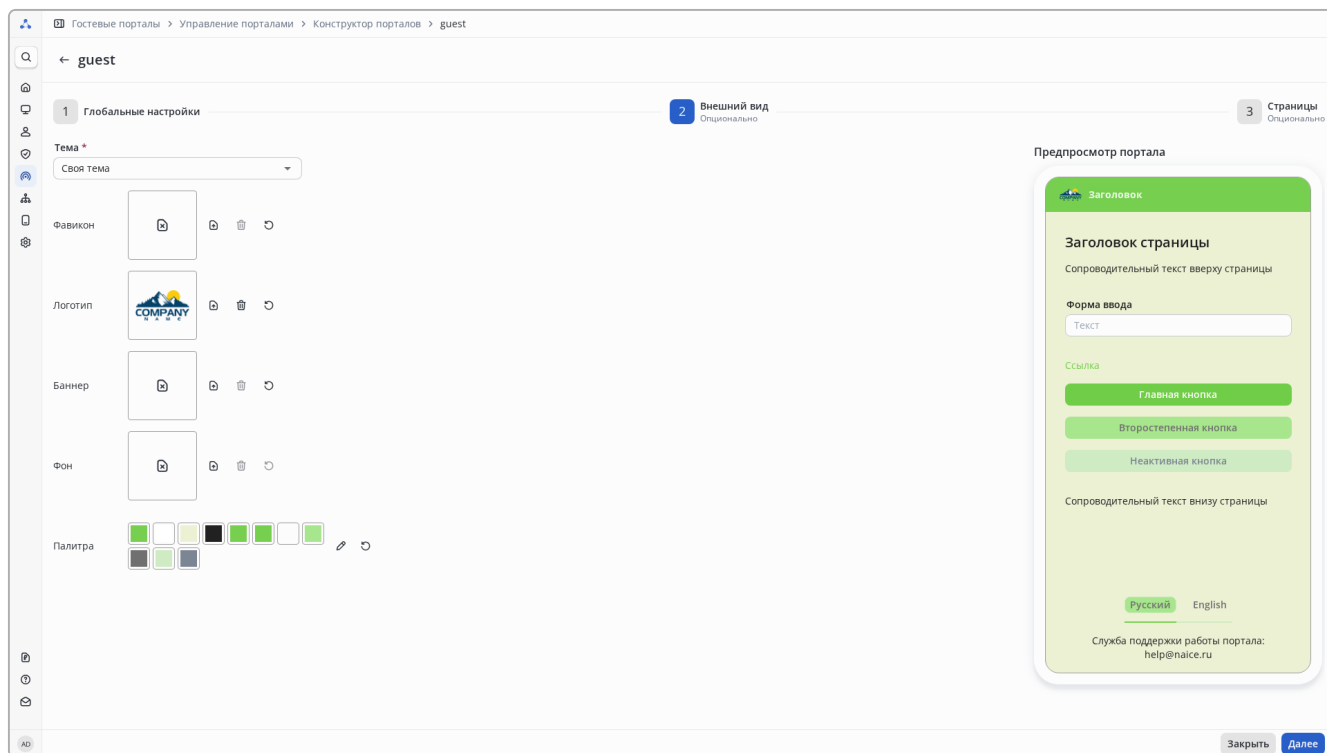


Рисунок 327. Пользовательская тема

Страницы

Данный этап настроек определяет текст, который будет отображаться на различных страницах портала в основных функциональных элементах - кнопках, заголовках, информационных блоках и т.п. Расположение самих элементов не настраивается.

Важно понимать, что функциональность таких элементов, как кнопки, предопределена и не меняется от настроенного на них текста. Например, если изменить текст на кнопке "Войти", то она продолжит вызывать попытку авторизации независимо от расположенного на ней текста.

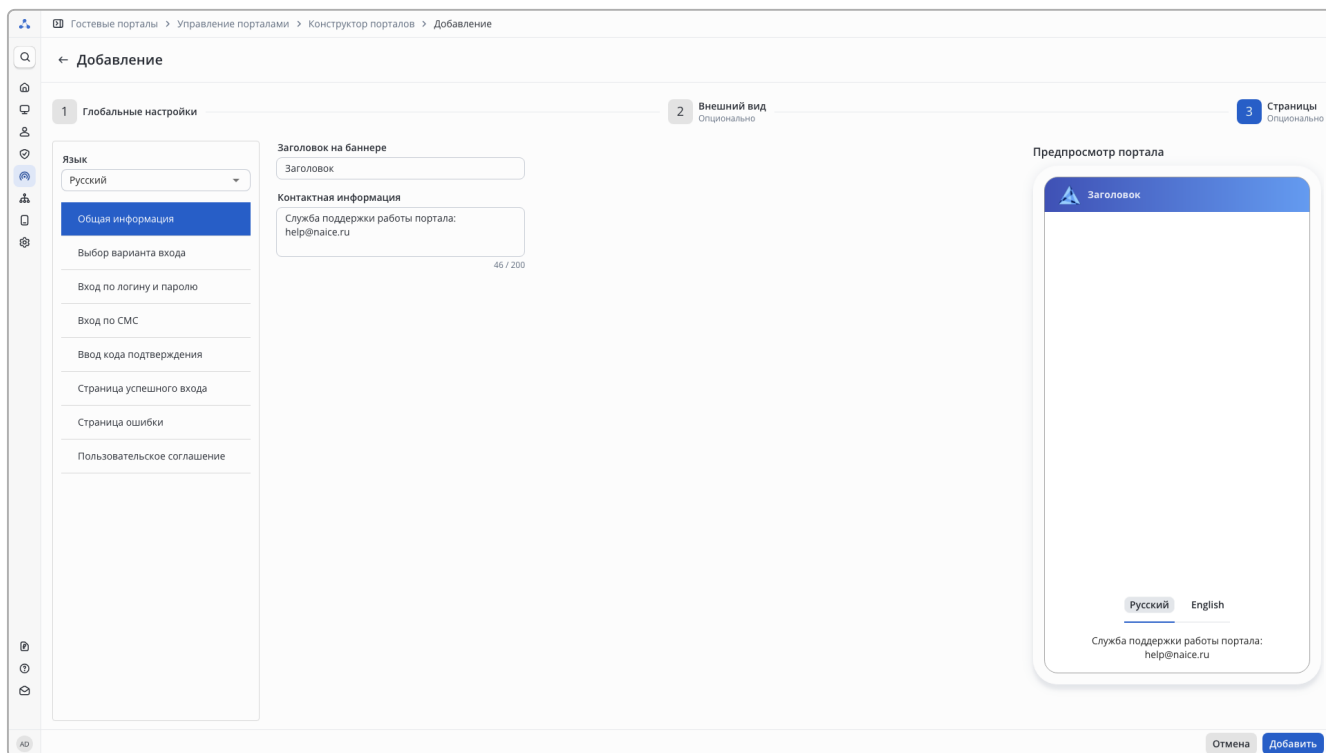


Рисунок 328. Настройка содержания страниц

Список доступных страниц зависит от настроек на этапе [Глобальные настройки](#).

- **Общая информация** - настройка заголовка в баннере и текста в футтере на всех остальных страницах;
- **Выбор варианта входа**
- **Вход по логину и паролю**
- **Вход по СМС** - доступна только при настроенном входе по СМС; помимо настройки текста на элементах страницы настраивает шаблон СМС сообщения для отправки пользователю;
- **Ввод кода подтверждения**
- **Страница успешного входа**
- **Страница ошибки**
- **Пользовательское соглашение** - доступна только при включенном в глобальных настройках использовании пользовательского соглашения; содержит в том числе редактор для форматирования текста соглашения.

Текст настраивается различный для каждого поддерживаемого на портале языка.

В процессе настройки можно отслеживать влияние изменений на итоговый внешний вид портала с помощью превью в правой части страницы.

После завершения настройки нажмите на кнопку **Добавить**.

Настройка сложности САРТСНА

При настройке раздела **Вход по СМС** важной частью является настройка сложности САРТСНА.

САРТСНА — это механизм проверки пользователя, при котором необходимо ввести код с изображения, искажённого добавлением шумов (линий, точек и контрастных геометрических фигур), сложность которых варьируется в зависимости от выбранного уровня сложности.

Настройка уровня сложности выполняется на странице **Вход по СМС** в соответствующей вкладке:

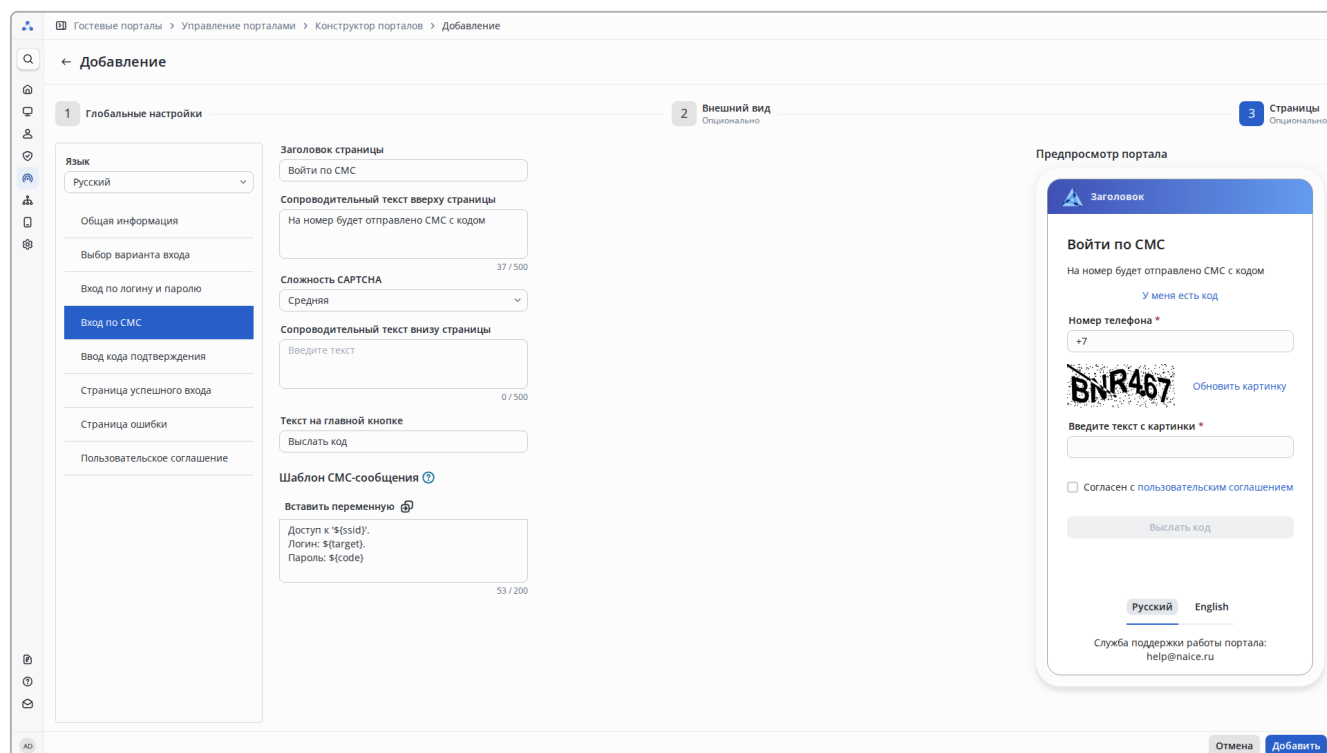


Рисунок 329. Страница "Вход по СМС"

Всего есть четыре уровня сложности САРТСНА:

- **Отключена** - САРТСНА не используется при авторизации пользователя.
- **Простая** - легкие изменения, код искажается волной, без добавления геометрических шумов. Читаемость высокая.



Рисунок 330. Простая САРТСНА

- **Средняя** - к волнообразному искажению добавляются шумы в виде наложения контрастных точек, линий и геометрических фигур. Читаемость средняя.



Рисунок 331. CAPTCHA среднего уровня сложности

- **Сложная** - добавляется большее количество точек, контрастные геометрические фигуры занимают больше пространства на изображении кода. Низкая читаемость.



Рисунок 332. Сложная CAPTCHA

Редактирование портала

Для редактирования ранее добавленного портала на странице просмотра нажмите на имя портала в таблице.

Гостевые порталы > Управление порталами > Конструктор порталов							
Управление порталами							
Гостевые эндпоинты Пользователи порталов Конструктор порталов							
+ ✖ 🔍							
☐	Статус	Имя ↑	Способ входа	СМС-шлюз	Перенаправление	Описание	Предпросмотр
☐	Включено	guest	По СМС, Логин/пароль	Demo gateway	https://eltex.loc	Guest portal	🔍
☐	Выключено	guest_copy	Логин/пароль		https://eltex.loc	Guest portal	🔍
☐	Включено	test	По СМС	Demo gateway	https://eltex-co.ru		🔍
Всего элементов: 3							

Рисунок 333. Просмотр списка порталов

Откроется страница редактирования, аналогичная странице добавления.

При редактировании сразу доступны все 3 этапа настройки для внесения изменений.



Особенности поведения системы при выключении ранее работающего портала

- При выключении портала для ранее подключенного клиента сохраняется возможность переподключения по МАВ до момента, пока не будет удален связанный [гостевой эндпоинт](#). Гостевой эндпоинт удаляется автоматически после истечения настроенного в портале периода, а также может быть удален в любой момент вручную.
- Удаление гостевых эндпоинтов выполнится даже если портал выключен. Для удаления применяется срок действия аккаунтов, настроенный на текущий момент, а не на момент выключения портала.

После редактирования необходимо нажать на кнопку **"Сохранить"**. Кнопка скрыта, пока не будет внесено хотя бы одно изменение.

Кнопка **"Отмена"** осуществляет сброс внесенных изменений до исходного состояния.

Дублирование портала

Новый портал может быть создан на основе существующего. Для этого выберете копируемый портал с помощью чекбокса, а затем нажмите на кнопку .

Откроется форма, аналогичная форме добавления пользователя, где все поля будут заполнены значениями из выбранного референса. По умолчанию к значению в поле Имя добавляется "_сору". Можно задать любое другое имя, которое еще не используется в системе.

Удаление портала

Для удаления порталов необходимо на странице просмотра, используя чекбокс ☐, выбрать удаляемые порталы и в левом верхнем углу над таблицей нажать на .



При удалении портала также будут автоматически удалены связанные [гостевые пользователи](#) и [гостевые эндпоинты](#). Это приведет к необходимости переавторизации ранее подключенных клиентов.

Доступ к оборудованию



Данный раздел содержит информацию по настройке функционала, доступ к которому приобретается отдельно с помощью дополнительной опции лицензии **NAICE-TACACS+**. По вопросам приобретения функционала обращайтесь к Вашему менеджеру или на электронную почту eltex@eltex-co.ru.

Раздел *Доступ к оборудованию* содержит записи для настройки доступа на сетевые устройства по протоколу TACACS+.

Протокол TACACS+ является развитием протокола TACACS (Terminal Access Controller Access Control System) и предназначен для централизованной аутентификации и авторизации администраторов сетевого оборудования. Протокол позволяет выполнять авторизацию каждой выполняемой на сетевом устройстве команды, а так же отправлять сведения о выполняемых командах (аккаунтинг). NAICE может выступать в качестве сервера авторизации TACACS+.

Раздел содержит страницы:

- **Условия** - управление условиями, используемыми в политиках сетевых устройств для определения соответствия текущего подключения одной из политик;
- **Наборы команд TACACS+** - управление наборами команд, определяющими разрешенные и запрещенные для выполнения администратором на оборудовании команды.
- **Профили TACACS+** - управление профилями TACACS+, определяющие уровни привилегий и другие дополнительные атрибуты авторизованных пользователей.
- **Политики TACACS+** - управление политиками сетевых устройств, которые являются основным элементом контроля доступа и определяют логику обработки и ответа на запросы аутентификации и авторизации TACACS+.

Элементы политик

Условия



Данный раздел содержит информацию по настройке функционала, доступ к которому приобретается отдельно с помощью дополнительной опции лицензии **NAICE-TACACS+**. По вопросам приобретения функционала обращайтесь к Вашему менеджеру или на электронную почту eltex@eltex-co.ru.

Описание

Логические условия являются основным элементом политик аутентификации и авторизации, которые отвечают за формирование критериев, определяющих может ли пользователь пройти аутентификацию и какие действия должны быть к нему применены при выполнении авторизации.

В основе создания и обработки логического условия лежит алгебра логики. Результатом выполнения условия является "Истина" или "Ложь". Результат может быть инвертирован. Условие может быть простым и сложным. В простом условии в качестве критерия проверки выступает

только один атрибут. В сложном условии можно использовать несколько различных атрибутов, объединив их логическими операциями "И" или "ИЛИ".



Раздел аналогичен [Доступ к сети - Элементы политик - Условия](#), однако для создания условий доступны только атрибуты, которые могут использоваться в [:policy-sets/index.html](#).

Просмотр списка логических условий

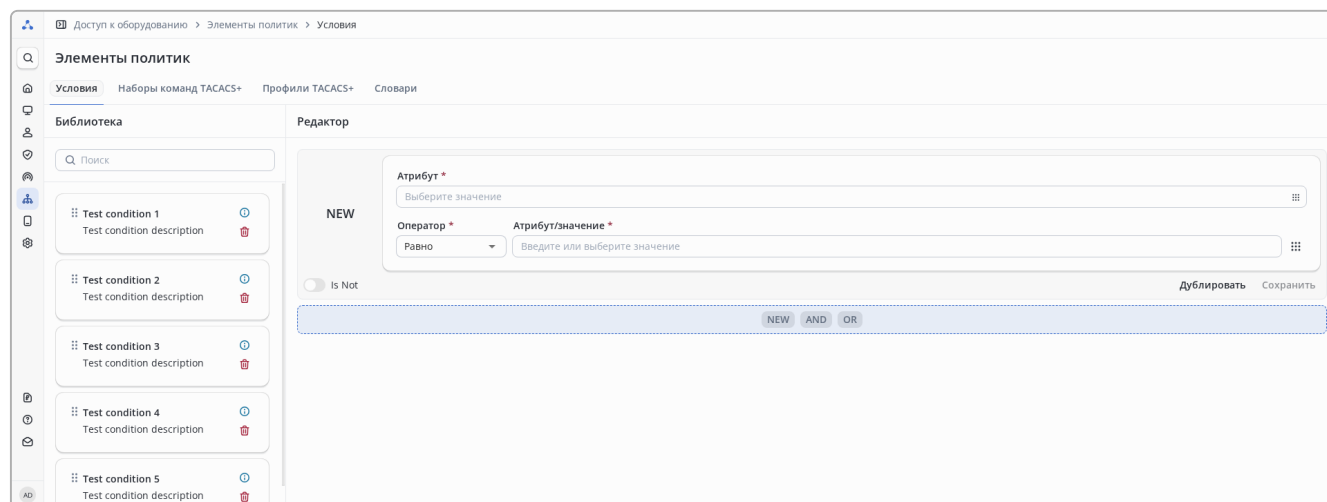


Рисунок 334. Библиотека логических условий

В левой части страницы расположена **Библиотека** логических условий.

Основной компонент страницы - **Редактор** логических условий:

- **Атрибут *** - атрибут логического условия.
- **Оператор *** - выбранный оператор логического условия. Может принимать значения (в зависимости от типа значения атрибута):
 - "Больше или равно" / "Меньше или равно"
 - "Больше чем" / "Меньше чем"
 - "Равно" / "Не равно"
 - "Равно NULL" / "Не равно NULL"
 - "Начинается на" / "Не начинается на"
 - "Заканчивается на" / "Не заканчивается на"
 - "Содержит" / "Не содержит"
 - "Соответствует" (полное соответствие строки с учетом регистра, так же есть поддержка [регулярных выражений](#))
 - "Диапазон IP"
 - "Маска IP"
 - "Пустое значение"
-

Атрибут/значение * - атрибут/значение, которые используются для сопоставления с атрибутом логического условия в соответствии с выбранным оператором. Для атрибута, предполагающего predetermined значения, выбор значения производится из списка.

- **Is Not** - выбор инвертирования результата выполнения условия (по умолчанию условие "Соблюдается", при включении настройки условие будет считаться "Не соблюдается")
- **NEW** - добавление нового логического условия в существующую иерархию на одном уровне с текущим.
- **AND** - добавление нового логического условия в качестве "дочернего" для существующего с логическим оператором "И".
- **OR** - добавление нового логического условия в качестве "дочернего" для существующего с логическим оператором "ИЛИ".

* - поля, обязательные для заполнения.

Элементы управления:

- **"Поиск"** - Выполняется регистронезависимая фильтрация по библиотеке логических условий по имени и описанию.
-  - Предпросмотр содержания логического условия.
-  - Удаление логического условия.
-  - Открыть словарь для добавления элемента.
-  - Удалить элемент из редактора. Действие зависит от расположения:
 - нажатие справа от поля "Атрибут" очистит соответствующее поле;
 - нажатие справа от поля "Атрибут/значение" очистит соответствующее поле;
 - нажатие справа от логического условия удалит данное условие.
- **"Сохранить"** - Сохранить соответствующее логическое условие.

Меню выбора атрибута

Для выбора атрибута, который будет использоваться в условии, необходимо нажать  - раскроется меню выбора атрибута.

Выбор атрибута для условия

Все

Device

Identity

LDAP

Network Access

TACACS+

Поиск

Словарь

ID

Выберите словарь

ID

Атрибут	Словарь	ID
Device Location	Device	4
Device Profile	Device	2
Device Type	Device	3
Model Name	Device	1
Endpoint Group	Endpoint identity	4
Logical Profile	Endpoint identity	6
MAC-Address	Endpoint identity	1
Profiling Policy	Endpoint identity	5

Рисунок 335. Меню выбора атрибута

Вверху находится список, позволяющий выполнить фильтрацию по типам словарей. Может быть выбран только один тип.

Типы словарей:

-  **DEVICE** - атрибуты на основе параметров [устройства](#), например - тип устройства.
-  **IDENTITY** - атрибуты [пользователей](#) и [эндпоинтов](#).
-  **LDAP** - атрибуты из [внешних источников идентификации](#).
-  **NETWORK_ACCESS** - содержит IP адрес устройства, на которое выполняет подключение администратор.
-  **TACACS_PLUS** - словарь атрибутов TACACS+.

Ниже находятся колонки для фильтрации атрибутов.

- "Атрибут" - регистронезависимая фильтрация по наименованию атрибута.
- "Словарь" - меню выбора словаря. Для использования должен быть выбран тип словаря.
- "ID" - фильтрация по номеру атрибута.

Создание логических условий

Создание простого логического условия

Создание логического условия выполняется в **Редакторе**.

NEW

Атрибут *

Выберите значение

Оператор *

Атрибут/значение *

Равно

Введите или выберите значение

Is Not

Дублировать

Сохранить

NEW

AND

OR

Рисунок 336. Исходное состояние редактора условия

После нажатия на  в правой части поля "Атрибут" раскроется [меню выбора атрибута](#).

Для поиска нужного атрибута можно воспользоваться фильтрацией по наименованию атрибута. Либо выбрать тип словаря и в нем, выбрав необходимый словарь путем прокрутки выпадающего списка, определить необходимый атрибут.

Редактор

NEW

Атрибут *

Выберите значение

Оператор *

Атрибут/значение *

Равно

Введите или выберите значение

Is Not

Дублировать

Сохранить

NEW

AND

OR

Выбор атрибута для условия

Все

Device

Identity

LDAP

Network Access

TACACS+

Поиск

Выберите словарь

ID

Атрибут	Словарь	ID
Device Location	Device	4
Device Profile	Device	2
Device Type	Device	3
Model Name	Device	1
Endpoint Group	Endpoint identity	4
Logical Profile	Endpoint identity	6
MAC-Address	Endpoint identity	1
Profile Policy	Endpoint identity	5

Рисунок 337. Выбор атрибута

После выбора атрибута необходимо кликнуть на него и он попадет в поле "Атрибут".

Далее необходимо выбрать оператор для сравнения значения атрибута (по умолчанию подставляется "Равно"). Список операторов зависит от типа данных используемых в значении выбранного атрибута.

Тип данных атрибута	Поддерживаемые операторы
Строка	Соответствует, Оканчивается на, Не оканчивается на, Начинается с, Не начинается с, Содержит, Не содержит, Равно, Не равно, Равно NULL, Не равно NULL, Пустое значение
Число	Больше или равно, Больше чем, Меньше или равно, Меньше чем, Равно, Не равно, Равно NULL, Не равно NULL, Пустое значение
IPv4 адрес	Равно, Не равно, Равно NULL, Не равно NULL, Диапазон IP, Маска IP, Пустое значение

Тип данных атрибута	Поддерживаемые операторы
MAC адрес	Равно, Не равно, Равно NULL, Не равно NULL, Начинается на, Не начинается на, Заканчивается на, Не заканчивается на, Содержит, Не содержит, Пустое значение
Наименование	Равно, Не равно, Равно NULL, Не равно NULL
Последовательность байт	Равно NULL, Не равно NULL

Затем в поле *Атрибут/значение* выбирается атрибут или вводится его значение.

Рисунок 338. Условие, в котором заполнены все параметры

Для сохранения условия в библиотеку условий нужно нажать кнопку **"Сохранить"**. Можно заменить существующее условие в библиотеке или сохранить новое.

Сохранение условия

☐ Заменить существующее условие в библиотеке

Условие *

Выберите условие

☒ Сохранить в библиотеку как новое условие

Имя *

New condition

Описание

Введите текст описания

0 / 200

Отмена Сохранить

Рисунок 339. Диалог сохранения условия в библиотеку

По умолчанию действие предполагает сохранение нового условия:

- **Имя *** - наименование условия. Максимальная длина - 100 символов.
- **Описание** - произвольное описание. Максимальная длина - 200 символов.

* - поля, обязательные для заполнения.

После нажать кнопку "Сохранить".

Для сохранения с заменой существующего условия в библиотеке необходимо выбрать "Заменить существующее условие в библиотеке" и выбрать условие в выпадающем списке. При необходимости можно выполнить фильтрацию по наименованию, введя соответствующий текст в поле перед списком.

После нажать кнопку "Сохранить".



Кнопка "Сохранить" всегда активна, чтобы иметь возможность сохранить существующее условие под другим именем.

Создание сложного логического условия

Для создания сложного логического условия из простого используется панель под логическим условием.



Рисунок 340. Панель для добавления дополнительного условия

- **New** - добавить логическое условие на одном уровне с существующим.
- **AND** - добавить дочернее условие с логическим "И".
- **OR** - добавить дочернее условие с логическим "ИЛИ".

При нажатии "New" в редакторе появится дополнительное правило на одном уровне с существующим, объединенные логическим "И".

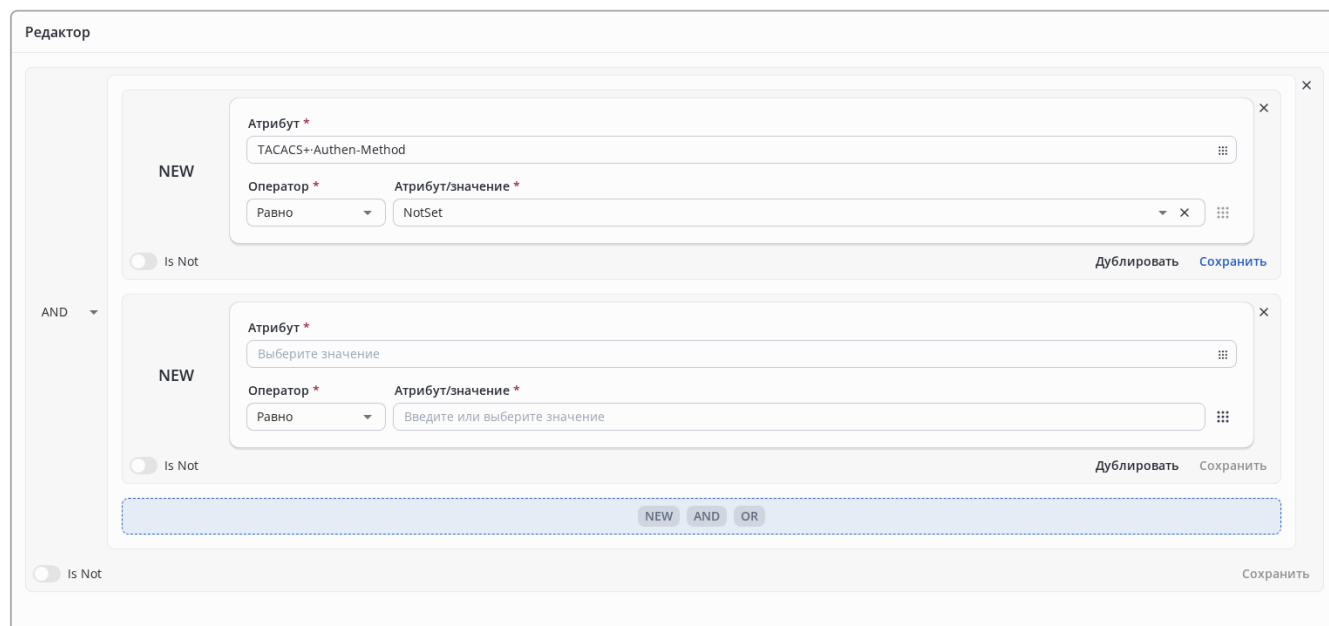


Рисунок 341. Условие, состоящее из двух условий, объединенные логическим "И"

- Логическое "И", объединяющее правила, можно изменить на "ИЛИ".
- Есть возможность сохранить каждое условие отдельно кнопкой "Сохранить" в его окне или все вместе, кнопкой "Сохранить" внизу.
- Для удаления условия надо нажать на **X** справа вверху в окне условия.
- Для полной очистки всех условий в редакторе надо нажать **X** вверху справа редактора, расположенный за окнами отдельных условий.

При нажатии "AND" или "OR" появится новое окно, в котором можно будет доступно новое меню, далее можно добавить условия на новом уровне или создать дочерние условия. Ограничение на вложенность условий нет.

Рисунок 342. Условие, содержащее вложенные правила

Для сохранения всех условий надо нажать кнопку "Сохранить" в нижнем правом углу.

Использование регулярных выражений

При добавлении условия в набор политик для атрибутов с оператором `соответствует` могут использоваться регулярные выражения. Это позволяет указать "шаблон", под который может подходить несколько значений, с помощью всего одной строки.

Пример 2. Использование регулярных выражений в логических условиях

Задача: Необходимо применить набор политик ко всем подключениям с устройств, имя которых начинается с префикса `MES`.

Возможное решение:

Для того, чтобы выделить только подключения с определенных устройств, в условии можно использовать атрибут `RADIUS·NAS-Identifier`. Обратите внимание, что как правило требуется настройка его отправки на NAS-устройстве.

Чтобы не создавать отдельные условия `RADIUS·NAS-Identifier равно MES1` и т.п. для каждого устройства, можно создать одно условие `RADIUS·NAS-Identifier соответствует MES.*`.

Конструкция `.*` означает "любое количество любых символов" после `MES`.

Также можно использовать более строгое выражение, если, например, предполагается, что после `MES` всегда идут 4 цифры и одна буква: `MES\d{4}[A-Z]`.

Здесь:

`\d{4}` — четыре цифры;

`[A-Z]` — одна заглавная буква.

Краткий список часто используемых метасимволов

- СИМВОЛЫ:
 - `.` - любой символ
 - `\d` - любая цифра
 - `\w` - любая буква в любом регистре
 - `\s` - пробельный символ
 - `\` - экранирование любого спецсимвола
- группировка:
 - `[abc]` - один из перечисленных в скобках символов (или a, или b, или c)
 - `[a-z]` - один из перечисленных в диапазоне символов
 - `(abc)` - объединение символов в указанном порядке в одну группу
- квантификаторы:
 - `a?` - 0 или 1 вхождение символа
 - `a*` - 0 и больше вхождений символа
 - `a+` - 1 и больше вхождений символа
 - `a{n}` - вхождение символа n раз
 - `a{n,}` - вхождение символа n или больше раз
 - `a{n,m}` - вхождение символа от n до m раз
- логические операции:
 - `^a` - отрицание
 - `a|b` - один из двух указанных символов (ИЛИ)
- полезные комбинации:
 - `.*` - любой символ любое количество раз
 - `\w+` - любое слово
 - `(word1)|(word2)` - одно из указанных слов



Редактирование логического условия

Для редактирования логического условия необходимо его захватить курсором в библиотеке и перенести в поле редактора.

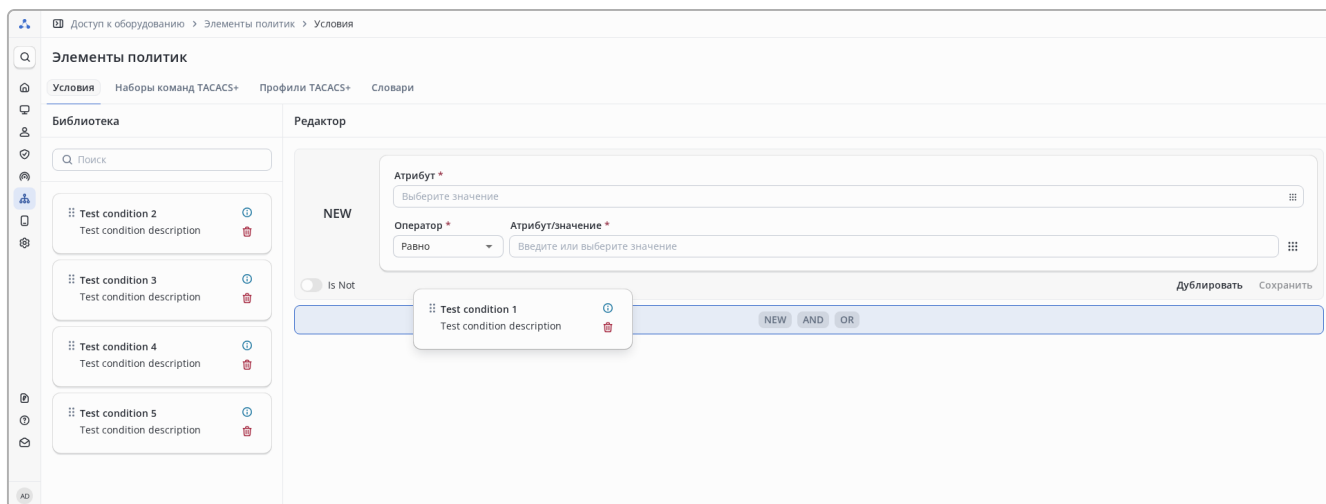


Рисунок 343. Выбор логического условия

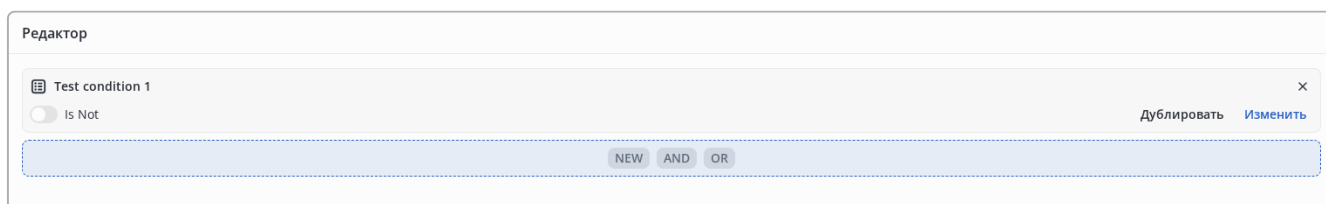


Рисунок 344. Редактирование логического условия

Для редактирования условия нажать кнопку "Изменить". После редактирования нажать кнопку "Сохранить". Так как условие ранее было сохранено в библиотеке - по умолчанию будет предложено сохранить его с тем же названием. При необходимости можно выбрать другое условие, которое будет перезаписано или выбрать "Сохранить в библиотеку как новое условие". Нажать кнопку "Сохранить".

Так же в ходе редактирования можно перетаскивать условия из библиотеки в поле редактора дочернего условия.

Удаление логического условия

Для удаления логического условия надо найти его в библиотеке и нажать кнопку  справа от имени условия.

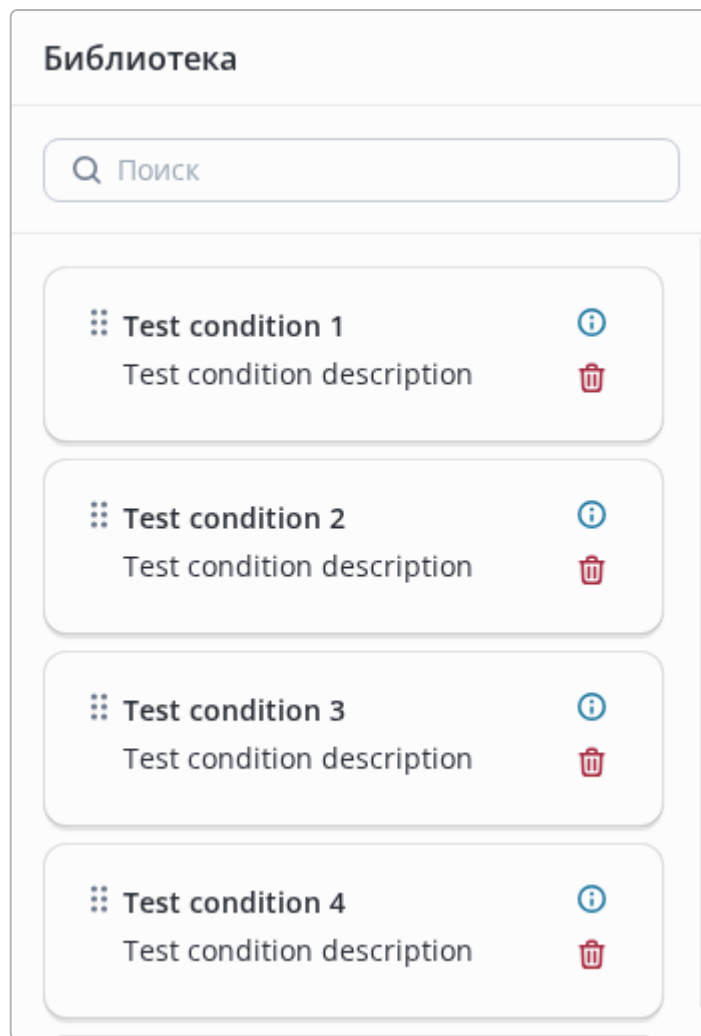


Рисунок 345. Выбор условия для удаления



Удаление элементов требует подтверждения в модальном окне. Выбранные элементы будут удалены только после явного подтверждения операции.

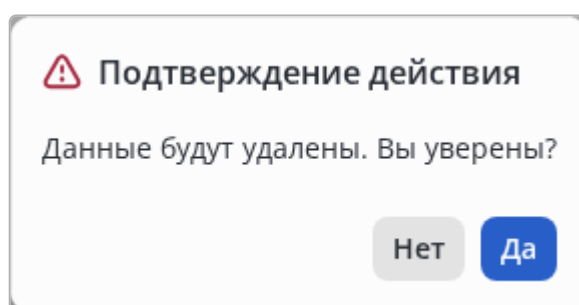


Рисунок 346. Диалоговое окно подтверждения действия



Ограничения:

- нельзя удалить или отредактировать некоторые системные логические условия;
- нельзя удалить логические условия, которые используются в других сложных логических условиях;
- нельзя удалить логические условия, которые используются в каком-либо наборе политик.

Наборы команд TACACS+



Данный раздел содержит информацию по настройке функционала, доступ к которому приобретается отдельно с помощью дополнительной опции лицензии **NAICE-TACACS+**. По вопросам приобретения функционала обращайтесь к Вашему менеджеру или на электронную почту eltex@eltex-co.ru.

Описание

Наборы команд TACACS+ предназначены для определения списка команд, которые разрешены или запрещены к выполнению на устройстве при использовании авторизации команд на сервере TACACS+. Эти наборы команд в дальнейшем используются в разделе [:policy-sets/index.html](http://policy-sets/index.html) при настройке политики авторизации.

Просмотр наборов команд TACACS+

На данной странице содержится таблица со списком всех наборов команд TACACS+.

Имя	Описание
Allow all	
Deny all	Deny All
Show only	
MES	
WLC	

Рисунок 347. Таблица со списком наборов команд TACACS+ на странице просмотра

Таблица содержит колонки:

- **Имя** - название набора команд.
 -  - Данная запись является системной и недоступна для удаления или редактирования.
- **Описание** - произвольное описание.

Сортировка возможна только по полю "Имя" в прямом и обратном порядке. По умолчанию сортировка выполняется в прямом (алфавитном) порядке.

Элементы управления:

-  — Добавить новый элемент.
-  — Дублировать выбранный чекбоксом элемент. Становится активным, если выбран только один элемент в списке.
-  — Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
-  — Обновить данные таблицы.
-  — Позволяет загрузить данные из csv-файла.
-  — Позволяет выгрузить данные в csv-файл.
- ☐ — Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).
-  — Изменить текущий порядок сортировки.
-  Поиск — Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.

Добавление нового набора команд

Для добавления набора команд нажмите  в левой верхней части поля над таблицей.

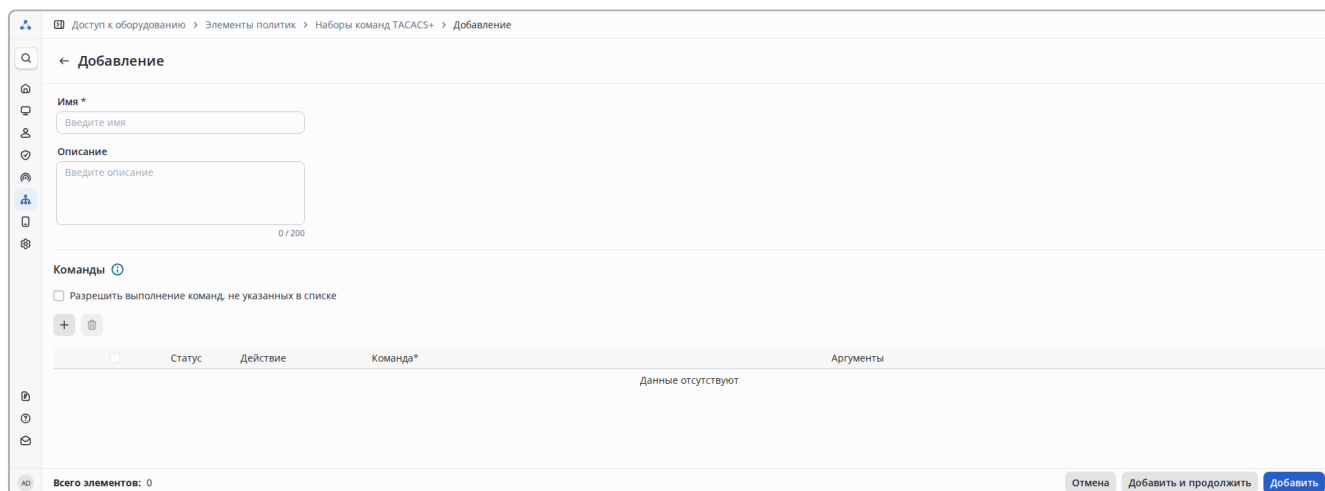


Рисунок 348. Форма добавления набора команд

На открывшейся странице представлены следующие параметры:

- **Имя *** - наименование условия профилирования. Максимальная длина - 100 символов.
- **Описание** - произвольное описание условия профилирования. Максимальная длина - 200 СИМВОЛОВ.

Параметры, отмеченные *, обязательны для заполнения.

Команда - блок настроек, отвечающий за определение разрешенных и запрещенных к авторизации команд. Для удобства конфигурирования команды задаются в таблице, которая содержит следующие колонки:

⋮ - содержит кнопки, потянув за которые можно изменить порядок строк в таблице.



Порядок указания команд важен, так как сравнение команды для авторизации с представленными в таблице командами происходит **сверху-вниз до первого совпадения**.

- ☐ - содержит чекбоксы для выбора элементов для выполнения дальнейших действий (например, удаления).
- Статус - может принимать значения Включено или Выключено. Выключенные команды не участвуют в процессе проверки авторизуемой команды. Выключение команды вместо ее удаления может быть полезно при отладке.
- Действие - какое действие выполнить при совпадении сравниваемых команд: разрешить или запретить авторизацию команды.
- Команда * - команда, авторизацию которой требуется разрешить или запретить. При указании команды могут использоваться регулярные выражения, см. [Использование регулярных выражений в наборах команд](#).
- Аргументы - разрешенные или запрещенные аргументы для указанной команды. Если ни один аргумент не указан, то любые аргументы для команды попадают под указанное в правиле Действие. При указании аргументов могут использоваться регулярные выражения, см. [Использование регулярных выражений в наборах команд](#).

Разрешаются/запрещаются только команды, содержащие **точно** те атрибуты, которые указаны в строке атрибутов. Если после атрибута команды следует другой атрибут, который не указан в наборе команд, то такая команда считается не подходящей под условия и будет обработана соответствующим образом.

Пример. Авторизуемая команда - `show running-config interface GigabitEthernet0/1`.

Набор команд выглядит следующим образом:

Действие	Команда	Аргументы
Разрешено	show	running-config

В этом случае авторизуемая команда **не попадает** под указанные правила и авторизация будет **запрещена** согласно поведению по умолчанию.

Для того, чтобы были разрешены любые аргументы после указанных, можно использовать регулярное выражение `.*` (любой символ ожидается любое количество раз) или любое другое подходящее выражение:

Действие	Команда	Аргументы
Разрешено	show	running-config .*

По умолчанию любые команды, которые не указаны в списке, запрещены. Данное поведение можно изменить с помощью настройки ☐ Разрешить выполнение команд, не указанных в списке.

Для добавления новой команды в таблицу используется кнопка . Команда будет добавлена в самый верх таблицы (то есть новая команда, если не менять ее порядок с помощью , будет самой приоритетной).

Для добавления набора команд в системе предусмотрены две кнопки добавления, различающиеся последующим поведением:

- **"Добавить и продолжить"** — после нажатия форма не закрывается.
- **"Добавить"** — после нажатия выполняется перенаправление на страницу со списком наборов команд TACACS+.

Редактирование набора команд

Для редактирования набора команд TACACS+ необходимо на странице со списком нажать на его имя.

☐	Имя ↑
☐	Allow all 
☐	Deny all 
☐	Show only 
☐	MES
☐	WLC

Рисунок 349. Гиперссылка на страницу редактирования набора команд

После этого откроется окно редактирования.

Форма редактирования набора команд аналогична форме создания, за исключением нескольких удобных функций, позволяющих редактировать таблицу с командами, не покидая страницу по кнопке сохранения:

-  - сбросить внесенные в команду изменения
- **Применить** - сохранить изменения в таблице команд, не покидая страницу редактирования текущего набора команд. Может быть полезно при отладке.

Для сохранения изменений в системе предусмотрены две кнопки, различающиеся последующим поведением:

- **"Сохранить и продолжить"** — после нажатия форма не закрывается.
- **"Сохранить"** — после нажатия выполняется перенаправление на страницу со списком наборов команд TACACS+.

Кнопка "Отмена" осуществляет сброс внесенных изменений до исходного состояния.

Использование регулярных выражений в наборах команд

При указании команды или ее аргументов в наборе команд могут использоваться регулярные выражения. Это позволяет указать "шаблон", под который может подходить несколько команд, с помощью всего одной строки.

Пример 3. Использование регулярных выражений при указании команды

Задача: Необходимо разрешить конфигурирование на устройстве настроек RADIUS сервера, при этом на устройстве возможны 2 команды - `radius` для настройки сервера на устройстве и `radius-server` для настройки внешнего сервера. Администратору должны быть доступны обе команды.

Возможные решения:

Чтобы не указывать обе команды полностью, можно использовать регулярное выражение: `radius.*`.

Символ `.` здесь означает любой символ, а `\*` - его повторение в выражении любое количество раз (в том числе 0 раз).

Также можно составить более строгое регулярное выражение: `radius-?\w*`.

Конструкция `-?` означает, что дефис может встретиться 0 или 1 раз, а `\w*` - 0 или больше вхождений любой буквы.

Пример 4. Использование регулярных выражений при указании аргументов команды

Задача: Ограничить команду `show`, разрешив вывод только информации о настроенных RADIUS- и TACACS-серверах.

Возможные решения:

Самое простое и прямое решение - указать две команды с соответствующими аргументами:

Команда	Аргументы
<code>show</code>	<code>radius-servers</code>
<code>show</code>	<code>tacacs</code>

Но более коротким решением будет указать аргументы через `|` (или):

Команда	Аргументы
<code>show</code>	<code>(radius-servers) (tacacs)</code>

Краткий список часто используемых метасимволов

- СИМВОЛЫ:
 - `.` - любой символ
 - `\d` - любая цифра
 - `\w` - любая буква в любом регистре
 - `\s` - пробельный символ
 - `\` - экранирование любого спецсимвола
- группировка:
 - `[abc]` - один из перечисленных в скобках символов (или a, или b, или c)
 - `[a-z]` - один из перечисленных в диапазоне символов
 - `(abc)` - объединение символов в указанном порядке в одну группу
- квантификаторы:
 - `a?` - 0 или 1 вхождение символа
 - `a*` - 0 и больше вхождений символа
 - `a+` - 1 и больше вхождений символа
 - `a{n}` - вхождение символа n раз
 - `a{n,}` - вхождение символа n или больше раз
 - `a{n,m}` - вхождение символа от n до m раз
- логические операции:
 - `^a` - отрицание
 - `a|b` - один из двух указанных символов (ИЛИ)
- полезные комбинации:
 - `.*` - любой символ любое количество раз
 - `\w+` - любое слово
 - `(word1)|(word2)` - одно из указанных слов



Удаление наборов команд

Для удаления наборов команд на странице просмотра необходимо выделить чекбокс слева от наборов, которые требуется удалить, и нажать кнопку  вверху слева.

	Имя ↑
☐	Allow all 
☐	Deny all 
☐	Show only 
☒	MES
☐	WLC

Рисунок 350. Выбор набора команд в таблице для удаления



Удаление элементов требует подтверждения в модальном окне. Выбранные элементы будут удалены только после явного подтверждения операции.

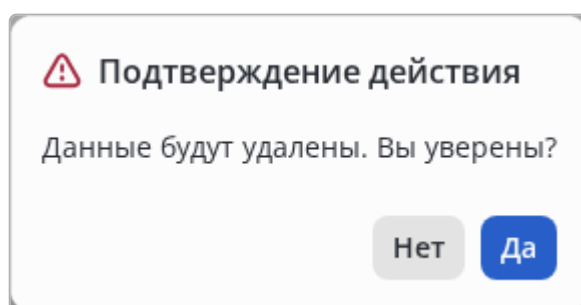


Рисунок 351. Диалоговое окно подтверждения действия



Ограничения:

- нельзя удалить наборы команд, которые используются в какой-либо политике TACACS+.
- нельзя удалить системные наборы команд `Allow all`, `Deny all` и `Show only`.

Импорт

NAICE поддерживает импорт данных из CSV-файлов.

Предварительная подготовка перед импортом

1. Создайте или проверьте наличие необходимых связанных записей (например, профиль устройства).
2. Ознакомьтесь с требованиями к CSV-файлу:
 - Файл должен быть в кодировке UTF-8;
 - Разделитель полей: запятая (,)
 - Разделитель строк/текста: двойная кавычка (")
 - Заголовки и значения должны быть взяты в двойные кавычки (")
 - Максимальный размер файла 2МБ.
3. Проверьте содержимое файла на наличие лишних кавычек перед импортом;

4. Проверьте то что значения, содержащие двойную кавычку (") или слэш (/) правильно экранированы.
- Значения, содержащие двойную кавычку (") экранируются с помощью \"
 - Значения, содержащие слэш (/) экранируются с помощью \/

Правильное написание значений (с экранированием помощью \) на примере содержания файла для импорта набора команд TACACS:

"name:Required"	"description"	"permit_unmatch ed(true/false)"	"commands(Grant/command/argume nts/enabled;...)"
"command_set"	"\"Test command set\""	"false"	"PERMIT/\"show/vlan 1 2 \"/true"

Некорректное написание значений (без экранирования) на примере содержания файла для импорта набора команд TACACS:

"name:Required"	"description"	"permit_unmatch ed(true/false)"	"commands(Grant/command/argume nts/enabled;...)"
"command_set"	"Test command set"	"false"	"PERMIT/show/vlan 1 2 /true"



Игнорирование экранирования приведёт к некорректному распознаванию данных.

Порядок выполнения импорта

Для импорта данных из CSV-файла нажмите  на панели действий, расположенной над таблицей. После чего откроется окно:

Импорт

При импорте дублирующиеся данные не будут перезаписаны или отредактированы - система пропустит их. Если вы хотите изменить старые данные, удалите их из системы вручную перед импортом.

Внимательно ознакомьтесь с [Документацией](#) , чтобы импорт прошёл без ошибок.

Выберите файл*
Максимальный размер файла 2МБ

 **Загрузите** или перетащите сюда

Поле обязательно для заполнения

Источник данных *

NAICE

☐ Игнорировать существующие данные 

☐ Остановить импорт при первой ошибке

Отмена

Импорт

Рисунок 352. Окно Импорта

Импорт данных из CSV-файла выполняется в несколько шагов:

1. Выберите необходимый CSV-файл, перетащив его в поле загрузки или выбрав через проводник, нажав кнопку "Загрузите";



Измененный CSV-файл нужно загрузить повторно, чтобы применить правки.

2. Выберите источник данных, если он заранее не определён;
3. При необходимости активируйте флаги импорта:

Игнорировать существующие данные

- Если переключатель включен — дубликаты записей считаются предупреждением.
- Если переключатель выключен — дубликаты расцениваются как ошибка.

Остановить импорт при первой ошибке

- Если переключатель включен — импорт останавливается при первой же ошибке. Будут импортированы только записи, которые были успешно обработаны до её возникновения.

Если переключатель выключен — ошибочные строки пропускаются, импорт продолжается до конца. Будут импортированы только валидные записи.

4. Для того чтобы импорт начался, нажмите кнопку **"Импорт"**.



При импорте дублирующиеся данные перезаписаны или отредактированы не будут - система пропустит их. Если вы хотите изменить старые данные, удалите их из системы вручную перед импортом.

Просмотр отчета по импорту

Сразу после завершения обработки файла откроется окно отчёта по импорту.

Если все записи в файле были обработаны корректно, вы увидите окно:

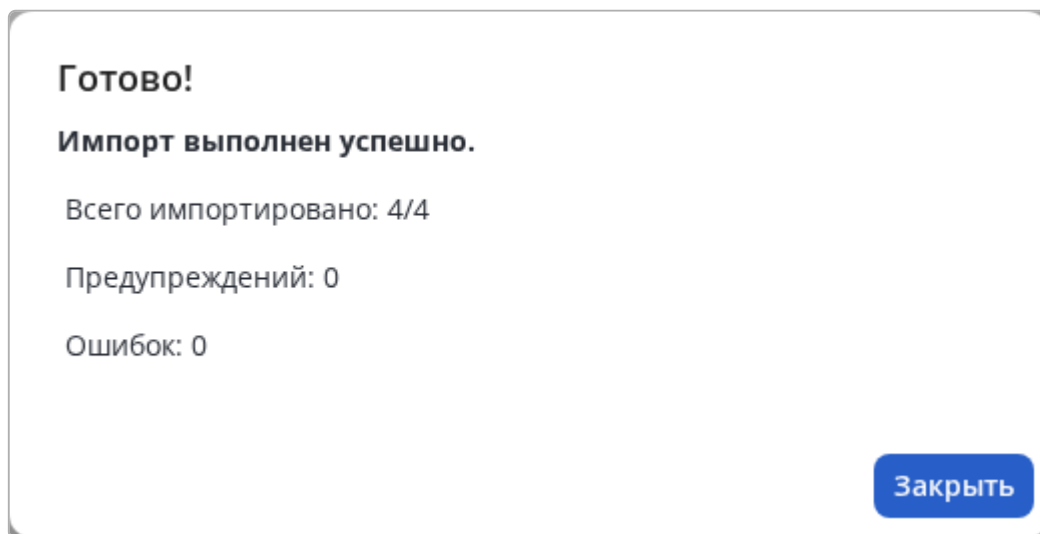


Рисунок 353. Отчет импорта (все записи обработаны корректно)

Блок с общей информацией содержит:

- **Всего импортировано** - Счётчик того, сколько записей было импортировано из общего импортируемого количества строк;
- **Предупреждений** - Количество возникших предупреждений;
- **Ошибок** - Количество возникших ошибок.

Если не все записи были обработаны корректно, вы увидите окно:

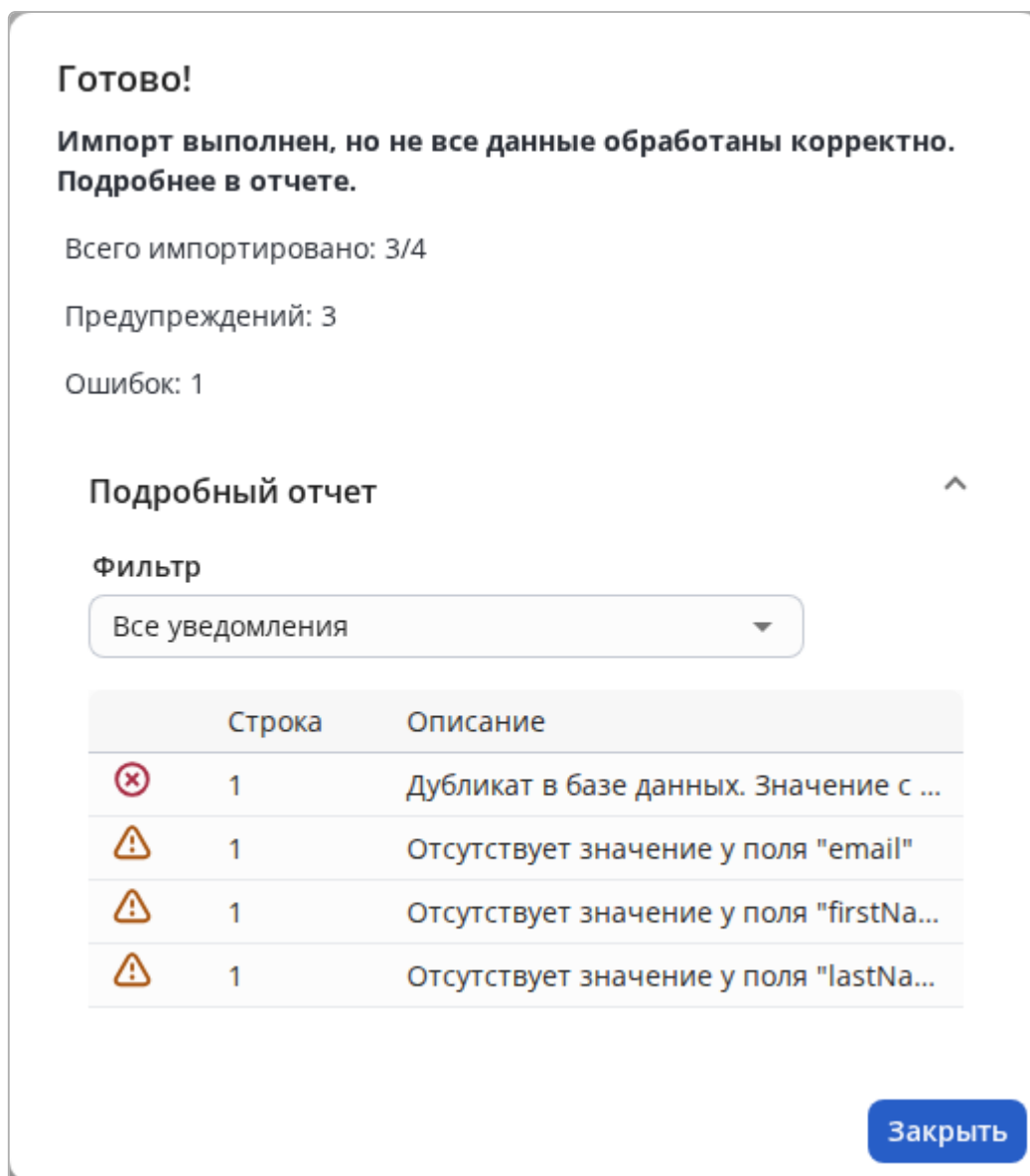


Рисунок 354. Отчет импорта (записи обработаны с ошибками/предупреждениями)

Подробный отчет содержит следующую информацию:

- **Фильтр** - Выпадающий список, в котором можно выбрать отображаемые уведомления (Все уведомления, Только ошибки или Только предупреждения)

Таблица уведомлений содержит колонки:

- **Строка** - Номер строки в CSV-файле, где обнаружена ошибка или предупреждение;
- **Описание** - Детальное текстовое объяснение ошибки или предупреждения.



Для просмотра полного текста описания наведите курсор мыши на соответствующую строку - во всплывающей подсказке отобразится полный текст сообщения об ошибке или предупреждении.

Особенности импорта наборов команд TACACS+



Для импорта наборов команд TACACS+ в качестве источника данных поддерживаются NAICE и CISCO.

В таблице ниже приведен список полей, их обязательность, описание и требования:

Поле	Описание	Требования
name:Required	Имя набора команд	Обязательное поле Максимальная длина - 100 символов Должно быть уникальным Нельзя использовать пробелы
description	Произвольное описание	Максимальная длина - 200 символов
permit_unmatched(true/false)	Разрешение выполнения команд, не указанных в таблице commands	Возможные значения: - true - статус "Включено" - false - статус "Выключено"
commands(Grant/command/arguments/enabled;...)	Блок настроек, отвечающий за определение разрешенных и запрещенных к авторизации команд	Разделитель команд: ; Требования по каждому полю будут рассмотрены отдельно

Столбец `commands(Grant/command/arguments/enabled;...)` содержит в себе поля `Grant`, `command`, `arguments`, `enabled`.

Список полей, их обязательность, описание и требования для столбца `commands(Grant/command/arguments/enabled;...)`:

Поле	Описание	Требования
Grant	Действие выполняемое при совпадении сравниваемых команд	Обязательное поле Возможные значения: - PERMIT - статус "Разрешено" - DENY - статус "Запрещено"
command	Команда	Обязательное поле Максимальная длина - 200 символов
arguments	Аргументы для команды	Максимальная длина - 200 символов
enabled	Разрешение на выполнение (Статус)	Обязательное поле Возможные значения: - true - статус "Включено" - false - статус "Выключено"



Если значение для поля `permit_unmatched(true/false)` не найдено/некорректно будет присвоено значение по умолчанию `false`.



Если значение для поля `commands(enabled)` не найдено/некорректно будет присвоено значение по умолчанию `true`.

Пример корректного содержания файла:

"name:Required"	"description"	"permit_unmatch ed(true/false)"	"commands(Grant/command/argume nts/enabled;...)"
"command_set"	"Тестовые набор команд"	"false"	"PERMIT/\"show/vlan 1 2 \"/true;PE RMIT/tacacs-server//true"



Как видно из примера, значения, содержащие слэш (/), должны быть экранированы с помощью \. Игнорирование экранирования приведёт к некорректному распознаванию данных.

Получение CSV-файла шаблона описано далее в разделе "Экспорт".

Экспорт

NAICE поддерживает экспорт данных в формате CSV. Значения и заголовки обрамляются двойными кавычками, разделитель полей: запятая (,).

Процедура экспорта

Доступны два режима экспорта данных:

- **Экспорт всего** - Выгрузка всех записей текущего раздела. Системные записи исключаются из экспорта;
- **Экспорт выбранного** - Выгрузка только отмеченных чекбоксом записей.

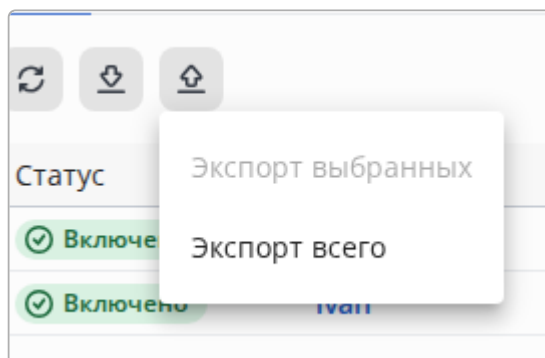


Рисунок 355. Окно выбора режима экспорта



Значения содержащие двойную кавычку (") или слэш (/) будут экранированы с помощью \.

Экспорт всех записей

На панели действий над таблицей нажмите  и выберите режим "Экспорт всего". В открывшемся окне подтвердите действие кнопкой "Экспорт":

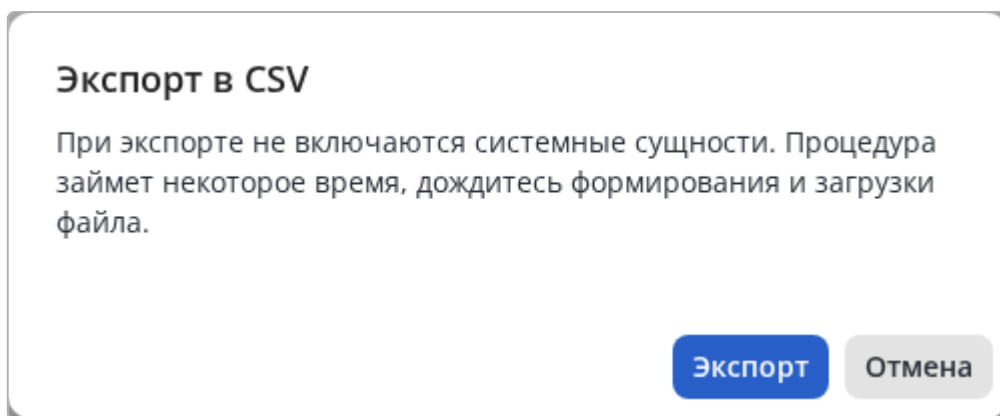


Рисунок 356. Экспорт всего

После нажатия кнопки "Экспорт" на устройство выгрузится файл, содержащий все записи из текущего раздела.

Экспорт выбранных записей

На панели действий над таблицей нажмите  и выберите режим "Экспорт выбранных". В открывшемся окне подтвердите действие кнопкой "Экспорт":

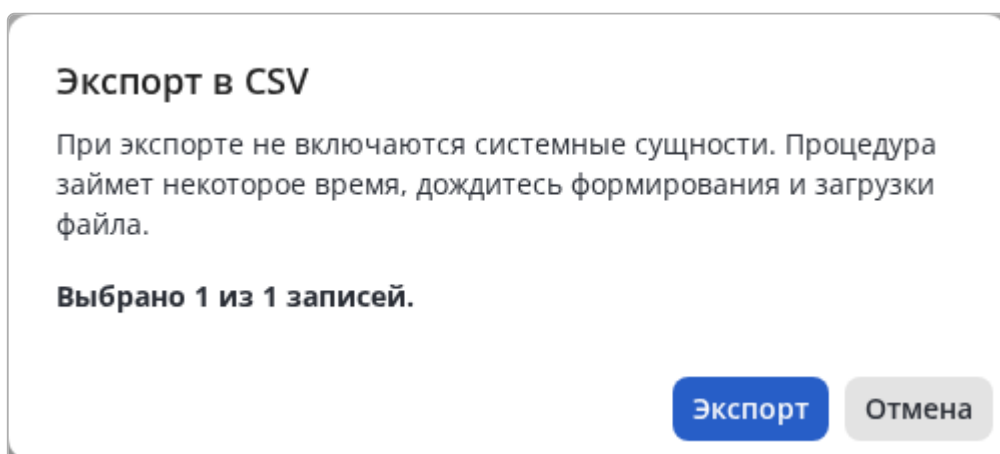


Рисунок 357. Экспорт выбранных

После нажатия кнопки "Экспорт" на устройство выгрузится файл, содержащий только отмеченные записи.



При **открытии** CSV-файлов в качестве разделителя полей **всегда** используйте **запятую (,)**, разделителем строк/текста могут быть **двойные кавычки (")** или **пустое значение**.

При **сохранении** CSV-файлов в качестве разделителя полей **всегда** используйте **запятую (,)**, а разделитель строк/текста - **пустое значение**.



Если при открытии файла использовался разделитель строк — двойная кавычка ("), то значения, содержащие символы двойной кавычки (") или слэша (/), экранированные как \", могут при сохранении получить лишнюю кавычку (") после (\"). Проверьте файл в текстовом редакторе и удалите лишние кавычки, если они появились.

Шаблон

Если в таблице отсутствуют записи (либо присутствуют только системные), при выборе режима **"Экспорт всего"** будет сформирован CSV-файл, содержащий исключительно заголовки столбцов. Данный файл может быть использован в качестве **шаблона** для подготовки данных перед импортом.

Особенности экспорта наборов команд TACACS+



Значения, содержащие двойную кавычку (") или слэш (/), будут экранированы с помощью \".

Структура csv-файла для наборов команд TACACS+ описана в разделе ["Особенности импорта наборов команд TACACS+"](#).

Профили TACACS+



Данный раздел содержит информацию по настройке функционала, доступ к которому приобретается отдельно с помощью дополнительной опции лицензии **NAICE-TACACS+**. По вопросам приобретения функционала обращайтесь к Вашему менеджеру или на электронную почту eltex@eltex-co.ru.

Описание

Профили TACACS+ предназначены для обобщения тонкой настройки уровней привилегий доступа к сетевым устройствам в отдельные записи, назначаемые Администраторам сетевых устройств, прошедшим аутентификацию и авторизацию по протоколу TACACS+.

Основными настройками в профилях устройств являются:

- Уровни привилегий назначаемые в рамках профиля (уровень по умолчанию и максимальный уровень).
- Пользовательские атрибуты.

Просмотр списка профилей

Рисунок 358. Таблица с перечнем профилей TACACS+

На данной странице содержится таблица со списком профилей TACACS+.

Таблица содержит колонки:

- **Имя** - наименование профиля.
 -  - Данная запись является системной и недоступна для редактирования и удаления.
- **Описание** - произвольное описание профиля.

Доступна сортировка по колонке **Имя**.

Элементы управления:

-  - Добавить профиль TACACS+.
-  - Дублировать профиль TACACS+.
-  - Удалить выбранный (отмеченный флажком) профиль TACACS+.
-  - Обновить список профилей.

Добавление профиля TACACS+

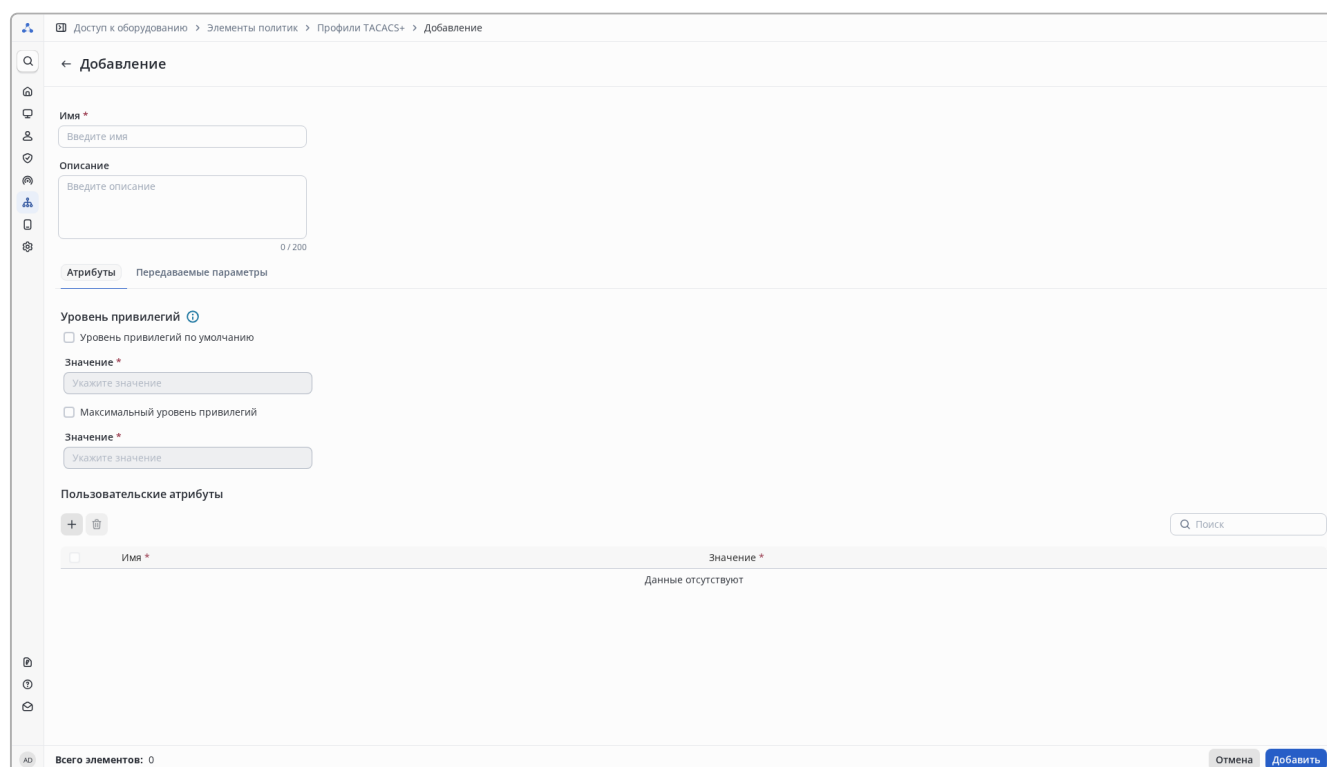


Рисунок 359. Страница добавления профиля TACACS+

Для добавления профиля устройства нажмите .

В открывшемся окне необходимо заполнить следующие параметры:

- **Имя *** - Наименование профиля.
- **Описание** - Описание профиля в произвольной форме (будет отображаться в списке профилей).
-

Уровень привилегий по умолчанию - Уровень привилегий доступный авторизуемому администратору сразу после авторизации.

- Максимальный уровень привилегий - Уровень привилегий доступный к повышению авторизованному администратору (данный уровень пользователь может включить при помощи авторизованных команд, например в процессе конфигурации сетевого устройства).

Параметры отмеченные символом * - обязательны для заполнения.



Если флажки включения параметров **Уровень привилегий по умолчанию** и **Максимальный уровень привилегий** сняты, авторизуемой учетной записи администратора будет назначен единственный доступный уровень привилегий "1" по умолчанию.

Пользовательские атрибуты или иначе **Attribute-Value pairs** - атрибуты определяющие параметры авторизации, учетных записей и сессий в рамках протокола TACACS+.

Для добавления и удаления пользовательских атрибутов используются следующие элементы управления:

-  - Добавить атрибут.
-  - Удалить выбранный (отмеченный флажком) атрибут.

При добавлении атрибута - поля отмеченные символом * обязательны для заполнения.

После завершения настройки профиля нажмите **Добавить** чтобы добавить созданный профиль и вернуться на страницу "Профили TACACS+".

Редактирование профиля TACACS+

Для редактирования профиля TACACS+ необходимо на странице со списком нажать на его имя.

☐	Имя ↑
☐	Both privilege 
☐	Deny all shell profile 
☐	Maximum privilege 
☐	Minimum privilege 
☐	MES

Рисунок 360. Гиперссылка на страницу редактирования профиля TACACS+



Ограничение:

- нельзя редактировать системные профили TACACS+ ().

После этого откроется окно редактирования.

Рисунок 361. Страница редактирования профиля TACACS+

После редактирования необходимо нажать на кнопку **"Сохранить"**. Кнопка скрыта, пока не будет внесено хотя бы одно изменение.

Кнопка **"Отмена"** осуществляет сброс внесенных изменений до исходного состояния.

Удаление профиля TACACS+

Для удаления профиля TACACS+ необходимо выделить чекбокс слева от профиля, который требуется удалить, и нажать кнопку  вверху слева.

	Имя ↑
☐	Both privilege 
☐	Deny all shell profile 
☐	Maximum privilege 
☐	Minimum privilege 
☒	MES

Рисунок 362. Выбор профиля TACACS+ в таблице для удаления



Удаление элементов требует подтверждения в модальном окне. Выбранные элементы будут удалены только после явного подтверждения операции.

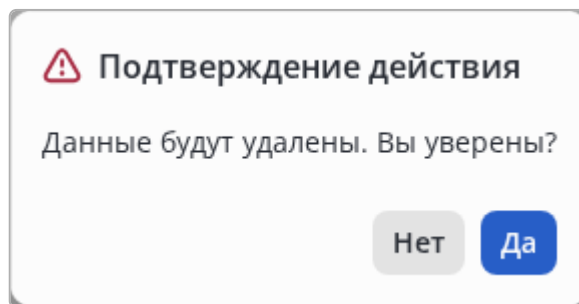


Рисунок 363. Диалоговое окно подтверждения действия



Ограничение:

- нельзя удалить системные профили TACACS+ (🔒).

Базовые профили TACACS+ доступные по умолчанию.

При включении функционала TACACS+ для администратора системы уже доступно несколько предустановленных базовых профилей TACACS+:

- **Both privilege** - Попадающим под данный профиль авторизуемым учетным записям будет назначен уровень привилегий по умолчанию "1", и доступный для повышения максимальный уровень привилегий "15".
- **Deny all shell profile** - Попадающим под данный профиль авторизуемым учетным записям будет отказано в авторизации.
- **Maximum privilege** - Попадающим под данный профиль авторизуемым учетным записям будет назначен уровень привилегий по умолчанию "15".
- **Minimum privilege** - Попадающим под данный профиль авторизуемым учетным записям будет назначен уровень привилегий по умолчанию "1".

Перечисленные профили являются системными (🔒) и не подлежат редактированию или удалению.

Политики TACACS+



Данный раздел содержит информацию по настройке функционала, доступ к которому приобретается отдельно с помощью дополнительной опции лицензии **NAICE-TACACS+**. По вопросам приобретения функционала обращайтесь к Вашему менеджеру или на электронную почту eltex@eltex-co.ru.

Описание

Политики TACACS+ определяют действия, которые необходимо выполнить при обработке запросов на аутентификацию и авторизацию администраторов сетевых устройств по протоколу TACACS+.

Порядок обработки запросов:

1. Обработка в таблице наборов политик:

- Выполняется проверка соответствия запроса согласно логическим условиям, используемым в политике авторизации.

Проверка выполняется последовательно сверху вниз. Отключенные политики не участвуют в проверке и пропускаются. Для политик, у которых установлен статус "Проверка условия" происходит увеличение счётчика срабатываний политики, но обработка запроса в них не выполняется поиск подходящей политики продолжается далее.

- При обнаружении подходящей политики дальнейший их перебор прекращается и продолжается проверка в рамках этого набора.
- Если политика с подходящим условием не будет найдена - обработка запроса будет выполняться в рамках политики по умолчанию **Default**. Данная политика всегда является последней, не может быть удалена и для нее недоступно редактирование условия. По умолчанию в данном наборе политик в политике авторизации настроен профиль авторизации **DenyAccess**, согласно которому подключение к сетевому устройству будет отклонено. Данное поведение может быть изменено путём добавления или редактирования политик аутентификации и авторизации в политике по умолчанию **Default**.

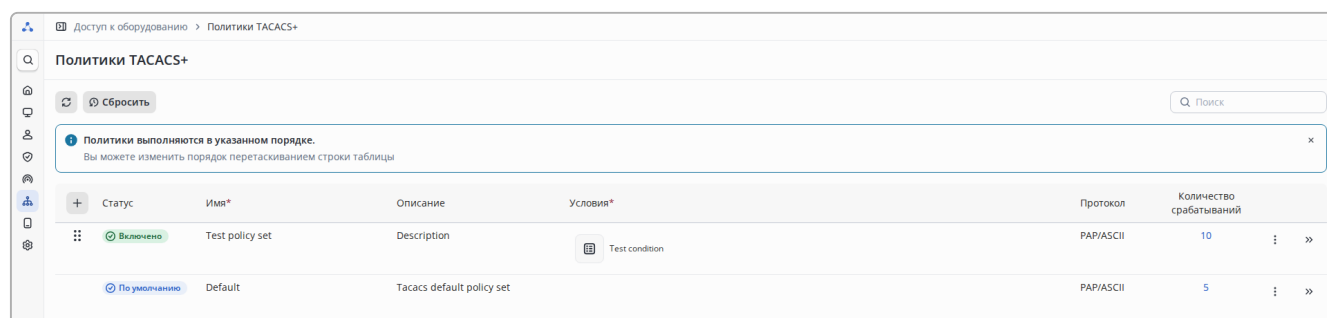
2. Обработка в рамках найденной политики:

- В рамках найденной политики из набора политик сначала выполняется проверка соответствия условиям политики аутентификации.
- После определения политики аутентификации выполняется поиск пользователя в выбранной для данной политики цепочке идентификаций. В случае если пользователь не найден или его пароль неверен - подключение отклоняется, обработка запроса на этом заканчивается.
- Для запросов пользователей успешно прошедших аутентификацию выполняется проверка соответствия условиям политик авторизации.
- После определения политики авторизации в зависимости от типа запроса выполняется:
 - Запрос на авторизацию уровня привилегий после аутентификации: из назначенного политике авторизации профиля TACACS+ выбирается значение поля "Уровень привилегий по умолчанию". Если оно не задано - выдаётся 1-й уровень привилегии.
 - Запрос на повышение уровня привилегий: из назначенного политике авторизации профиля TACACS+ выбирается значение поля "Максимальный уровень привилегий" и сравнивается с запрошенным уровнем привилегий - если запрошенный уровень привилегий меньше или равен указанному в настройке - повышение разрешается, в противном случае отклоняется. Если в выбранном профиле значение не задано - запрос на повышение привилегии отклоняется.
 - Запрос на авторизацию команды, выполняемой на сетевом устройстве: проверяется соответствие команды выбранному в политике авторизации набору команд TACACS+. Если в выбранном наборе команда разрешена - ее выполнение разрешается, в противном случае отклоняется.



Если в настройках политики авторизации выбран профиль по умолчанию "Deny all shell profile" - запросы аутентификации и авторизации попадающие под этот профиль отклоняются, в том числе для пользователей успешно прошедших аутентификацию.

Просмотр списка наборов политик



Статус	Имя*	Описание	Условия*	Протокол	Количество срабатываний
Включено	Test policy set	Description	Test condition	PAP/ASCII	10
По умолчанию	Default	Tacacs default policy set		PAP/ASCII	5

Рисунок 364. Просмотр всех политик.

Описание колонок таблицы:

- Статус - статус политики.
- Имя * - наименование политики.
- Описание - произвольное описание.
- Условия * - используемые логические условия. Если используется библиотечное условие - отображается его имя. Если используется не библиотечное условие - отображается его структура.
- Протокол * - всегда PAP/ASCII.
- Количество срабатываний - количество попыток авторизации, подпадающих под указанные Условия.

Элементы управления:

- обновить данные.
- Сбросить** - сбросить счетчики количества срабатываний всех наборов политик (попыток).
- Поиск - регистронезависимый поиск по имени набора политик (найденные совпадения будут подсвечены).
- +
- элемент для изменения порядка политик в списке путем перетаскивания.
- Количество срабатываний - Счетчик количества попыток авторизации, подпадающих под указанные Условия.
- действия:
 - Добавить сверху - добавить новый набор политик *ДО* выбранного;
 - Добавить снизу - добавить новый набор политик *ПОСЛЕ* выбранного;
 - Удалить - удалить выбранную политику.
- » - перейти к управлению выбранной политикой.
- Сохранить - сохранить изменения.
- Отмена - отменить изменения.

Все политики проверяются в порядке отображения на экране: сверху вниз. По этой причине на странице всегда отображаются все политики. Данные, вводимые в поле Поиск подсвечивают найденные политики, не скрывая их из списка.

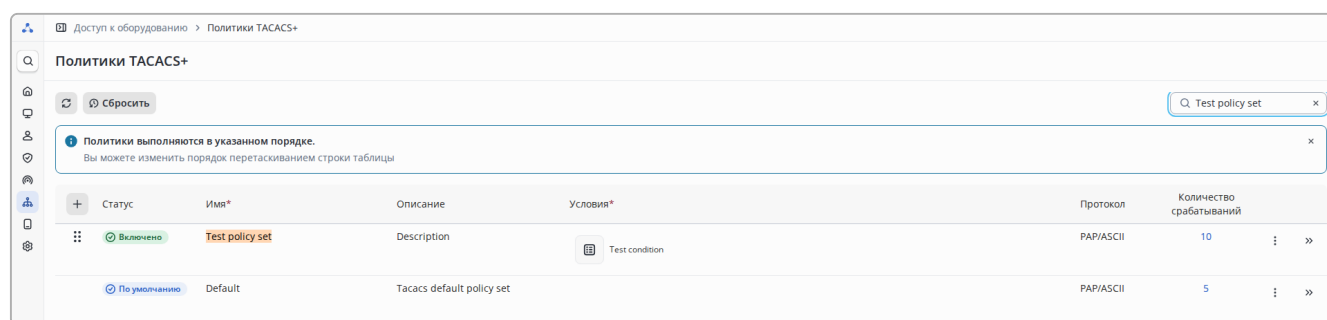


Рисунок 365. Поиск Политики.

Для изменения порядка перетащите политику за элемент  в колонке .



После изменения порядка политик требуется нажать кнопку **Сохранить**, иначе изменения не вступят в силу.

Для просмотра списка [политик аутентификации и авторизации](#) необходимо нажать **>>** справа от выбранного набора политик.

Редактирование списка наборов политик

Добавление набора политик

Для добавления набора политик в список необходимо нажать вверху слева кнопку  - новая политика будет добавлена первой в списке.

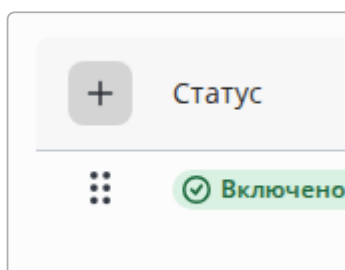


Рисунок 366. Иконка добавления политики.

При необходимости добавить политику в произвольное место необходимо нажать на кнопку  справа от выбранной политики и в выпадающем меню выбрать **Добавить сверху** или **Добавить снизу**.

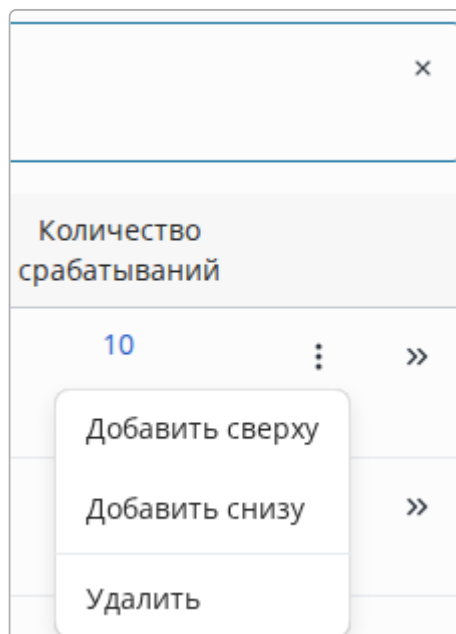


Рисунок 367. Отображение политики. Выпадающее меню с действиями.

Информация по Статусу :

- **Включено** - разрешается обрабатывать запросы;
- **Выключено** - исключить из обработки, не проверять Условие, не обрабатывать запросы;
- **Проверка условий** - разрешается проверять Условие (и инкрементировать счётчик срабатываний), обрабатывать запросы - нет;
- **По умолчанию** - используется только для политики по умолчанию Default .

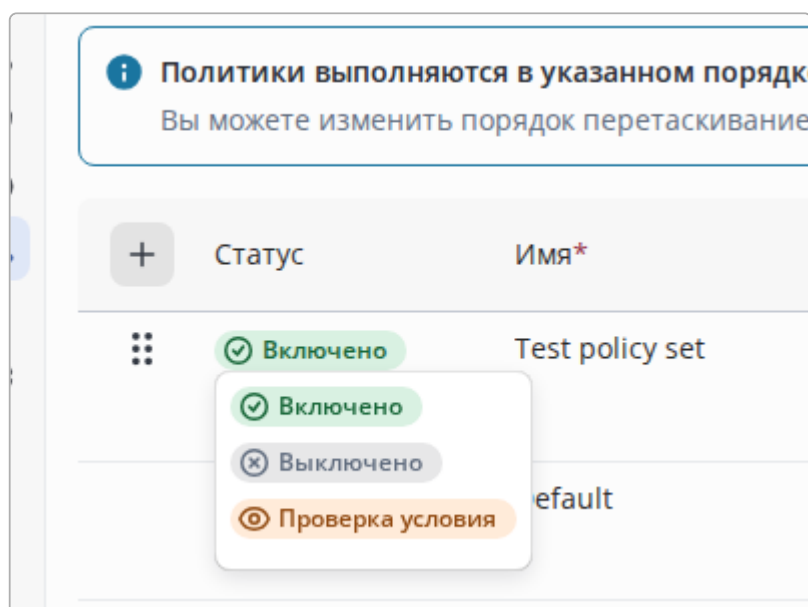


Рисунок 368. Изменение статуса политики.

Во вновь созданной политике в поле **Имя** можно ввести читаемое наименование или оставить неизменным автоматически сформированное название.

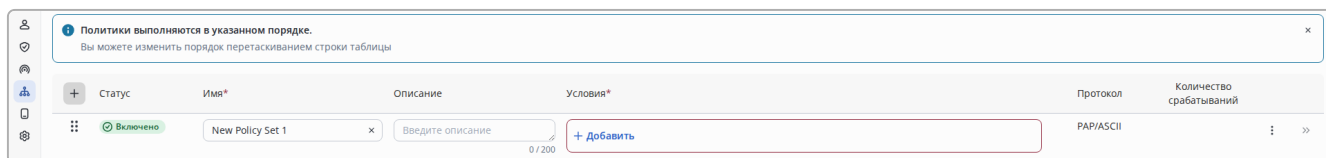


Рисунок 369. Отображение записи новой политики. Элементы обязательные для заполнения.

Для редактирования условия необходимо нажать **+ Добавить** и откроется редактор условий.

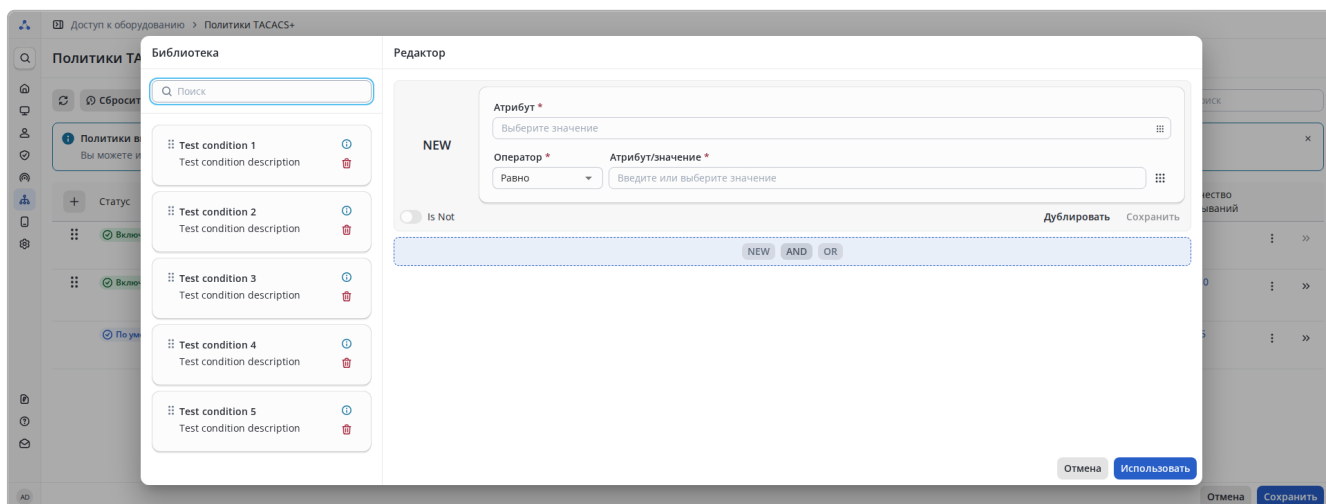


Рисунок 370. Редактор условий.

Редактирование условий выполняется способом, аналогичным описанному в [условиях](#).



При настройке входного условия набора политик есть ограничение по используемым типам словарей. Можно использовать словари: `NETWORK_ACCESS`, `TACACS_PLUS`, `DEVICE`.

При редактировании условий непосредственно в политике добавляется возможность использовать настроенное условие без сохранения его в **Библиотеке**. Для этого необходимо после настройки, не сохраняя условие, нажать кнопку **Использовать**.

По нажатию кнопки **Сохранить** изменения будут сохранены.



После создания нового набора политик необходимо настроить для него [политики аутентификации и авторизации](#). Без этого все попытки подключения, попавшие под логическое условие, будут отклонены согласно запрещающим правилам по умолчанию!



Набор политик по умолчанию `Default` также можно редактировать.

Удаление набора политик

Удаление набора политик доступно в меню **Действия**. Доступно удаление только одного набора политик за раз.

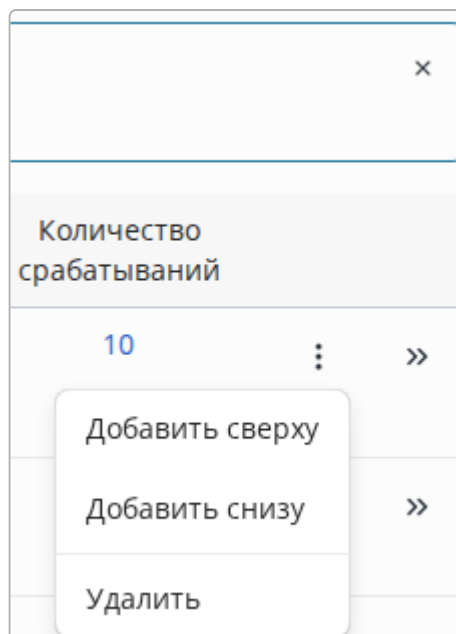


Рисунок 371. Выпадающее меню для удаления политики.

Количество срабатываний политики

Счётчики в колонке **Количество срабатываний** показывают, сколько попыток подключения было обработано с использованием этой политики. Изменения значений свидетельствует, что **Условие** срабатывает.



Используя статус **🔍 Проверка условий** и наблюдая за счётчиками срабатывания, можно сначала подобрать и отладить условие, а лишь потом включать политику в работу, переводя её в статус **✅ Включено**.

Счетчики срабатывания всех наборов политик можно сбросить по клику на **🔄 Сбросить**. Для сброса счетчика конкретного набора нажмите на число в колонке **Количество срабатываний**, нажмите на кнопку **Сбросить** и подтвердите действие.

Настройка политик аутентификации и авторизации



Данный раздел содержит информацию по настройке функционала, доступ к которому приобретается отдельно с помощью дополнительной опции лицензии **NAICE-TACACS+**. По вопросам приобретения функционала обращайтесь к Вашему менеджеру или на электронную почту eltex@eltex-co.ru.

Просмотр списка политик в выбранном наборе политик

Для просмотра списка политик аутентификации и авторизации TACACS необходимо нажать **»** справа от выбранного **набора политик**. Откроется детальная страница набора политик, на которой можно изменить правила политик аутентификации и авторизации.

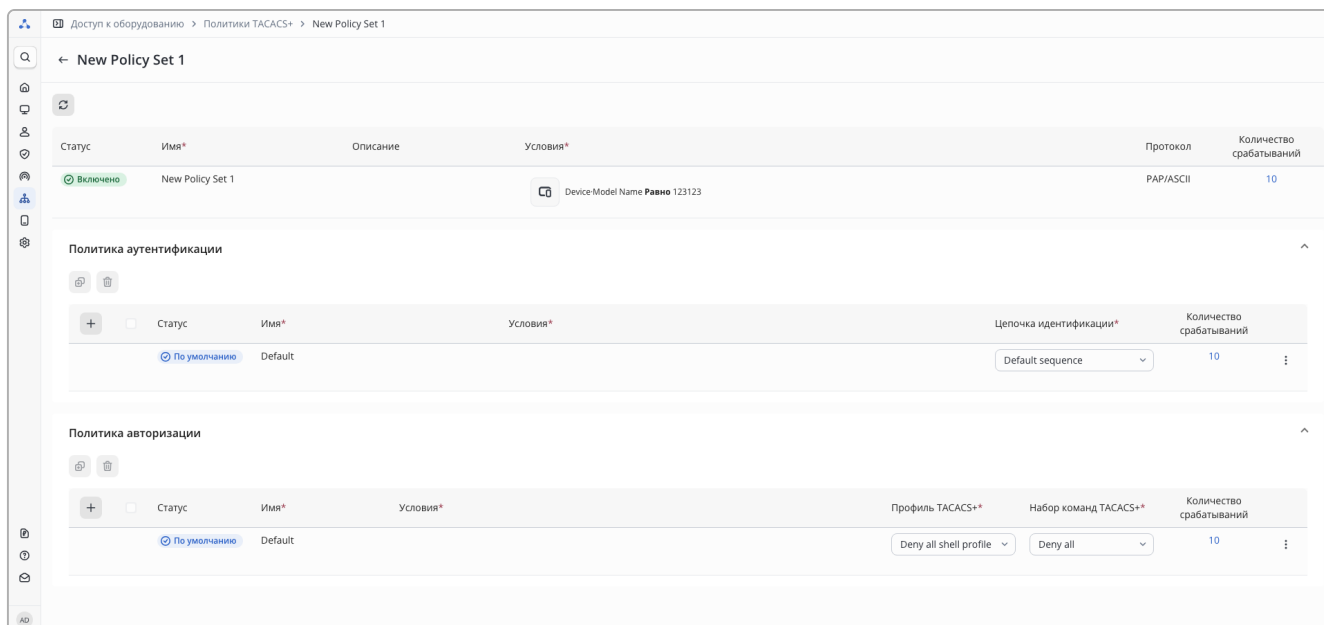


Рисунок 372. Страница просмотра и редактирования набора политик



Последние правила политик аутентификации и авторизации с именем **Default** нельзя переименовать или изменить им условие срабатывания. Они всегда будут последние в списке, ниже расположить другие правила нельзя. Данные правила предназначены для определения поведения по умолчанию, когда другие правила не подходят.

Форма просмотра отдельного набора политик разбита на блоки:

- Блок, отвечающий за управление набором политик, который отображает содержимое выбранного набора политик в формате аналогичном используемому на странице [:policy-sets/index.html](http://policy-sets/index.html).
- **Политика аутентификации** - управление аутентификацией пользователей.
- **Политика авторизации** - управление авторизацией пользователей, для доступа к профилю уровней привилегий, а так же доступа к списку разрешенных команд.

Элементы управления:

- - запрос актуального количества срабатываний всех политик.
- **Статус** - включить/выключить/поставить на мониторинг соответствующую политику.
- **Имя *** - наименование политики.
- **Описание** - произвольное описание.
- **Условия *** - используемые [логические условия](#). Если используется библиотечное условие - отображается его имя. Если используется не библиотечное условие - отображается его структура.
- **Протокол *** - всегда PAP/ASCII.
- **Цепочка идентификации *** - выбранная [цепочка источников идентификации](#).
- **Профиль TACACS *** - выбор доступных [профилей TACACS](#).
- **Набор команд TACACS *** - выбор доступных [наборов команд](#).

-  - действия:
 - **Добавить сверху** - добавить правило политики *ДО* выбранного;
 - **Добавить снизу** - добавить правило политики *ПОСЛЕ* выбранного;
 - **Дублировать** - добавить новое правило политики, аналогичное выбранному, перед дублируемым правилом;
 - **Удалить** - удалить выбранное правило политики.
- **Количество срабатываний** - количество попыток авторизации, подпадающих под указанные Условия. При нажатии на число срабатываний счётчик можно **Сбросить**.
- **Сохранить** - сохранить изменения.
- **Отмена** - отменить изменения.

Параметры, отмеченные звёздочкой *, обязательны для заполнения.

Для изменения порядка правил Политик аутентификации и авторизации перетащите выбранное правило за элемент  в колонке  аналогично разделу [:policy-sets/index.html](https://policy-sets/index.html).

Редактирование политик

Для редактирования политик необходимо нажать **>>** справа от выбранного набора политик.

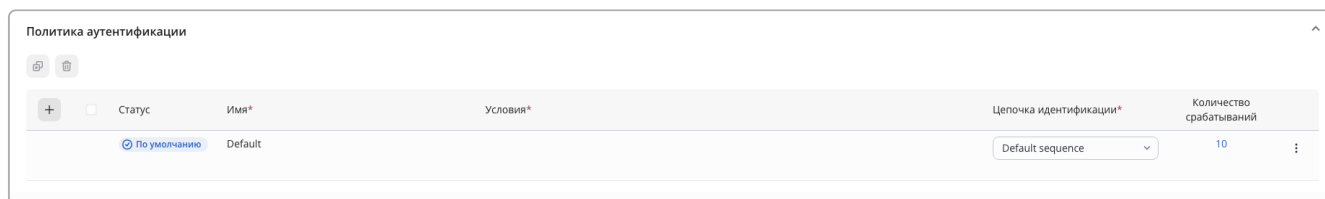


Требуется настроить как минимум одно правило политики аутентификации и одно правило политики авторизации для возможности успешного подключения клиента с использованием данной политики TACACS, или перенастроить запрещающее правило по умолчанию Default.



Политику по умолчанию Default можно отредактировать, настроив другое поведение, однако для безопасности рекомендуется настраивать собственные правила, а поведение по умолчанию оставить запрещающим.

Политика аутентификации



Статус	Имя*	Условия*	Цепочка идентификации*	Количество срабатываний
 По умолчанию	Default		Default sequence	10

Рисунок 373. Панель политики аутентификации.

Для настройки политики аутентификации в блоке **Политика аутентификации** необходимо нажать кнопку . Появится новое правило.

Рисунок 374. Новое правило политики аутентификации.

В поле **Имя** ввести наименование правила политики.

Редактирование условий выполняется способом, аналогичным описанному в [условиях](#).



При настройке условия политики есть ограничение по используемым типам словарей. Можно использовать словари: `NETWORK_ACCESS`, `TACACS_PLUS`, `DEVICE`.

При редактировании условий непосредственно в политике добавляется возможность использовать настроенное условие без сохранения его в **Библиотеке**. Для этого необходимо после настройки, не сохраняя условие, нажать кнопку **Использовать**.

Выбрать в выпадающем меню **Цепочка идентификации** необходимую [цепочку](#).

Новое правило политики также можно создать из существующего, дублировав его. Для этого необходимо выбрать желаемое правило/правила через , а затем нажать над таблицей. Будет создано новое правило выше выбранного с аналогичными настройками и именем, оканчивающимся на "_сору".

Кнопкой справа от политики можно добавить новое правило выше или ниже, дублировать либо удалить текущее.

По нажатию кнопки **Сохранить** изменения будут сохранены.

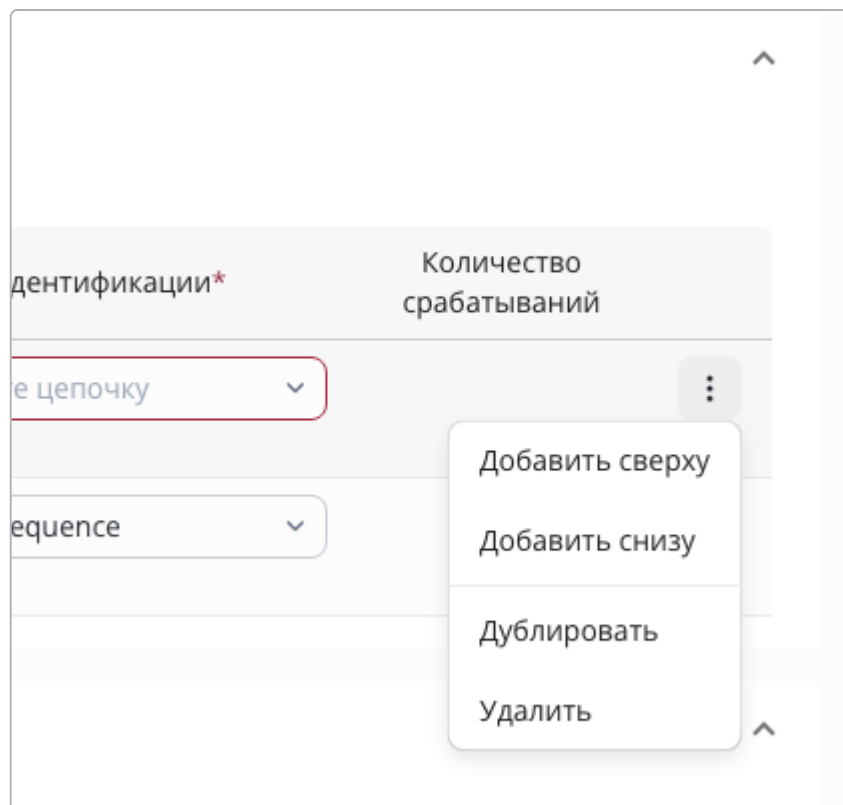


Рисунок 375. Политика аутентификации. Выпадающее меню. Действия.

Также можно изменить статус политики аналогично статусам в наборах политик.

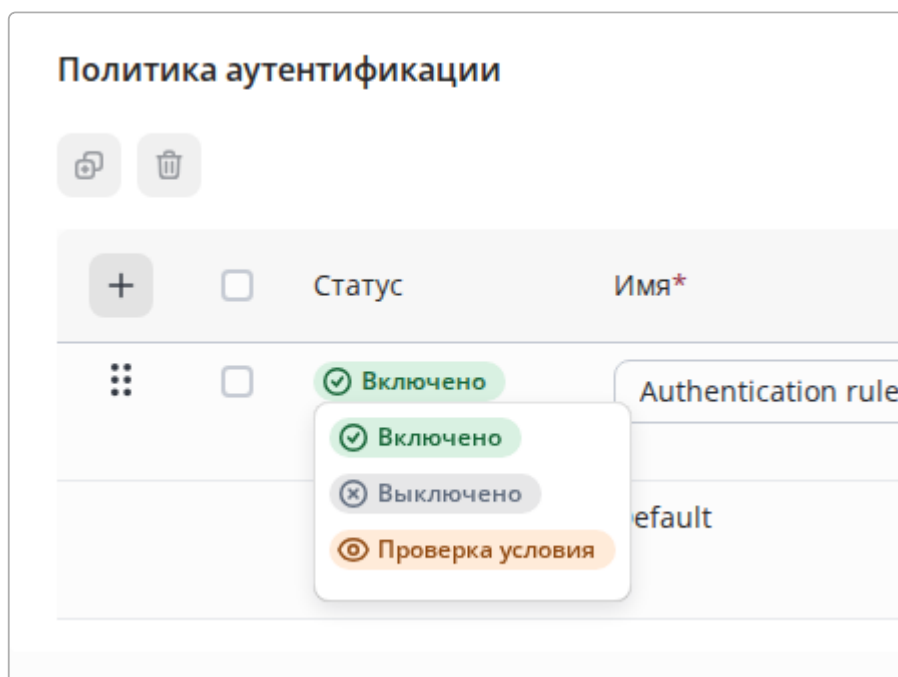


Рисунок 376. Политика аутентификации. Изменение статуса политики.

Политика авторизации



Рисунок 377. Панель политики авторизации.

Для настройки правила политики авторизации в блоке **Политики авторизации** нажать **+**. Появится новое правило.

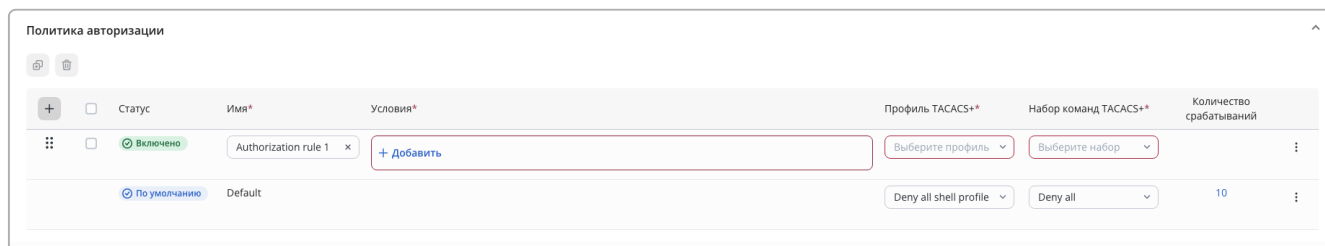


Рисунок 378. Новое правило политики авторизации.

В поле **Имя** ввести наименование правила политики.

Для редактирования условия необходимо нажать **+ Добавить** - откроется редактор условий. Редактирование условий выполняется аналогично описанному в [Условия](#).

При настройке политики авторизации можно использовать следующие словари: **LDAP**, **NETWORK_ACCESS**, **TACACS+**, **IDENTITY**, **DEVICE**.

При редактировании условий непосредственно в политике добавляется возможность использовать настроенное условие без сохранения его в Библиотеке. Для этого надо после настройки не сохраняя условие нажать кнопку **Использовать**.

Выбрать в выпадающем меню **Профиль TACACS** необходимый **профиль TACACS**.

Выбрать в выпадающем меню **Набор команд TACACS** необходимый **набор команд TACACS**.

Новое правило политики также можно создать из существующего, дублировав его. Для этого необходимо выбрать желаемое правило/правила через ☐, а затем нажать  над таблицей. Будет создано новое правило выше выбранного с аналогичными настройками и именем, оканчивающимся на "_copy".

Кнопкой  справа от политики можно добавить новое правило выше или ниже, дублировать либо удалить текущее.

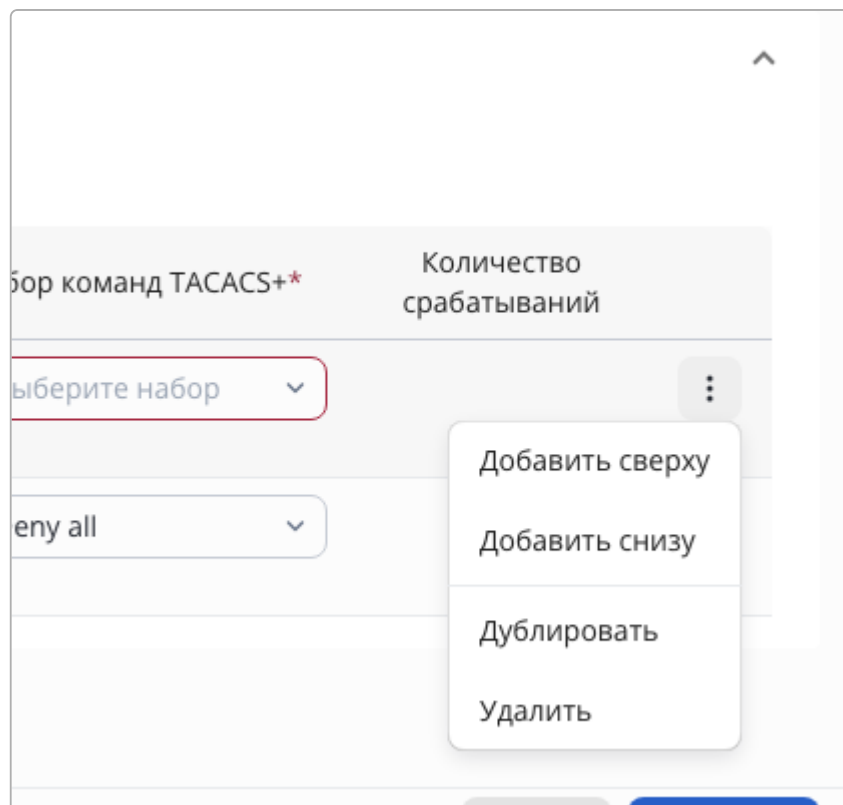


Рисунок 379. Политика авторизации. Выпадающее меню. Действия.

Также можно изменить статус политики аналогично статусам в наборах политик.

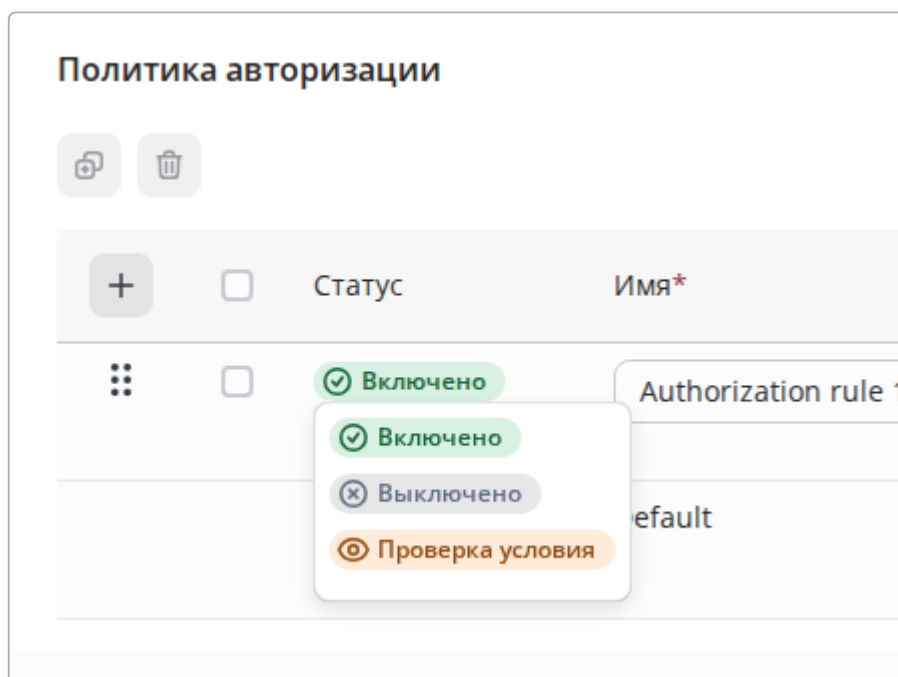


Рисунок 380. Политика авторизации. Изменение статуса политики.

Для удаления нескольких правил необходимо выбрать их с помощью ☐, а затем нажать  над таблицей с правилами.

Кнопка **Сохранить** станет доступна только после добавления хотя бы одной, полностью настроенной, политики аутентификации и политики авторизации.

Нажать кнопку **Сохранить**.

Шлюзы уведомлений

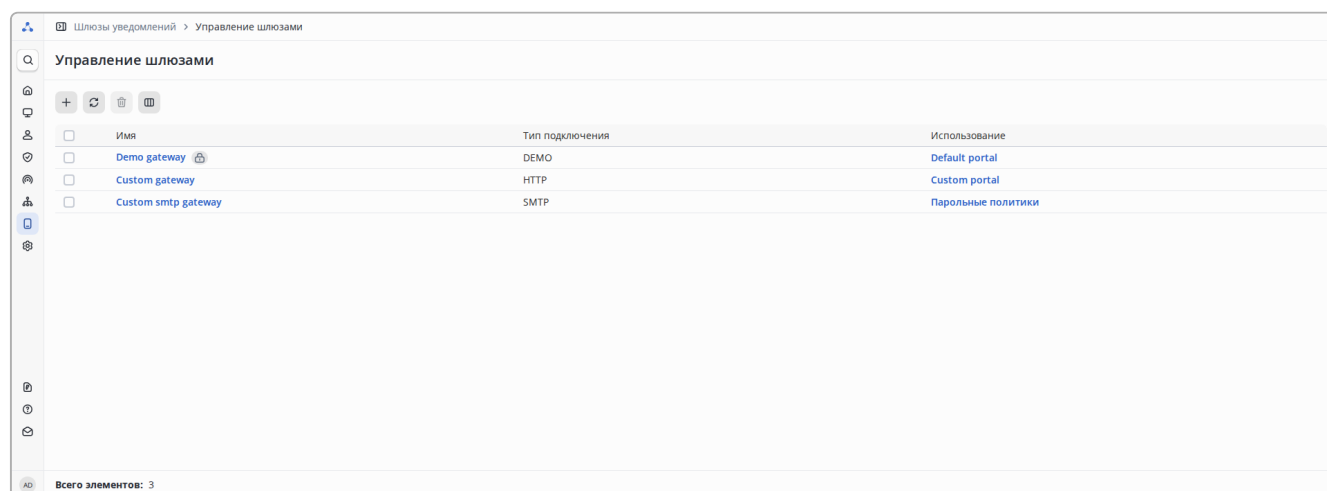
Управление шлюзами

Описание

Управление шлюзами позволяет создавать, настраивать и использовать интеграции с сервисами отправки СМС для осуществления portalной авторизации и почтовыми серверами для настройки уведомлений о создании и редактировании пользователей системы. Существует возможность настройки нескольких СМС-шлюзов, что позволяет гибко настраивать интеграции для каждого гостевого портала.

В данный момент реализована интеграция только по протоколам HTTP/HTTPS для гостевого портала и SMTP для парольных политик.

Просмотр списка шлюзов уведомлений



Управление шлюзами		
Имя	Тип подключения	Использование
☐ Demo gateway	DEMO	Default portal
☐ Custom gateway	HTTP	Custom portal
☐ Custom smtp gateway	SMTP	Парольные политики

Рисунок 381. Таблица со списком имеющихся шлюзов уведомлений

Снизу расположена таблица со списком, которая содержит колонки:

- Имя - название шлюза.
 - Данная запись является системной и недоступна для удаления или редактирования.
- Тип подключения - Тип подключения шлюза. Может принимать значения: DEMO, HTTP, SMTP
- Использование - Перечень записей, в которых используется данный шлюз.

Также доступны дополнительные колонки, настраиваемые в в шапке таблицы:

- Описание - Описание шлюза уведомлений.
- Дополнительная информация - Содержит дополнительные данные о существующей интеграции.

Элементы управления:

- Добавить новый элемент.
- Обновить данные таблицы.

-  - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
-  - Открыть окно настройки отображаемых колонок таблицы.
- ☐ - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).

Добавление шлюза уведомлений

Для добавления шлюза уведомлений нажмите .

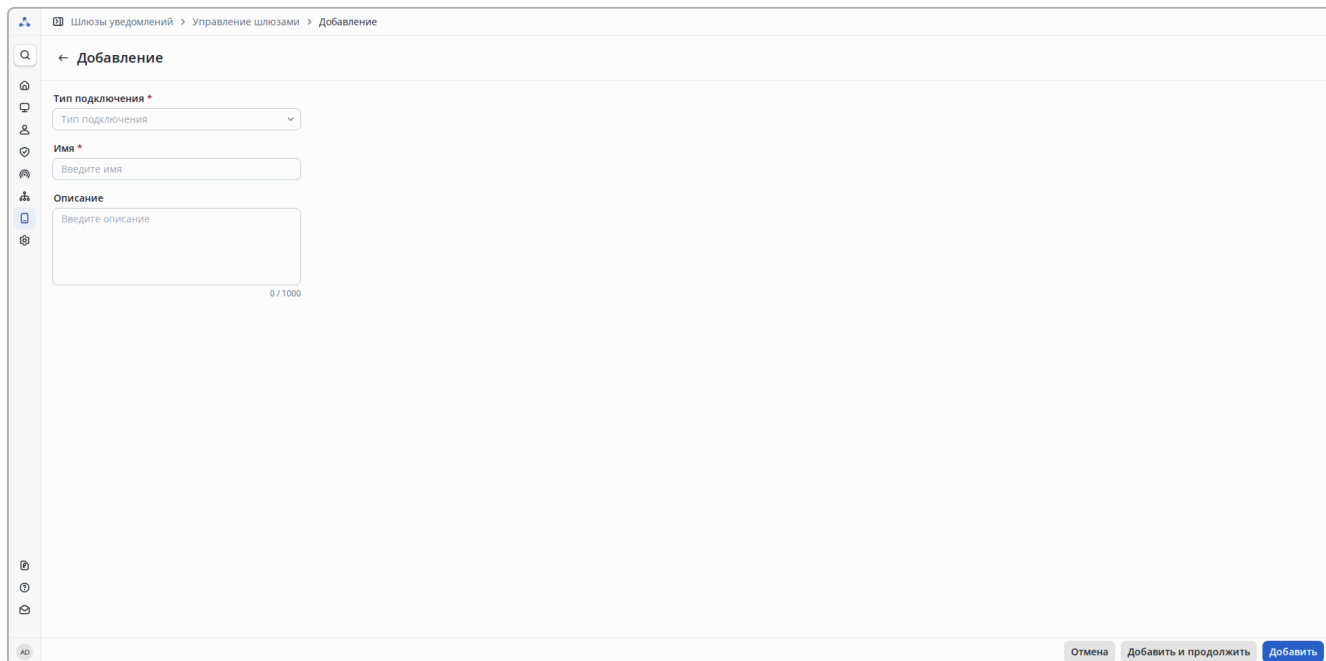


Рисунок 382. Страница добавления шлюза уведомлений

В открывшейся форме можно заполнить следующие параметры:

- **Тип подключения *** - тип подключения шлюза.
- **Имя *** - наименование шлюза уведомлений; должно быть уникально в рамках списка шлюзов. Максимальная длина - 200 символов.
- **Описание** - описание шлюза уведомлений. Максимальная длина - 1000 символов.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

Рисунок 383. Страница добавления шлюза уведомлений с выбором типа подключения

Дальнейшая настройка шлюза зависит от выбранного типа подключения. Подробнее о настройке [HTTP/HTTPS](#) и [SMTP](#) шлюзов можно прочитать в соответствующих разделах.

Для добавления шлюза в системе предусмотрены две кнопки добавления, различающиеся последующим поведением:

- **"Добавить и продолжить"** — после нажатия форма не закрывается, становится доступной кнопка **"Отправить тестовое СМС/письмо"**.
- **"Добавить"** — после нажатия выполняется перенаправление на страницу списка шлюзов уведомлений.

Редактирование шлюза уведомлений

Для редактирования шлюза уведомлений необходимо на странице со списком нажать на его имя.

☐	Имя
☐	Demo gateway
☐	Custom gateway
☐	Custom smtp gateway

Рисунок 384. Гиперссылка на страницу редактирования шлюза.

После этого откроется окно редактирования, аналогичное странице добавления.



При внесении изменений в форму кнопка **"Отправить тестовое СМС/письмо"** становится недоступной. Повторная активация кнопки происходит только после сохранения изменений.

Шлюзы оповещений > Управление шлюзами > Custom gateway

← Custom gateway

Тип подключения *

HTTP/HTTPS

Имя *

Custom gateway

Описание

Введите описание

0 / 1000

Редактор запроса на отправку сообщения

Таймаут подключения * ⓘ

3

HTTP-метод *

POST

Таймаут чтения * ⓘ

3

URL API *

https://test.test/api/?param=\${key}

Таймаут ответа * ⓘ

3

Проверка SSL/TLS сертификата при установке соединения с HTTP/HTTPS-шлюзом

☐ использовать проверку SSL/TLS сертификата

Пользовательские переменные

Заголовки

Тело запроса

В качестве значений атрибутов можно использовать системные переменные, либо задать текстом свои.

×

Атрибут *

key

Значение атрибута *

value

+

Отправить тестовое СМС

AD

Рисунок 385. Страница редактирования HTTP/HTTPS шлюза уведомлений

Шлюзы оповещений > Управление шлюзами > Custom gateway

← Custom gateway

Тип подключения *

SMTP

Имя *

Custom gateway

Описание

Введите описание

0 / 1000

Настройки SMTP-шлюза

Имя сервера *

testHost

Порт *

4200

Имя отправителя *

userName

Адрес отправителя *

username@naice.ru

Таймаут ответа * ⓘ

3

Авторизация при установке соединения с SMTP-шлюзом

☐ использовать авторизацию

Имя пользователя * ⓘ

Введите имя

Пароль *

Введите пароль

Проверка SSL/TLS сертификата при установке соединения с SMTP-шлюзом

☐ использовать проверку SSL/TLS сертификата

Отправить тестовое письмо

AD

Рисунок 386. Страница редактирования SMTP шлюза уведомлений

Для сохранения изменений в системе предусмотрены две кнопки, различающиеся последующим поведением:

•

"Сохранить и продолжить" — после нажатия форма не закрывается, кнопка "Отправить тестовое СМС/письмо" снова становится доступной.

- "Сохранить" — после нажатия выполняется перенаправление на страницу списка шлюзов уведомлений.

Кнопка "Отмена" осуществляет сброс внесенных изменений до исходного состояния.

Удаление шлюза уведомлений

Для удаления в окне со списком надо выделить чекбокс слева от наименования шлюзов уведомлений, которые требуется удалить, и нажать кнопку  вверху слева.

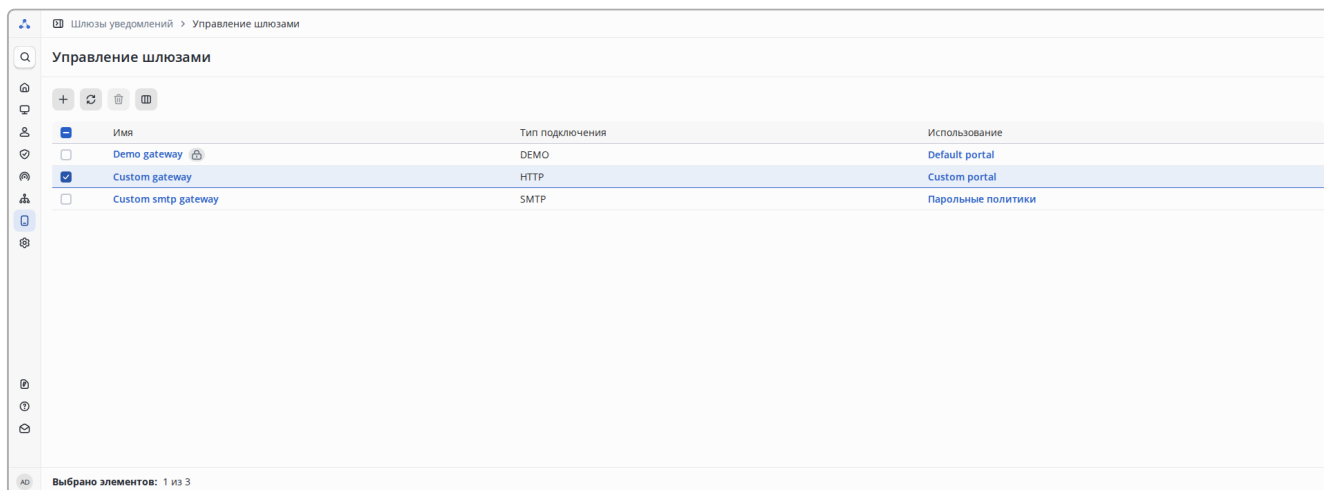


Рисунок 387. Выбор шлюза в таблице для удаления



Удаление элементов требует подтверждения в модальном окне. Выбранные элементы будут удалены только после явного подтверждения операции.

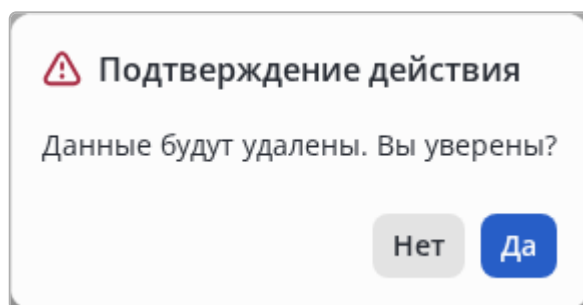


Рисунок 388. Диалоговое окно подтверждения действия

HTTP/HTTPS

Редактор запроса на отправку сообщения

Рисунок 389. Страница создания HTTP/HTTPS шлюза

При выборе типа подключения HTTP/HTTPS в форме создания шлюза становятся доступными следующие параметры:

- **Таймаут подключения *** - максимальное время ожидания соединения с сервером (сек.). По умолчанию 3 секунды.
- **Таймаут чтения *** - максимальное время ожидания данных от сервера (сек.). По умолчанию 3 секунды.
- **Таймаут ответа *** - максимальное время ожидания ответа от сервера (сек.). По умолчанию 3 секунды.
- **HTTP-метод *** - выпадающий список с выбором HTTP-метода для интеграции. На выбор доступны значения: GET, POST, PUT. По умолчанию POST.
- **URL API *** - адрес, на который будет выполняться запрос на отправку сообщения в рамках интеграции.

В рамках создания HTTP/HTTPS интеграции доступна гибкая настройка запроса на отправку сообщения. На странице создания СМС шлюза доступно 3 раздела для редактирования запроса:

- **Пользовательские переменные** - раздел создания пользователем системы собственных переменных, необходимых для создания запроса, например, логин/пароль/API-key для интеграции. Для создания переменной необходимо указать ее имя в графе "Атрибут" и ее значение в графе "Значение атрибута". Добавление новой переменной осуществляется с помощью кнопки , а удаление с помощью кнопки .
-

Заголовки - раздел создания пользователем системы HTTP заголовков для запроса. Для создания заголовка необходимо указать его имя в поле "Атрибут" и его значение в поле "Значение атрибута". Значением так же может быть переменная. Для выбора переменной нажмите . Аналогично разделу с пользовательскими переменными, добавление нового заголовка осуществляется с помощью кнопки , а удаление с помощью кнопки .

- **Тело запроса** - раздел редактирования тела запроса. Запись данных осуществляется в JSON формате. В данном разделе также разрешается использование переменных в качестве значения.

Работа с переменными

Для гибкой настройки СМС интеграции предполагается использование пользовательских и системных переменных при составлении запроса. Системными переменными считаются "Текст сообщения" и "Номер телефона". Все переменные можно использовать для подстановки значений в URL, заголовки и тело запроса. Помимо переменных настраиваемых пользователем системы, существуют системные переменные `${msg}` и `${target}`, означающие текст сообщения и номер телефона соответственно.

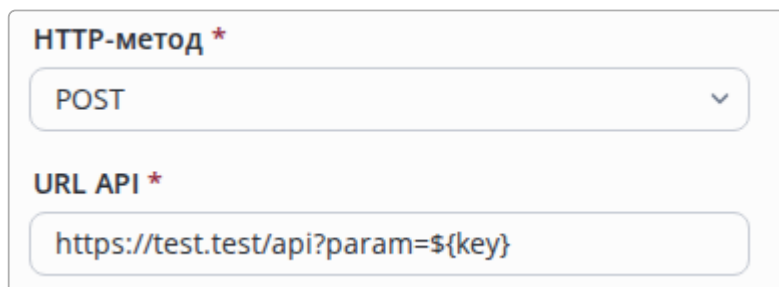


Рисунок 390. Пример добавления переменной в URL запроса

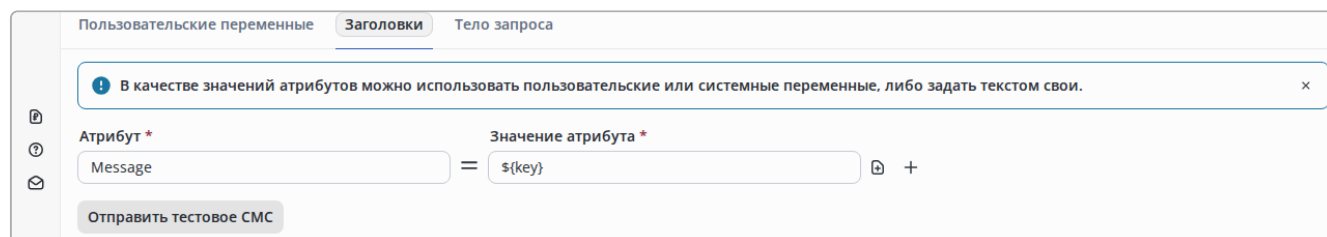


Рисунок 391. Пример добавления переменной в заголовок запроса

Пользовательские переменные Заголовки **Тело запроса**

```
{
  "destination": "${target}",
  "text": "${msg}"
}
```

Формат: JSON

Отправить тестовое СМС

Рисунок 392. Пример добавления переменной в тело запроса

Проверка SSL/TLS сертификата при установке соединения с HTTP/HTTPS-шлюзом

Проверка SSL/TLS сертификата при установке соединения с HTTP/HTTPS-шлюзом

☐ использовать проверку SSL/TLS сертификата

Рисунок 393. Настройка отвечающая за проверку сертификатов

Если при установлении соединения с HTTP/HTTPS сервером необходимо осуществлять проверку его сертификата, то необходимо включить чекбокс **использовать проверку SSL/TLS сертификата**. Подробнее можно прочитать в разделе документации для [доверенных сертификатов](#).

Отправка тестового сообщения

После добавления шлюза становится доступной кнопка **"Отправить тестовое СМС"**. При нажатии на нее откроется окно проверки созданной интеграции с полем ввода номера телефона.

Проверка интеграции ×

Номер телефона *

+7 999 999-99-99

Отмена **Отправить**

Рисунок 394. Окно проверки созданной СМС интеграции

После заполнения номера телефона и отправки СМС пользователю системы откроется окно с результатом проверки.

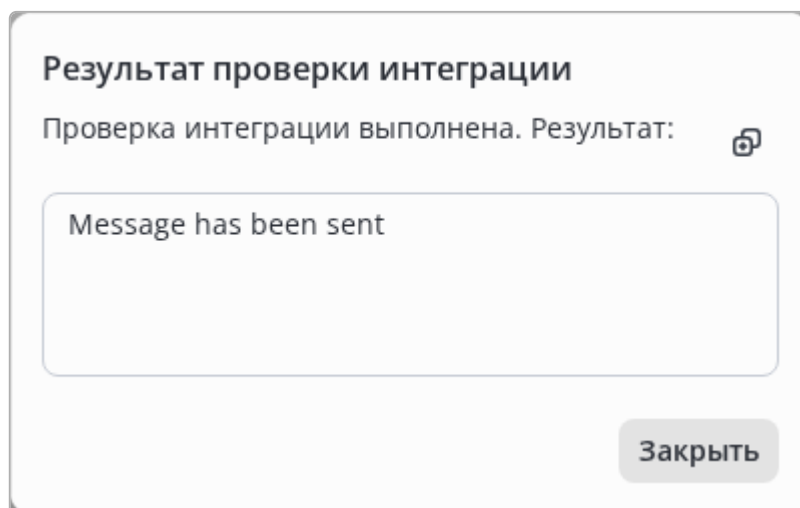


Рисунок 395. Окно результата проверки созданной СМС интеграции

SMTP

Настройки SMTP-шлюза

A web interface for adding an SMTP gateway. The breadcrumb trail is "Шлюзы уведомлений > Управление шлюзами > Добавление". The page title is "← Добавление". There are three main sections. The first section has a "Тип подключения *" dropdown set to "SMTP", an "Имя *" text field with placeholder "Введите имя", and an "Описание" text area with placeholder "Введите описание" and a "0 / 1000" character count. The second section, "Настройки SMTP-шлюза", contains "Адрес сервера *" (placeholder "Введите имя"), "Порт *" (value "25"), "Имя отправителя *" (placeholder "Введите имя"), "Адрес отправителя *" (value "mail@naice.ru"), and "Таймаут ответа *" (value "3"). The third section, "Авторизация при установке соединения с SMTP-шлюзом", has a checkbox "Использовать авторизацию", "Имя пользователя *" (placeholder "Введите имя"), and "Пароль *" (placeholder "Введите пароль"). Below this is "Проверка SSL/TLS сертификата при установке соединения с SMTP-шлюзом" with a checkbox "Использовать проверку SSL/TLS сертификата" and a button "Отправить тестовое письмо". At the bottom right are buttons "Отмена", "Добавить и продолжить", and "Добавить".

Рисунок 396. Страница создания SMTP шлюза

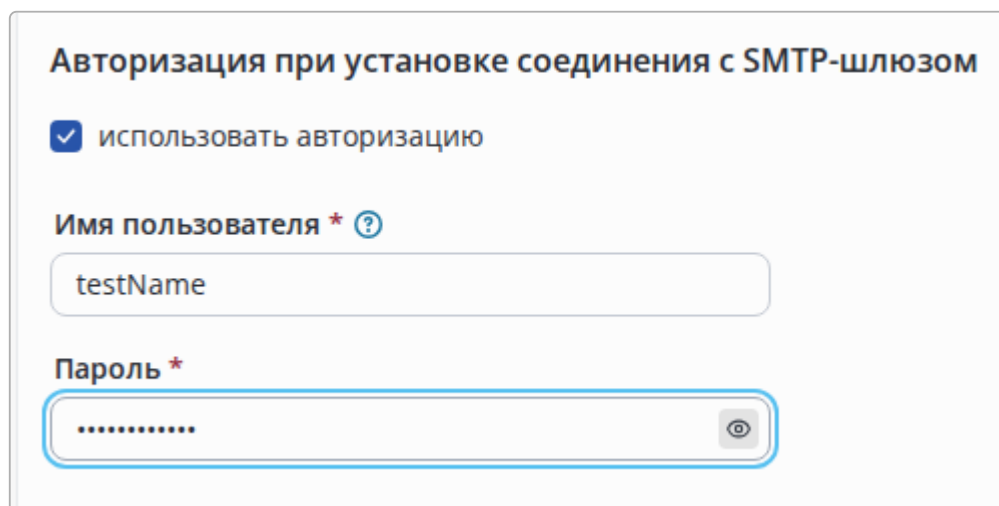
При выборе типа подключения SMTP в форме создания шлюза становятся доступными следующие параметры:

-

Имя сервера * - IP-адрес, или доменное имя почтового сервера, к которому будет выполняться обращение.

- Порт * - порт SMTP сервера, на который будет выполняться обращение. По умолчанию 25 порт.
- Имя отправителя * - имя, которое будет указываться в письме.
- Адрес отправителя * - почтовый адрес, который будет указываться в письме
- Таймаут ответа * - максимальное время ожидания ответа от сервера (сек.). По умолчанию 3 секунды.

Авторизация при установке соединения с SMTP-шлюзом



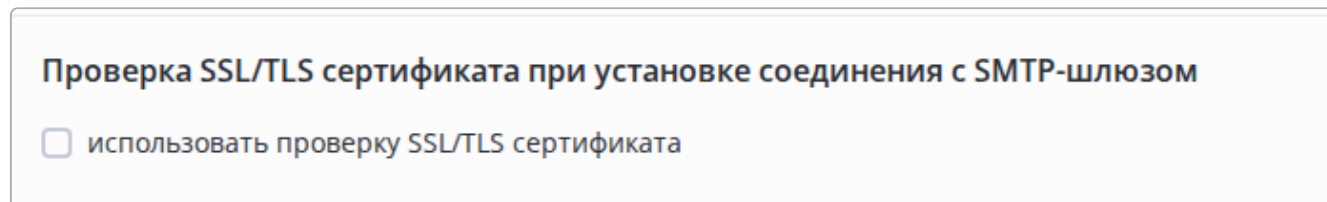
The screenshot shows a dialog box titled "Авторизация при установке соединения с SMTP-шлюзом". It contains a checked checkbox labeled "использовать авторизацию". Below this are two input fields: "Имя пользователя *" with a help icon and the text "testName", and "Пароль *" with a masked password "....." and a toggle icon for visibility.

Рисунок 397. Настройка отвечающая за авторизацию пользователя на SMTP сервере

Если почтовый сервер требует авторизовывать пользователя для отправки письма, то необходимо включить чекбокс **использовать авторизацию**, после чего для редактирования станут доступны еще два параметра:

- Имя пользователя * - почтовый адрес, или логин пользователя, под которым будет выполнять авторизация на SMTP сервере.
- Пароль * - пароль пользователя, под которым будет выполнять авторизация на SMTP сервере.

Проверка SSL/TLS сертификата при установке соединения с SMTP-шлюзом



The screenshot shows a dialog box titled "Проверка SSL/TLS сертификата при установке соединения с SMTP-шлюзом". It contains an unchecked checkbox labeled "использовать проверку SSL/TLS сертификата".

Рисунок 398. Настройка отвечающая за проверку сертификатов

Если при установлении соединения с SMTP сервером необходимо осуществлять проверку его сертификата, то необходимо включить чекбокс **использовать проверку SSL/TLS сертификата**. Подробнее можно прочитать в разделе документации для [доверенных сертификатов](#).

Отправка тестового письма

После добавления плюза становится доступной кнопка "Отправить тестовое письмо". При нажатии на нее откроется окно проверки созданной интеграции с полем ввода почтового адреса.

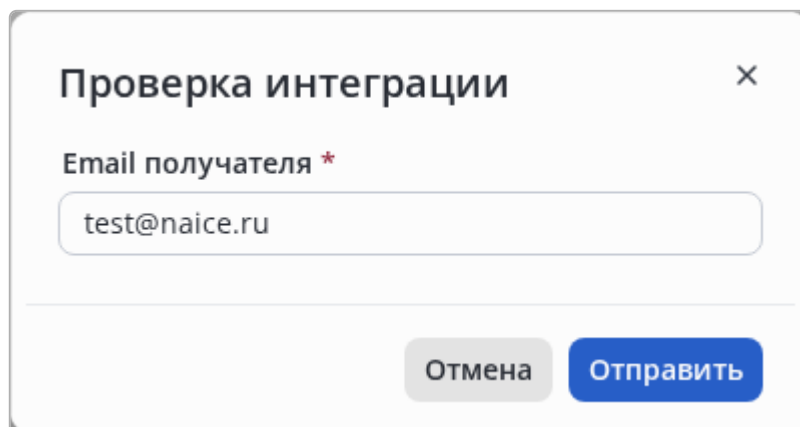


Рисунок 399. Окно проверки созданной SMTP интеграции

После заполнения почтового адреса и отправки письма пользователю системы отобразится сообщение со статусом отправки.



Рисунок 400. Окно результата проверки созданной SMTP интеграции

Настройки системы

Система

Общие настройки

Раздел **Общие настройки** включает в себя настройки системы, влияющие на работу NAICE в целом.

Система

Общие настройки

Адрес базы данных *
Перед внесением изменений ознакомьтесь с [Документацией](#)

Язык системы * ?

Русский

Рисунок 401. Общие настройки

Адрес базы данных

Данная группа настроек позволяет указать один (в случае установки без резервирования) или два (в случае кластера) адреса базы данных PostgreSQL.



От корректности указания адреса/адресов базы данных зависит работоспособность всей системы. При указании неправильного адреса возможна **полная** потеря доступа к NAICE.

После разворачивания NAICE для настроек будут указаны значения по-умолчанию, в зависимости от схемы установки:

- однохостовая установка без резервирования - `naice-postgres:5432` (адрес docker-контейнера с БД в docker сети будет получен автоматически)
- кластер - оба адреса будут заполнены значениями `IPv4-адрес-ноды:5432`

Требования к указываемому адресу

- Адрес указывается в формате `доменное-имя:порт` или `IPv4-адрес:порт`.
- Если указанное доменное имя не является именем контейнера в docker сети, то требуется обеспечить разрешение этого имени.
- По указанному адресу должен быть доступен PostgreSQL с актуальной для NAICE этой версии schema.



Перед сохранением настроек происходит попытка прочитать данные по указанному адресу из БД phosa. Если в PostgreSQL присутствует только БД phosa и отсутствуют другие БД, то проверка пройдет ложноположительно и настройки будут сохранены.

Механизм сохранения адреса

1. При старте сервиса naice-phosa адрес БД вычитывается из файла с переменными окружения.
2. При редактировании адреса новый адрес изменяется в файле с переменными окружения и в PostgreSQL по старому и новому адресу.



Для применения настроек произойдет перезапуск сервиса naice-radius, что приведет к кратковременному перерыву обработки RADIUS запросов.

Особенности настройки кластера

При смене адресов БД в схеме установки с резервированием необходимо, чтобы только одна нода находилась в состоянии primary. Если обе ноды будут находиться в состоянии read-only (standby), произойдет потеря доступа к NAICE.

Язык системы

Язык, используемый некоторыми сервисами для определения локализации текста для пользователя. Настройка влияет на:

- язык по-умолчанию для новых системных пользователей (как локальных, так и из внешних источников)
- язык системных событий в разделе [Системные события](#)
- язык текста email-уведомлений, отправляемых [шлюзами оповещений](#) типа SMTP



Язык сообщения, которое отправляется пользователю в ходе портальной авторизации, зависит от выбранного пользователем языка портала.



Локализация интерфейса для каждого системного пользователя настраивается на странице [Настройки аккаунта](#).

Сервисы

RADIUS

На данной странице настраивается работа RADIUS-сервера в составе NAICE.

Сервисы

RADIUS

TACACS+

Журнал событий

Общие настройки

Порт аутентификации RADIUS *

1812

Срок хранения сессии RADIUS, дней *

31

☒

Обработка RADIUS-аккаунтинга

Серверный сертификат * ?

⚠ RADIUS certificate 01

▼

Рисунок 402. Настройка сервиса RADIUS

К настройке доступны следующие параметры:

- Порт аутентификации RADIUS - UDP-порт, на котором RADIUS сервер ожидает RADIUS-запросы. По умолчанию - 1812.



При сохранении конфигурации выполняется проверка занятости только тех UDP-портов, которые используются контейнерами Docker. Порт, занятый службами или приложениями, установленными непосредственно на хост-машине (вне Docker), не проверяется. Во избежание конфликтов настоятельно рекомендуется перед сохранением вручную убедиться, что выбранный порт не используется другими процессами на сервере.



Для применения настройки произойдет перезапуск сервиса naice-radius, что приведет к кратковременному перерыву обработки RADIUS запросов.

- Срок хранения сессии RADIUS, дней - количество полных дней с даты создания RADIUS-сессий, в течение которых они хранятся в базе данных. По истечению данного срока сессии удаляются. По умолчанию - 31.



Сессии проверяются на истечение срока хранения периодически и удаляются по расписанию.

- Обработка RADIUS-аккаунтинга - флаг включения/отключения обработки RADIUS Accounting пакетов. По умолчанию включен.
 - Если обработка включена: система принимает и обрабатывает Accounting пакеты, обновляет состояние активных сессий и завершает их по таймауту.
 - Если обработка отключена: система продолжает принимать пакеты и отвечает корректными RADIUS Accounting-Response, но не выполняет обработку полученных пакетов.



При отключенной обработке RADIUS Accounting скрывается раздел [Лимит RADIUS-сессий](#).

TACACS+

На данной странице настраивается работа TACACS-сервера в составе NAICE.

Сервисы

RADIUS **TACACS+** Журнал событий

Порт TACACS+ * ?

Срок хранения аккаунтинга TACACS+, дней *

Срок хранения сессии TACACS+, дней *

Рисунок 403. Настройка сервиса TACACS

К настройке доступны следующие параметры:

- **Порт TACACS+** - TCP-порт, на котором TACACS сервер ожидает запросы аутентификации, авторизации и аккаунтинга по протоколу TACACS+. По умолчанию - 49.



При сохранении конфигурации выполняется проверка занятости только тех TCP-портов, которые используются контейнерами Docker. Порт, занятый службами или приложениями, установленными непосредственно на хост-машине (вне Docker), не проверяется. Во избежание конфликтов настоятельно рекомендуется перед сохранением вручную убедиться, что выбранный порт не используется другими процессами на сервере.



Для применения настройки произойдет перезапуск сервиса naice-aquila, что приведет к кратковременному перерыву обработки TACACS+ запросов.

- **Срок хранения аккаунтинга TACACS+, дней** - количество полных дней с даты создания TACACS-сессий аккаунтинга, в течение которых они хранятся в базе данных. По истечению данного срока сессии удаляются. По умолчанию - 31.
- **Срок хранения сессии TACACS+, дней** - количество полных дней с даты создания TACACS-сессий, в течение которых они хранятся в базе данных. По истечению данного срока сессии удаляются. По умолчанию - 31.



Сессии проверяются на истечение срока хранения периодически и удаляются по расписанию.

Журнал событий

На данной странице настраиваются параметры работы [Журнала системных событий](#).

Сервисы

[RADIUS](#) [TACACS+](#) **Журнал событий**

Срок хранения событий в журнале, дней * ?

31

Рисунок 404. Настройка параметров журнала событий

К настройке доступны следующие параметры:

- Срок хранения событий в журнале, дней - количество полных дней с даты создания событий, в течении которых они хранятся в базе данных. По истечении данного срока события удаляются. По умолчанию - 31.



События проверяются на истечение срока хранения периодически и удаляются по расписанию.

Лицензирование

Подключение к ELM

На данной странице настраиваются параметры подключения NAICE к серверу лицензий ELM (Eltex License Manager) при лицензировании через сервер лицензий.



Для лицензий типа ELM при изменении настроек, связанных с лицензированием, происходит сброс текущей активной лицензии и перевод ее в статус Backup. Это приводит к тому, что лицензируемый функционал (RADIUS, TACACS+, порталная авторизация и др.) перестает действовать до момента повторной активации лицензии на странице [Лицензирование](#).

Перейти к настройкам лицензирования 

Настройка адресов ELM сервера

Лицензирование

Подключение к ELM

 Изменение **любого** параметра приведет к сбросу активных лицензий и приостановке функционала авторизации. После изменения активируйте лицензии вручную на странице [Лицензирование](#).

Адрес сервера лицензирования ELM 

192.0.0.1:8099

Введите хост:порт 

☐ Использовать прокси 

Рисунок 405. Настройка подключения к ELM без прокси

Адрес ELM сервера настраивается в формате `доменное-имя:порт` или `IPv4-адрес:порт`, без указания используемого протокола (без "https://"). При отсутствии явного указания порта системой автоматически во время сохранения применяется порт 8099.

При резервировании доступа до сервера лицензий есть возможность указать адрес второго ELM сервера. Если резервирование не предполагается, то настраивать второй адрес не нужно.

Использование HTTP-прокси

Лицензирование

Подключение к ELM

 Изменение **любого** параметра приведет к сбросу активных лицензий и приостановке функционала авторизации. После изменения активируйте лицензии вручную на странице [Лицензирование](#).

Адрес сервера лицензирования ELM 

☒ Использовать прокси 

Хост прокси для ELM *

Логин прокси для ELM * 

Пароль прокси для ELM * 
 

Рисунок 406. Настройка подключения к ELM через HTTP-прокси



HTTPS-прокси не поддерживается!

Поддержана возможность доступа до ELM сервера через HTTP-прокси.

- **Хост прокси для ELM** - адрес прокси-сервера в формате **доменное-имя:порт** или **IPv4-адрес:порт**, без указания используемого протокола.
- **Логин прокси для ELM** - заполняется, если для работы с прокси-сервером требуется аутентификация.
- **Пароль прокси для ELM** - заполняется, если для работы с прокси-сервером требуется аутентификация.

Безопасность и доступ

Вход в систему

Описание

Раздел "Вход в систему" предназначен для настройки источника аутентификации, через который пользователи получают доступ к системе NAICE.

По умолчанию вход в систему выполняется только по **локальным учетным записям**.

При необходимости может быть включено использование внешнего источника идентификации в качестве основного источника аутентификации.



Аутентификация по локальным учетным записям остается доступной всегда.

Настройка входа



Чтобы предоставить пользователям возможность входить через корпоративные учетные записи из внешних источников (OpenLDAP, MS Active Directory и т.п.) необходимо предварительно настроить внешний источник в разделе [«Внешние источники идентификации»](#).

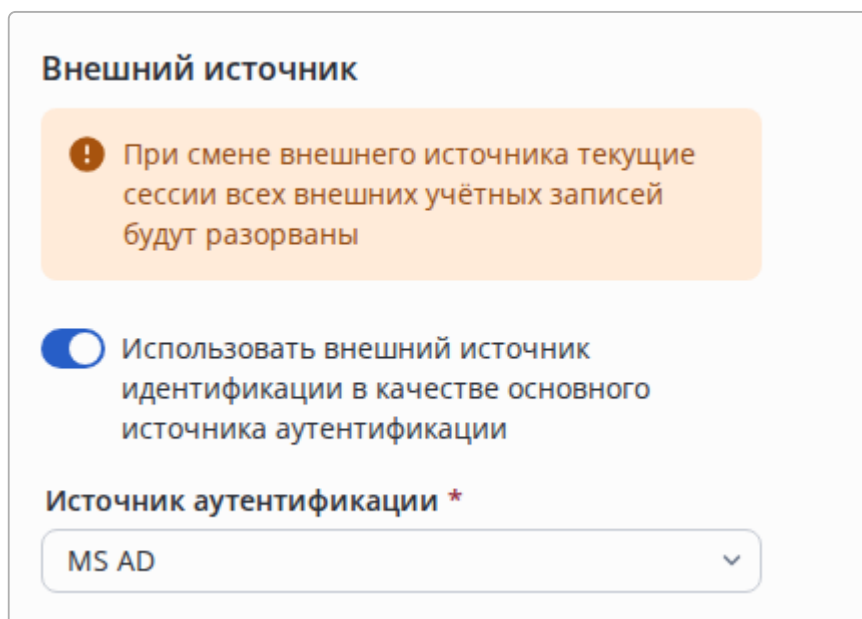
Если в системе нет ни одного настроенного внешнего источника, опция выбора источника недоступна. Доступен только вход по локальным учетным записям.

Рисунок 407. Форма настройки входа при отсутствии внешних источников



Для настройки внешних источников идентификации роль пользователя должна включать привилегию "Внешние источники" с уровнем доступа не ниже (2) "Создание".

Выбор внешнего источника в качестве основного источника аутентификации



Внешний источник

! При смене внешнего источника текущие сессии всех внешних учётных записей будут разорваны

☒ Использовать внешний источник идентификации в качестве основного источника аутентификации

Источник аутентификации *

MS AD

Рисунок 408. Форма настройки входа при наличии внешних источников

В форме доступны следующие параметры:

Использовать внешний источник идентификации в качестве основного источника аутентификации — чекбокс, включающий использование внешнего источника. При активации чекбокса станет доступно поле **Источник аутентификации**:

- **Источник аутентификации** — выбор внешнего источника из списка добавленных в систему. Учетные данные пользователей будут проверяться именно в этом источнике.

Для применения настроек необходимо нажать кнопку **"Сохранить"**.

После успешного сохранения на странице авторизации появляется вкладка **«Корпоративная УЗ»** для входа по внешним учетным записям:

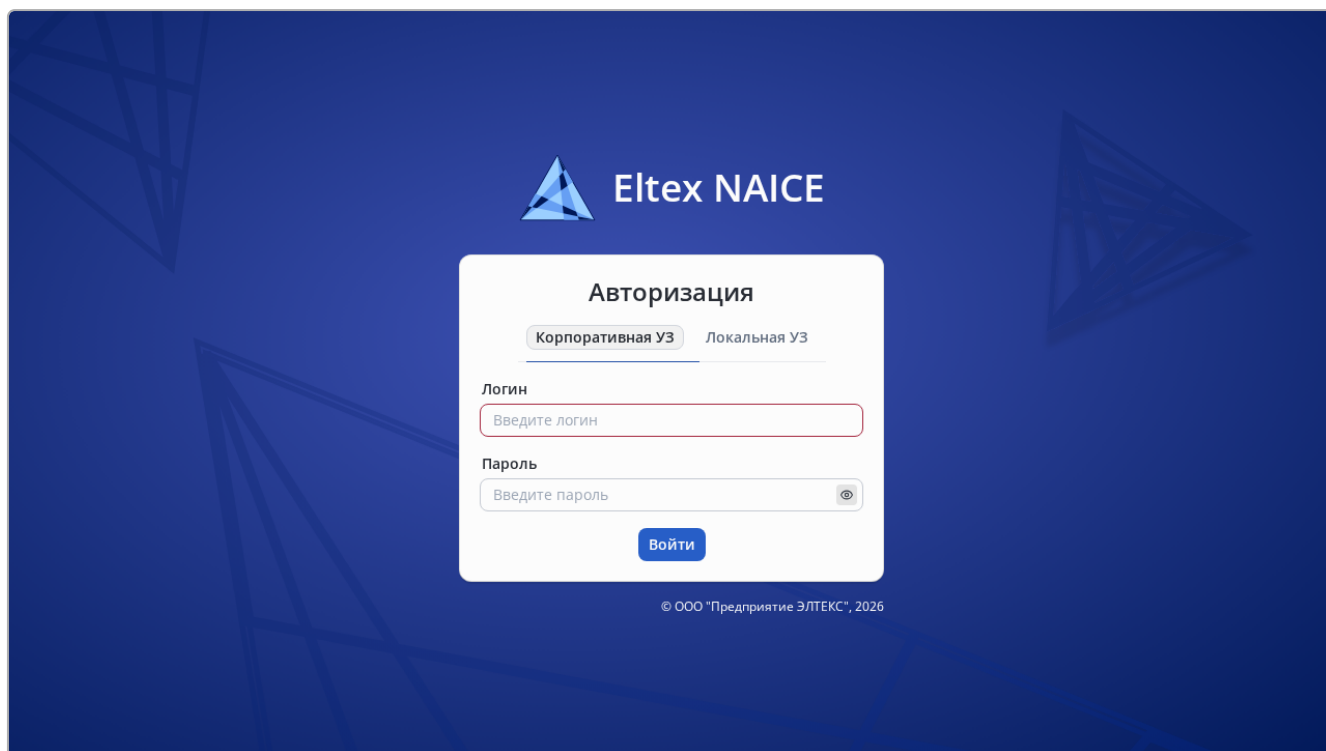


Рисунок 409. Вкладка «Корпоративная УЗ» на странице входа



Логин корпоративной учетной записи не должен превышать 100 символов.



Вкладка «Локальная УЗ» остается доступной всегда для аутентификации по локальным учетным записям.

Изменение конфигурации входа



Любое изменение конфигурации входа, связанное с внешними источниками, приводит к **немедленному завершению всех активных сессий пользователей, аутентифицированных через старый внешний источник:**

- при смене одного внешнего источника на другой;
- при отключении внешней аутентификации (при снятии чекбокса).

После сохранения изменений пользователям потребуется повторная авторизация.

Применение изменений настроек входа в систему (смена одного внешнего источника на другой или отключение использования внешней аутентификации) требует подтверждения:

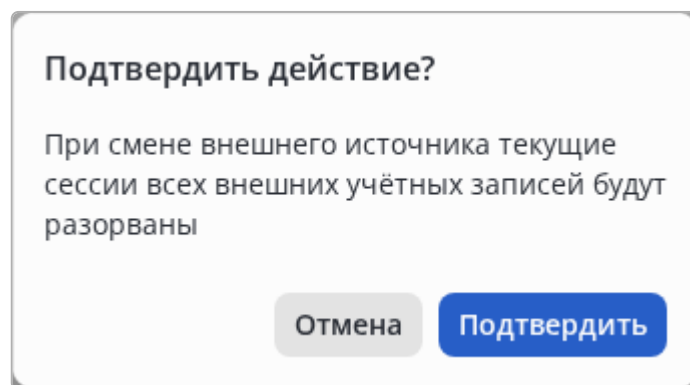


Рисунок 410. Подтверждение изменения настроек входа

Обработка ошибок

При возникновении проблем с аутентификацией через внешний источник отображаются соответствующие сообщения.

Ошибка «У вас недостаточно прав»

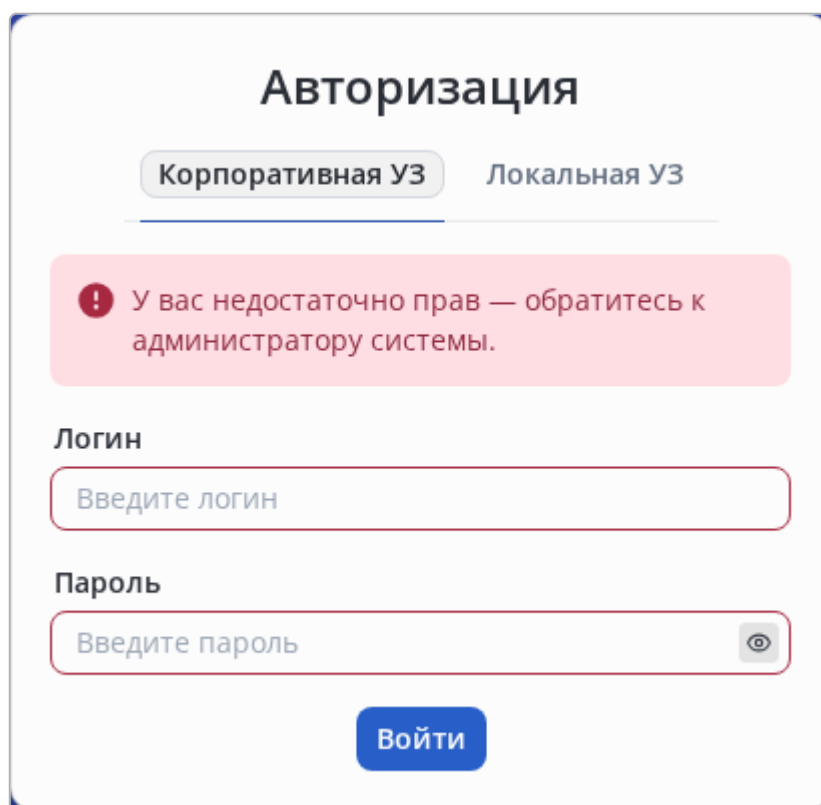


Рисунок 411. Ошибка при отсутствии подходящей роли

Возможные причины:

- Для пользователя не настроена внешняя роль, соответствующая группам пользователя.
- Настроенная роль имеет статус **⊗ Недоступно** (например, после смены или отключения внешнего источника).
- Группы пользователя не считываются из внешнего источника (проблемы с настройкой атрибутов).



При использовании схемы `CUSTOM` для внешнего источника возможна ситуация, когда группы не считываются из-за некорректной настройки атрибутов. Это приводит к невозможности сопоставления групп и, как следствие, назначения ролей.

Ошибка «Внешний источник недоступен»

Авторизация

Корпоративная УЗ Локальная УЗ

❗ Внешний источник недоступен. Обратитесь к администратору или попробуйте позже.

Логин

Введите логин

Пароль

Введите пароль

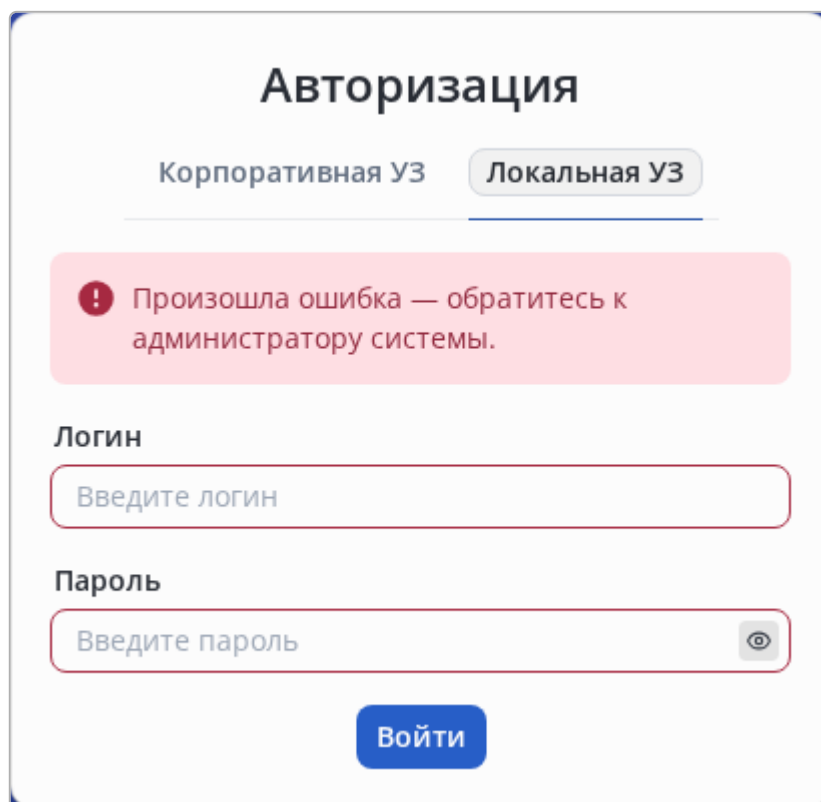
Войти

Рисунок 412. Ошибка при недоступности внешнего источника

Возникает при отсутствии ответа от внешнего источника или его некорректной настройке. Требуется проверка:

- доступности сервера внешнего источника;
- корректности параметров подключения в настройках источника;
- сетевого взаимодействия между NAICE и внешним сервером.

Общая ошибка аутентификации



The screenshot shows a login window titled 'Авторизация'. At the top, there are two tabs: 'Корпоративная УЗ' (Corporate UZ) and 'Локальная УЗ' (Local UZ). Below the tabs is a red error message box with a warning icon and the text: 'Произошла ошибка — обратитесь к администратору системы.' (An error has occurred — contact the system administrator). Below the error message are two input fields: 'Логин' (Login) with the placeholder 'Введите логин' (Enter login) and 'Пароль' (Password) with the placeholder 'Введите пароль' (Enter password) and a toggle icon. At the bottom is a blue button labeled 'Войти' (Login).

Рисунок 413. Общая ошибка при проблемах с входом в систему

Отображается при прочих ошибках аутентификации, не связанных с ролью или доступностью источника.

Диагностика проблем



Детальная информация о причинах ошибок аутентификации доступна на странице «[Системные события](#)». В таблице событий фиксируются:

- попытки входа пользователей;
- ошибки назначения ролей;
- проблемы подключения к внешним источникам;
- изменения конфигурации входа в систему.

Парольные политики

На данной странице настраиваются требования к паролям [системных пользователей](#), а также уведомления по действиям с учетными записями системных пользователей.

Безопасность и доступ

Вход в систему

Парольные политики

Политика блокировки

Двухфакторная аутентификация

Требования к созданию пароля

Только для пользователей системы

Минимальное количество символов *

8

Пароль должен содержать

☐ заглавные буквы (A-Z)

☐ строчные буквы (a-z)

☐ цифры (1-9)

☐ специальные символы ("!@#\$%^&*_-=[])

Дополнительное требование

☒ не должен содержать логин

Уведомления

Только для пользователей системы

☒ отправлять уведомления на email ⓘ

Типы уведомлений *

☒ создание нового пользователя системы ⓘ

☐ изменение учетных данных пользователя системы ⓘ

Шлюз для отправки *

Notification gateway ▾

Рисунок 414. Настройка парольной политики

Требования к созданию пароля

- **Минимальное количество символов** - пароль системного пользователя не может быть меньше указанного числа символов. Максимальное количество символов в пароле - 72.
- **Пароль должен содержать** - включение/выключение требований к присутствию в пароле заглавных/строчных букв, цифр, специальных символов.
- **Дополнительное требование** - включение/выключение требования к отсутствию в пароле логина пользователя.



Требования предъявляются к паролям вновь создаваемых пользователей или при редактировании пароля пользователя. Редактирование парольной политики не приводит к необходимости приведения к соответствию паролей ранее созданных пользователей.

Уведомления



Настройки отображаются только если настроен хотя бы один [шлюз уведомлений](#) с типом подключения SMTP.

- **отправлять уведомления на email** - отправлять письма с выбранными далее типами уведомлений на email адрес системного пользователя, указанный в его аккаунте.



Если email адрес не указан, то письма отправляться не будут.

- **Типы уведомлений :**
 - **создание нового пользователя системы** - на email адрес нового системного пользователя будет отправлено письмо с его учетными данными.
 - **изменение учетных данных пользователя системы** - уведомление системного пользователя о редактировании его учетной записи.



Настройка шаблонов писем на данный момент недоступна. Язык текста в письмах настраивается на странице [:system/common-settings.html](#), настройка "язык системы".

- **Шлюз для отправки** - выбрать один из существующих в системе SMTP-шлюзов, через который планируется отправка email.

Политика блокировки

Раздел «**Политика блокировки**» предназначен для настройки автоматической временной блокировки учетных записей пользователей системы при превышении допустимого количества неудачных попыток входа.



Политика блокировки применяется только к учётным записям пользователей системы (администраторов).

Настройка политики блокировки

В блоке «**Блокировка учетной записи**» задаются параметры, по которым система определяет необходимость временной блокировки учетной записи.

Для включения политики переведите переключатель в положение **Включено**.

Настройки системы > Безопасность и доступ > Политика блокировки

Безопасность и доступ

Вход в системуПарольные политикиПолитика блокировкиДвухфакторная аутентификацияВзаимодействие с Active Directory

Блокировка учетной записи

Только для пользователей системы

Включено

Количество попыток входа * ⓘ

3

Время блокировки, мин *

15

Время наблюдения до блокировки, мин * ⓘ

10

Отмена

Сохранить

Если политика включена, становятся доступными следующие параметры:

После изменения параметров политики блокировки необходимо сохранить настройки, нажав кнопку **«Сохранить»**.



Принцип работы политики блокировки

Политика блокировки защищает учётные записи от подбора паролей и кодов двухфакторной аутентификации (брутфорс-атак). Система фиксирует все неудачные попытки входа, включая:

- неверный пароль;
- неверный одноразовый код TOTP;
- неверный код Email OTP;
- неверный резервный код.

Учетная запись блокируется, если в течение заданного **времени наблюдения до блокировки** количество неудачных попыток достигает значения, указанного в поле **Количество попыток входа**.

После блокировки пользователь не сможет войти в систему до наступления одного из условий:

- истечёт заданное **время блокировки**;
- администратор вручную разблокирует учётную запись через раздел **«Учетные записи»** (см. [«Заблокированная учетная запись»](#)).

Пример 5. Пример работы политики блокировки

Если заданы следующие значения:

- **Количество попыток входа** — 3;
- **Время блокировки** — 15 минут;
- **Время наблюдения до блокировки** — 10 минут,

то учетная запись будет заблокирована на 15 минут, если пользователь совершит 3 неудачных попытки входа (ввод пароля или кодов 2FA) в течение любых 10 минут.



Для того, чтобы пользователи получали email-уведомления о блокировке или разблокировке их учетных записей, необходимо настроить отправку уведомлений в разделе **Настройки системы** → **Безопасность и доступ** → [Парольная политика](#).

Отключение политики блокировки

Для отключения политики блокировки переведите переключатель в положение **Выключено** и сохраните настройки.

После отключения политики:

- автоматическая блокировка учётных записей **прекращается**;
- уже заблокированные учётные записи **остаются в статусе "Заблокирована"** до истечения времени блокировки или ручной разблокировки администратором;

- счётчики неудачных попыток **не сбрасываются**, но перестают учитываться до повторного включения политики.



Отключение политики блокировки снижает уровень защиты учётных записей от брутфорс-атак. Рекомендуется использовать данную функцию только для диагностики или в исключительных случаях.

Двухфакторная аутентификация

Взаимодействие с Active Directory

Описание

На странице *Взаимодействие с Active Directory* настраивается периодическая автоматическая смена паролей учетных записей компьютеров, используемых для взаимодействия с Active Directory. Данная настройка применяется ко всем учетным записям компьютеров, настроенным во всех источниках идентификации, использующих схему Active Directory.

Настройка расписания смены пароля

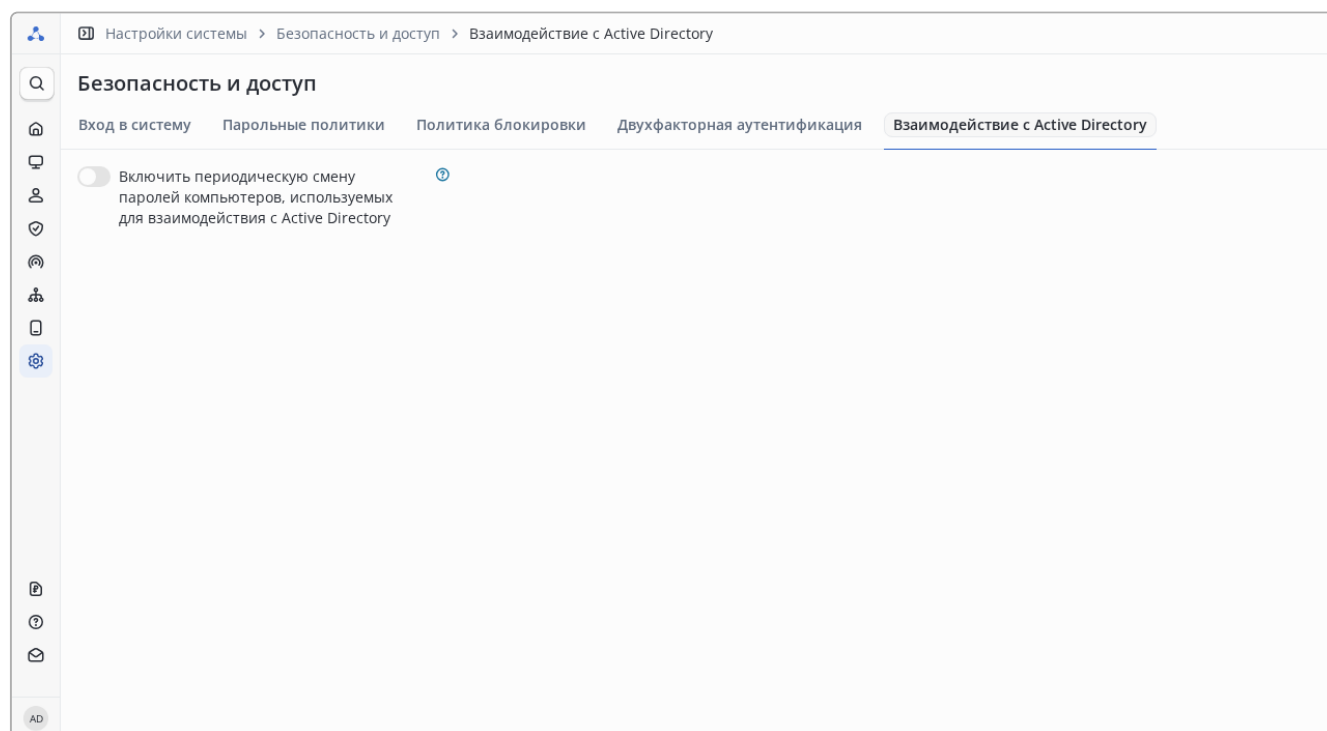


Рисунок 416. Взаимодействие с Active Directory - отключено

В верхней части страницы расположен переключатель:

- Включить периодическую смену паролей компьютеров, используемых для взаимодействия с Active Directory - включает/отключает автоматическую смену паролей для всех учетных записей компьютеров во всех источниках идентификации схемы Active Directory. При наведении на  появляется описание указанной настройки.

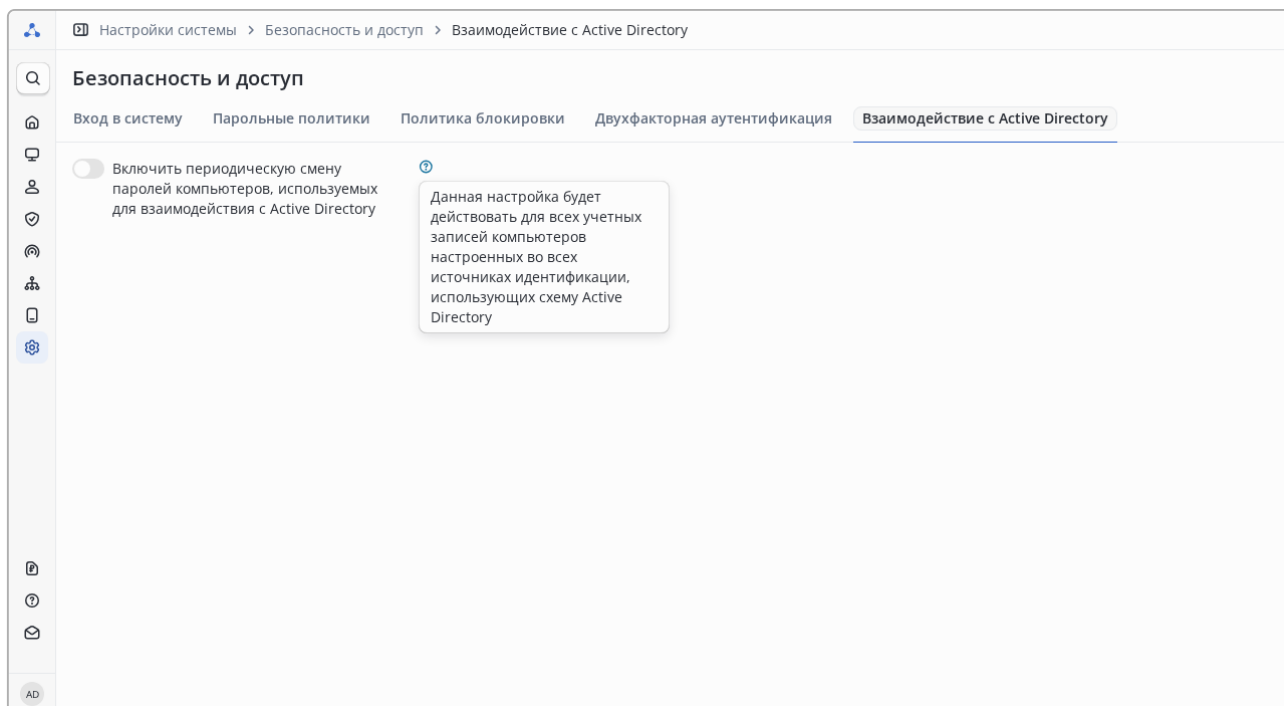


Рисунок 417. Описание настройки

При включении переключателя открывается блок **Расписание смены пароля**:

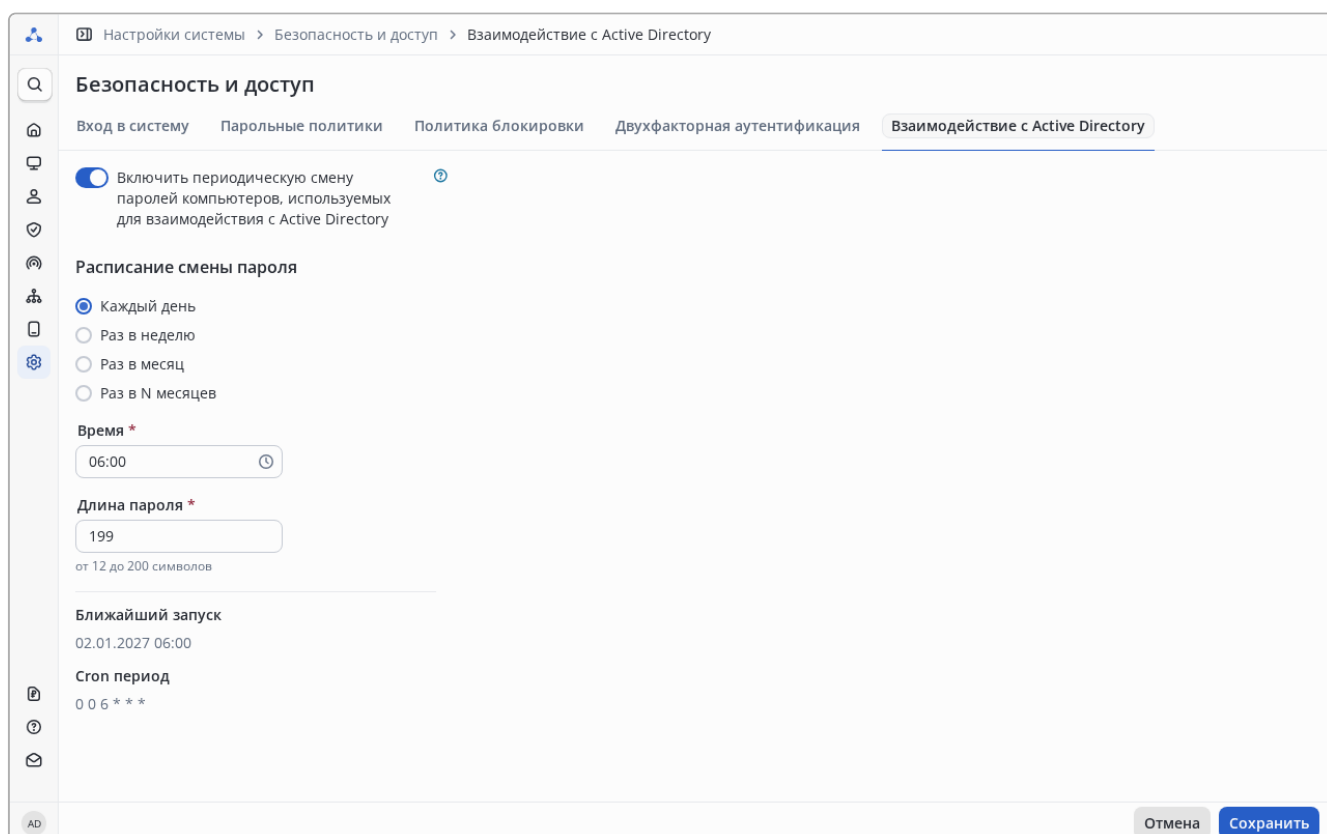


Рисунок 418. Расписание смены пароля

Блок расписания содержит следующие параметры:

- **Тип расписания** - выбор одного из вариантов:
 - **Каждый день** - смена пароля выполняется ежедневно в указанное время.

- **Раз в неделю** - появляется дополнительное поле **День недели ***.

Настройки системы > Безопасность и доступ > Взаимодействие с Active Directory

Безопасность и доступ

Вход в систему | Парольные политики | Политика блокировки | Двухфакторная аутентификация | **Взаимодействие с Active Directory**

☒ Включить периодическую смену паролей компьютеров, используемых для взаимодействия с Active Directory ⓘ

Расписание смены пароля

☐ Каждый день
☒ **Раз в неделю**
☐ Раз в месяц
☐ Раз в N месяцев

День недели *

Понедельник ▾

Время *

09:30 ⌚

Длина пароля *

199

от 12 до 200 символов

Ближайший запуск

04.01.2027 09:30

Срок период

0 30 9 * * 1

AD

Отмена Сохранить

Рисунок 419. Расписание смены пароля - еженедельно

- **Раз в месяц** - появляется дополнительное поле **Число месяца ***.

Настройки системы > Безопасность и доступ > Взаимодействие с Active Directory

Безопасность и доступ

Вход в систему Парольные политики Политика блокировки Двухфакторная аутентификация Взаимодействие с Active Directory

☒ Включить периодическую смену паролей компьютеров, используемых для взаимодействия с Active Directory ⓘ

Расписание смены пароля

☐ Каждый день
☐ Раз в неделю
☒ Раз в месяц
☐ Раз в N месяцев

Число месяца *
15

Время *
06:00

Длина пароля *
199
от 12 до 200 символов

Ближайший запуск
15.01.2027 06:00

Срок периода
0 0 6 15 * *

AD

Отмена Сохранить

Рисунок 420. Расписание смены пароля - ежемесячно

- Раз в N месяцев - появляются поля Период смещения N * и Число месяца *.

Настройки системы > Безопасность и доступ > Взаимодействие с Active Directory

Безопасность и доступ

Вход в систему Парольные политики Политика блокировки Двухфакторная аутентификация Взаимодействие с Active Directory

☒ Включить периодическую смену паролей компьютеров, используемых для взаимодействия с Active Directory ⓘ

Расписание смены пароля

☐ Каждый день
☐ Раз в неделю
☐ Раз в месяц
☒ Раз в N месяцев

Период смещения N *

3

Число месяца *

10

Время *

06:00

Длина пароля *

199

от 12 до 200 символов

Ближайший запуск

10.01.2027 06:00

Cron период

0 0 6 10 */3 *

AD

Отмена Сохранить

Рисунок 421. Расписание смены пароля - раз в N месяцев

- **Время *** - время выполнения смены пароля в формате **чч:мм**.
- **Длина пароля *** - длина нового пароля. Допустимая длина: от 12 до 200 символов.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

В нижней части страницы отображается дополнительная информация:

- **Ближайший запуск** - рассчитанная дата и время следующей автоматической смены пароля.
- **Cron период** - сгенерированная Cron-строка расписания.



Если обязательные параметры заполнены не полностью, отображается значение *Неизвестно*.

Для применения изменений нажмите кнопку **Сохранить**. Для отмены - кнопку **Отмена**.

Хранилище сертификатов

Доверенные сертификаты

Описание

Раздел **Доверенные сертификаты** предназначен для управления сертификатами, которым система NAICE доверяет при установке защищённых соединений, например, при подключении к внешним сервисам.

Добавленные сертификаты формируют список доверенных, используемый системой для проверки подлинности сертификата удалённого узла. В разделе предусмотрены следующие операции для работы с сертификатами: просмотр, редактирование, скачивание и удаление.

Элементы управления

Элементы управления в разделе являются стандартными и используются аналогично другим разделам системы.

-  - Добавить новый сертификат.
-  - Удалить выбранные сертификаты (неактивно, пока не выбран ни один сертификат).
-  - Обновить данные таблицы.
- ☐ - Чекбокс выбора элементов для выполнения дальнейших действий, например, удаления.
-  - Изменить текущий порядок сортировки.
-  - Скачать загруженный ранее сертификат.
-  - Индикатор, сигнализирующий о скором истечении срока действия сертификата.
-  - Индикатор, сигнализирующий об истечении срока действия сертификата.

Просмотр списка доверенных сертификатов

Настройки системы > Хранилище сертификатов > Доверенные сертификаты

Хранилище сертификатов

Доверенные сертификатыСерверные сертификаты

☐	Статус	Имя 	Использование	Описание	Кому выдан	Кем выдан	Дата начала	Дата окончания	
☐	 Включено	Test certificate 01	 Да	Test description 01	CN=example.com, O=Exempl...	CN=Example CA, O=Example...	01.01.2027 10:00:00	20.02.2027 10:00:00	
☐	 Включено	Test certificate 02	 Нет	Test description 02	CN=example.com, O=Exempl...	CN=Example CA, O=Example...	01.01.2027 10:00:00	20.02.2027 10:00:00	
☐	 Включено	Root CA bundle 01 	 Нет	Trusted bundle description 01	CN=example.com, O=Exempl...	CN=Example CA, O=Example...	01.01.2027 10:00:00	12.01.2027 10:00:00	
☐	 Выключено	Root CA bundle 02 	 Нет	Trusted bundle description 02	CN=example.com, O=Exempl...	CN=Example CA, O=Example...	01.01.2027 10:00:00	01.01.2027 10:00:00	

Всего элементов: 4

Рисунок 422. Таблица доверенных сертификатов

На странице отображается таблица со списком доверенных сертификатов, добавленных в систему пользователем.

Таблица содержит следующие колонки:

- Статус** - текущее состояние сертификата ("Включено" или "Выключено").
- Имя** - уникальное имя сертификата в системе.
- Описание** - произвольное описание, присвоенное сертификату пользователем.
- Кому выдан** – значение из поля **Subject** сертификата (владелец сертификата, для кого выдан сертификат).

Кем выдан – значение из поля **Issuer** сертификата (издатель сертификата).

- Дата начала - значение из поля **Not Before** сертификата (начало срока действия сертификата).
- Дата окончания - значение из поля **Not After** сертификата (окончание срока действия сертификата).

Добавление доверенного сертификата

Для добавления нового сертификата нажмите **+**.

The screenshot shows a web-based interface for adding a trusted certificate. The breadcrumb trail at the top reads: 'Настройки системы > Хранилище сертификатов > Доверенные сертификаты > Добавление'. The main heading is '← Добавление'. Below this, there is a toggle switch labeled 'Включено' which is turned on. The form contains three input fields: 'Имя *' (Name) with a placeholder 'Введите имя', 'Создан' (Created) with a placeholder 'Администратором', and 'Описание' (Description) with a placeholder 'Введите описание' and a character count '0 / 200'. Below these fields is a section for the certificate file, labeled 'Файл сертификата (.cer, .crt) *', with a dashed box containing the text 'Выберите файл или перетащите его в эту область'. At the bottom right, there are two buttons: 'Отмена' (Cancel) and 'Добавить' (Add).

Рисунок 423. Окно добавления доверенного сертификата

На странице добавления отображаются следующие параметры:

- Статус - Определяет, будет ли сертификат включён сразу после добавления.
- Имя * - Используется для идентификации сертификата в интерфейсе и событиях.
- Описание - Произвольное описание сертификата.
- Файл сертификата * - Поле для добавления файла сертификата.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

Также на данной странице можно увидеть реальные имя и расширение загруженного сертификата.

Требования к сертификатам:



- Поддерживаются сертификаты форматов `.cer` и `.crt`, соответствующие стандарту X.509. Сертификаты в формате `.pem` не поддерживаются.
- Приватные ключи загружать в систему не требуется.
- Допускается загрузка файлов содержащих только один сертификат. Загрузка файлов содержащих цепочку сертификатов (например Root CA (корневых сертификатов) и Intermediate CA (промежуточных сертификатов) или нескольких произвольных сертификатов не допускается.
- Сертификат для защищенного подключения к LDAP должен содержать поле SAN (Subject Alternative Name) с указанием доменного имени (пример `DNS:ldap.example.org`) или IP-адреса (пример `IP Address:192.168.0.10`) хоста.

Возможные ошибки при загрузке сертификатов в систему

Ниже приведены основные ошибки, которые могут возникать при загрузке доверенных сертификатов, а также причины их появления.



Файл сертификата недействителен

Рисунок 424. Файл сертификата недействителен

Причина: Возможно, сертификат имеет несовместимую структуру, или файл сертификата содержит повреждённые/неполные данные.



Не удалось добавить доверенный сертификат.
Недопустимый формат.

Рисунок 425. Неподдерживаемый формат сертификата

Причина: Выбранный файл не является сертификатом, или при именовании присвоено недопустимое расширение (в примере `docx`).



Срок действия сертификата истек

Рисунок 426. Срок действия сертификата истек

Причина: Срок действия сертификата истек.



Сертификат с серийным номером "CERT-7X9P" уже существует

Рисунок 427. Сертификат с указанным серийным номером уже существует

Причина: Попытка загрузить уже существующий сертификат в систему.

Скачивание сертификата из системы

Для скачивания сертификата необходимо нажать на  в таблице просмотра всех сертификатов.

Дата окончания		
:00	20.02.2027 10:00:00	
:00	20.02.2027 10:0	Скачать сертификат
:00	12.01.2027 10:00:00	
:00	01.01.2027 10:00:00	

Рисунок 428. Скачивание сертификата из системы

Просмотр сертификата

Для просмотра подробной информации о сертификате необходимо нажать на его имя в таблице.

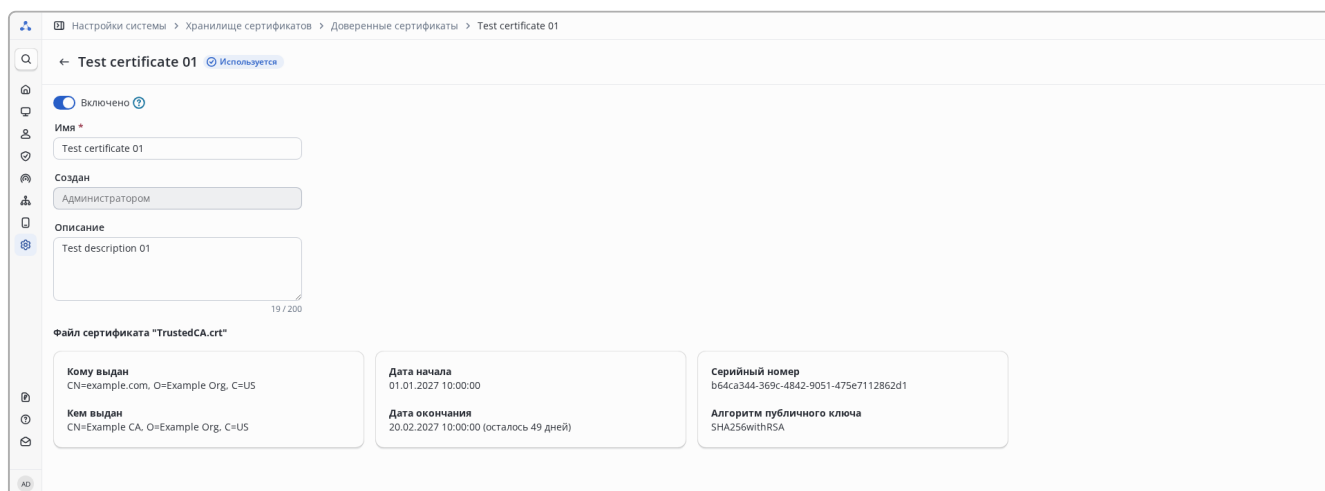


Рисунок 429. Страница просмотра доверенного сертификата

На странице просмотра отображаются следующие параметры:

Основные поля

- **Статус** - Определяет состояние сертификата ("Включено" или "Выключено").
- **Имя *** - Имя сертификата для идентификации в системе NAICE.
- **Описание** - Произвольное описание сертификата, созданное пользователем системы NAICE.
- **Имя файла** - Имя загруженного файла сертификата.

Идентификация сертификата

- **Кому выдан** – значение из поля **Subject** сертификата (владелец сертификата, для кого выдан сертификат).
- **Кем выдан** – значение из поля **Issuer** сертификата (издатель сертификата).
- **Дата начала** - значение из поля **Not Before** сертификата (начало срока действия сертификата).

Дата окончания - значение из поля **Not After** сертификата (окончание срока действия сертификата).

- Серийный номер - уникальный идентификатор сертификата **Serial Number**, задаётся издателем (CA).
- Алгоритм публичного ключа - алгоритм, которым подписан сертификат - **Signature Algorithm**.

Индикация истекающих/истекших сертификатов

Истекает срок действия – срок действия сертификата подходит к концу и истечёт в ближайшее время. Данное состояние отображается, если до истечения срока действия сертификата осталось менее 30 дней. В этом случае, при необходимости, следует заранее заменить сертификат, чтобы избежать ошибок установки защищённых соединений.

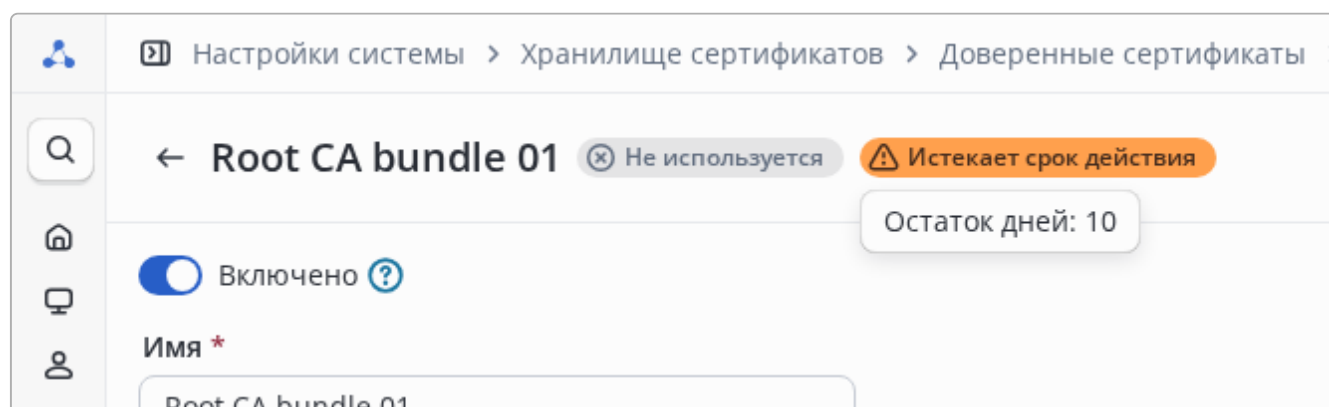


Рисунок 430. Истекает срок действия сертификата

Срок действия истёк – текущая дата и время превышают значение даты окончания действия сертификата. Такой сертификат следует немедленно заменить на действующий.

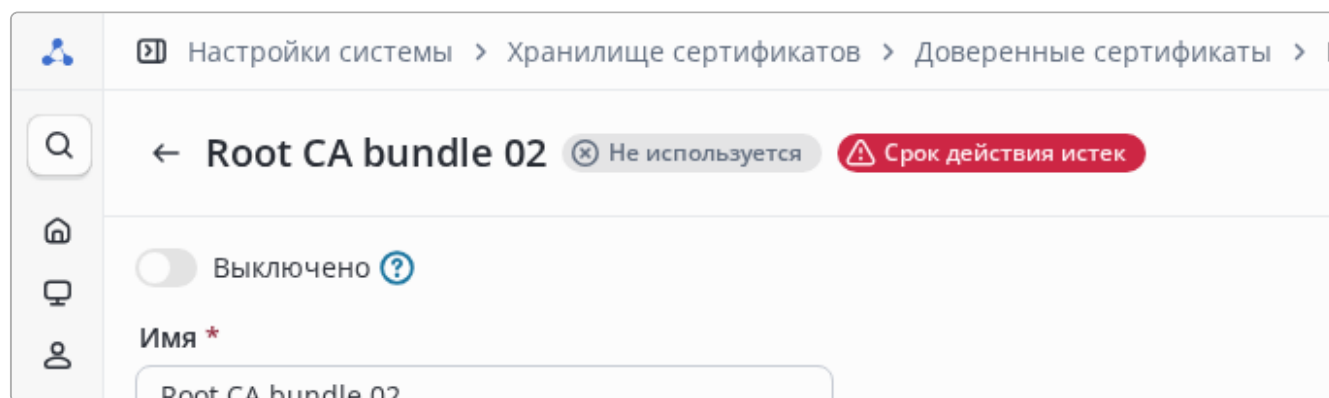


Рисунок 431. Срок действия сертификата истек



Истекшие сертификаты все еще можно использовать для подтверждения подлинности внешних сервисов, пока они находятся в состоянии "Включено", если это позволяет сам сервис.

Редактирование сертификата

Редактирование выбранного сертификата выполняется на странице его просмотра, доступ к которой осуществляется по нажатию на имя сертификата.

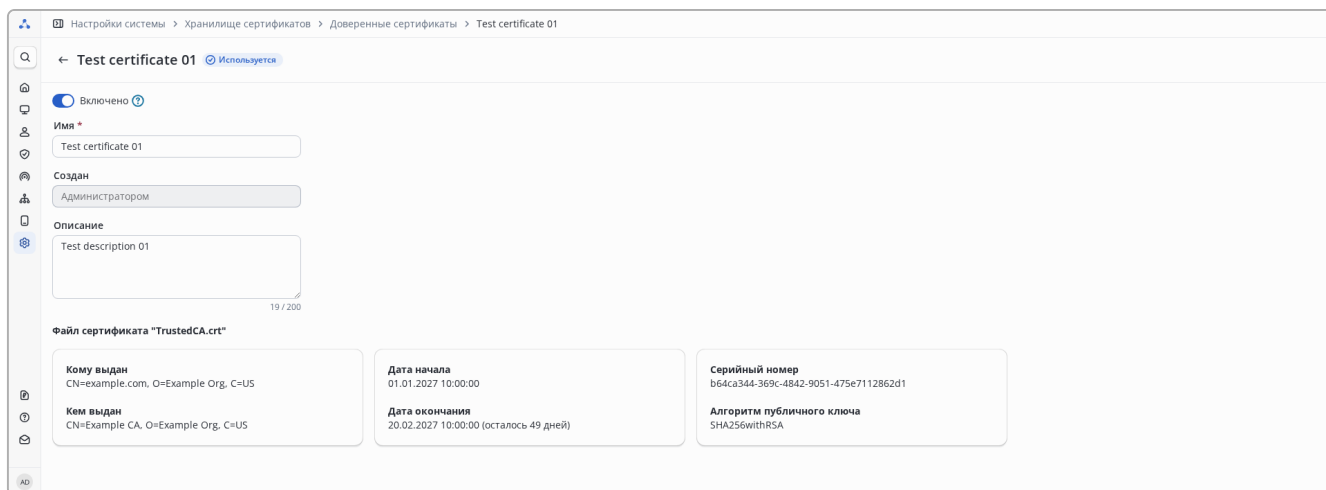


Рисунок 432. Редактирование параметров сертификата

Допускается изменение следующих параметров сертификата:

- Имя
- Описание
- Статус



Замена файла сертификата при редактировании не поддерживается. Для изменения содержимого сертификата необходимо удалить запись и загрузить сертификат заново.

Включение и отключение сертификата

Использование сертификата может быть приостановлено без удаления из системы. Для этого необходимо изменить поле Статус на "Выключено" в форме редактирования и сохранить изменения.

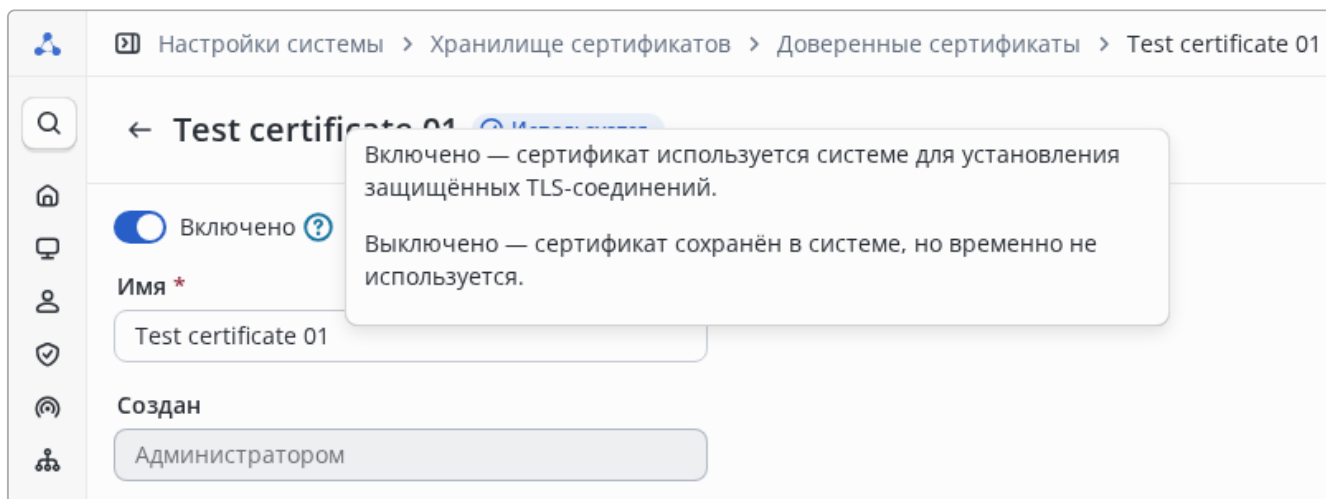


Рисунок 433. Включение и отключение сертификата

Отключённый сертификат:

- Остаётся в списке;
- Отображается в системных событиях;

Не используется системой при установке TLS-соединений.

Удаление доверенных сертификатов

Для удаления выберите один или несколько сертификатов с помощью ☐ и нажмите .



Удаление элементов требует подтверждения в модальном окне. Выбранные элементы будут удалены только после явного подтверждения операции.

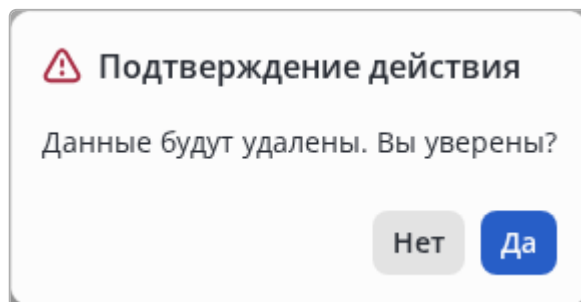


Рисунок 434. Диалоговое окно подтверждения действия



Удаление сертификата является необратимой операцией. Перед удалением убедитесь, что сертификат не используется в активной конфигурации системы, например, во [внешних источниках идентификации](#).

События, связанные с сертификатами

Операции с доверенными сертификатами фиксируются в [журнале системных событий](#).

Фиксируются действия:

- Добавление сертификата.
- Редактирование имени и описания сертификата.
- Изменение статуса (включение/отключение).
- Удаление сертификатов.
- Предупреждение о скором истечении сертификата.
- Предупреждение об истечении сертификата.



Предупреждения об истечении или скором истечении срока действия сертификата в [журнале системных событий](#) фиксируются только для сертификатов, находящихся в состоянии "Включено". Для сертификатов в состоянии "Выключено" события не фиксируются.

Серверные сертификаты

Решение проблем

Логи

На данной странице выполняется настройка уровня логирования сервисов NAICE. Настройка применяется ко всем сервисам сразу, настроить для одного из сервисов уровень логов, отличный от остальных, нельзя.



Для применения настройки не требуется рестарт сервисов NAICE, поэтому при изменении значения прерывания услуги не происходит.

Решение проблем

Логи

⚠️ Высокий уровень детализации логов снижает производительность. Рекомендуется использовать только для диагностики и отключать после завершения работ.

Общие настройки

Глобальный уровень логирования

DEBUG

Настройки отдельных сервисов

☐ Расширенные логи сервиса RADIUS

Рисунок 435. Настройка уровня логирования

В сервисах NAICE существует 6 уровней логирования. Каждый следующий уровень включает в себя логи предыдущего, а также логи, специфичные для данного уровня.

Список уровней в порядке возрастания:

- **FATAL** - включает только происшествия, приводящие к остановке работы сервисов NAICE. **Не рекомендуется к настройке**, так как причина остановки обычно лежит на следующих уровнях. Минимальное количество генерируемых логов.
- **ERROR** - включает происшествия, приводящие к ошибкам в предоставлении основного функционала NAICE.
- **WARN** - включает неожиданные/подозрительные происшествия, которые напрямую не приводят к остановке в работе основного функционала, однако потенциально могут привести к ошибкам.
-

INFO (по умолчанию) - включает как негативные, так и основные положительные происшествия, учет которых запланирован.

- **DEBUG** - включает детальные логи, необходимые для диагностики возникающих в процессе работы NAICE проблем. Требуемый уровень логов при анализе проблемы технической поддержкой.
- **TRACE** - самый детальный уровень логов, используемый для глубокой диагностики сложных проблем. **Не рекомендуется к настройке** без соответствующего указания сотрудника технической поддержки, так как приводит к генерации огромного количества логов.



Важно учитывать, что более высокий уровень логирования приводит к большему числу генерируемых логов, а соответственно и к их более частой ротации. Параметры ротации логов указываются на этапе установки NAICE.

Узлы

Лицензирование

Описание

Система контроля сетевого доступа NAICE распространяется по коммерческой лицензии. Это означает, что для получения доступа к функционалу необходимо приобрести и активировать лицензию.

Лицензирование может осуществляться по одной из следующих схем:

- С помощью сервера лицензий **Eltex License Manager** (далее - **ELM**), осуществляющего функцию лицензирования программных и аппаратных продуктов компании «Элтекс». Предполагает периодический запрос к серверу лицензий. Может использоваться:
 - сервер лицензий компании «Элтекс» (далее - Online ELM), доступный по адресу <https://elm.eltex-co.ru:8099>;
 - сервер ELM, установленный в инфраструктуре заказчика (далее - Offline ELM).

В обоих случаях адрес ELM сервера указывается в настройках системы в разделе [Подключение к ELM](#) и на момент активации лицензии он должен быть доступен. Поддержана возможность работы с ELM сервером с использованием HTTP-прокси сервера (с использованием аутентификации по логину/пароллю или без аутентификации).

- Файловое лицензирование (далее - **PLR**, permanent license request) - лицензирование с привязкой к физическим параметрам хоста, на котором установлен NAICE. При изменении параметров хоста требуется ре-активация.

После установки NAICE находится в **демонстрационном режиме** с ограничениями в функционале. Ограничения демонстрационного режима указаны [далее](#).

При приобретении доступа к продукту с определенным уровнем лицензирования генерируется **файл ключа продукта**, уникальный для каждого экземпляра NAICE. Для разблокировки функционала NAICE, соответствующего данной лицензии, файл необходимо загрузить и активировать на странице *Лицензирование*.

Уровни лицензии и лицензируемый функционал

В текущей версии поддерживаются 2 уровня лицензирования - **BASIC** и **ADVANCED**. Каждый следующий уровень включает в себя весь функционал предыдущего и добавляет поддержку расширенного функционала.

Лицензии любого уровня могут быть выданы сроком на 1, 3 или 5 лет.



По вопросам получения лицензии обращайтесь на нашу электронную почту eltex@eltex-co.ru.

Уровень лицензии BASIC

На уровне **BASIC** предоставляется доступ к основной услуге - RADIUS-авторизации [эндпоинтов](#). Лицензируемым параметром является **количество успешно авторизованных уникальных**

конечных устройств за сутки. Данное количество согласовывается на этапе приобретения лицензии и зависит от числа клиентских устройств в сети.

Пример расчета количества конечных устройств в сети

В организации "А" работает 1000 сотрудников, каждый из которых имеет ноутбук для работы. Сотрудники компании "А" не подключаются с личных устройств. В компании также к сети подключены 10 камер, 5 принтеров и 2 телевизора. Все эти устройства необходимо авторизовать в NAC-системе.

Расчет количества уникальных конечных точек в сети: $1000 * 1$ (количество устройств 1 сотрудника) + 10 (камеры) + 5 (принтеры) + 2 (телевизоры) = 1017 шт. – уникальных устройств в компании.

Рекомендуется приобретать лицензии на большее число эндпоинтов, чем рассчитано уникальных устройств.



При необходимости количество эндпоинтов в лицензии можно увеличить. Для этого обратитесь к вашему менеджеру или отправьте запрос на нашу электронную почту eltex@eltex-co.ru.

Уровень лицензии ADVANCED

На данном уровне лицензии активируется функционал, необходимый для настройки и работы портальной авторизации. Для любой лицензии с данным уровнем количество **гостевых эндпоинтов** не ограничивается, то есть авторизация доступна для любого количества гостей.

Дополнительные модули

Для приобретения также доступен дополнительный модуль **NAICE-TACACS**, активирующий TACACS-сервер в составе NAICE. Модули приобретаются дополнительно для основной лицензии любого уровня.

Демонстрационный режим

После установки NAICE находится в демонстрационном режиме (демо-режим). В данном режиме доступен весь функционал, соответствующий максимальному уровню лицензии и со всеми дополнительными модулями, но со следующими ограничениями:

- максимальное количество добавленных в систему **устройств** - 15;
- максимальное количество успешно авторизованных уникальных **эндпоинтов** за сутки - 15;
- максимальное количество **гостевых эндпоинтов** - 15.



Демонстрационный режим не ограничен во времени, однако он доступен только **до первой успешной активации лицензии**. После активации лицензии демо-режим будет отключен без возможности восстановления.

О том, что система находится в демонстрационном режиме, сигнализирует соответствующее предупреждение в нижней левой части меню навигации.

Рисунок 436. Предупреждение о демонстрационном режиме

При нажатии на предупреждение будет осуществлен переход на страницу *Лицензирование*, содержащей актуальные параметры и лимиты демо-режима, а также элементы управления для загрузки и администрирования лицензий.

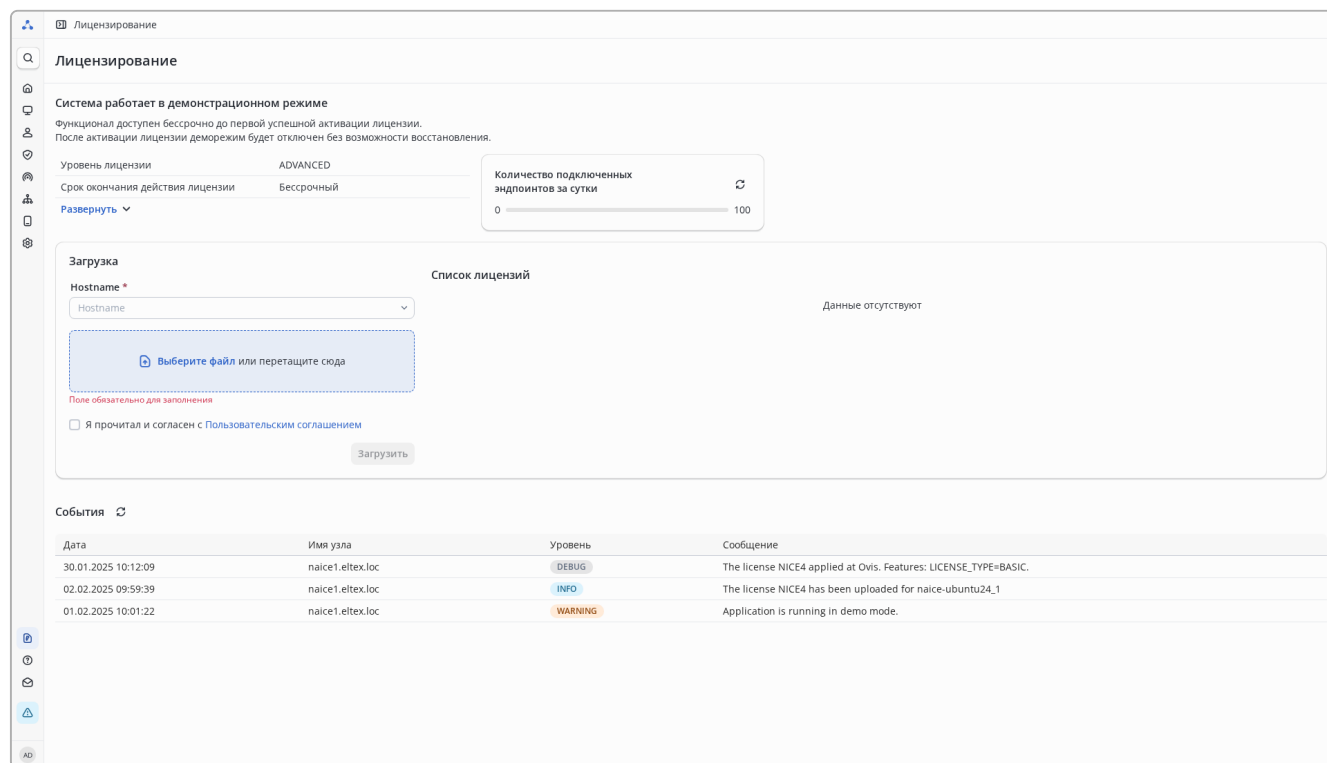


Рисунок 437. Страница *Лицензирование* в демонстрационном режиме

Действия для активации лицензии

Активация лицензии осуществляется на странице *Лицензирование*, изображение которой приведено выше.

Страница, помимо актуальных параметров демо-режима или лицензии, содержит следующие элементы управления:

- блок "Загрузка" - элементы для загрузки лицензионных файлов;
- блок "Список лицензий" - управление загруженными лицензиями;
- блок "События" - системные события, относящиеся к лицензированию.

Загрузка ключа продукта

Для активации лицензии необходимо иметь *файл ключа продукта*, полученный от Вашего менеджера при приобретении системы. Файл ключа продукта содержит *Product ID* - серийный номер, идентифицирующий один экземпляр ПО и *Product Key* (ключ лицензии), идентифицирующий владельца лицензии.



Формат имени файла ключа продукта - **NICENNNNNNN.txt** для ELM-лицензии (например - NICE1111111.txt) и **FNICENNNNNNN.txt** для PLR-лицензии (например - FNICE1111111.txt).



Валидный файл ключа продукта не может быть пустым или иметь размер более 1 Мб.



Product ID может быть привязан только к одному хосту. Попытки загрузить *Product ID*, который уже присутствует в таблице, запрещены системой. Ограничение не снимается даже если *Product ID* находится в состоянии Backup. Все загружаемые *Product ID* должны быть из одной лицензии (иметь одинаковый Ключ лицензии, *License key*). Попытки загрузить *Product ID* из разных *License key* запрещены системой.

Загрузка ключа продукта выполняется в блоке "Загрузка" в несколько шагов:

1. **Выбрать хост** для загрузки лицензии из списка по его hostname. При стандартной установке hostname совпадает с именем хоста, на котором развернут NAICE.
2. **Выбрать файл ключа продукта**, перетащив его в поле загрузки или выбрав через проводник при клике на "Выберите файл". При необходимости до нажатия на кнопку Загрузить файл можно заменить, кликнув на  в правой части поля загрузки.
3. Ознакомиться и подтвердить **согласие с Пользовательским соглашением**.
4. Нажать на кнопку Загрузить.

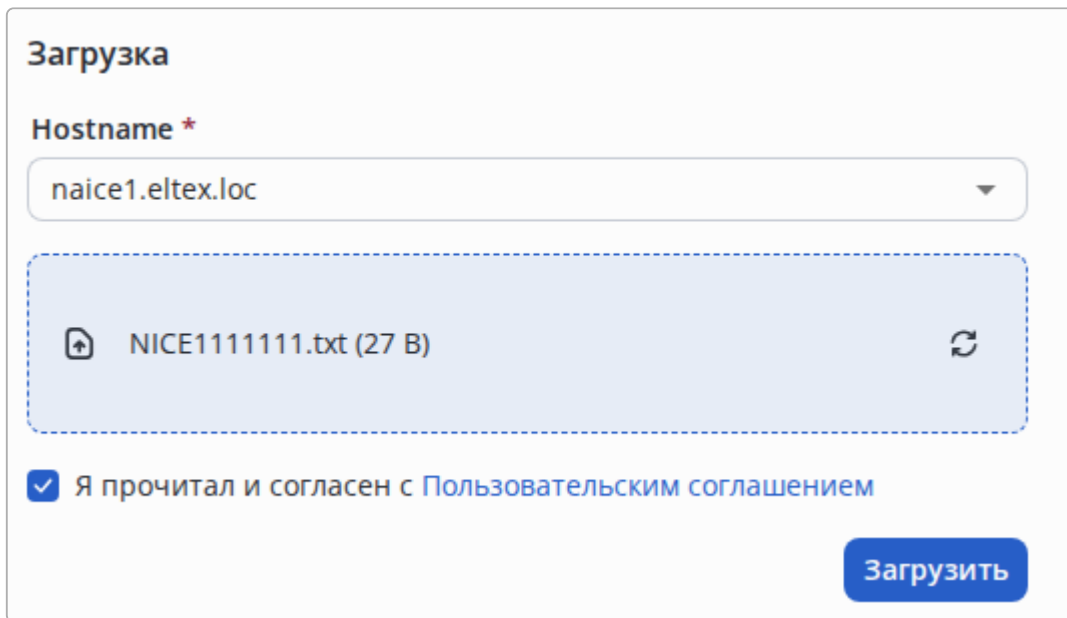


Рисунок 438. Загрузка файла ключа продукта

При использовании NAICE в кластере необходимо загрузить свой ключ продукта для каждого хоста NAICE.

После загрузки файла ключа продукта лицензия будет добавлена в таблицу лицензий в блоке "Список лицензий".

Активация лицензии

Механизмы активации ELM и PLR лицензий существенно различаются.

ELM

ELM лицензия активируется *автоматически* путем подключения к Online или Offline ELM серверу. При успешной активации лицензия приобретает статус **Active** в списке лицензий, функционал становится доступным согласно параметрам лицензии. Параметры активной лицензии отображаются в верхнем блоке "Информация о лицензии".

Список лицензий				
Hostname	ID продукта	Тип	Статус	Действия
naice1.eltex.loc	NICE1111111	ELM	Active	  

Рисунок 439. Активация ELM-лицензии

PLR

PLR режим активируется загрузкой ключа продукта, который поставляется в виде файла. Данный файл выпускается на основании запроса компанией «Элтекс».

После загрузки ключа продукта PLR-лицензии она появится в таблице "Список лицензий" в статусе **Init**. Этот статус означает, что лицензия проинициализирована и сгенерирован *файл активации лицензии*. Файл, помимо всего прочего, содержит слепок параметров окружения хостовой машины, к которым и привязывается лицензия.

Список лицензий 				
Hostname	ID продукта	Тип	Статус	Действия
naice1.eltex.loc	FNICE1111111	PLR	Init	  

Рисунок 440. PLR-лицензия после загрузки ключа продукта

Файл активации лицензии необходимо выгрузить и передать в компанию «Элтекс» для выпуска файла лицензии - итогового файла, содержащего параметры приобретенной лицензии с привязкой их активации только в определенном окружении. Для этого:

1. Нажать на  в таблице "Список лицензий" в колонке Действия и выбрать **Скачать файл активации**.

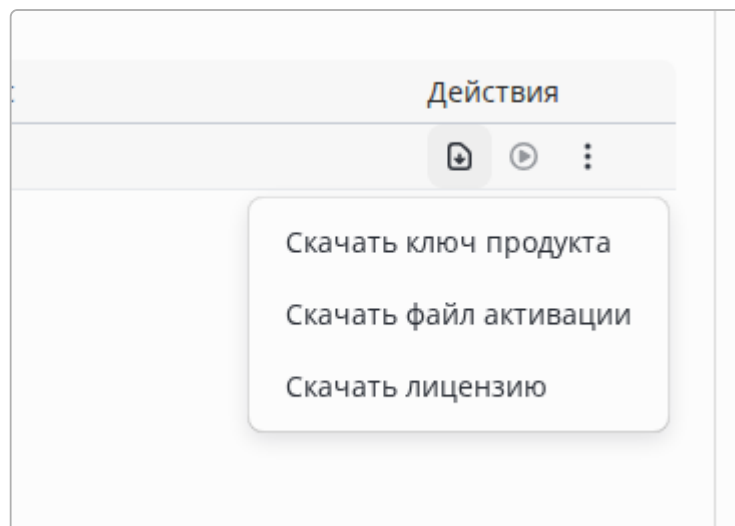


Рисунок 441. Меню скачивания лицензионных файлов



Формат имени файла активации **request-`<YYYY-MM-DD>-<Product ID>-<NAICE Version>.txt`**, например - **request-2026-06-17-FNICE1111111-1.2.0.txt**.

2. Передать файл активации в компанию «Элтекс» для выпуска файловой лицензии, соответствующей предоставленному файлу активации.
3. Получить файл лицензии в компании «Элтекс».
4. Загрузить файл лицензии в систему аналогично [загрузке ключа продукта](#). При успешной загрузке и проверке файла произойдет попытка автоматической активации лицензии. При отсутствии ошибок лицензия приобретает статус **Active** в списке лицензий, функционал становится доступным согласно параметрам лицензии. Параметры активной лицензии отображаются в верхнем блоке "Информация о лицензии".

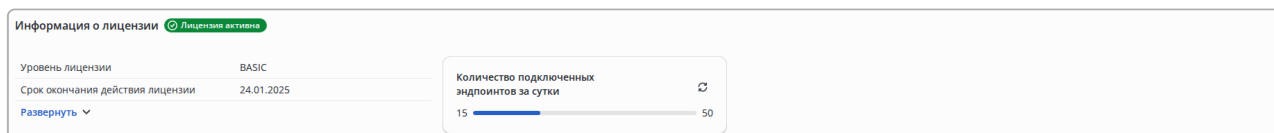


Рисунок 442. Информация об активной лицензии

Ошибки при активации лицензии

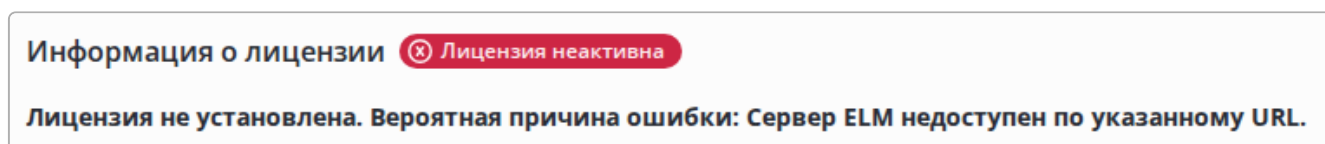


Рисунок 443. Ошибка при активации лицензии

При возникновении ошибок активации лицензии на странице под статусом лицензии отобразится ошибка, возникшая в процессе активации. Также сообщение об ошибке в первоначальном виде отображается в [Событиях](#). При этом сама лицензия приобретает статус **Invalid**.

Как правило, ошибки при активации лицензии связаны:

- При взаимодействии с сервером ELM: проблемы с доступом к серверу (некорректный адрес ELM в конфигурации NAICE, отсутствие сетевой связности) или с ошибками самой лицензии (не

наступивший или истекший срок лицензии).

- При использовании PLR лицензирования: изменение параметров окружения после создания файла активации лицензии или с ошибками самой лицензии.

Для активации лицензии необходимо сначала устранить первоначальную ошибку, а затем нажать на  напротив нужной лицензии в таблице "Список лицензий" в колонке Действия.

В случае возникновения проблем при автоматической активации лицензии она остается в статусе **Ready**. В таком случае необходимо провести ручную активацию лицензии, нажав на  напротив нужной лицензии в таблице "Список лицензий" в колонке Действия.

Список лицензий 				
Hostname	ID продукта	Тип	Статус	Действия
naice1.eltex.loc	NICE1111111	ELM	Ready	  

Рисунок 444. Лицензия в статусе Ready

Лицензия отозвана

Информация о лицензии

 Лицензия неактивна

Лицензия отозвана

Рисунок 445. Лицензия отозвана

Ошибка "Лицензия отозвана" возникает в случае если активируемая PLR лицензия не входит в перечень актуальных PLR лицензий. Это может произойти при аннулировании лицензии компанией «Элтекс» в связи с получением информации о ее массовом распространении на публичных ресурсах. Также отзыву подлежат устаревшие версии [реактивированных](#) или [продленных](#) лицензий.



Если вы считаете что ваша лицензия была отозвана ошибочно, то обратитесь к вашему менеджеру, в техническую поддержку компании «Элтекс» или отправьте запрос на нашу электронную почту eltex@eltex-co.ru.

Управление и мониторинг лицензий

После успешной активации лицензий их состояние можно продолжать отслеживать на странице *Лицензирование*.

 Лицензирование

Рисунок 446. Пункт Лицензирование в меню навигации

Информация об активной лицензии

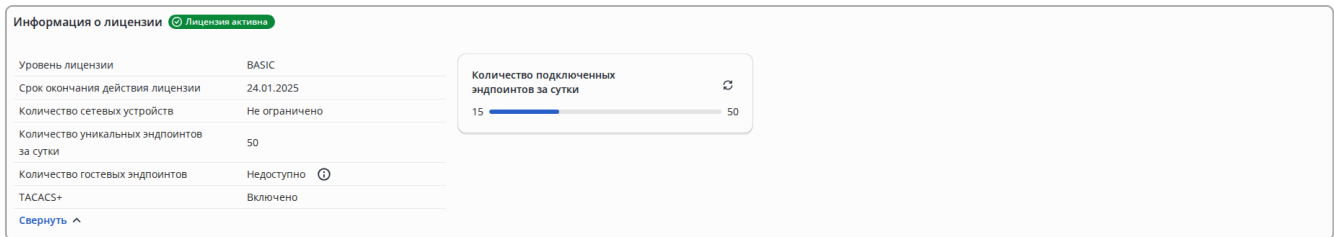


Рисунок 447. Информация о лицензии

Страница содержит следующие элементы:

- Лицензия активна - текущий статус лицензии.
- Параметры лицензии:
 - **Уровень лицензии** определяет доступный для настройки и использования функционал NAICE, см. [Уровни лицензии и лицензируемый функционал](#)
 - **Срок окончания действия лицензии** - дата, при наступлении которой текущая срочная лицензия истекает.



При истечении срока действия лицензии лицензируемый функционал NAICE будет заблокирован, **в том числе авторизация конечных устройств**. Продлевайте лицензию заранее при появлении [предупреждения](#) для избежания таких ситуаций.

- **Количество сетевых устройств** - лимит по количеству добавленных в систему [сетевых устройств](#).
- **Количество уникальных эндпоинтов за сутки** - лимит по количеству подключенных [эндпоинтов](#) за сутки, предусмотренный лицензией.



При достижении лимита по количеству подключенных эндпоинтов за сутки конечные устройства сверх этого лимита авторизованы не будут. Ранее авторизованные в последние сутки устройства будут успешно переавторизованы.

- **Количество гостевых эндпоинтов** - лимит по количеству активных [гостевых эндпоинтов](#).
- **TACACS+** - наличие или отсутствие дополнительного модуля NAICE-TACACS в лицензии.
- Счетчик текущего количества подключенных эндпоинтов за сутки. Автоматически обновляется раз в 5 минут.
- - ручное обновление счетчика.

Особенности подсчета количества подключенных устройств за сутки

- Счетчик подключенных эндпоинтов увеличивается только при подключении *уникального* эндпоинта, то есть эндпоинта, который не был успешно авторизован NAICE в последние 24 часа.
- Для определения уникальности эндпоинта используется атрибут `Calling-station-id`.
-

В случае отсутствия указанного атрибута используется косвенное определение с использованием атрибутов:

- **User-Name** - атрибут должен присутствовать в RADIUS запросе.
 - **NAS-IP-Address** или **NAS-Identifier** - должен присутствовать хотя бы один атрибут из указанных.
 - **NAS-Port** - не обязательный атрибут.
 - **NAS-Port-Type** - не обязательный атрибут
- Эндпоинты, авторизованные через портал (**Гостевые эндпоинты**), не участвуют в подсчете.
 - Устройство считается подключенным ровно 24 часа с момента последнего успешного подключения. При повторной успешной авторизации время отсчета 24 часов обновляется.

Пример.

Эндпоинт был авторизован 10 июня в 13:31:10. "Освободит место" в лицензируемом лимите эндпоинт 11 июня в 13:31:11.

Если конечное устройство было успешно повторно авторизовано 10 июня в 20:20:10, то время сдвинется до 11 июня в 20:20:11.

Управление загруженными лицензиями

Все лицензии, которые загружены в NAICE, отображаются в таблице "Список лицензий".

Список лицензий ⚠				
Hostname	ID продукта	Тип	Статус	Действия
naice1.eltex.loc	NICE1111111	ELM	Ready	🔍 ⚙ ⋮
naice1.eltex.loc	FNICE1111111	PLR	Backup	🔍 ⚙ ⋮

Рисунок 448. Список лицензий

Таблица содержит колонки:

- **Hostname** - для какого хоста загружена данная лицензия;
- **ID продукта** - уникальный идентификатор программного обеспечения в системе лицензирования;
- **Тип** - тип лицензии: обычная (ELM) или файловая (PLR);
- **Статус** - текущий статус лицензии, который может принимать одно из следующих значений:
 - **Init** (только для PLR) - ключ продукта загружен, параметры окружения собраны, сгенерирован файл активации лицензии;
 - **Ready** - лицензия готова к активации, имеется ключ продукта и файл PLR-лицензии в случае файлового лицензирования;
 - **Active** - лицензия прошла активацию, ее параметры применены на указанном хосте;
 - **Invalid** - ключ продукта (или файловая лицензия) не прошел активацию

Mismatch (только для PLR) - получено событие о не совпадении параметров окружения;

- **Revoked** (только для PLR) - лицензия отозвана со стороны компании «Элтекс»;
- **Expired** - срок действия лицензии истек;
- **Backup** - неактивная лицензия, на данный момент выключенная из лицензирования; при необходимости может быть активирована.



Система позволяет оставить в базе данных любое количество *Product ID* в состоянии Backup. В случае переключения между типами ELM-PLR удалять записи неиспользуемого *Product ID* не обязательно. Их можно держать в базе данных для быстрого восстановления работы "по другой схеме".

- **Действия** - доступные действия с лицензией, в числе которых:

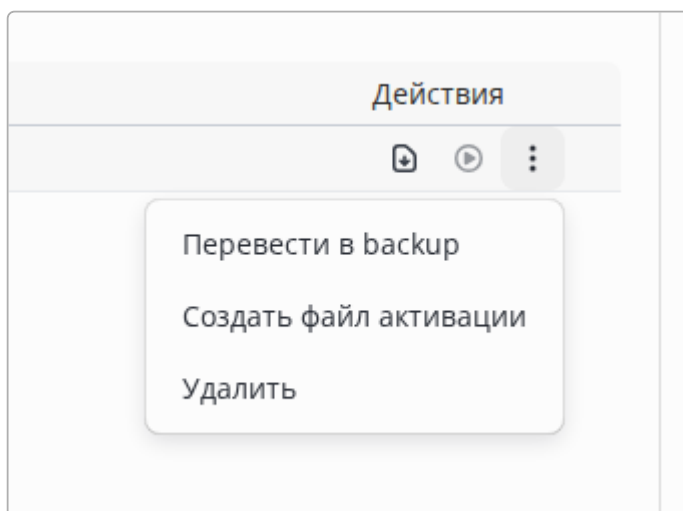


Рисунок 449. Действия с лицензией

- - скачивание лицензионных файлов различных типов;
- - активация неактивной лицензии / обновление параметров активной лицензии;
- - дополнительные действия:
 - **Перевести в backup** - установить для лицензии статус **Backup**;
 - **Создать файл активации** (только для PLR) - ручной запрос при проблемах автоматической генерации файла активации, а также при [реактивации лицензии](#);
 - **Удалить** - удалить лицензию из списка загруженных, а также все связанные с ней лицензионные файлы.



В целях непрерывного предоставления услуги перевод в статус **Backup** и удаление активных лицензий (лицензий со статусом **Active**) не происходит мгновенно. Сброс удаленной или переведенной в **Backup** лицензии с переходом NAICE в состояние "Без лицензии" произойдет только если перезагрузить сервисы NAICE. До этого момента следует активировать другую лицензию, иначе лицензируемый функционал будет отключен.

События

События

Дата	Hostname узла	Уровень	Сообщение
01.02.2025 20:35:20	naice1.eltex.loc	DEBUG	The license NICE4 applied at Ovis. Features: LICENSE_TYPE=BASIC.
01.02.2025 01:51:07	naice1.eltex.loc	INFO	The license NICE4 has been uploaded for naice-ubuntu24_1
01.02.2025 21:04:05	naice1.eltex.loc	WARNING	Application is running in demo mode.

Рисунок 450. Системные события лицензирования

Блок "События" является аналогом страницы [Системные события](#), в которые помещаются только события, связанные с лицензированием.

Таблица содержит следующие колонки:

- **Дата** - время записи события в базу данных; время отображается с учетом часового пояса, указанного в настройках аккаунта;
- **Hostname узла** - имя хоста, связанного с событием;
- **Уровень** - важность события, может принимать одно из следующих значений:
 - **INFO** - информационные события, как правило об успехе выполненных действий;
 - **WARNING** - события, на которые стоит обратить внимание;
 - **ERROR** - важные события с ошибками лицензий;
 - **DEBUG** - отладочные события.
- **Сообщение** - содержание события.

Фильтрация и изменение порядка сортировки недоступны. Частота автообновления списка событий - раз в 5 секунд. Доступно ручное обновление списка событий по кнопке



При пролистывании первых 25 элементов таблицы автообновление списка событий отключается.
Для включения необходимо выполнить ручное обновление по кнопке .

Предупреждения

Предупреждения о достижении лимитов

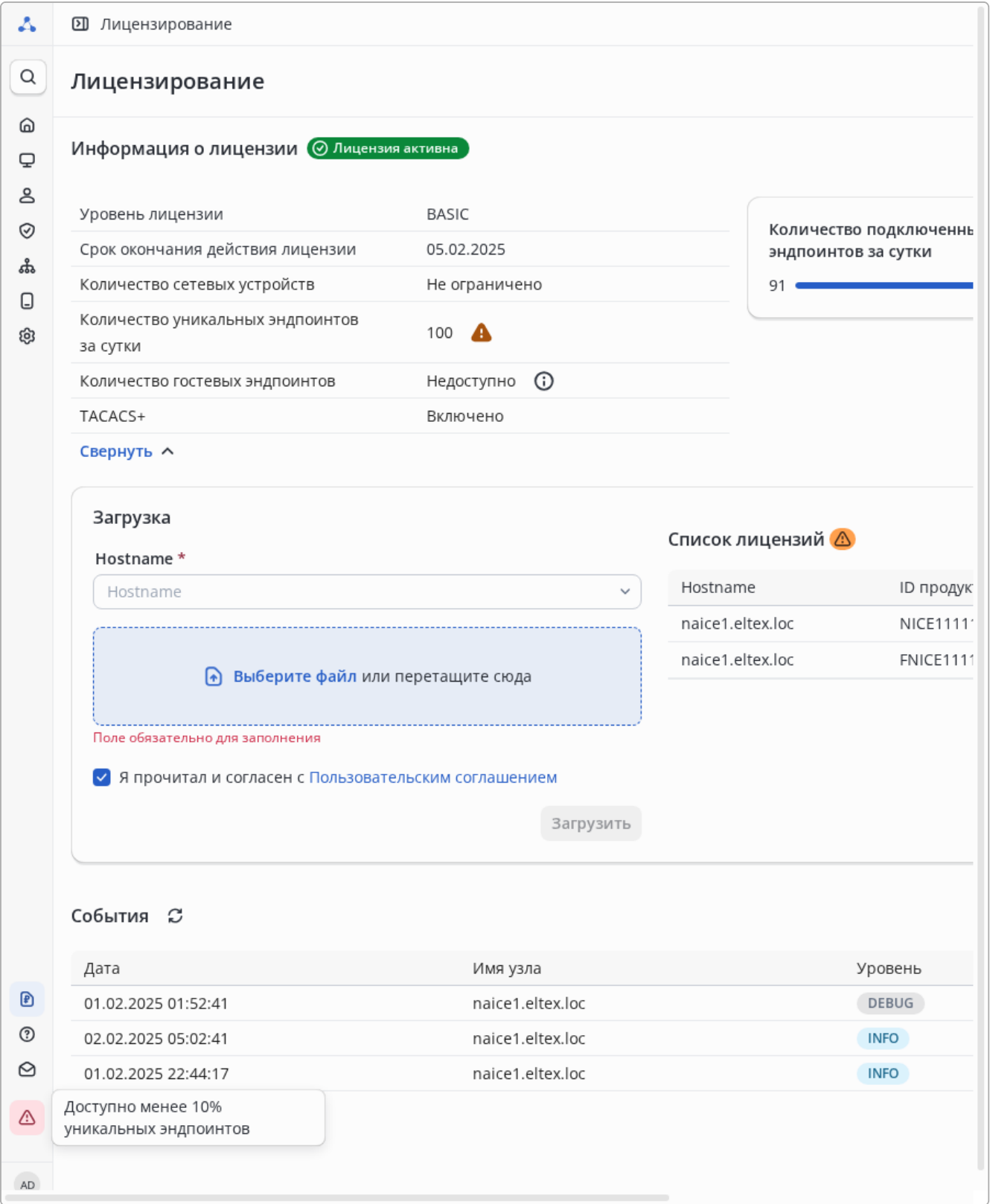


Рисунок 451. Предупреждения о достижении лимитов

При приближении к лимиту лицензии или демонстрационного режима по количеству подключенных эндпоинтов или при приближении к дате истечения лицензии в нижней левой части меню навигации будут отображаться предупреждения о приближении или достижении лимитов. При клике на предупреждение осуществляется переход на страницу *Лицензирование*.

Предупреждение о лимите по эндпоинтам начинает отображаться при достижении счетчиком значения в 90% от лицензируемого лимита.

Предупреждение о приближении даты окончания действия лицензии начинает отображаться за 90 дней до этого срока.

Помимо отображения в нижней левой части меню навигации, данные предупреждения отображаются на странице Лицензирование напротив соответствующего параметра в виде .

Недоступность сервера ELM

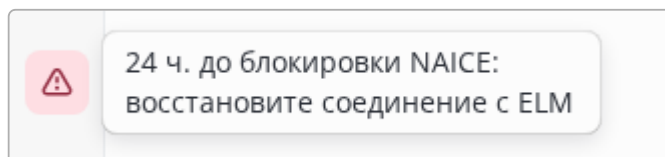


Рисунок 452. Предупреждение о недоступности ELM

NAICE периодически должен актуализировать параметры текущей ELM-лицензии на сервере ELM. В случае, если при очередной актуализации NAICE не смог получить параметры, то с этого времени стартует обратный отсчет до блокировки NAICE. Обратный отсчет отображается в нижней левой части меню навигации аналогично предупреждениям о достижении лимитов.



Если доступ до ELM не будет восстановлен в течение **72 часов**, то лицензируемый функционал NAICE будет заблокирован и лицензия будет сброшена. После сброса лицензии потребуется ее повторная активация.

Для проверки доступности сервера ELM можно воспользоваться следующей командой:

```
$ curl -k https://<IP адрес ELM>:<порт ELM>/elm/Hello
```

Если сервер ELM доступен, то вывод команды будет иметь вид:

```
{"server-info":  
{"version":"1.4","build":"10","root":true,"serverType":"elm","daemonMode":"server","serverMode":"r  
type":"elm","protocol-supported":2,"protocol-actual":4},"status":2,"result":"OK"}
```

Недоступность ERG сервиса

Для бесперебойной работы файловой лицензии необходима постоянная работа контейнера erg-service. В случае отключения или потери связи с данным контейнером лицензия будет сброшена через 12 часов. Контейнер erg-service входит в состав NAICE по умолчанию и работает вместе с другими контейнерами.

Смена параметров окружения

Если суммарное время работы с лицензией на текущей конфигурации сервера меньше 30 дней, то при изменении параметров окружения сервера лицензия будет принудительно сброшена через 14 дней.

Если суммарное время работы с лицензией на текущей конфигурации сервера больше 30 дней, то при изменении параметров окружения сервера лицензия будет принудительно сброшена через 30 дней.

Сценарии лицензирования

Перенос лицензии на другой хост

Существует возможность отредактировать hostname загруженной лицензии. Это может потребоваться при использовании кластера NAICE, когда лицензионные файлы были ошибочно загружены на другой хост.

Для редактирования hostname загруженной лицензии необходимо [перевести лицензию в статус Backup](#), а затем навести курсором на значение hostname выбранной лицензии. Справа от значения hostname появится иконка .

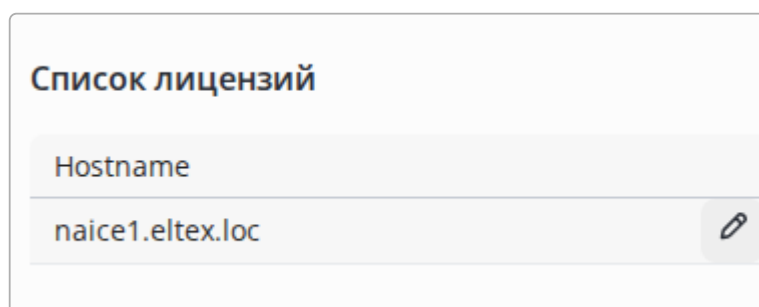


Рисунок 453. Редактирование hostname

После нажатия на иконку появится выбор нового хоста для лицензии. Сохранить сделанный выбор.

При необходимости активируйте новую лицензию, нажав на  в колонке Действий.

Изменение состава лицензии

В случае, если требуется изменить состав лицензии - увеличить количество эндпоинтов, включить функционал TACACS+ - необходимо обратиться в компанию «Элтекс».

Онлайн подключения к серверу ELM

В случае использования online подключения к публичному серверу лицензирования компании «Элтекс» после внесения изменений в состав лицензии обновление произойдет автоматически, в течение 1 часа.

Если требуется выполнить принудительное обновление лицензии:

1. Перевести текущую лицензию в статус [в статус Backup](#).
2. Выполнить повторно активацию лицензии 

Подключение к Offline ELM

В случае использования Offline ELM сервера потребуется получить в компании «Элтекс» новый файл бандла лицензии с измененным составом лицензии и установить его в Offline ELM.

После загрузке нового бандла лицензии обновление произойдет автоматически, в течение 1 часа. Принудительное обновление параметров лицензии выполняется аналогично как для online подключения.

PLR лицензия

В случае использования PLR лицензии потребуется получить в компании «Элтекс» новый файл лицензии с измененным составом лицензии.

После получения нового файла лицензии необходимо выполнить реактивацию лицензии согласно [Реактивация PLR-лицензии](#).

Полная замена лицензии

При необходимости замены одной лицензии на другую общий алгоритм действий заключается в следующем:

1. Перевести текущую лицензию в статус **Backup**.
2. Загрузить ключ продукта новой лицензии согласно [Загрузка ключа продукта](#).
3. Активировать новую лицензию согласно [Активация лицензии](#).
4. При желании [удалить](#) предыдущую лицензию.

Реактивация PLR-лицензии

Реактивация лицензии - повторная активация файловой лицензии при изменении параметров окружения, к которым привязана лицензия.

Реактивация может потребоваться в следующих случаях:

- Клонирование образа виртуальной машины.
- Изменение конфигурации дисков, оперативной памяти и процессора.
- Переустановка системы, на которой запущено ПО.

Допускается *увеличение* оперативной памяти и количества ядер процессора без необходимости реактивации.

Процедура реактивации похожа на процедуру [активации](#), за тем исключением, что ключ продукта уже загружен. Необходимо выполнить следующие действия:

1. Повторно сформировать файл активации лицензии для изменившегося окружения, выбрав [соответствующее дополнительное действие](#) в таблице "Список лицензий" для нужной лицензии.
2. Передать новый файл активации в компанию «Элтекс».



В случае изменения одного из собираемых параметров окружения уже *после* отправки файла активации сгенерированная лицензия перестанет соответствовать хостовой машине. В этом случае потребуется скачать новый файл активации и приложить его к заявке. Лучше этого не допускать.

3. Получить новый файл лицензии.

4. Файл лицензии необходимо загрузить в систему аналогично [загрузке ключа продукта](#).

Продление PLR лицензии

В связи с особенностями реализации файлового лицензирования требуется периодическое регулярное продление PLR-лицензии.

Процедура продления аналогична процедуре [реактивации](#).

Пользовательское соглашение

Лицензионное соглашение с конечным пользователем (настоящее «Соглашение») содержит информацию о правоотношениях пользователей настоящего программного обеспечения с правообладателем – ООО «Предприятие «ЭЛТЕКС» (ЭЛТЕКС).

1. Настоящее Соглашение представляет собой договор, заключаемый между физическим или юридическим лицом, соглашающимся с настоящими условиями и ООО «Предприятие «ЭЛТЕКС» (ЭЛТЕКС), который регулирует использование конечным пользователем программного обеспечения, встроенных программ, программных интерфейсов, пользовательских интерфейсов и любого другого типа инструкций или кода, предоставленных ЭЛТЕКС, которые сопровождают настоящее Соглашение или ссылаются на него, вместе с любой соответствующей документацией (далее — «Программное обеспечение»).
2. При установке, выполнении или использовании Программного обеспечения иным образом пользователь (i) подтверждает, что прочитал и понимает настоящее Соглашение, (ii) соглашается соблюдать настоящее Соглашение, (iii) подтверждает, что имеет законные права для заключения настоящего соглашения как от физического, так и от юридического лица.
3. Настоящее Соглашение вступает в силу в ту дату, которая наступит ранее, а именно: при установке, запуске или иным образом использовании Программного обеспечения, и заканчивается после прекращения действия в соответствии с настоящим пунктом (далее – «Срок действия»).
4. Настоящее Соглашение автоматически прекращает свое действие без уведомления от ЭЛТЕКС в случае нарушения пользователем любого положения или условия настоящего Соглашения.
5. После прекращения действия настоящего Соглашения пользователь немедленно прекращает использование Программного обеспечения и удаляет (i) Программное обеспечение, (ii) любое другое приложение, предоставленное пользователю от имени ЭЛТЕКС для взаимодействия с Программным обеспечением, и (iii) любой объект, полученный в результате использования Программного обеспечения.
6. Пользователь может расторгнуть настоящее Соглашение, прекратив любое использование Программного обеспечения и удалив Программное обеспечение со своих устройств.
7. При условии соблюдения пользователем условий настоящего Соглашения ЭЛТЕКС предоставляет пользователю ограниченную, отзывную, неисключительную, не подлежащую сублицензии лицензию на использование Программного обеспечения в течение Срока действия исключительно для внутренних целей пользователя (не для дальнейшей передачи прав на Программное обеспечение третьим лицам, не для продажи), а для Программного обеспечения, поставляемого с оборудованием ЭЛТЕКС, — исключительно для целей поддержки оборудования ЭЛТЕКС.

Права собственности, в том числе права на интеллектуальную собственность, в отношении Программного обеспечения принадлежат ЭЛТЕКС.

9. Пользователь не имеет права изменять, распространять, публично демонстрировать, публично исполнять или создавать производные продукты Программного обеспечения.
10. Пользователь не имеет права деассемблировать, детранслировать, декомпилировать, пытаться обнаружить или получить исходный код Программного обеспечения или разрешать это делать другим лицам.
11. Пользователь не имеет права: сдавать в аренду, продавать, передавать в пользование, предоставлять на условиях займа, sublicenzировать, предоставлять услуги коммерческого хостинга с использованием Программного обеспечения или каким-либо иным образом разрешать третьим лицам использовать Программное обеспечение.
12. Пользователь не имеет права: изменять, обходить, деактивировать, ухудшать или блокировать любой программный или аппаратный механизм защиты, который ЭЛТЕКС использует для защиты Программного обеспечения.
13. Пользователь признает, что, если Программному обеспечению требуется доступ к оборудованию или программному обеспечению, не принадлежащим ЭЛТЕКС, для выполнения работы или предоставления функции, и пользователь отказывается от такого разрешения, соответствующие функция или свойство не будут доступны или выполняться должным образом.
14. Для некоторых функций Программного обеспечения может потребоваться доступ к определенному программному обеспечению и/или оборудованию. В тех случаях, когда требуется разрешение, пользователь данным соглашением предоставляет ЭЛТЕКС разрешение в течение Срока действия доступ ко всему программному обеспечению, встроенному в оборудование ЭЛТЕКС, если это необходимо для выполнения Программным обеспечением этих функций.
15. Ничто в этом Соглашении не дает пользователю права на новые версии Программного обеспечения. Если ЭЛТЕКС по своему усмотрению вводит обновления, исправления или корректирующие вставки в Программное обеспечение, доступные в течение Срока действия, без предоставления заменяющих условий, настоящее Соглашение применяется к таким обновлениям, исправлениям и корректирующим вставкам.
16. При условии, что функциональные возможности и функции Программного обеспечения в дальнейшем останутся практически такими же, ЭЛТЕКС может автоматически обновлять Программное обеспечение без согласия пользователя.
17. Пользователь признает и соглашается с тем, что ЭЛТЕКС может в соответствии с законом собирать обезличенные персональные данные, связанные с использованием пользователем Программного обеспечения, включая данные, созданные Программным обеспечением, и/или данные, созданные любым устройством, на котором установлено программное обеспечение, которое взаимодействует с Программным обеспечением.
18. Пользователь признает и соглашается с тем, что ЭЛТЕКС может в соответствии с законом создавать записи агрегированных данных с использованием обезличенных персональных данных.
- 19.

Пользователь признает и соглашается с тем, что ЭЛТЕКС может в соответствии с законом использовать записи агрегированных данных для улучшения Программного обеспечения, разработки нового программного обеспечения или услуг, понимания отраслевых тенденций, создания и публикации технической документации, отчетов или баз данных, обобщающих вышеизложенное, в целях исследования и помощи в решении и/или предотвращении фактической или потенциальной незаконной деятельности и, в целом, для любых законных целей, связанных с коммерческой деятельностью ЭЛТЕКС, а также сохранять обезличенные персональные данные при удалении Программного обеспечения.

20. Письменное согласие с предложением ЭЛТЕКС о замене соглашения об использовании Программного обеспечения и, соответственно, одобрение такой замены может быть дано путем нажатия кнопки, представленной в заменяющем соглашении, или использования Программного обеспечения после представления заменяющего соглашения.
21. Сторонние ресурсы, которые могут быть связаны или доступны через Программное обеспечение, не считаются частью Программного обеспечения, и ЭЛТЕКС может по своему усмотрению отключить интеграцию стороннего ресурса или совместимость Программного обеспечения со сторонним ресурсом.
22. Программное обеспечение предоставляется «как есть» и на условиях как «при наличии». В соответствии с максимально допустимым по закону пределом, ЭЛТЕКС отказывается от всех гарантий, явных, подразумеваемых или законных, включая, в частности, косвенные гарантии коммерческого качества, удовлетворительного качества или качественного соответствия, соответствия конкретным целям, надежности или доступности, точности, отсутствия вирусов, ненарушения прав третьих сторон или иных прав. ЭЛТЕКС не гарантирует, что это программное обеспечение будет работать и оставаться доступным без перебоев или ошибок. Консультация или информация, полученная пользователем от ЭЛТЕКС или его партнеров в письменном или устном виде, никоим образом не влияет на данный отказ от гарантий в отношении программного обеспечения и не создает дополнительных гарантий.
23. Определенный сторонний ресурс может быть включен в программное обеспечение или доступен через программное обеспечение. ЭЛТЕКС не делает никаких заявлений о любом стороннем ресурсе. Поскольку ЭЛТЕКС имеет ограниченный контроль над таким ресурсом или не осуществляет его, пользователь признает и соглашается, что ЭЛТЕКС не несет ответственности за такой ресурс. В частности, пользователь осознает и соглашается с тем, что пользователь осуществляет использование стороннего ресурса на собственный риск и принимает на себя все риски, связанные с неудовлетворительным качеством, работой, точностью или трудозатратами. Пользователь соглашается, что ЭЛТЕКС не несет прямой или косвенной ответственности за любые повреждения и убытки, в том числе любые повреждения или утрату данных в результате или предположительно в результате, либо в связи с использованием или расчетом на его надежность, стороннего ресурса, доступного в таком программном обеспечении или через него. Пользователь осознает и соглашается с тем, что на использование любого стороннего ресурса распространяются условия, лицензионное соглашение, политика конфиденциальности или другие подобные соглашения, а также, что на любую информацию или персональные данные, предоставляемые пользователем осознанно или неосознанно поставщикам таких ресурсов, будет распространяться политика о конфиденциальности третьей стороны, если таковая существует. ЭЛТЕКС не несет ответственности за раскрытие информации и любые другие действия третьей стороны. В частности, ЭЛТЕКС не дает никаких гарантий в отношении получения данных пользователя

третьей стороной и использования персональной информации пользователя такой третьей стороной.

24. Ни при каких обстоятельствах ЭЛТЕКС не несет никакой ответственности перед пользователем или третьей стороной за ущерб, нанесенный в связи с использованием или доступом к любому компоненту программного обеспечения или невозможностью использовать или получать доступ к любому компоненту программного обеспечения, включая, в частности, ущерб, возникающий в результате ошибок, пропусков, остановок, дефектов, задержек работы или передачи, компьютерных вирусов и любых других прямых, не прямых, фактических, случайных, штрафных или косвенных убытков, даже если ЭЛТЕКС был осведомлен о возможности их возникновения. Несмотря на вышесказанное, совокупная ответственность ЭЛТЕКС за все убытки, повреждения, основания для предъявления исков, в том числе на основании договорной, деликтной или иной ответственности, возникающие в связи с использованием программного обеспечения либо в связи с какими-либо положениями настоящего соглашения, не может превышать справедливой рыночной стоимости этого компонента программного обеспечения.
25. Вышеуказанные ограничения, исключения и отказы от ответственности в настоящем соглашении применяются в максимально допустимой действующим законодательством степени, даже если примененное средство правовой защиты не достигает своей основной цели.
26. В случае нарушения пользователем любого положения настоящего Соглашения, ЭЛТЕКС вправе взыскать с пользователя денежную компенсацию понесенных убытков.
27. Настоящее Соглашение регулируется законодательством Российской Федерации.

Настройки аккаунта

Описание

На данной странице доступен просмотр/редактирование учетных данных текущего пользователя системы (под учетной записью которого был выполнен вход в систему), а также смена языка интерфейса.

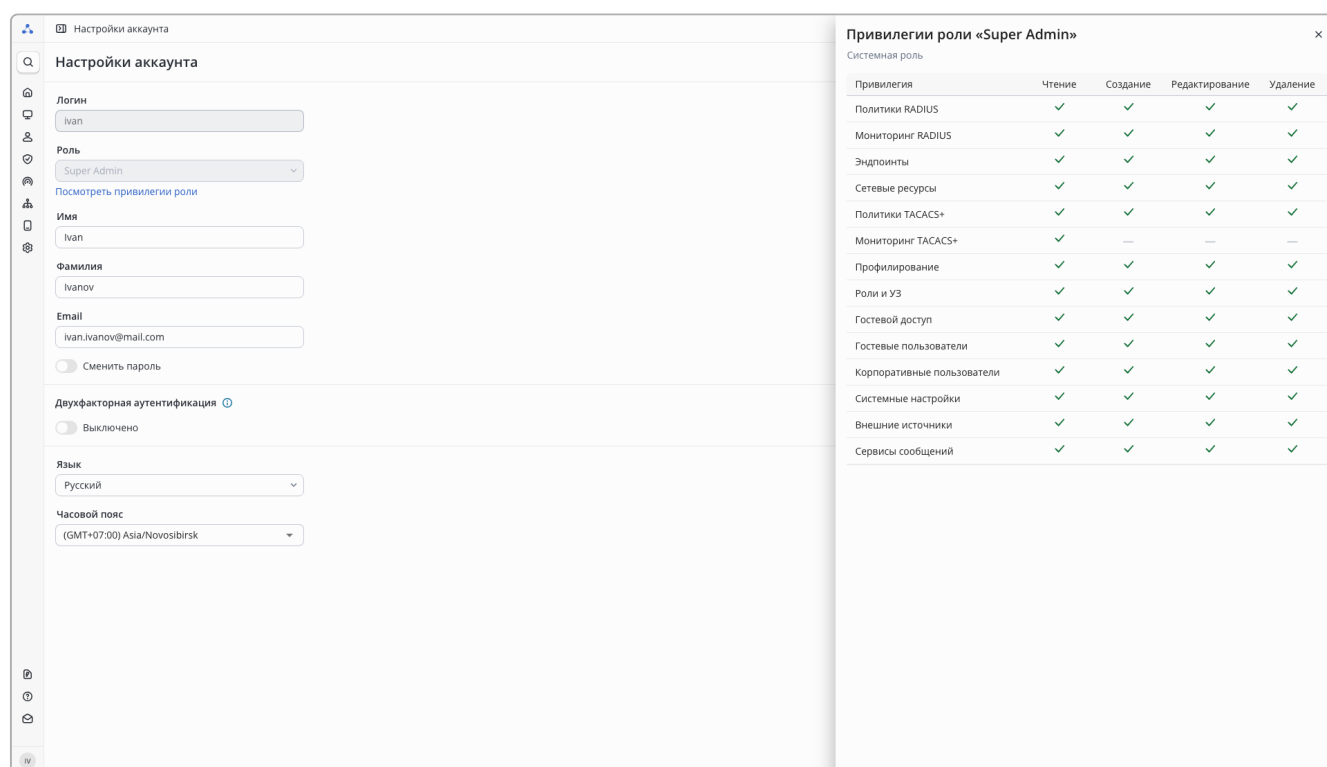


Если вход был выполнен под внешним пользователем системы будет доступно редактирование только полей **языка** и **часового пояса**.

Настройка часового пояса влияет на отображаемое время последней активности эндпоинта при мониторинге подключений, время указанное в наименовании экспортируемого файла и время в виджетах на дашборде.

Просмотр/редактирование учетных данных пользователя системы

Настройки аккаунта текущего пользователя системы доступны на любой странице при нажатии на  нижнем левом углу меню.



Привилегия	Чтение	Создание	Редактирование	Удаление
Политики RADIUS	✓	✓	✓	✓
Мониторинг RADIUS	✓	✓	✓	✓
Эндпоинты	✓	✓	✓	✓
Сетевые ресурсы	✓	✓	✓	✓
Политики TACACS+	✓	✓	✓	✓
Мониторинг TACACS+	✓	—	—	—
Профилирование	✓	✓	✓	✓
Роли и УЗ	✓	✓	✓	✓
Гостевой доступ	✓	✓	✓	✓
Гостевые пользователи	✓	✓	✓	✓
Корпоративные пользователи	✓	✓	✓	✓
Системные настройки	✓	✓	✓	✓
Внешние источники	✓	✓	✓	✓
Сервисы сообщений	✓	✓	✓	✓

Рисунок 454. Настройка аккаунта текущего пользователя системы

Форма настройки аккаунта пользователя системы включает в себя следующие поля:

- **Логин** — Логин текущего пользователя системы;
- **Роль** — Уровень доступа к функционалу системы, определяющий права пользователя системы;
- **Имя** — Личное имя пользователя системы (максимальная длина - 100 символов);

Фамилия — Фамилия пользователя системы (максимальная длина - 100 символов);

- **Email** — Электронная почта (максимальная длина - 200 символов);
- **Язык** — Язык интерфейса системы (поддержаны Русский и Английский);
- **Часовой пояс** — Временная зона для отображения времени в системе.

С помощью кнопки ["Посмотреть привилегии роли"](#) есть возможность раскрыть окно с таблицей привилегий и выданных на них уровней прав для выбранной роли.

Таблица просмотра привилегий и уровней прав на них, включает в себя:

- **Привилегия** - наименование привилегии;
- **Чтение, Создание, Редактирование, Удаление** - уровни доступа.
- **Статусы выданных прав** :
 -  - у пользователя системы есть доступ,
 -  - доступ не предусмотрен,
 -  - у пользователя системы нет доступа.

Для изменения пароля текущего пользователя системы необходимо включить переключатель **"Сменить пароль"**, после чего ввести текущий и желаемый пароль в соответствующие поля. Пароль должен соответствовать текущей [парольной политике](#).

- **Текущий пароль *** — пароль, под которым был выполнен текущий вход в систему;
- **Новый пароль *** (максимальная длина - 72 символа). По нажатию на  можно включить отображение вводимого пароля, по умолчанию текст скрыт;
- **Подтверждение нового пароля *** (максимальная длина - 72 символа).

Рисунок 455. Смена пароля для текущего пользователя системы



После сохранения изменений **для пароля** сессия прервется — потребуется повторная авторизация.

После внесения изменений необходимо нажать кнопку "**Сохранить**". Кнопка скрыта, пока не будет изменено хотя бы одно поле.

После сохранения формы будет произведен возврат на страницу, с которой был выполнен переход в Настройки аккаунта.

Кнопка "**Отмена**" осуществляет сброс внесенных изменений до исходного состояния.

Смена текущего пользователя системы (выход из системы)

Для выхода из системы на любой странице необходимо нажать на иконку профиля  в нижнем левом углу и выбрать "**Выход**".

Далее необходимо подтвердить выход из системы, нажав кнопку "**Выйти**".