

NAICE

Версия: 0.8-10066  
Дата публикации: 28.03.2025

# Содержание

Начальная страница .....	1
Администрирование .....	0
Администраторы .....	15
Сетевые ресурсы .....	20
Устройства .....	20
Группы устройств .....	24
Профили устройств .....	29
Управление идентификацией .....	37
Пользователи сети .....	37
Группы пользователей сети .....	42
Эндпоинты .....	45
Группы эндпоинтов .....	51
Внешние источники идентификации .....	56
Цепочки идентификаций .....	79
Контроль сетевых устройств .....	84
Элементы политик .....	0
Условия .....	84
Наборы команд TACACS .....	92
Профили TACACS .....	98
Политики сетевых устройств .....	101
Настройка политики контроля сетевых устройств .....	106
Политики доступа .....	0
Элементы .....	0
Разрешенные протоколы .....	112
Профили авторизации .....	115
Словари .....	119
Условия .....	121
Наборы политик .....	129
Политики аутентификации и авторизации .....	136
Профилирование .....	141
Условия профилирования .....	141
Политики профилирования .....	146
Логические профили .....	155
Мониторинг .....	0
RADIUS .....	0
Пользовательские сессии .....	159
TACACS .....	0
Журнал подключений .....	163
Лицензирование .....	168

# Начальная страница

## 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 администратора;
- Все изменения в расположении и составе набора виджетов применяются только к текущему администратору;
- 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

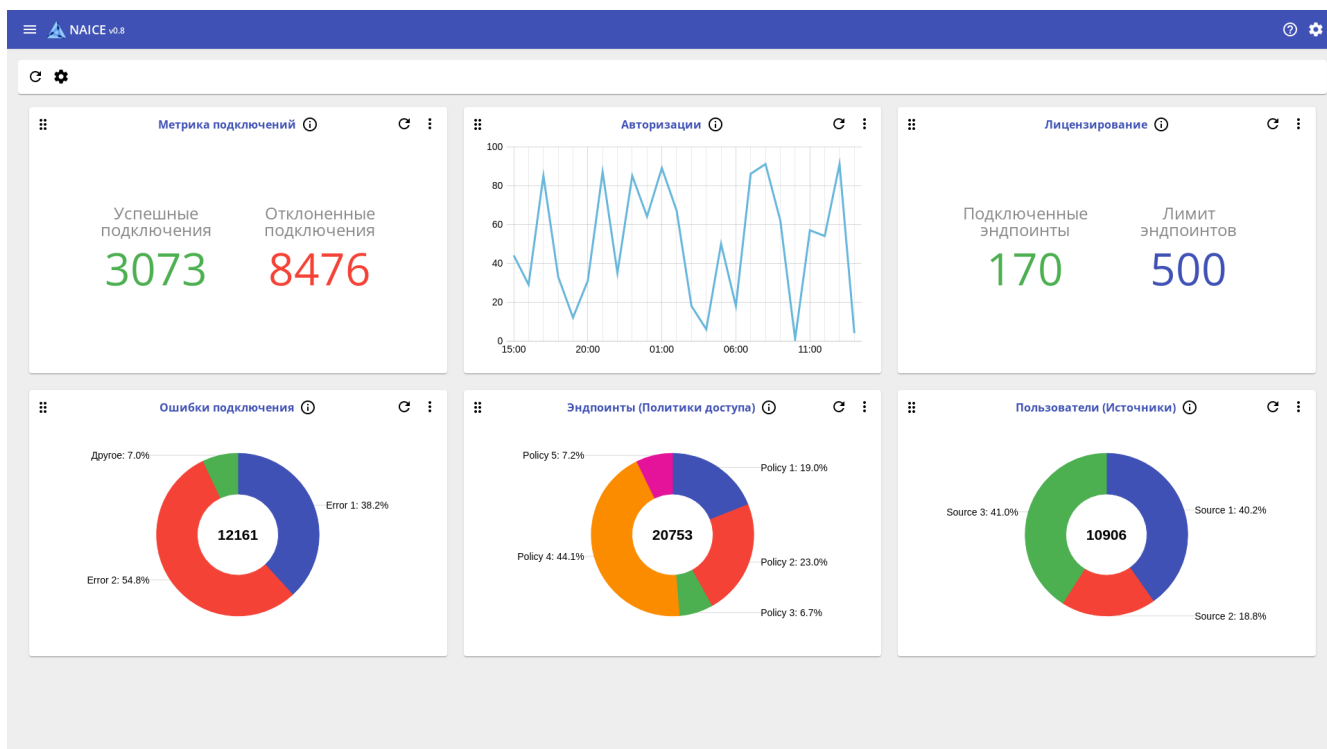








Рисунок 1. Панель управления дашбордом и виджеты, отображаемые на нем


Элементы управления дашбордом:

-  - Обновить данные для всех виджетов, представленных на дашборде.
-  - 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.
-  - 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 , после чего откроется окно **Настройки панели дашборда**:

### Настройки панели дашборда

- |  |  |
|--|--|
| <input checked="" type="checkbox"/>  Авторизации                  | <input type="checkbox"/>  Эндпоинты (Группы)                  |
| <input checked="" type="checkbox"/>  Эндпоинты (Политики доступа) | <input type="checkbox"/>  Эндпоинты (Политики профилирования) |
| <input type="checkbox"/>  Устройства (Тип)                        | <input type="checkbox"/>  Устройства (Локации)                |
| <input checked="" type="checkbox"/>  Пользователи (Источники)     | <input checked="" type="checkbox"/>  123 Лицензирование       |
| <input checked="" type="checkbox"/>  Ошибки подключения           | <input type="checkbox"/>  123 Всего эндпоинтов                |
| <input checked="" type="checkbox"/>  123 Метрика подключений      | <input type="checkbox"/>  Наборы политик                      |


Сбросить настройки

Сохранить

Отменить

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.
- Сбросить настройки - 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.

## Список доступных виджетов

Виджет	Тип отображения данных	Краткое описание виджета
Авторизации	График	Количество авторизаций за последние сутки по часам
Лицензирование	Метрика с двумя числами	Текущее количество подключённых эндпоинтов и максимально разрешённое согласно лицензии
Метрика Подключений	Метрика с двумя числами	Количество успешных и отклоненных подключений за последние сутки
Метрика Всего эндпоинтов	Метрика с одним числом	Общее количество изученных эндпоинтов
Устройства (Тип)	Гистограмма	Количество сетевых устройств, через которые происходило подключение клиента, по типам сетевых устройств
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 доступа)	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



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

## 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 настройки" в окне [Настройки панели дашборда](#).

Стандартный набор включает в себя следующие виджеты:

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

## 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.

### Виджет "Авторизации"

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

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.

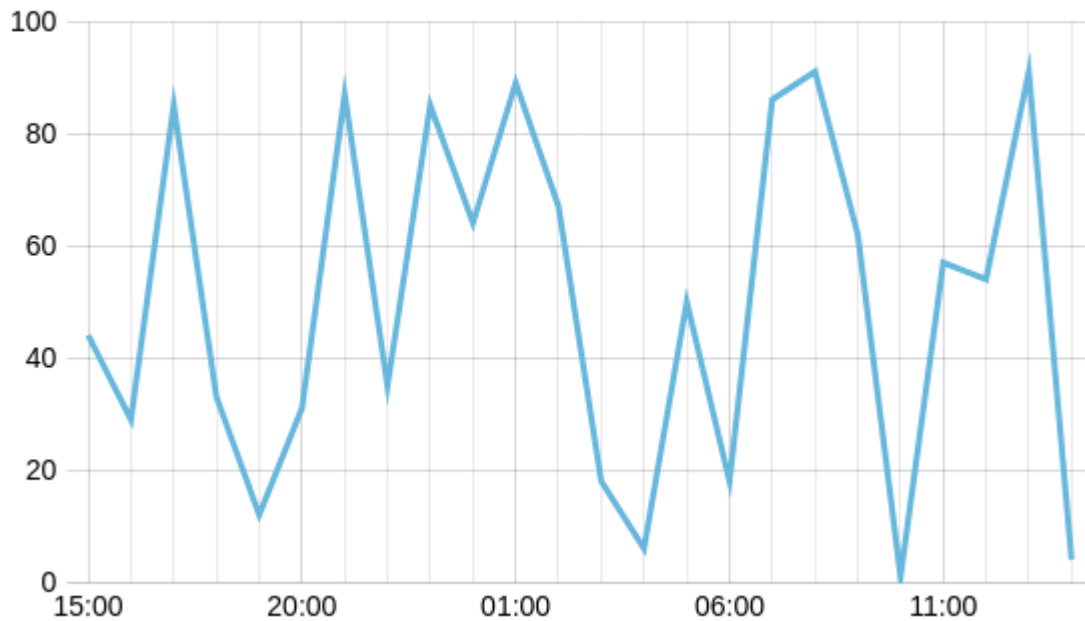


Рисунок 3. Виджет "Авторизации"

## Виджеты с типом отображения — Метрика 123

Функциональные возможности:

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

## 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 4. Виджет "Лицензирование"

### Виджет "Метрика подключений"

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

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

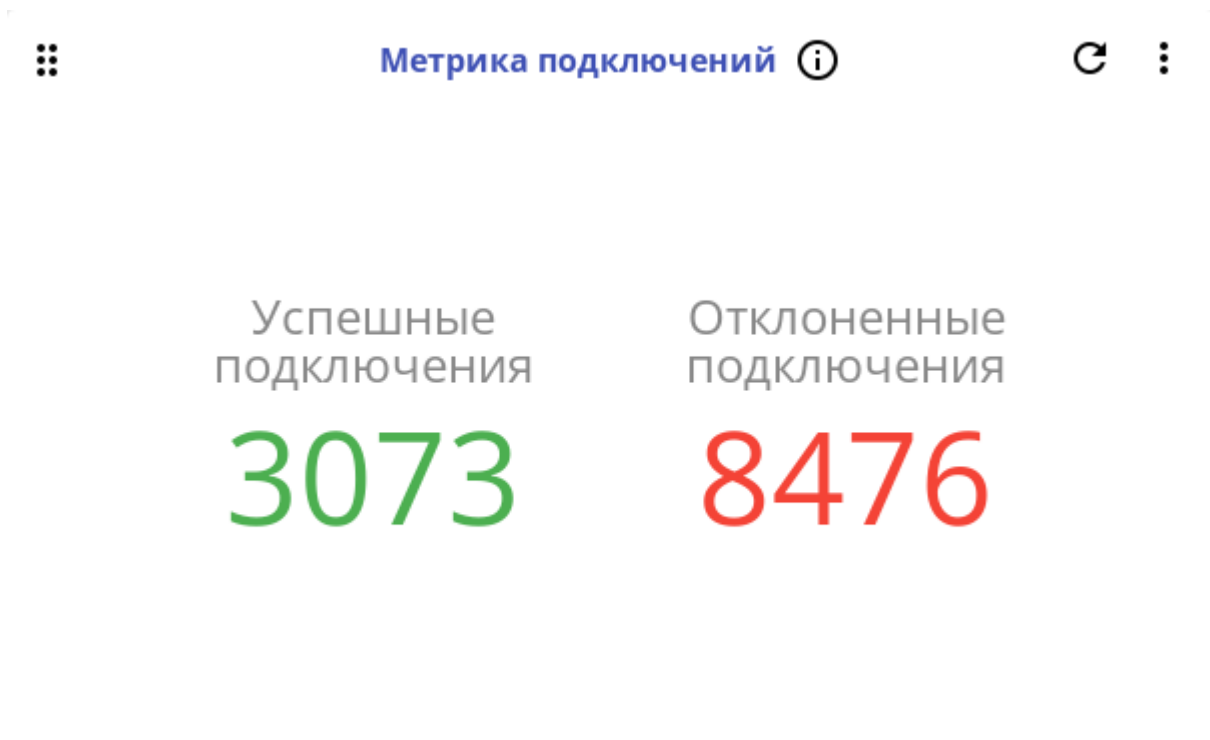


Рисунок 5. Виджет "Метрика подключений"

## Виджет "Всего эндпоинтов"

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

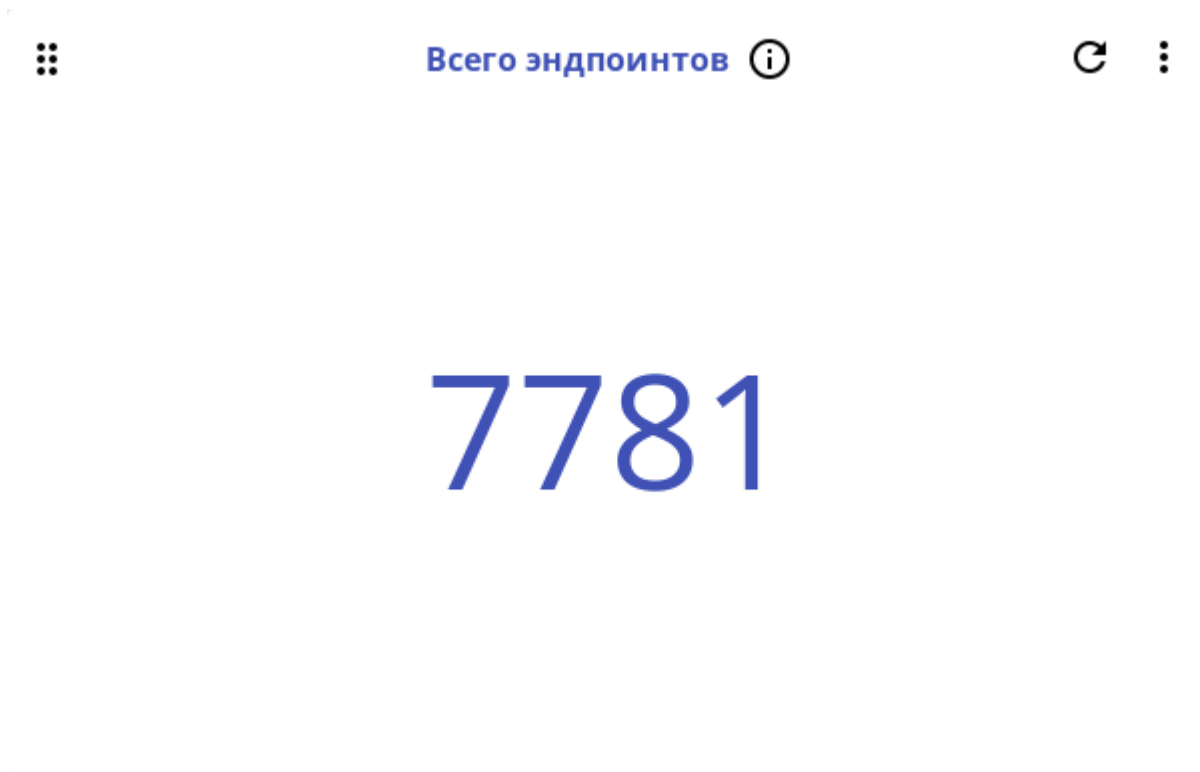


Рисунок 6. Виджет "Всего эндпоинтов"

## 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.

## 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 7. 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 8. Виджет "Устройства (Локации)"

## 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.

### Виджет "Эндпоинты (Группы)"

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

Данные для виджета берутся из таблицы [Эндпоинты](#) и [Пользовательских сессий](#).

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](#).

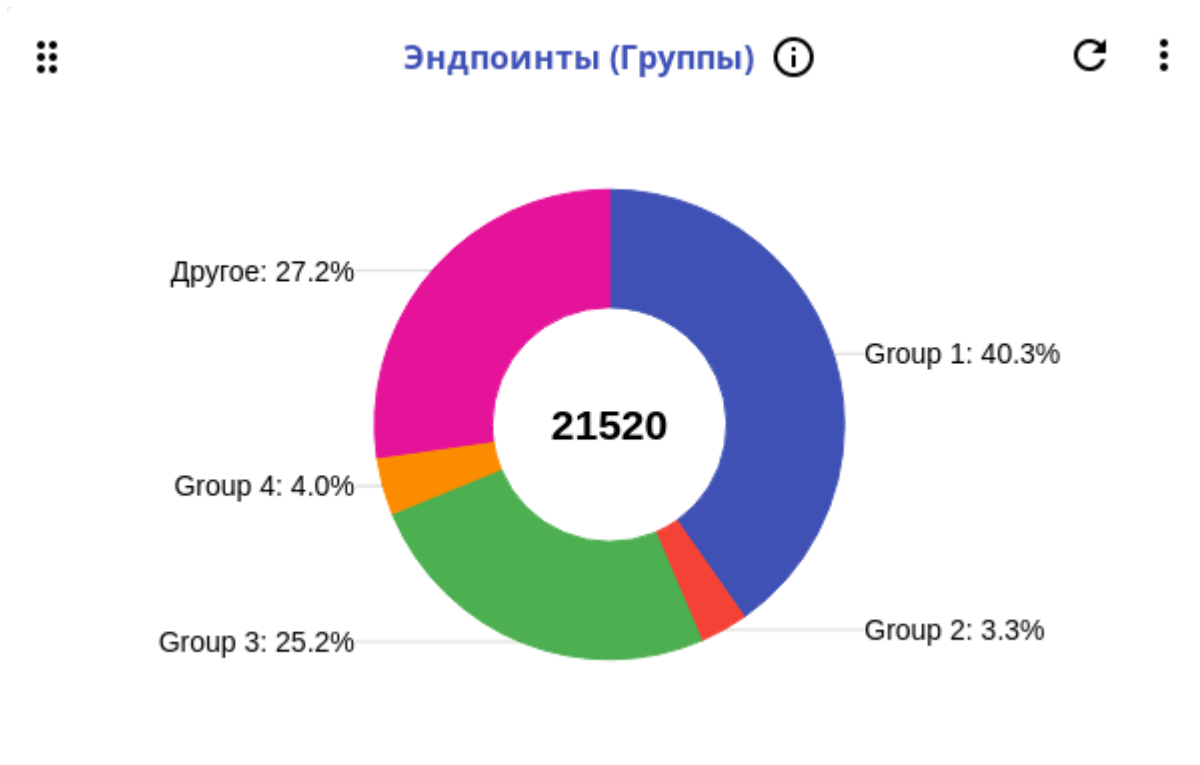


Рисунок 9. Виджет "Эндпоинты (Группы)"

## 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 [Пользовательских сессий](#).

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](#).

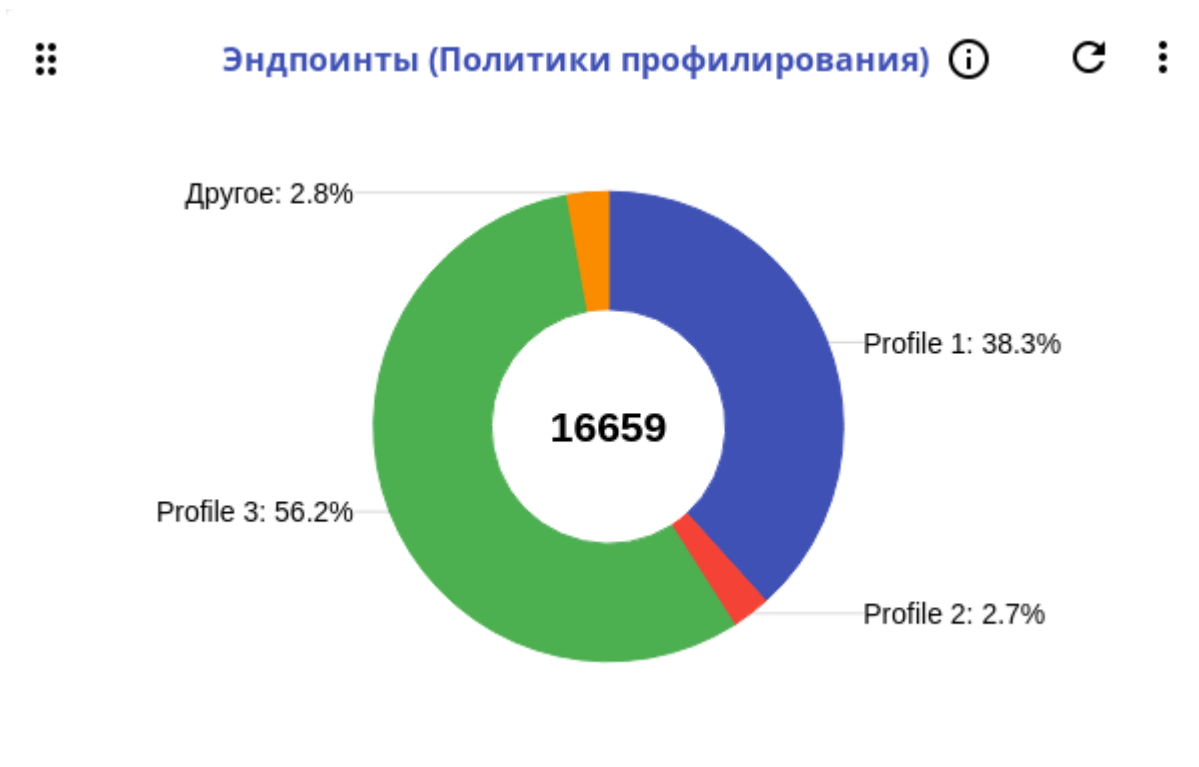


Рисунок 10. Виджет "Эндпоинты (Политики профилирования)"

## Виджет "Эндпоинты (Политики доступа)"

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

Данные для виджета берутся из таблицы [Эндпоинты](#) и [Пользовательских сессий](#).

Виджет позволяет оценить распределение эндпоинтов по политикам доступа.

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](#).

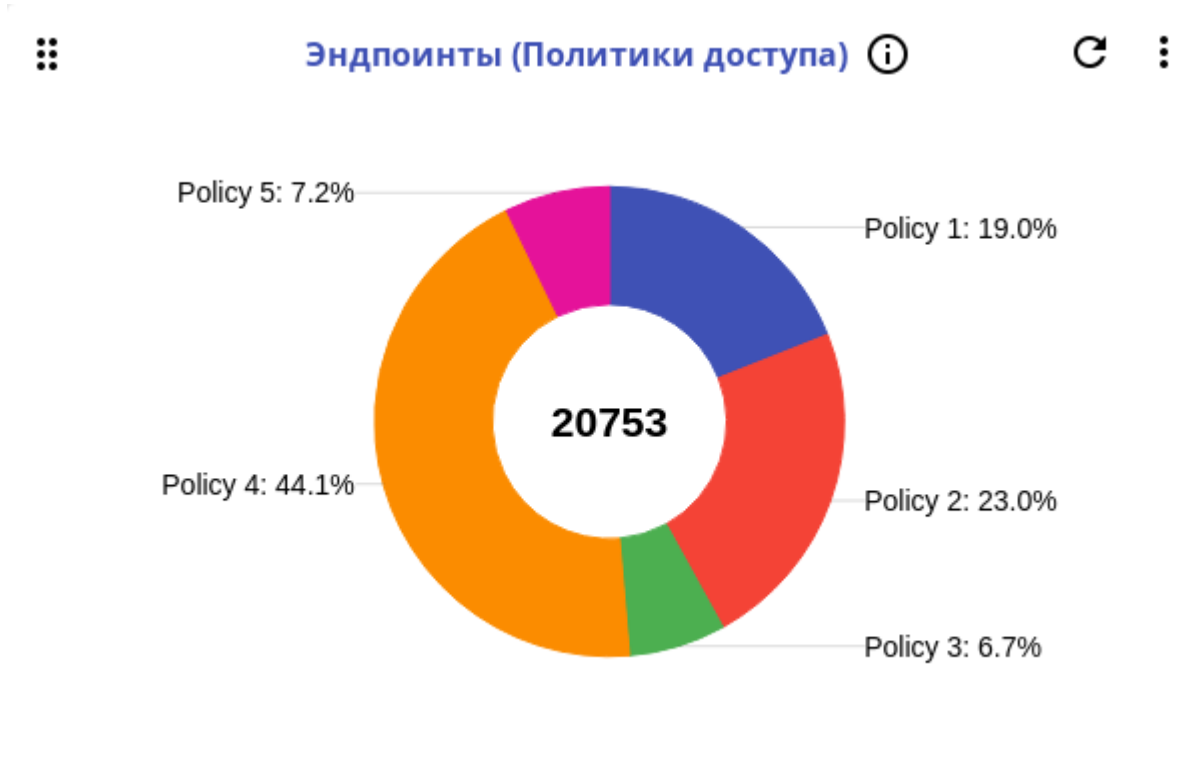


Рисунок 11. Виджет "Эндпоинты (Политики доступа)"

## 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.

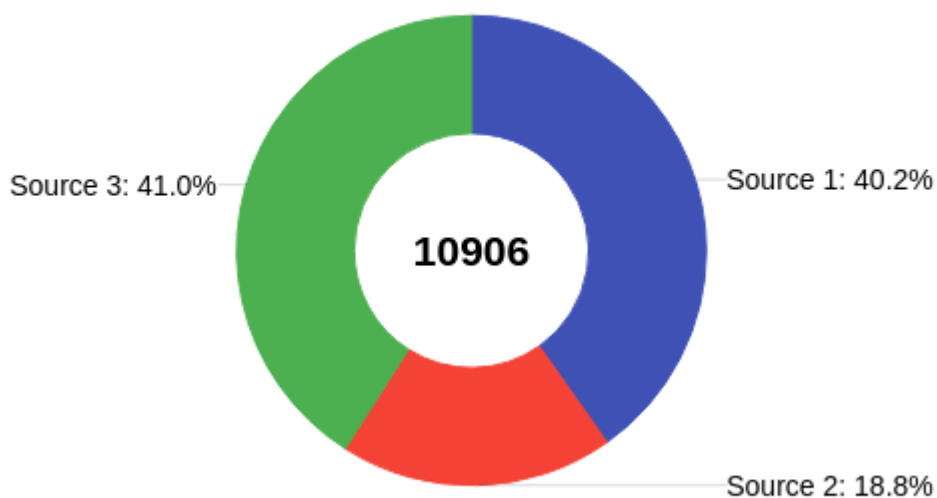


Рисунок 12. Виджет "Пользователи (Источники)"

### 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.



## Наборы политик

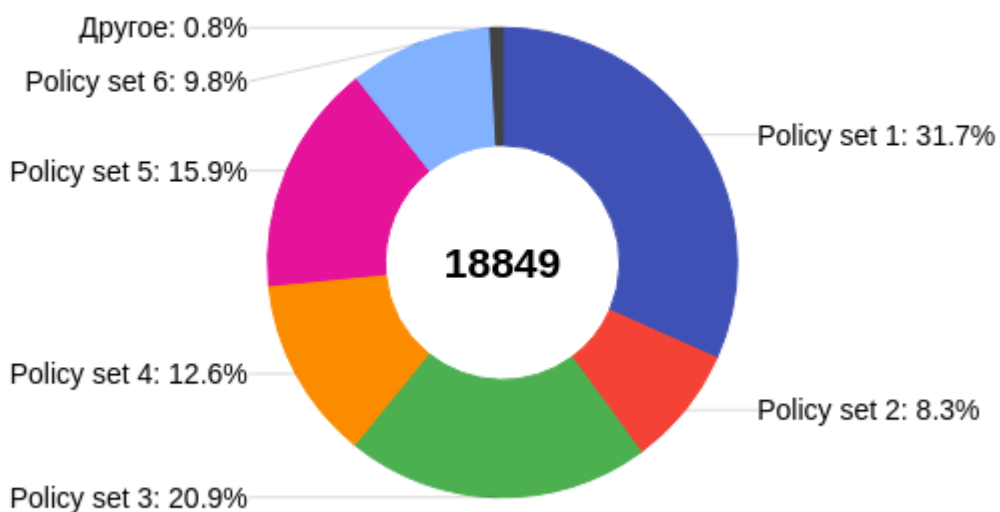


Рисунок 13. Виджет "Наборы политик"

## Виджет "Ошибки подключения"

Виджет отображает ошибки подключения клиентов за последние сутки.

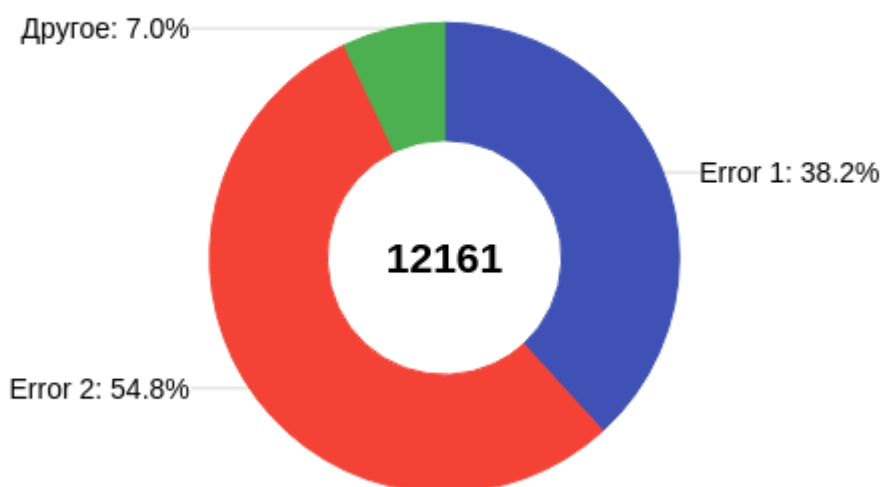
Отклонённые политикой доступа подключения не учитываются.

Данные по возникшим ошибкам берутся из [Пользовательских сессий](#).

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



## Ошибки подключения



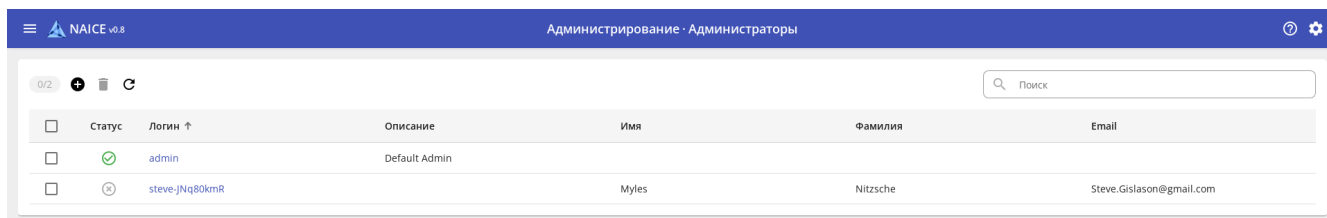
*Рисунок 14. Виджет "Ошибки подключения"*

# Администрирование

## Администраторы

Раздел "Администраторы" предназначен для управления учётными данными администраторов NAICE.

### Просмотр учетных записей администраторов



<input type="checkbox"/>	Статус	Логин ↑	Описание	Имя	Фамилия	Email
<input type="checkbox"/>	✓	admin	Default Admin			
<input type="checkbox"/>	⊗	steve-jNq80kmR		Myles	Nitzsche	Steve.Gislason@gmail.com

Рисунок 15. Таблица с перечнем администраторов на странице просмотра

На данной странице содержится таблица со списком всех администраторов системы.

Таблица содержит следующую информацию об администраторах системы:

- **Статус** - управляет разрешением на вход в систему: выключенный администратор не сможет авторизоваться;
- **Логин** - логин администратора (должен быть уникальным);
- **Описание** - произвольное описание;
- **Имя** - имя администратора;
- **Фамилия** - фамилия администратора;
- **Email** - адрес электронной почты администратора.

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

Элементы управления:

- **0/1** - Счетчик выбранных чекбоксом элементов / общего количества элементов.
- **+** - Добавить новый элемент.
- **🗑** - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- **↻** - Обновить данные таблицы.
- **🔍 Поиск** - Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
- **↑** - Изменить текущий порядок сортировки.
- - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).

## Добавление учетной записи администратора

Для добавления учетной записи администратора нажмите  на панели действий, расположенной над таблицей.

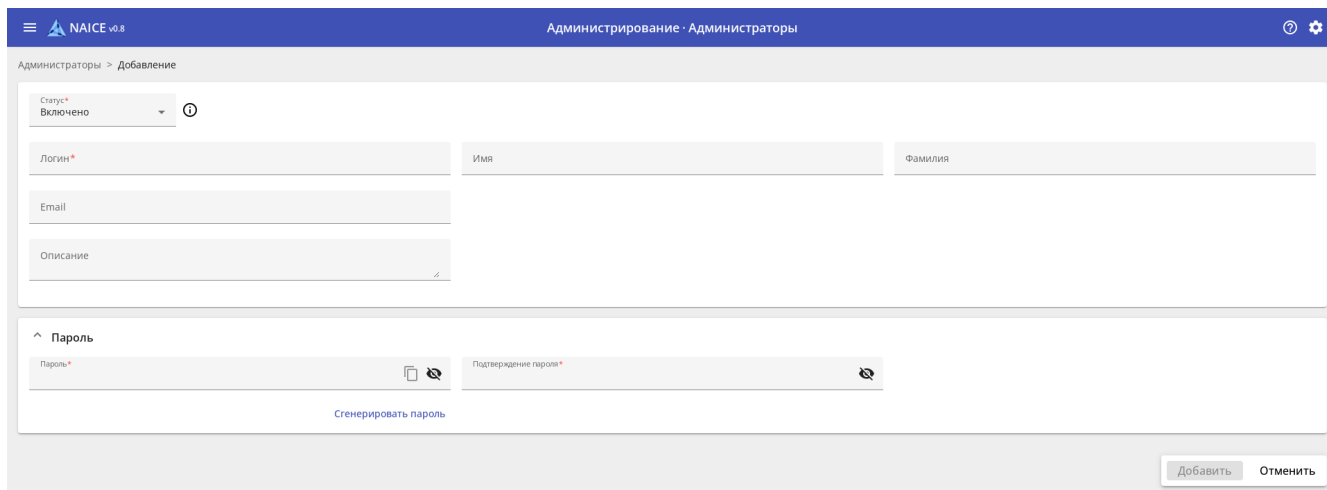



Рисунок 16. Страница добавления администратора

Форма добавления администратора включает в себя следующие поля:

- **Статус \*** - включение или выключение возможности авторизации в системе данной учетной записи;
- **Логин \*** (максимальная длина - 100 символов);
- **Имя** (максимальная длина - 100 символов);
- **Фамилия** (максимальная длина - 100 символов);
- **Email** (максимальная длина - 100 символов);
- **Описание** (максимальная длина - 250 символов);
- **Пароль** (максимальная длина - 100 символов);
- **Подтверждение пароля** (максимальная длина - 100 символов).

\* - поля, обязательные для заполнения.

Пароль для входа в учетную запись администратора можно сгенерировать, нажав на кнопку "**Сгенерировать пароль**", либо указать вручную. Сгенерированный пароль помещается в поля "Пароль" и "Подтверждение пароля", его можно скопировать по клику на .

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

## Редактирование учетной записи администратора

Для редактирования учетной записи администратора необходимо на странице со списком нажать на его логин:

<input type="checkbox"/>	Статус	Логин ↑
<input type="checkbox"/>		admin
<input type="checkbox"/>		steve-JNq80kmR

Рисунок 17. Гиперссылка на страницу редактирования администратора

После этого откроется страница редактирования администратора, аналогичная странице добавления:

Рисунок 18. Страница изменения администратора

После редактирования нажать на кнопку **"Сохранить"**. Кнопка остается неактивной, пока не будет изменено хотя бы одно поле.

## Удаление учетной записи администраторов

Для удаления учетной записи администратора в окне со списком администраторов надо выделить чекбокс слева от учетных записей, которые требуется удалить и нажать кнопку вверху слева.

<input type="checkbox"/>	Статус	Логин ↑	Описание	Имя	Фамилия	Email
<input type="checkbox"/>		admin	Default Admin			
<input checked="" type="checkbox"/>		steve-JNq80kmR		Myles	Nitzsche	Steve.Gislason@gmail.com

Рисунок 19. Выбор администраторов в таблице для удаления



Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.

## Подтверждение действия


Данные будут удалены. Вы уверены?

Рисунок 20. Модальный диалог подтверждения



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

## Настройка аккаунта текущего администратора

Настройки аккаунта текущего администратора доступны на любой странице при нажатии на  в вернем правом углу окна в подменю "Настройки аккаунта".

На данной странице доступен просмотр учетных данных текущего администратора (с учетной записью которого выполнен вход в систему), а также смена языка интерфейса. Поддержаны следующие языки: русский, английский.

Настройка часового пояса влияет на отображаемое время последней активности эндпоинта при мониторинге подключений.

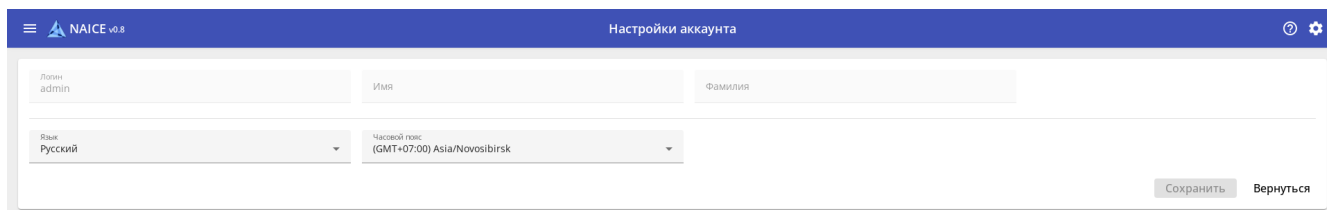



Рисунок 21. Настройка аккаунта текущего администратора

Кнопка "Сохранить" сохраняет внесенные в аккаунт изменения, кнопка "Вернуться" осуществляет возврат на страницу, с которой был выполнен переход в Настройки аккаунта.

## Смена текущего администратора (выход из системы)

Для выхода из системы на любой странице необходимо нажать на  в вернем правом углу окна и выбрать подменю "Выход".

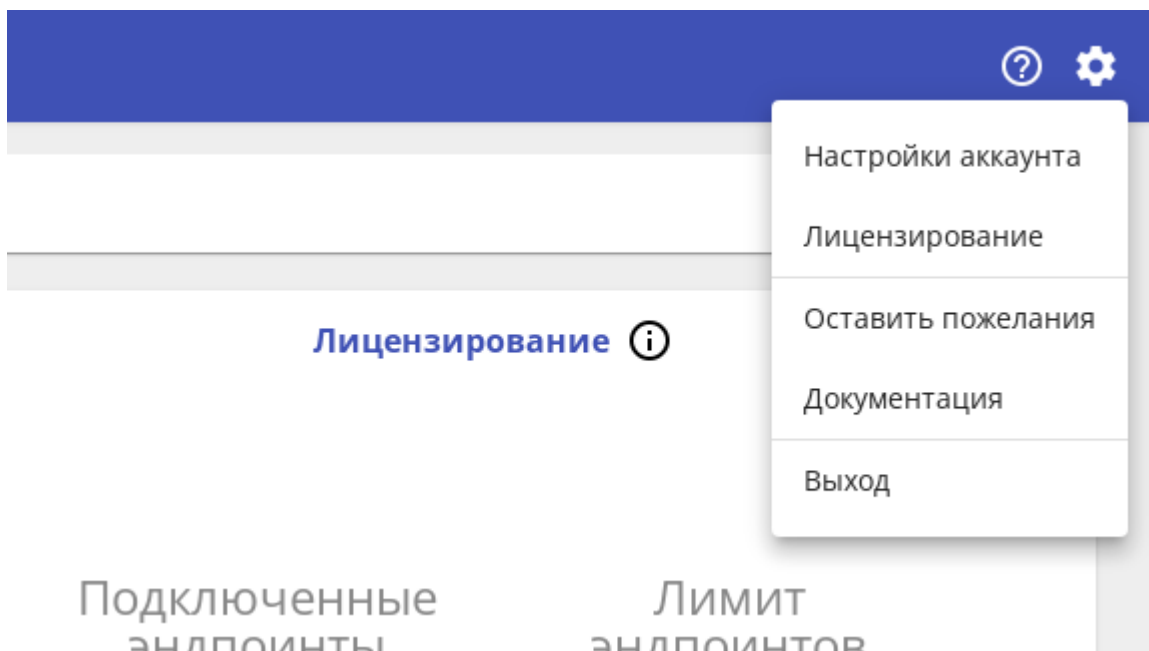


Рисунок 22. Пункт меню Выход

Далее необходимо подтвердить выход из системы, нажав на кнопку **"Выйти"**.

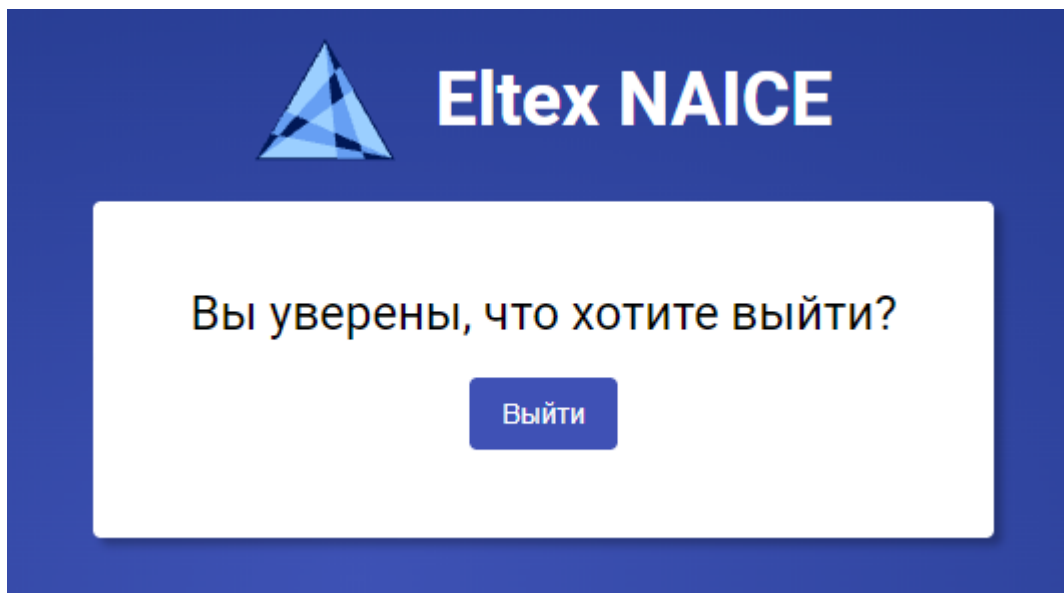


Рисунок 23. Страница подтверждения выхода из системы

После чего произойдет перенаправление на страницу авторизации.

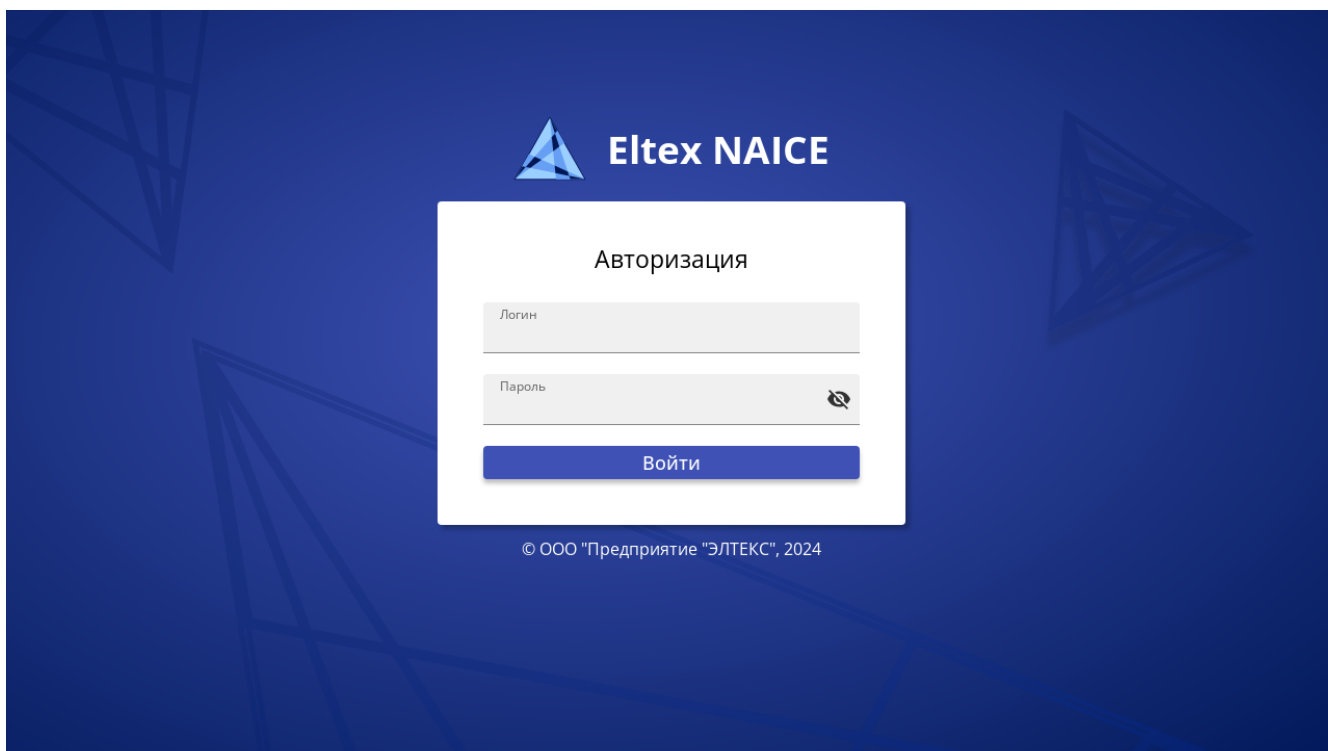


Рисунок 24. Страница авторизации в системе

## Сетевые ресурсы

Сетевое устройство (authenticator, NAS - Network Attached Storage) - 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 *"Администрирование"* → *"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 протоколу RADIUS.

## Устройства

### Описание

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

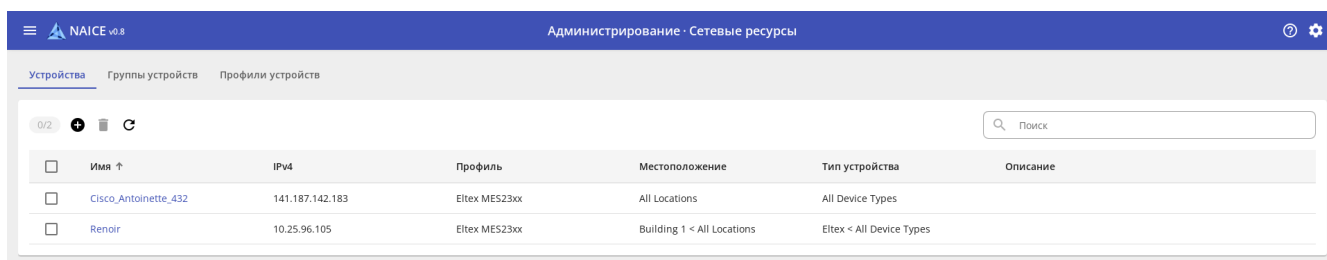
Раздел "Устройства" отвечает за просмотр, добавление, удаление, редактирование сетевых устройств в системе NAICE.



**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



<input type="checkbox"/>	Имя ↑	IPv4	Профиль	Местоположение	Тип устройства	Описание
<input type="checkbox"/>	Cisco_Antoinette_432	141.187.142.183	Etetx ME523xx	All Locations	All Device Types	
<input type="checkbox"/>	Renoir	10.25.96.105	Etetx ME523xx	Building 1 < All Locations	Etetx < All Device Types	

Рисунок 25. 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 устройства.
- **Местоположение** — группа, определяющая местоположение устройства.
- **Тип устройства** — группа, определяющая тип устройства.
- **Описание** — произвольное описание устройства.

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:

- **0/1** - Счетчик выбранных чекбоксом элементов / общего количества элементов.
- **+** - Добавить новый элемент.
- **🗑** - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- **↻** - Обновить данные таблицы.
- **🔍 Поиск** - Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
- **↑** - Изменить текущий порядок сортировки.
- - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).



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 .

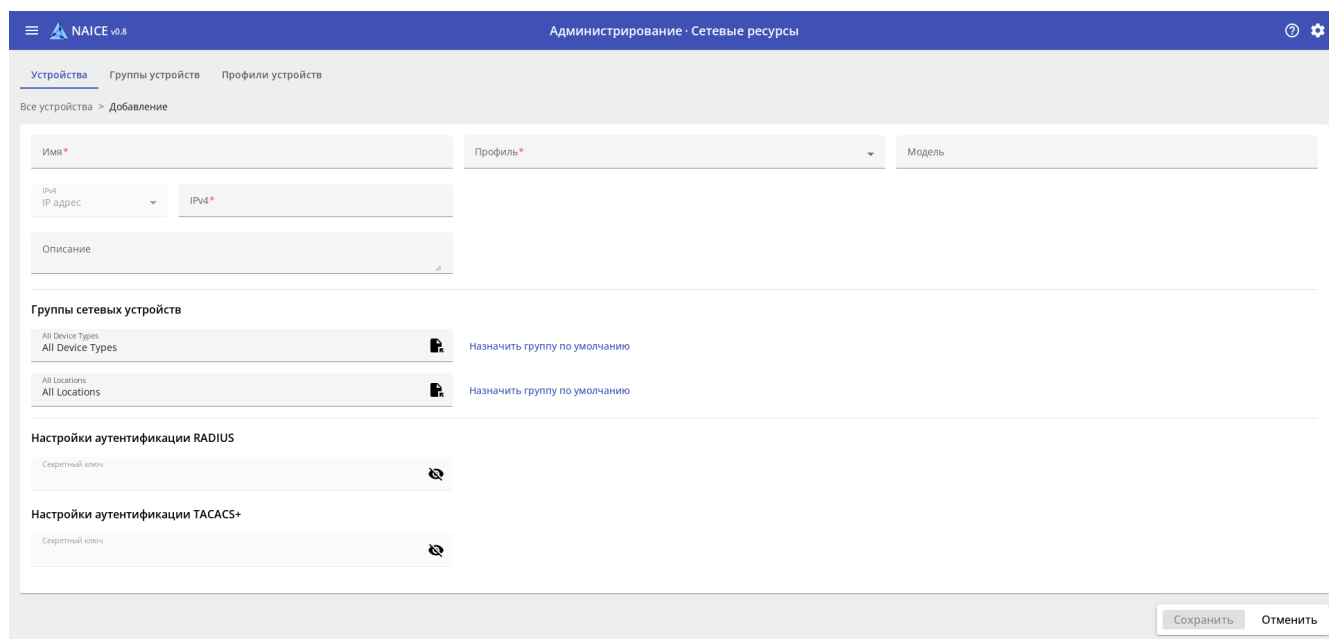


Рисунок 26. Страница добавления сетевого устройства

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. Длина от 8 до 200 символов.

**Настройка аутентификации TACACS+** содержит:

- **Секретный ключ \*** для взаимодействия с сетевым устройством по протоколу TACACS+. Длина от 8 до 200 символов.

Параметры, отмеченные звездочкой \*, обязательны для заполнения.

После ввода необходимых данных нажмите кнопку "Сохранить".

## Редактирование сетевого устройства

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

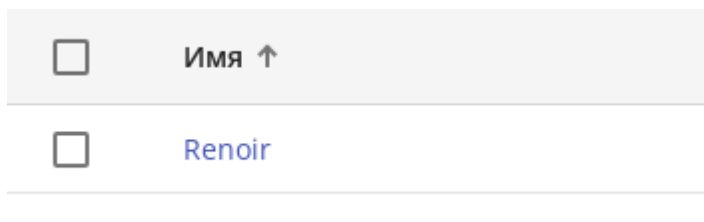


Рисунок 27. Гиперссылка на страницу редактирования устройства

После этого откроется окно редактирования, аналогичное странице добавления.

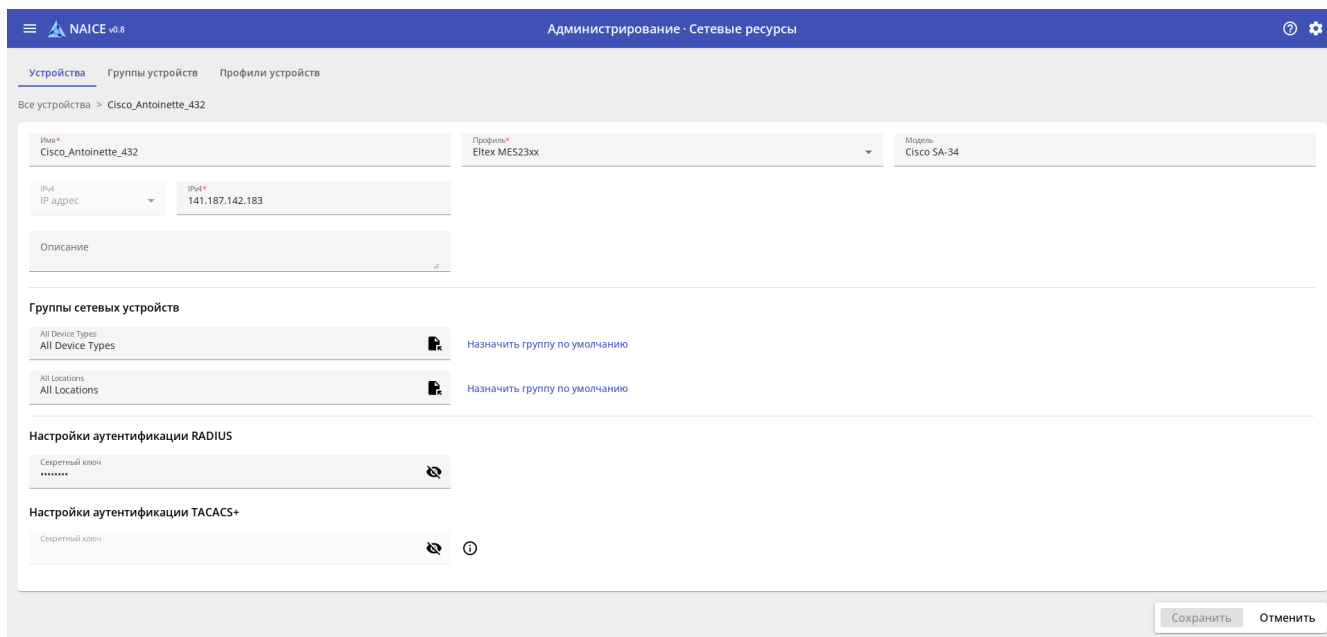



Рисунок 28. Страница редактирования устройства



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 нажать на кнопку "Сохранить". Кнопка остается неактивной, пока не будет изменено хотя бы одно поле.

## 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.

Имя ↑	IPv4	Профиль	Местоположение	Тип устройства	Описание
<input checked="" type="checkbox"/> Cisco_Antoinette_432	141.187.142.183	Etex ME523xx	All Locations	All Device Types	
<input type="checkbox"/> Renoir	10.25.96.105	Etex ME523xx	Building 1 < All Locations	Etex < All Device Types	

Рисунок 29. Выбор устройства в таблице для удаления



Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.



### Подтверждение действия

Данные будут удалены. Вы уверены?

Рисунок 30. Модальный диалог подтверждения

## Группы устройств

### Описание

Группы устройств предназначены для агрегации [сетевых устройств](#) по различным признакам, с дальнейшей возможностью определения различных сценариев авторизации для разных групп в [наборах политик](#).

### Просмотр групп

На данной странице содержится таблица со списком всех групп.

Имя	Описание	Устройства
<input type="checkbox"/> > All Device Types	Default Device Type group	-
<input type="checkbox"/> > All Locations	Default Location group	-

Рисунок 31. 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;
- **Описание** - произвольное описание группы;
- **Устройства** - количество устройств в группе; для корневых групп количество устройств не отображается.

Сортировка не предусмотрена.

Элементы управления:

-  - раскрыть все группы.
-  - обновить данные таблицы.
-  - показать устройства группы и ее подгрупп (неактивно, пока не выбрана группа).
-  - добавить группу.
-  - удалить группу (неактивно, пока не выбрана группа).
-  - 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.

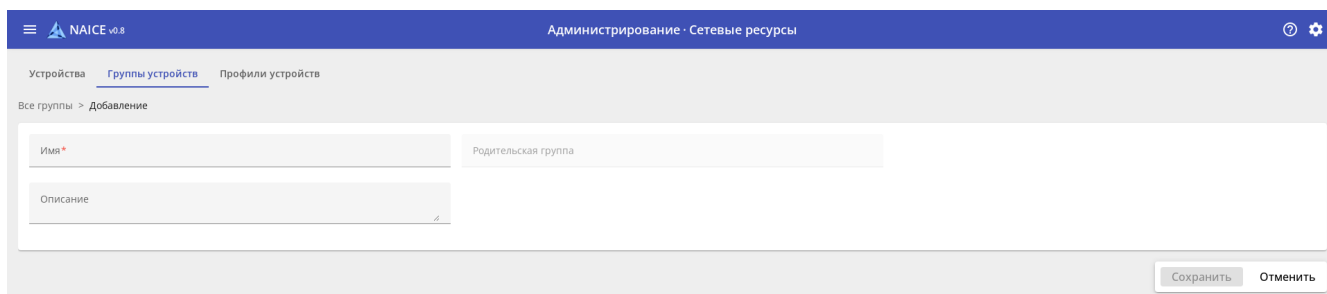


Рисунок 32. Страница добавление группы

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 "Сохранить".

## Добавление подгруппы в существующую группу

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

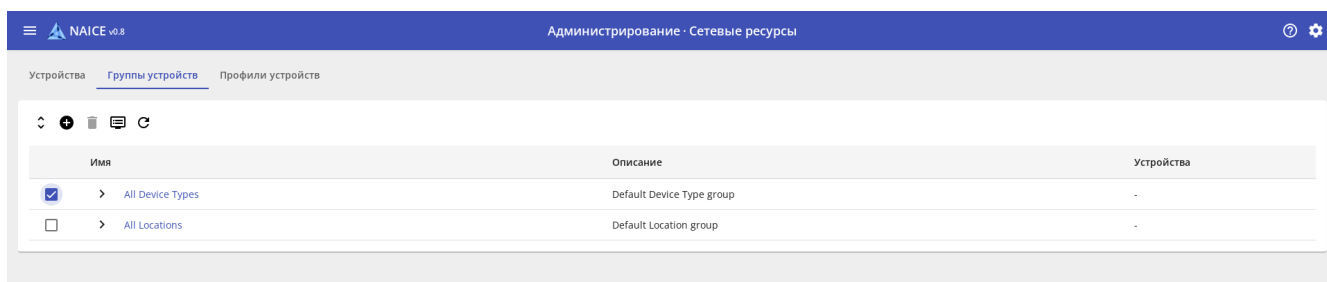


Рисунок 33. Страница с выбором корневой группы для добавления дочерней группы

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

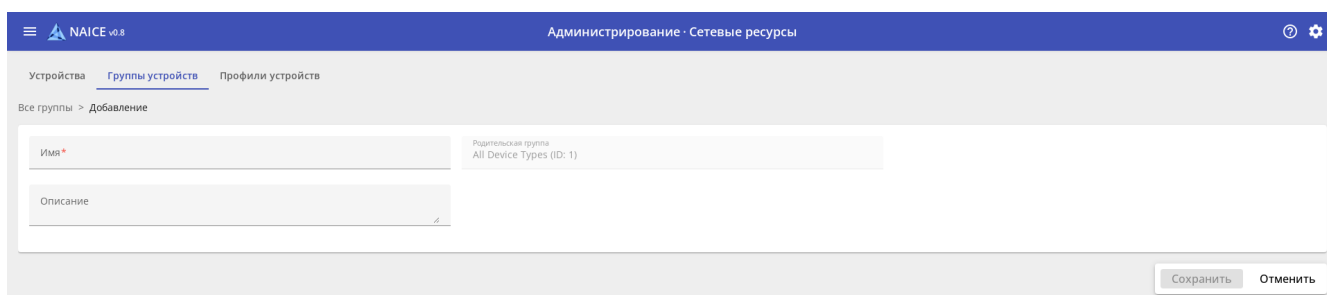


Рисунок 34. Страница с добавлением дочерней группы

## Редактирование группы

Для редактирования группы необходимо нажать на её наименование.

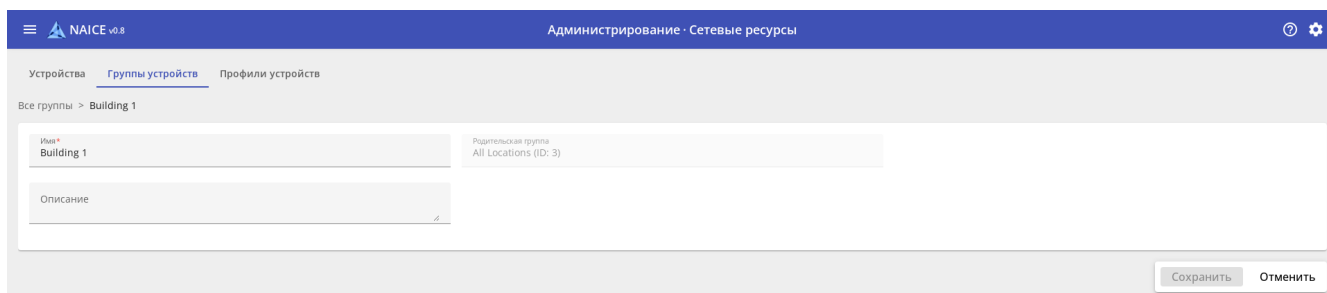



Рисунок 35. Страница редактирования группы

После редактирования нажать на кнопку "Сохранить". Кнопка остается неактивной, пока не будет изменено хотя бы одно поле.



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.

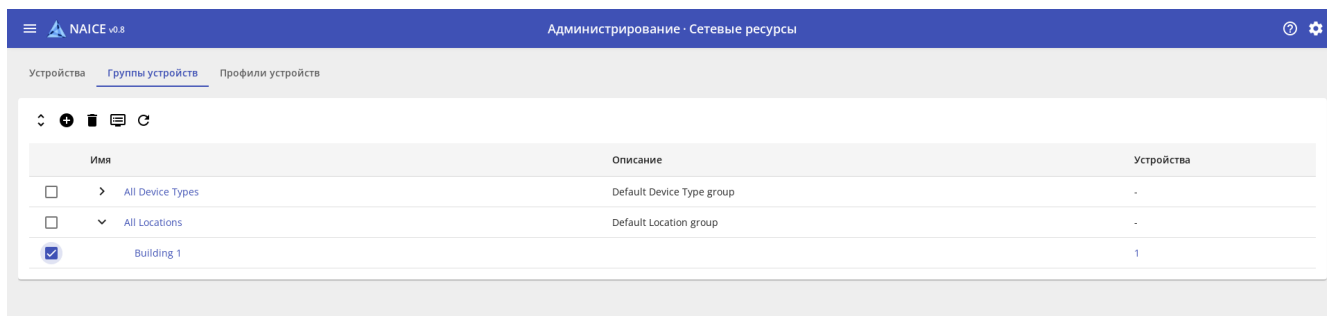


Рисунок 36. Страница с выделенной группой для удаления



Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.



### Подтверждение действия

Данные будут удалены. Вы уверены?

Да

Нет

Рисунок 37. Модальный диалог подтверждения




#### 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.

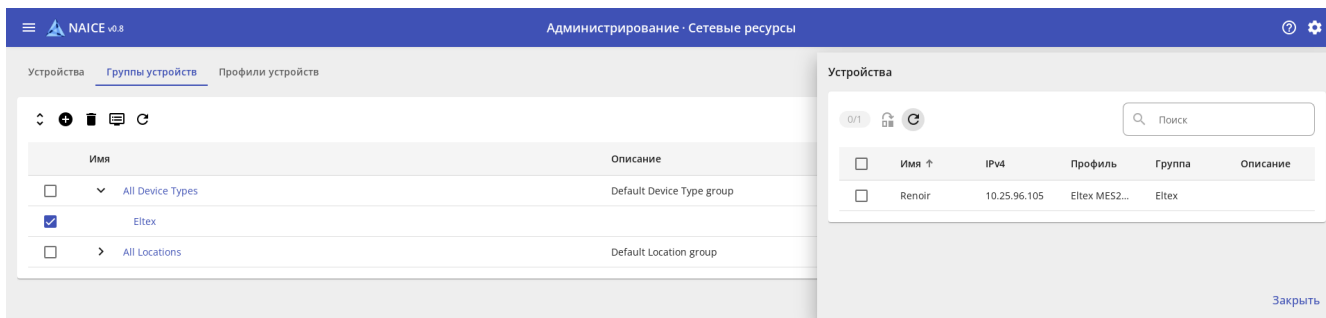


Рисунок 38. Панель просмотра устройств в группе

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".

Элементы управления:

- **0/1** - Счетчик выбранных чекбоксом элементов / общего количества элементов.
- **+** - Добавить новый элемент.
- **🗑️** - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- **🔄** - Обновить данные таблицы.
- **🔍 Поиск** - Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
- **↑** - Изменить текущий порядок сортировки.
- **☐** - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).

## Перемещение устройства в другую группу

После нажатия на кнопку перемещения устройства  откроется окно с выбором группы для перемещения в рамках этой же корневой группы.

## Перемещение устройств



Рисунок 39. Панель перемещения устройств в группу

Группа выбирается из списка, открывающегося по нажатию на .

## Профили устройств

### 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.

## Просмотр списка профилей устройств

Имя ↑	Производитель	Описание
<input type="checkbox"/> AccessPoint - example	Other	Example profile for wireless access points
<input type="checkbox"/> ArubaWireless	Aruba	Profile for Aruba wireless network access devices
<input type="checkbox"/> BrocadeWired	Brocade	Profile for Brocade switches
<input type="checkbox"/> Cisco	Cisco	Generic profile for Cisco network access devices
<input type="checkbox"/> DEFAULT	default	
<input type="checkbox"/> Eltex L2-552	Eltex	CFIW2f1
<input type="checkbox"/> Eltex MES23xx	Eltex	
<input type="checkbox"/> HPWireless	HP	Profile for HP wireless network access devices
<input type="checkbox"/> MotorolaWireless	Motorola	Profile for Motorola wireless network access devices
<input type="checkbox"/> Profile for devices without service-type attribute	Generic	Profile for devices that do not send the service-type attribute in RADIUS request
<input type="checkbox"/> Switch - example	Other	Example profile for wired switches

Рисунок 40. Таблица с перечнем профилей сетевых устройств

На данной странице содержится таблица со списком профилей устройств.

Таблица содержит колонки:

- **Имя** - наименование профиля;
- **Производитель** - наименование вендора устройств;
- **Описание** - произвольное описание профиля.

Доступна сортировка по колонкам **Имя** , **Производитель** .

Элементы управления:

- **0/1** - Счетчик выбранных чекбоксом элементов / общего количества элементов.
- **+** - Добавить новый элемент.
- **🗑** - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- **↻** - Обновить данные таблицы.
- **🔍 Поиск** - Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
- **↑** - Изменить текущий порядок сортировки.
- **☐** - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).

# Добавление профиля устройства

Имя\*      Производитель\*

Описание

Поддерживаемые протоколы

RADIUS

TACACS+

^ Аутентификация/Авторизация

^ Условия определения типа подключения

Wired 802.1x будет обнаружен при следующих условиях

Атрибут\*      =      Значение атрибута\*      +

Wireless 802.1x будет обнаружен при следующих условиях

Атрибут\*      =      Значение атрибута\*      +

Wired MAB будет обнаружен при следующих условиях

Атрибут\*      =      Значение атрибута\*      +

Wireless MAB будет обнаружен при следующих условиях

Атрибут\*      =      Значение атрибута\*      +

^ MAB

Настроить MAB ⓘ

PAP

Проверять совпадение Calling-Station-Id и MAC адреса

Условие пароля:

Атрибут\*      =      Атрибут/Значение\*      ⋮

EAP\_MD5

Проверять совпадение Calling-Station-Id и MAC адреса

Условие пароля:

Атрибут\*      =      Атрибут/Значение\*      ⋮

^ Разрешения

Настроить VLAN


Атрибуты по умолчанию

Уникальные атрибуты      ID\*      Имя

Настроить ACL      Имя\*

Сохранить      Отменить



Рисунок 41. Страница добавления сетевого профиля устройств

Для добавления профиля устройства нажмите .

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, который используется для взаимодействия с сетевым устройством. По умолчанию включены протоколы RADIUS и TACACS+.

**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.
- **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.

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

- **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.
- **Условие пароля** - условие, при котором пароль будет считаться корректным. По умолчанию задано условие равенства пароля логину пользователя.

**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.

Параметры, отмеченные звездочкой \*, обязательны для заполнения.

Устройства Группы устройств Профили устройств

Все профили > Добавление

Имя\* Aruba UR-223 Производитель\* Aruba

Описание

Поддерживаемые протоколы

- RADIUS
- TACACS+

^ Аутентификация/Авторизация

^ Условия определения типа подключения

- Wired 802.1x будет обнаружен при следующих условиях
- Атрибут\* = Значение атрибута\*
- Wireless 802.1x будет обнаружен при следующих условиях
- Атрибут\* = Значение атрибута\*
- Wired MAB будет обнаружен при следующих условиях
- Атрибут\* = Значение атрибута\*
- Wireless MAB будет обнаружен при следующих условиях
- Атрибут\* = Значение атрибута\*

^ MAB

- Настроить MAB
- PAP
- Проверять совпадение Calling-Station-Id и MAC адреса
- Условие пароля: Атрибут\* = Атрибут/Значение\*
- EAP\_MD5
- Проверять совпадение Calling-Station-Id и MAC адреса
- Условие пароля: Атрибут\* = Атрибут/Значение\*

^ Разрешения

- Настроить VLAN
- Атрибуты по умолчанию
- Уникальные атрибуты ID\* Имя
- Настроить ACL Имя\*

Сохранить Отменить

Рисунок 42. Страница с заполненными параметрами профиля устройств

После ввода необходимых данных нажмите кнопку "Сохранить".

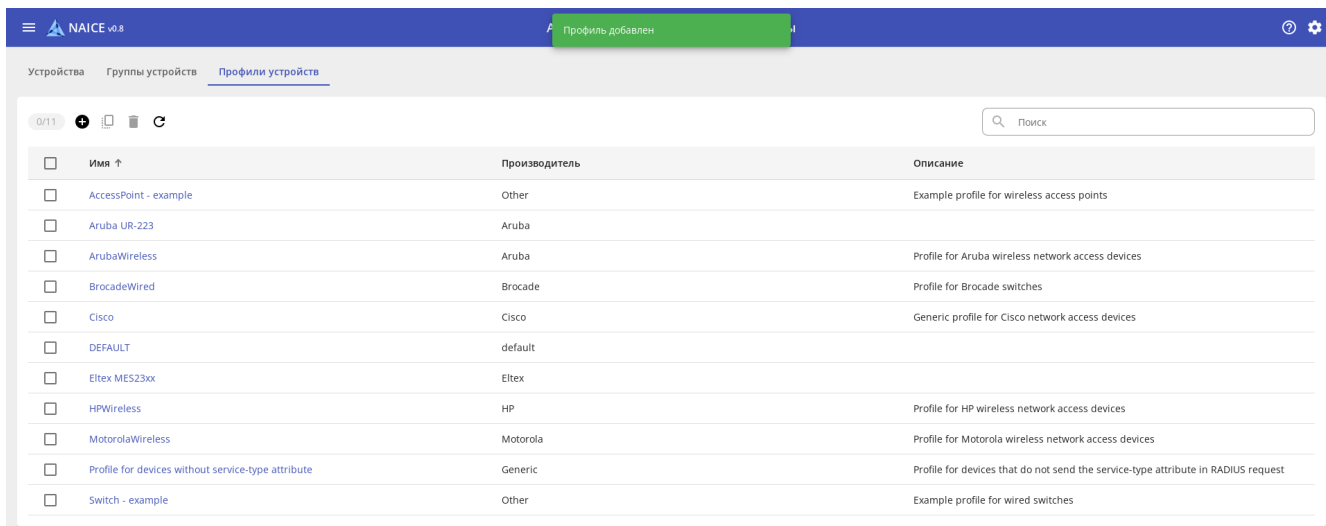


Рисунок 43. Страница успешного создания профиля сетевых устройств

## Редактирование профиля устройства

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

NAICE v0.8 Администрирование · Сетевые ресурсы

Устройства Группы устройств Профили устройств

Все профили > Aruba UR-223

Имя\* Aruba UR-223 Провайдер\* Aruba

Описание

**Поддерживаемые протоколы**

RADIUS  
 TACACS+

**Аутентификация/Авторизация**

**Условия определения типа подключения**

Wired 802.1x будет обнаружен при следующих условиях

Атрибут\* = Значение атрибута\* 🗑️ +

Wireless 802.1x будет обнаружен при следующих условиях

Атрибут\* = Значение атрибута\* 🗑️ +

Wired MAB будет обнаружен при следующих условиях

Атрибут\* = Значение атрибута\* 🗑️ +

Wireless MAB будет обнаружен при следующих условиях

Атрибут\* = Значение атрибута\* 🗑️ +

**MAB**

Настроить MAB ⓘ

PAP

Проверять совпадение Calling-Station-Id и MAC адреса

Условие пароля:

Атрибут\* = Атрибут/Значение\* ⋮

EAP\_MDS

Проверять совпадение Calling-Station-Id и MAC адреса

Условие пароля:

Атрибут\* = Атрибут/Значение\* ⋮

**Разрешения**

Настроить VLAN

Атрибуты по умолчанию


Уникальные атрибуты ID\* 🗑️ Имя 🗑️

Настроить ACL Имя\* 🗑️

Рисунок 44. Страница редактирования профиля сетевых устройств

После редактирования нажать на кнопку **"Сохранить"**. Кнопка остается неактивной, пока не будет изменено хотя бы одно поле.

## Удаление профиля устройства

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

Устройства Группы устройств Профили устройств

1/11

Поиск

Имя ↑	Производитель	Описание
<input type="checkbox"/> AccessPoint - example	Other	Example profile for wireless access points
<input type="checkbox"/> ArubaWireless	Aruba	Profile for Aruba wireless network access devices
<input type="checkbox"/> BrocadeWired	Brocade	Profile for Brocade switches
<input type="checkbox"/> Cisco	Cisco	Generic profile for Cisco network access devices
<input type="checkbox"/> DEFAULT	default	
<input checked="" type="checkbox"/> Eltex LZ-552	Eltex	CFIW2f1
<input type="checkbox"/> Eltex MES23xx	Eltex	
<input type="checkbox"/> HPWireless	HP	Profile for HP wireless network access devices
<input type="checkbox"/> MotorolaWireless	Motorola	Profile for Motorola wireless network access devices
<input type="checkbox"/> Profile for devices without service-type attribute	Generic	Profile for devices that do not send the service-type attribute in RADIUS request
<input type="checkbox"/> Switch - example	Other	Example profile for wired switches

Рисунок 45. Страница с выбранным для удаления профилем устройств



Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.



### Подтверждение действия

Данные будут удалены. Вы уверены?

Да

Нет

Рисунок 46. Модальный диалог подтверждения

После удаления произойдет переход на страницу просмотра списка профилей устройств.

Устройства Группы устройств Профили устройств

0/10

Поиск

Имя ↑	Производитель	Описание
<input type="checkbox"/> AccessPoint - example	Other	Example profile for wireless access points
<input type="checkbox"/> ArubaWireless	Aruba	Profile for Aruba wireless network access devices
<input type="checkbox"/> BrocadeWired	Brocade	Profile for Brocade switches
<input type="checkbox"/> Cisco	Cisco	Generic profile for Cisco network access devices
<input type="checkbox"/> DEFAULT	default	
<input type="checkbox"/> Eltex MES23xx	Eltex	
<input type="checkbox"/> HPWireless	HP	Profile for HP wireless network access devices
<input type="checkbox"/> MotorolaWireless	Motorola	Profile for Motorola wireless network access devices
<input type="checkbox"/> Profile for devices without service-type attribute	Generic	Profile for devices that do not send the service-type attribute in RADIUS request
<input type="checkbox"/> Switch - example	Other	Example profile for wired switches

Рисунок 47. 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 "Администрирование" → "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:

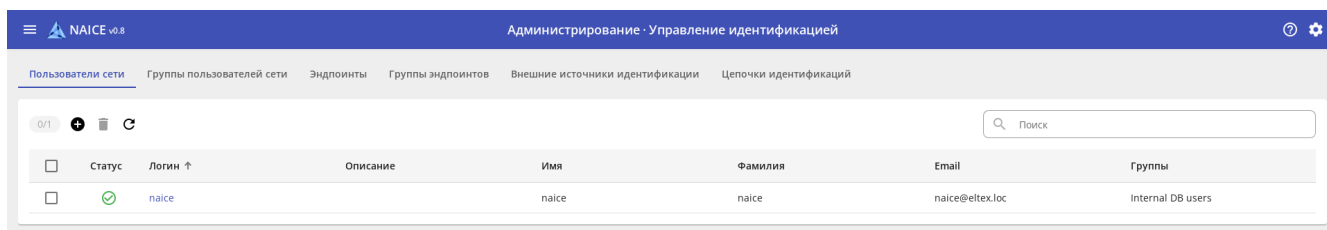
- [Пользователи сети](#) - раздел управления учетными данными пользователей, с которыми производится авторизация на устройствах.
- [Группы пользователей сети](#) - раздел настроек, позволяющий создать сущности для группировки пользователей.
- [Эндпоинты](#) - раздел для работы со списком конечных устройств, 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 учётными данными пользователей, с которыми производится авторизация на устройствах.

### Просмотр пользователей сети



Статус	Логин ↑	Описание	Имя	Фамилия	Email	Группы
<input checked="" type="checkbox"/>	naice		naice	naice	naice@eltex.loc	Internal DB users

Рисунок 48. 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:

- **0/1** - Счетчик выбранных чекбоксом элементов / общего количества элементов.
- **+** - Добавить новый элемент.
- **🗑** - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- **↻** - Обновить данные таблицы.
- **🔍 Поиск** - Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
- **↑** - Изменить текущий порядок сортировки.
- - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).

## Добавление пользователя

Для добавления пользователя нажмите **+** в левой части поля над таблицей.



Скриншот интерфейса администрирования NAICE v0.8. Вкладка: Пользователи сети > Добавление. Поле "Статус\*" установлено на "Включено". Поля ввода: Логин\*, Пароль\*, Подтверждение пароля\*, Имя, Фамилия, Email, Описание. Таблица "Группы пользователя" с поиском и заголовками "Имя ↑" и "Описание". Кнопки "Добавить" и "Отменить".

Рисунок 49. Страница добавления пользователя

В открывшейся странице представлены следующие параметры:

- **Статус \*** - статус пользователя, может принимать значения "включено" или "выключено". Аутентификация по выключенным учетным данным запрещена.




**Логин** \* - логин пользователя. Максимальная длина логина - 200 символов.


- **Пароль** \* - пароль пользователя. Минимальная длина пароля - 8 символов, максимальная - 100 символов. По нажатию на  можно включить отображение вводимого пароля, по-умолчанию текст скрыт.
- **Подтверждение пароля** \* - поле подтверждения пароля пользователя, должно совпадать со значением из **Пароль**. По нажатию на  можно включить отображение вводимого пароля, по-умолчанию текст скрыт.
- **Имя** - имя пользователя. Максимальная длина - 200 символов.
- **Фамилия** - фамилия пользователя. Максимальная длина - 200 символов.
- **Email** - адрес электронной почты пользователя. Должно соответствовать определенному формату (например, [naice@eltex.loc](mailto:naice@eltex.loc)) и не превышать 200 символов.
- **Описание** - произвольное описание пользователя. Максимальная длина - 1000 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.
-  - удалить пользователя из выбранных чекбоксом групп (неактивно, пока не выбрана хотя бы одна группа).
-  - изменить текущий порядок сортировки.
- - чекбокс, который отвечает за выбор групп для выполнения дальнейших действий (например, удаления пользователя из группы).
-  - добавить пользователя в группы.

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

## Добавление пользователя в группы

Поиск

Employees

Internal DB users

>

Выбранные\*

Не выбрано

Добавить Отменить

Рисунок 50. 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).
- **Отменить** - 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.

<input type="checkbox"/>	Статус	Логин ↑
<input type="checkbox"/>	✓	ivan.ivanov
<input type="checkbox"/>	✓	naice

Рисунок 51. Гиперссылка на страницу редактирования пользователя

Откроется страница редактирования.

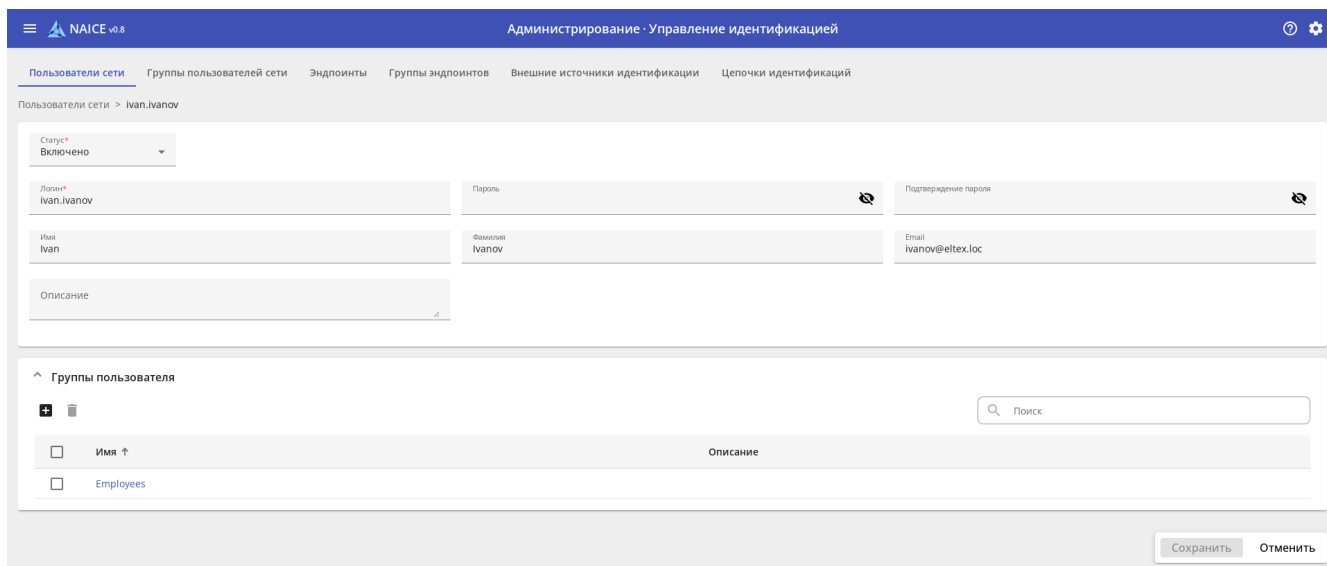



Рисунок 52. Страница редактирования пользователя



Старый пароль пользователя не отображается на странице редактирования! Если вы не хотите изменять пароль пользователя, то оставьте поля "Пароль" и "Подтверждение пароля" пустыми.

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 .

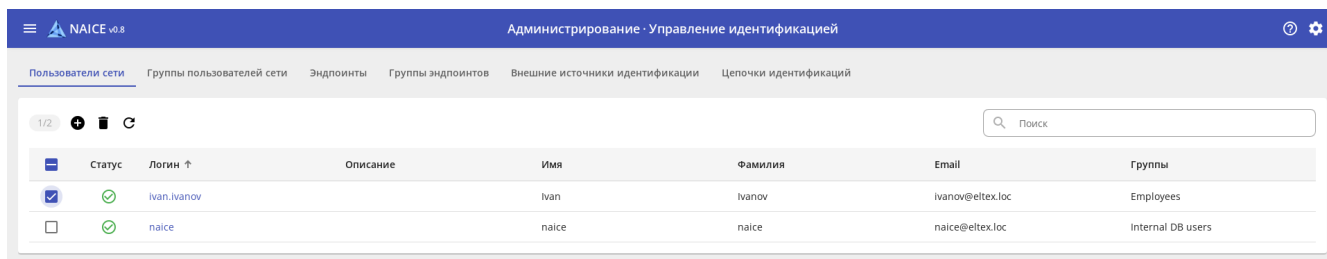


Рисунок 53. Выбор пользователей в таблице для удаления



Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.



### Подтверждение действия

Данные будут удалены. Вы уверены?

Да

Нет

## Группы пользователей сети

### Описание

Существует возможность объединять [пользователей сети](#) в *группы* и использовать в дальнейшем признак принадлежности пользователя к группе при настройке [политик доступа](#).

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

### Просмотр групп пользователей сети

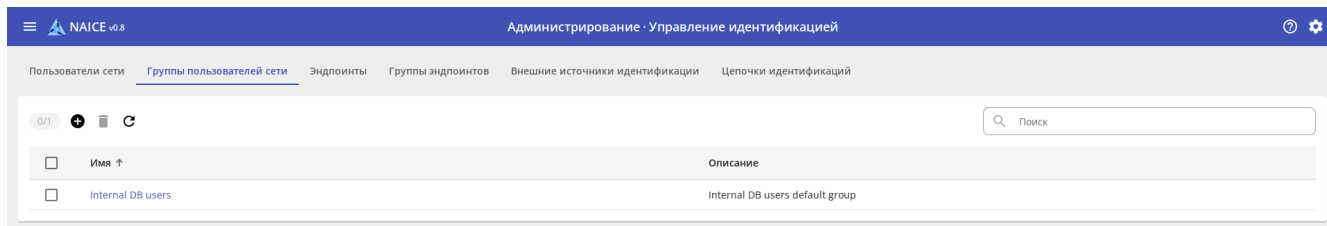


Рисунок 55. Таблица с перечнем групп пользователей сети на странице просмотра

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:

- **0/1** - Счетчик выбранных чекбоксом элементов / общего количества элементов.
- **+** - Добавить новый элемент.
- **✖** - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- **↻** - Обновить данные таблицы.
- **🔍 Поиск** - Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
- **↑** - Изменить текущий порядок сортировки.
- - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).

### Добавление группы пользователей

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

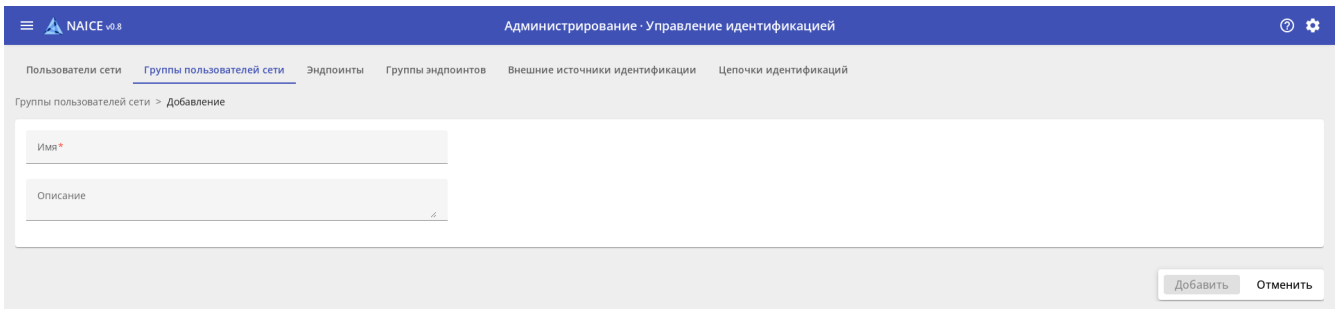


Рисунок 56. Страница добавления группы пользователей

Для заполнения доступны следующие параметры:

- **Имя \*** - название группы. Максимальная длина - 200 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.

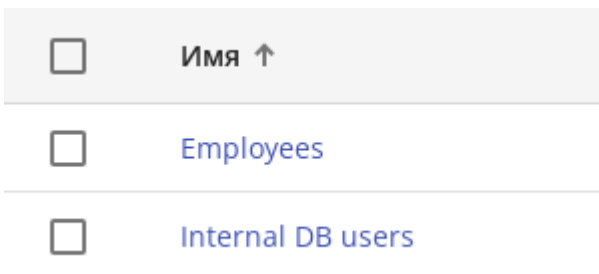


Рисунок 57. Гиперссылка на страницу редактирования группы пользователей

Откроется страница редактирования с возможностью добавления пользователей в группу.

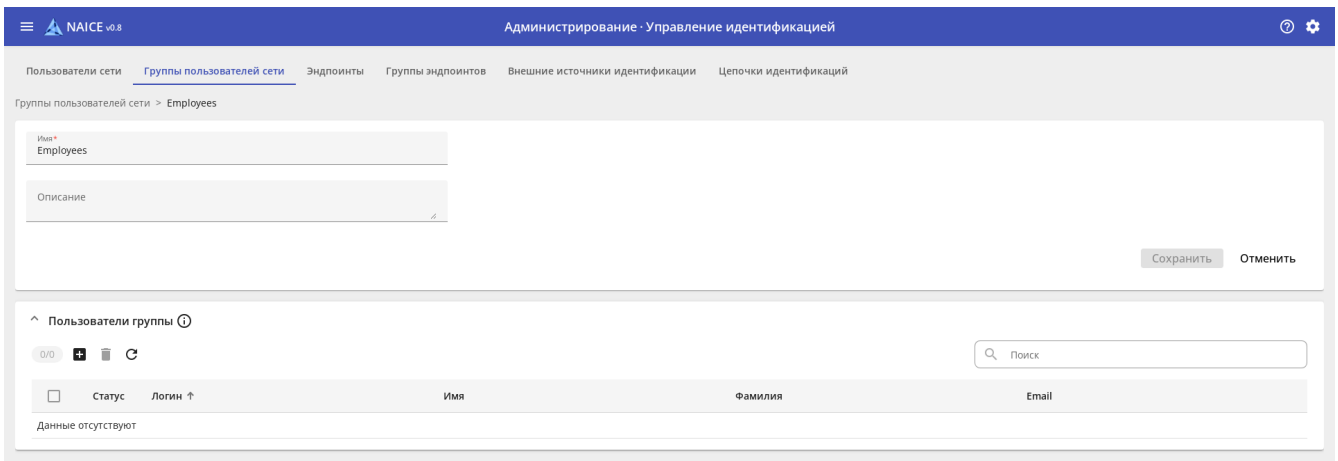






Рисунок 58. Страница изменения группы пользователей

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).
- 0/1 - счетчик выбранных чекбоксом элементов / общего количества элементов.
-  - добавить пользователей в группу.

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

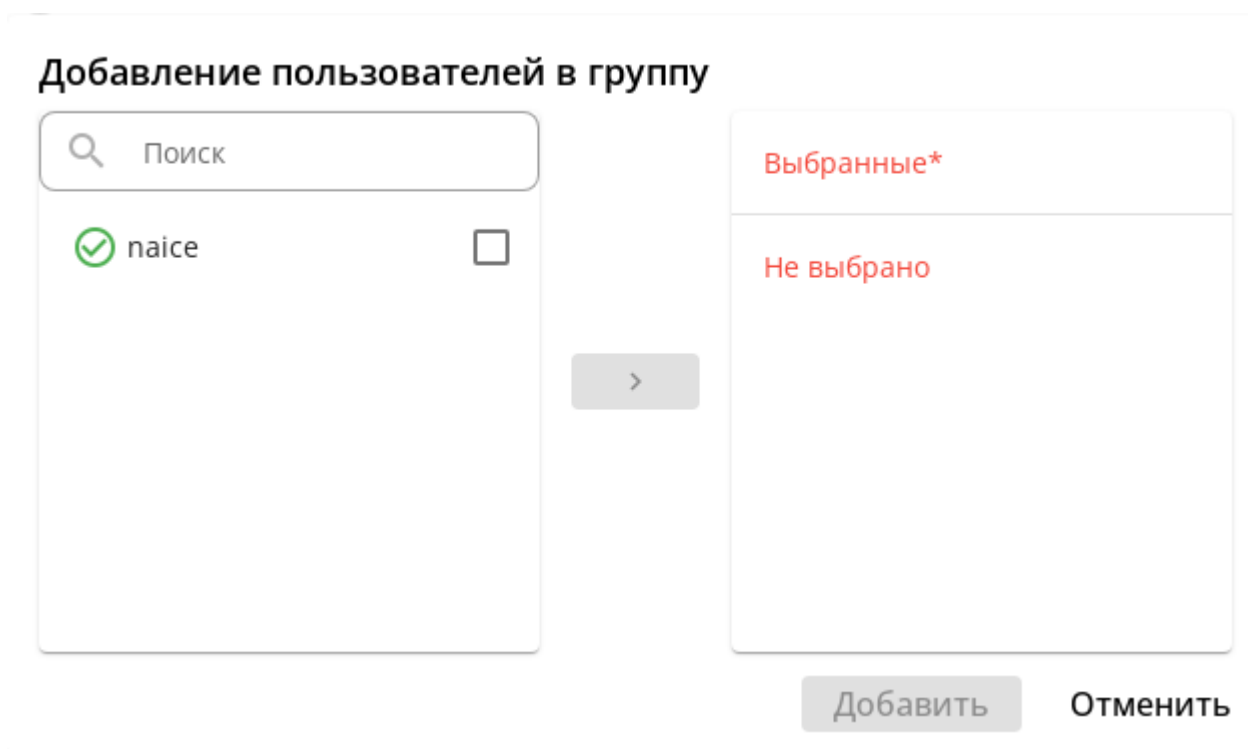




Рисунок 59. Окно добавления пользователей в группу

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 .

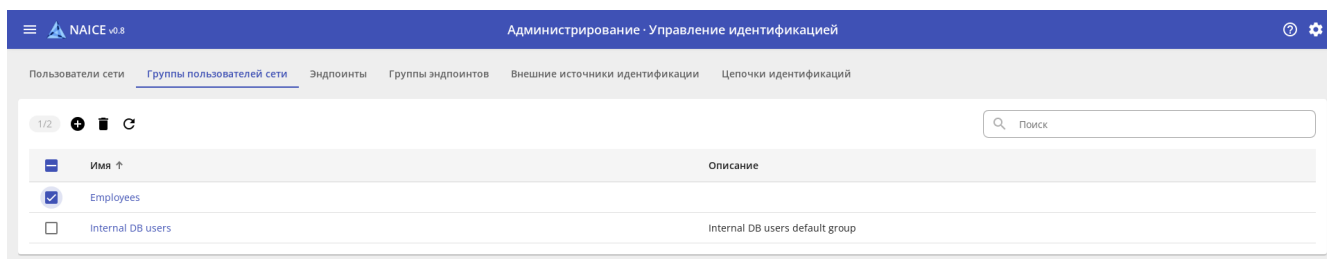


Рисунок 60. Выбор групп пользователей в таблице для удаления



Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.



### Подтверждение действия

Данные будут удалены. Вы уверены?

Да

Нет

Рисунок 61. Модальный диалог подтверждения



### 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.

## 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 [политик доступа](#) разрешать или запрещать доступ к сети.

## Заполнение таблицы эндпоинтов

Заполнение таблицы эндпоинтов происходит в автоматическом и ручном режиме.

- *в ручном режиме:* добавление эндпоинтов выполняется администратором системы по аналогии с добавлением других сущностей.
- *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.



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

MAC адрес	Статус	Подробнее	Описание	Производитель	IP адрес эндпоинта	Имя пользователя	Имя хоста	Профиль эндпоинта
03:47:AF:A9:9B:98			Vespillo facilis amicitia carbo p...					Unknown

Рисунок 62. 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**.

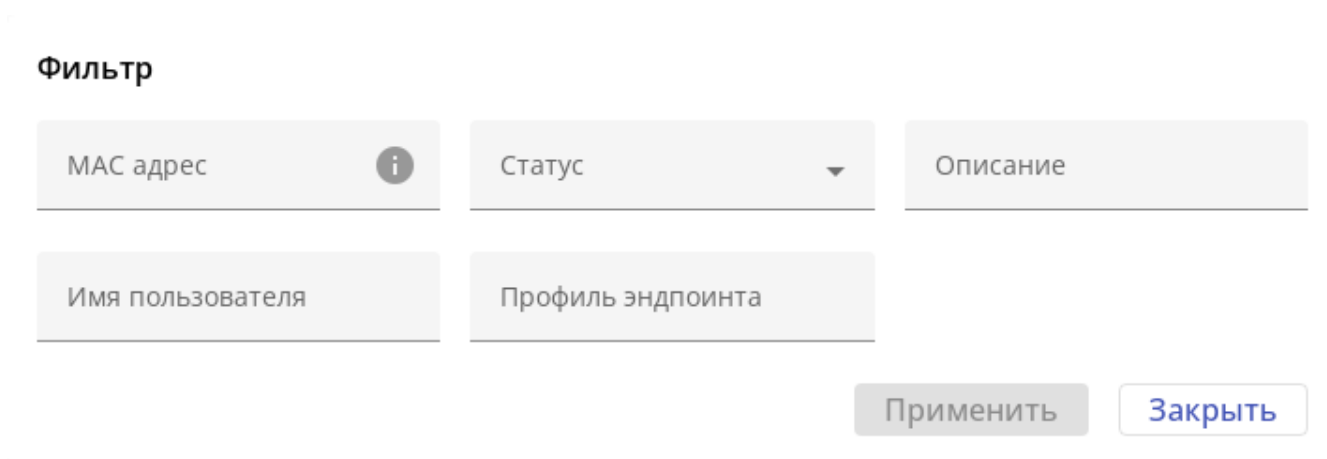
Страница содержит следующие элементы управления:

-  - Обновить данные таблицы.
- **0/1** - Счетчик выбранных чекбоксом элементов / общего количества элементов.
-  - Добавить новый элемент.
-  - Открыть окно настройки фильтрации данных по таблице.
-  - Настроить отображение колонок таблицы.
-



 - Запустить процесс перепрофилирования выбранных эндпоинтов (неактивно, пока не выбран хоть один 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).

Фильтрация данных в таблице настраивается в следующем окне:



**Фильтр**

MAC адрес  Статус  Описание

Имя пользователя Профиль эндпоинта


Применить **Заккрыть**

Рисунок 63. Настройка фильтрации данных в таблице


Фильтрация доступна по параметрам Профиль эндпоинта, MAC адрес, Статус, Описание и Имя пользователя.

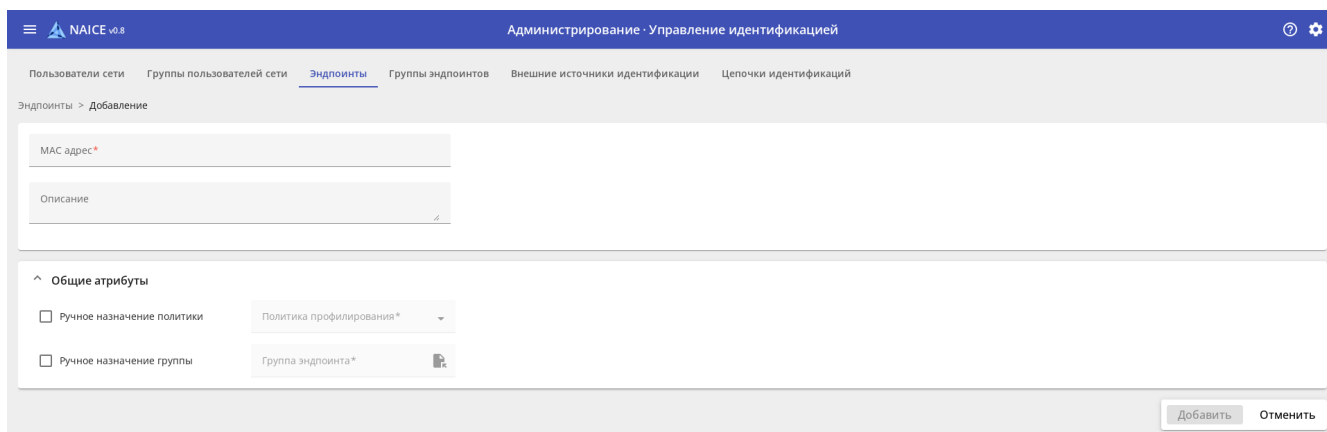
В настройках таблицы  можно сменить состав отображаемых колонок.

Кнопка  выбирает или снимает выбор всех колонок для отображения.

Кнопка  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.



Администрирование · Управление идентификацией

Пользователи сети Группы пользователей сети **Эндпоинты** Группы эндпоинтов Внешние источники идентификации Цепочки идентификаций

Эндпоинты > Добавление

MAC адрес\*

Описание

Общие атрибуты

Ручное назначение политики Политика профилирования\*

Ручное назначение группы Группа эндпоинта\*

Добавить Отменить

Рисунок 64. 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.

<input type="checkbox"/>	<b>MAC адрес</b>	C
<input type="checkbox"/>	03:47:AF:A9:9B:98	

Рисунок 65. Гиперссылка на страницу редактирования эндпоинта

Откроется страница редактирования, аналогичная странице добавления.


Рисунок 66. Редактирование эндпоинта

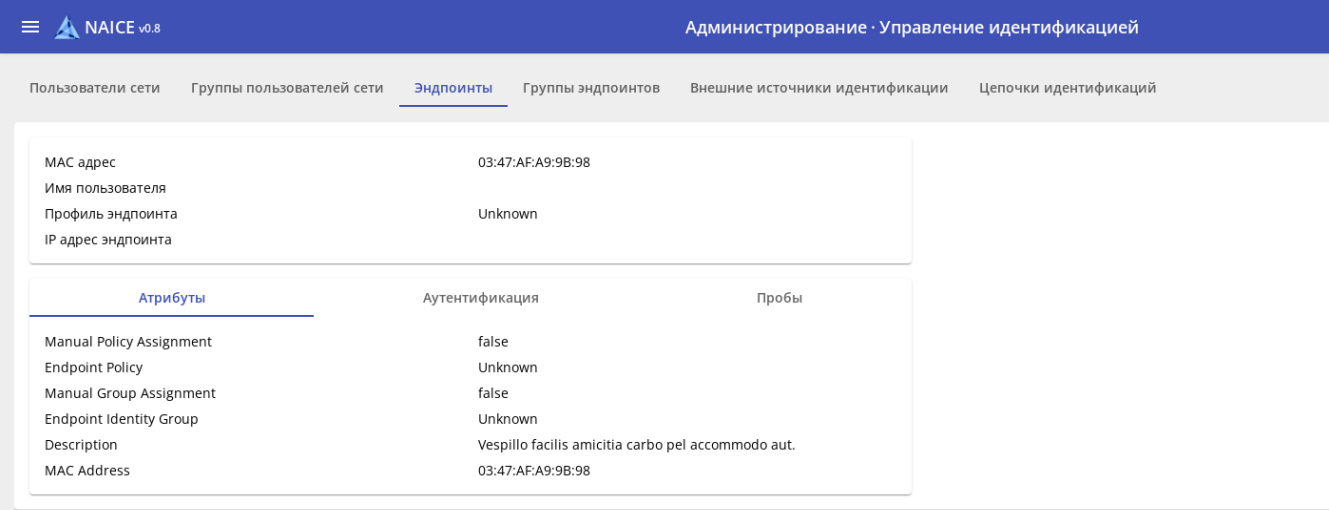


Редактирование MAC адреса эндпоинта недоступно.  
Если необходимо отредактировать адрес, то удалите и создайте эндпоинт заново.

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.



MAC адрес	03:47:AF:A9:9B:98
Имя пользователя	
Профиль эндпоинта	Unknown
IP адрес эндпоинта	

Атрибуты	Аутентификация	Пробы
Manual Policy Assignment	false	
Endpoint Policy	Unknown	
Manual Group Assignment	false	
Endpoint Identity Group	Unknown	
Description	Vespillo facilis amicitia carbo pel accommo aut.	
MAC Address	03:47:AF:A9:9B:98	

Рисунок 67. 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 администратором;
- **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 .

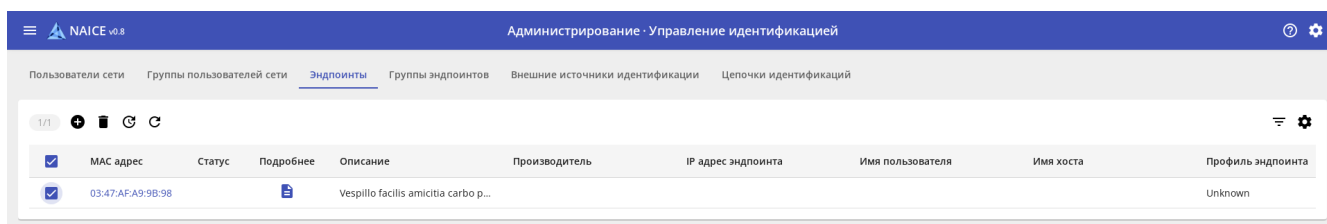


Рисунок 68. Выбор эндпоинтов в таблице для удаления



Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.



### Подтверждение действия

Данные будут удалены. Вы уверены?

Да

Нет

Рисунок 69. Модальный диалог подтверждения

## 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.

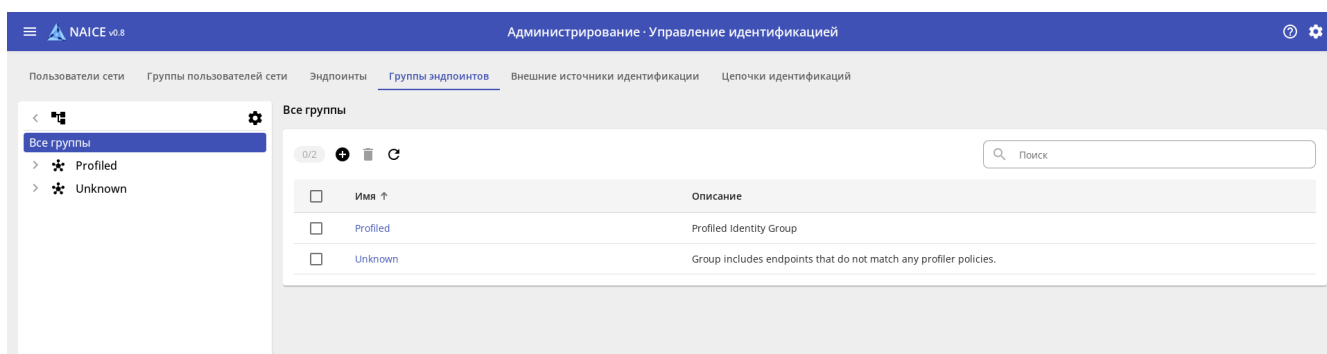


Рисунок 70. Просмотр списка групп эндпоинтов

Таблица содержит колонки:

- **Имя** - Имя группы
- **Описание** - Полное описание группы

Элементы управления:

- **0/1** - Счетчик выбранных чекбоксом элементов / общего количества элементов.
- **+** - Добавить новый элемент.
- **🗑️** - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- **↻** - Обновить данные таблицы.
- **🔍 Поиск** - Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
- **↑** - Изменить текущий порядок сортировки.
- - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).

В левой стороне располагается панель быстрого просмотра в виде дерева или списка

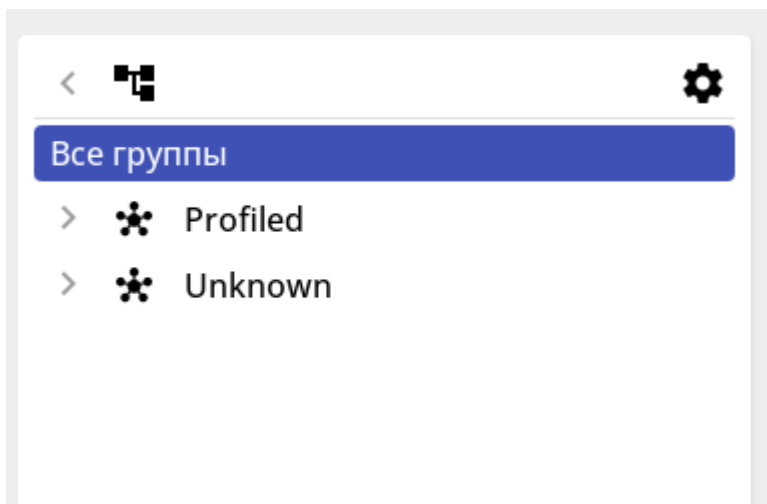


Рисунок 71. Меню навигации по дереву групп эндпоинтов

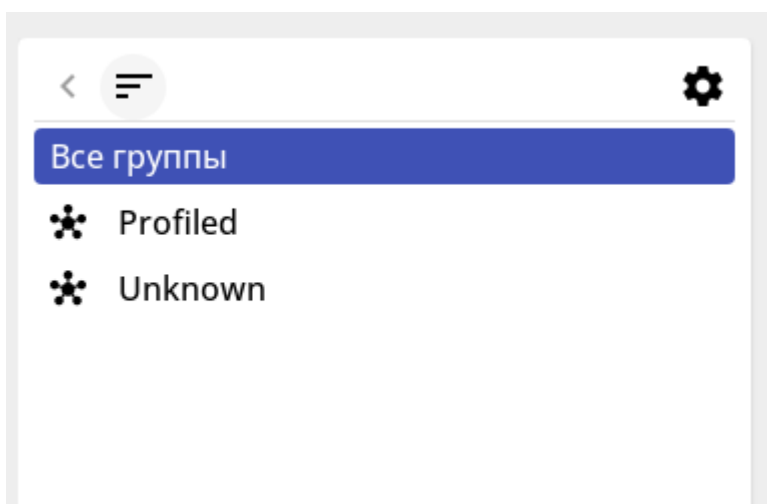







Рисунок 72. Вид Меню навигации в режиме списка


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:**

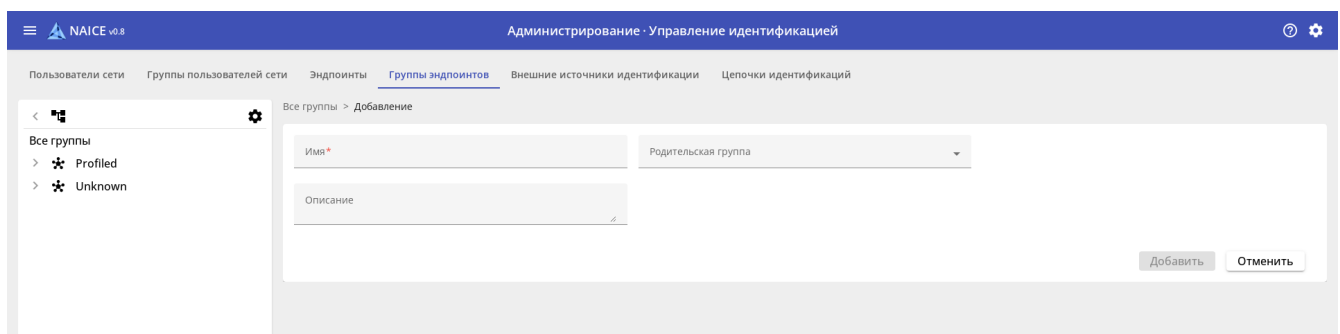




Рисунок 73. Форма добавления группы эндпоинтов

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.

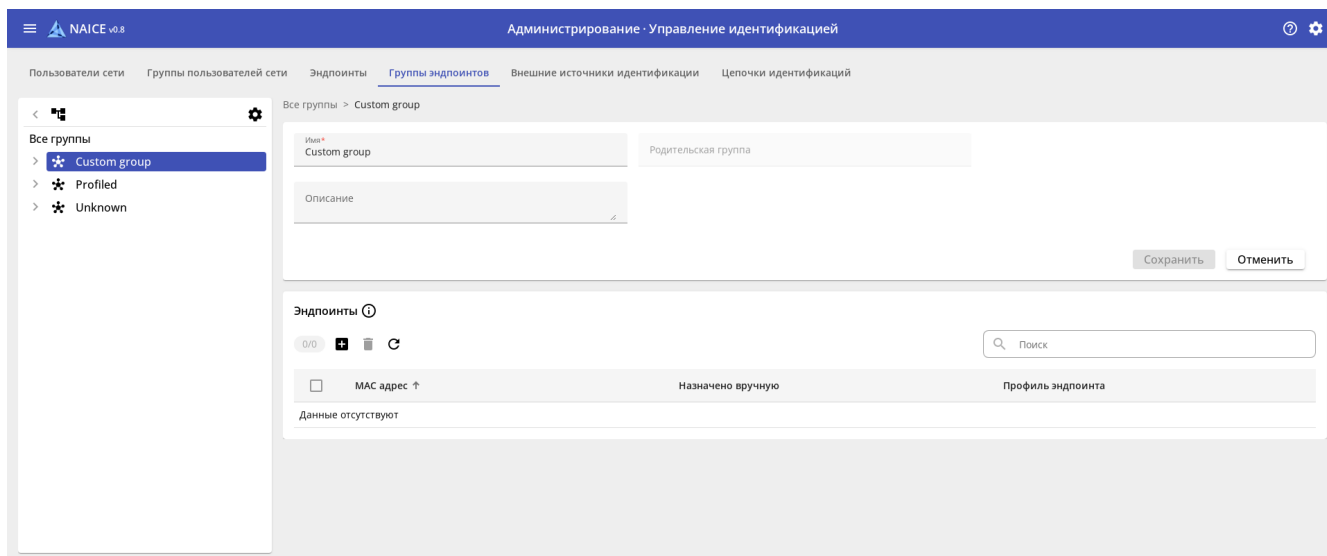


Рисунок 74. Форма редактирование группы эндпоинтов

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:

- **0/1** - Счетчик выбранных чекбоксом элементов / общего количества элементов.
- **+** - Добавить новый элемент.
- **🗑** - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- **↻** - Обновить данные таблицы.
- **🔍 Поиск** - Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.

↑ - Изменить текущий порядок сортировки.

- - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).



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 **>**.

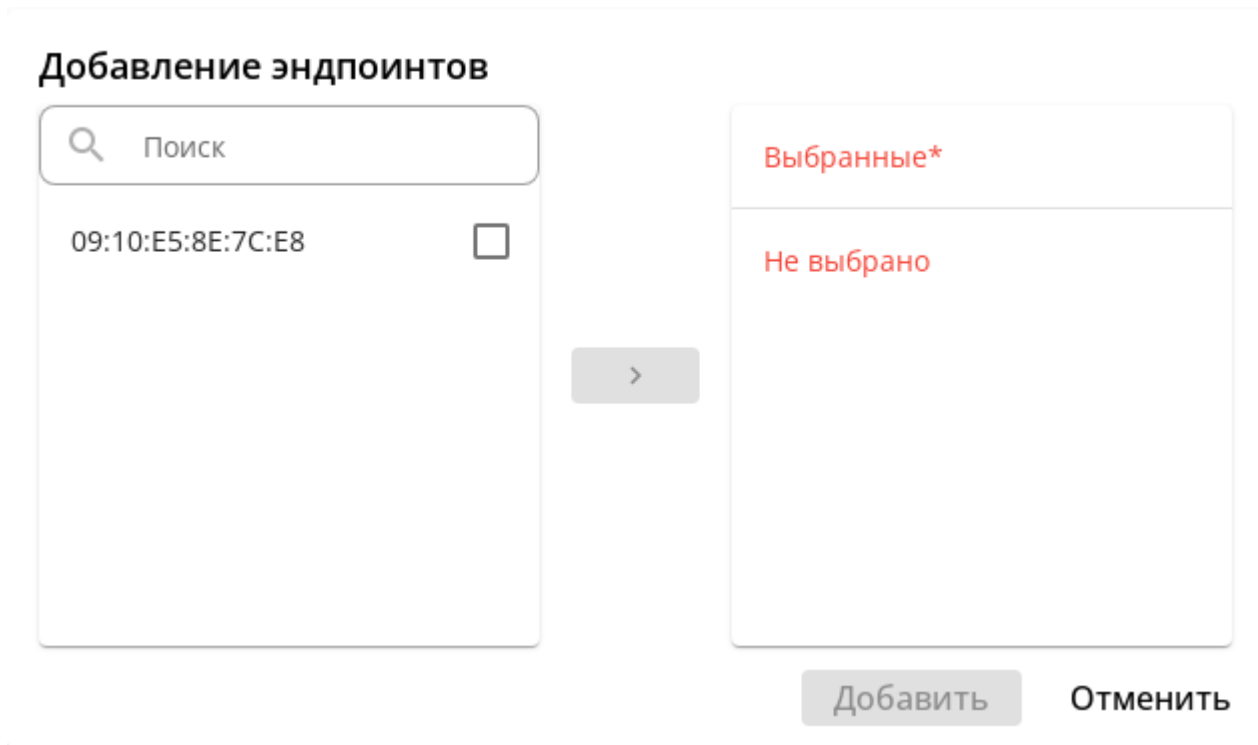


Рисунок 75. Модальный диалог добавления эндпоинтов

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 распространяются 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 **🗑**.

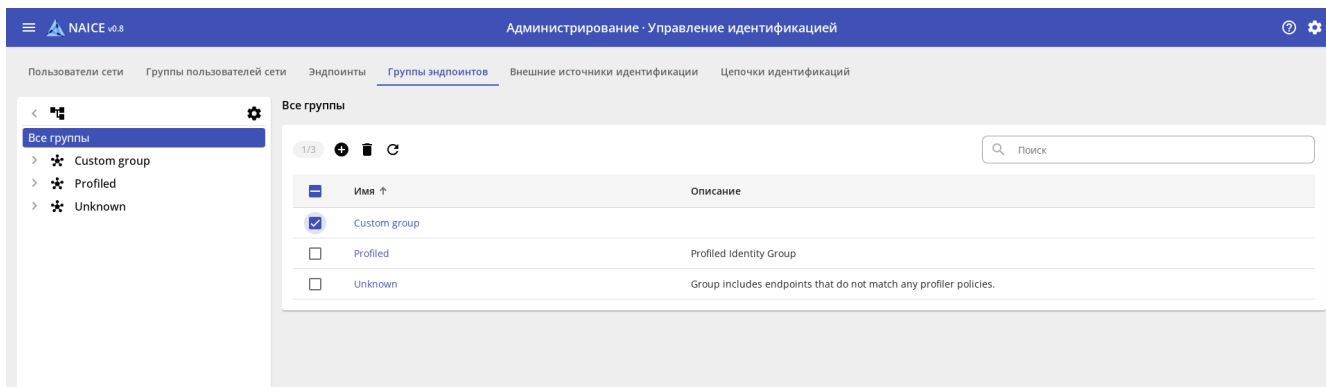


Рисунок 76. Выбор групп для удаления



Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.



### Подтверждение действия

Данные будут удалены. Вы уверены?

Да

Нет

Рисунок 77. Модальный диалог подтверждения



#### Ограничения:

- нельзя удалить группу, которая имеет дочернюю группу;
- нельзя удалить группу в которой есть эндпоинты;
- нельзя удалить системные группы Profiled и Unknown.

## 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 или LDAP.

В данном разделе производится настройка подключения к внешним источникам и добавление групп пользователей и/или атрибутов, которые в дальнейшем могут быть использованы при настройке [политик доступа](#).

### Просмотр внешних источников идентификации

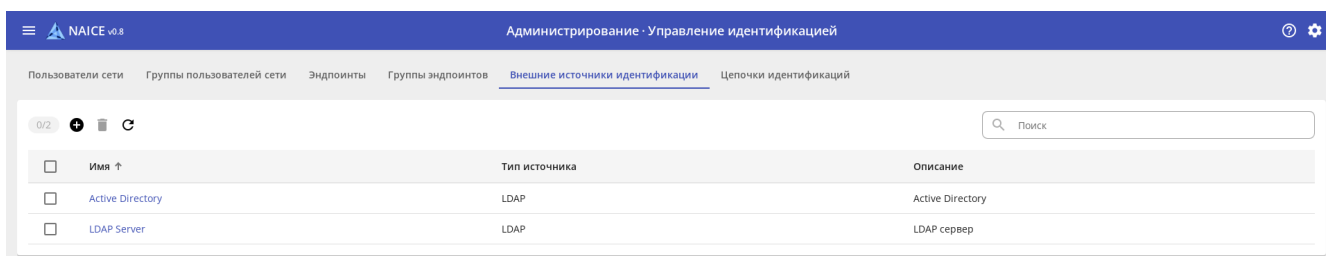


Рисунок 78. Просмотр внешних источников идентификации

На данной странице содержится 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:

- **0/1** - Счетчик выбранных чекбоксом элементов / общего количества элементов.
- **+** - Добавить новый элемент.
- **🗑** - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- **↻** - Обновить данные таблицы.
- **🔍 Поиск** - Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
- **↑** - Изменить текущий порядок сортировки.
- - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).



Поддержано взаимодействие с источниками идентификации типа "Microsoft Active Directory" и "LDAP".  
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 Eltex-NAICE, должен обеспечивать:
  - разрешение полного имени домена (например: EXAMPLE.ORG), в котором будет работать Eltex-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 пользователя для взаимодействия с Eltex-NAICE.
- Учетная запись пользователя и компьютера должны иметь пароль.

Задать пароль компьютера на сервере с MS Active Directory через можно командой в оболочке PowerShell, входящей в состав Active Directory, запущенной с правами администратора:

```
Set-ADAccountPassword -Identity Computer-Name$ -Reset
```

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 "\$".  
WARNING: 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	
TCP/UDP	3268	LDAP GC	Можно использовать вместо порта 389, если нет леса деревьев
TCP/UDP	49152-65535	RPC Dynamic Port Range	

### Ограничения реализации

Есть следующие ограничения реализации взаимодействия с Active Directory:

- Возможно использовать пользователей, их атрибуты и группы только в рамках указанного в настройке домена.
- Имя пользователя на клиентском устройстве требуется вводить в формате UPN: <пользователь>@<домен> или в формате пред-Windows 2000: <ИМЯ ДОМЕНА>\<пользователь>.
- В именах пользователей и их паролях допускаются только латинские символы, цифры, знаки препинания.
- Возможна авторизация только с использованием протокола MS-CHAPv2 или EAP-MS-CHAPv2.

### Добавление источника идентификации

Для добавления источника идентификации нажмите  в правой части поля над таблицей, откроется следующая страница.

NAICE v0.8 Администрирование · Управление идентификацией

Пользователи сети Группы пользователей сети Эндпоинты Группы эндпоинтов **Внешние источники идентификации** Цепочки идентификаций

Внешние источники идентификации > Добавление

1 Основные настройки 2 Группы Optional 3 Атрибуты Optional

Имя\*

Описание

^ 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

^ Подключение

Имя домена\* ⓘ

Имя компьютера\* ⓘ Пароль компьютера\* ⓘ

Admin dn\* ⓘ Admin password\* ⓘ

FQDN\* ⓘ Port\*

^ Структура каталога

Subject search base\* ⓘ

Group search base\* ⓘ


Проверить связь с сервером


Добавить Отменить

Рисунок 79. Окно добавления источника идентификации

В данной форме представлены следующие параметры:

- Блок **Основные настройки:**
  - **Имя \*** - наименование источника идентификации. Максимальная длина поля 64 знака.
  - **Описание** - описание. Максимальная длина поля 200 знаков.
- 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.
  - **Имя компьютера \*** - имя административного компьютера для взаимодействия с Active Directory. Необходимо указывать только имя, без доменной части. Поле доступно только для схемы "ACTIVE\_DIRECTORY". Максимальная длина поля 63 знака.
  -


Пароль компьютера \* - пароль административного компьютера для взаимодействия с Active Directory. По умолчанию не отображается, для просмотра требуется нажать . Поле доступно только для схемы "ACTIVE\_DIRECTORY". Максимальная длина поля 200 знаков.

- 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 домен, 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 в подсказке ниже. - Проверить связь с сервером - проверить корректность настроек и связь с сервером Active Directory.

Параметры, отмеченные звездочкой \*, обязательны для заполнения.

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),
- русские 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

После заполнения всех необходимых данных станет активна кнопка **Добавить и Проверить связь с сервером**.

Кнопка **Добавить** становится активной при условии добавления всех параметров и не зависит от успешности проверки связи с сервером.

При успешной проверки связи с сервером появится сообщение вида:

## Результат подключения

Привязка LDAP к "example.org:389" выполнена успешно:

кол-во предметов: "25",

кол-во групп: "25".

Макс. кол-во запрашиваемых предметов и групп - 25.

Аутентификация netlogon прошла успешно

[Заккрыть](#)

Рисунок 80. 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, что бы 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 через внешний источник идентификации добавление групп не является обязательным. Группы можно использовать в политиках авторизации пользователей.

После добавления источника идентификации кнопка **Добавить** примет значение **Далее**. Так же можно выполнить переход нажав на надпись **(2) Группы**, откроется страница:

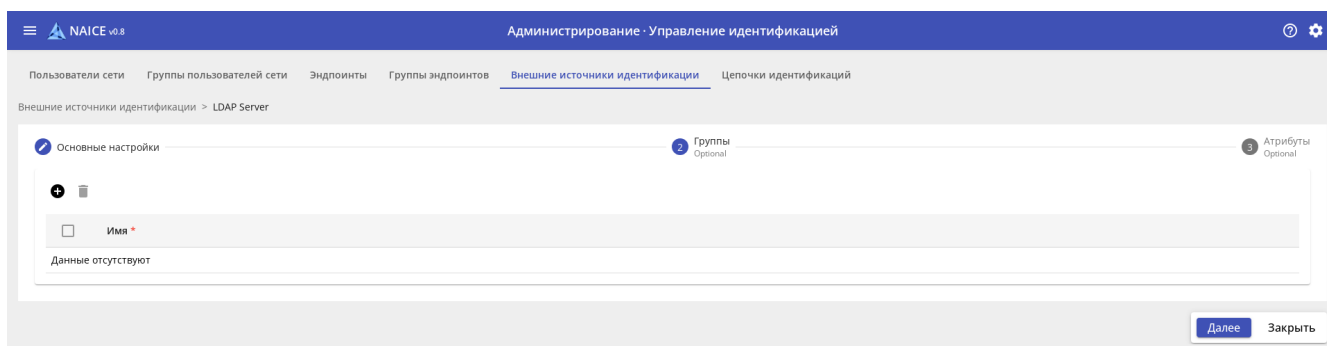


Рисунок 81. Пустая таблица групп

Таблица содержит колонки:

- **Имя \*** - имя группы

Элементы управления:

- - добавить группу.
- - удалить выбранные чекбоксом группы (неактивно, пока не выбран хоть одна группа).
- - редактировать группу (не отображается, пока не добавлена хотя бы одна группа).
- - сохранить группу после редактирования (не отображается, пока не начато редактирование группы).

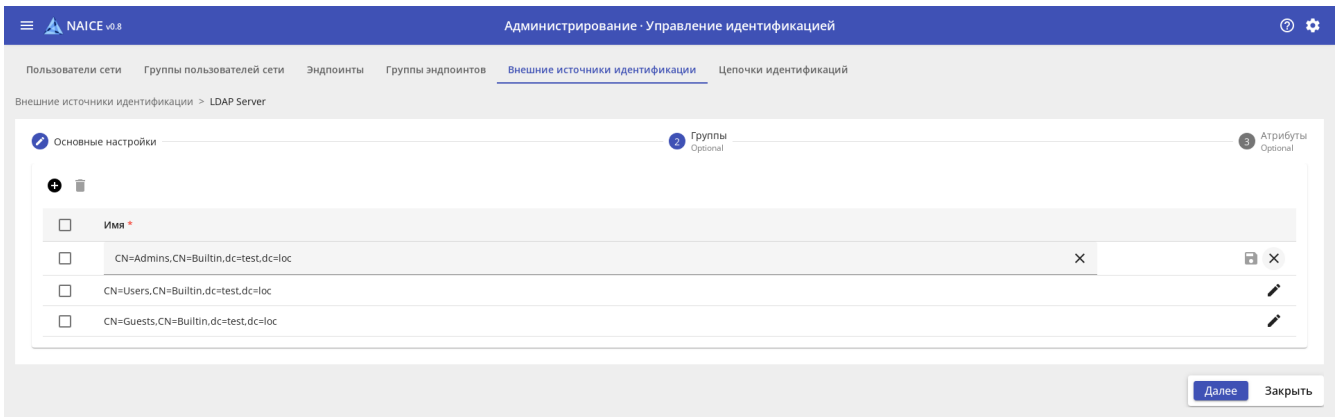


Рисунок 82. Таблица групп в режиме редактирования

После нажатия на кнопку **+** откроется меню:

- **Добавить новую группу** - создать произвольную новую группу.
- **Выбрать группы из службы каталогов** - добавить группы из источника идентификации.

### Добавить новую группу



Рисунок 83. 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

#### Выбрать группы из службы каталогов

Список групп службы каталогов может быть использован при настройке условий. Нажмите "Получить данные", чтобы прочитать их из службы каталогов.

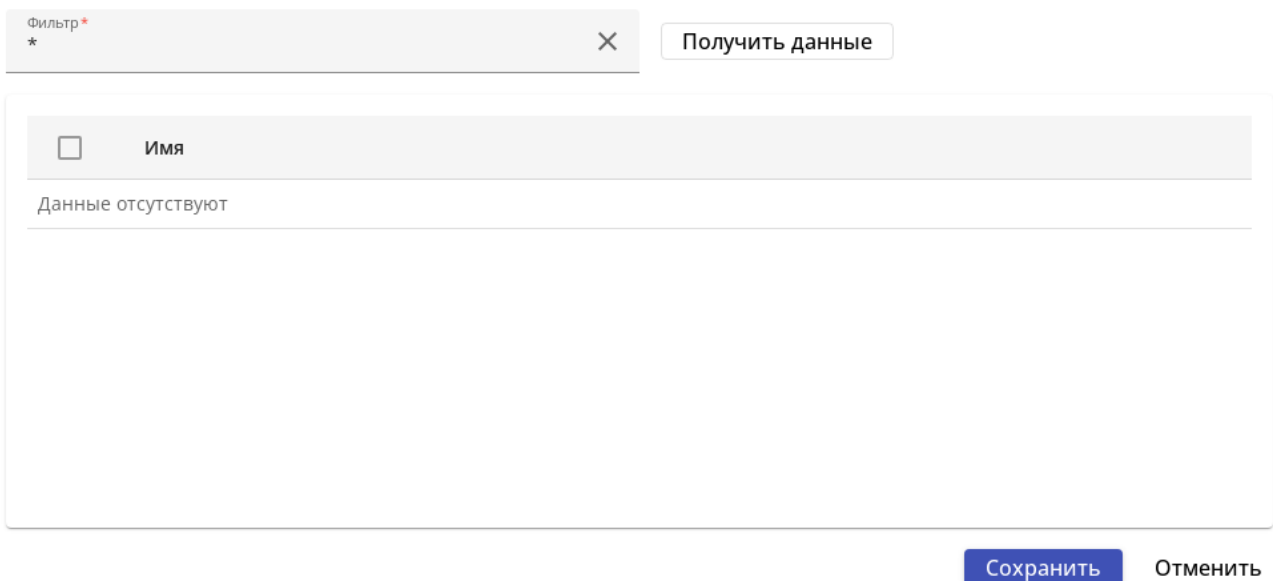


Рисунок 84. Окно выбора групп

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=Администраторы, CN=Builtin, dc=ws, dc=loc

CN=Пользователи, CN=Builtin, dc=ws, dc=loc

CN=Гости, CN=Builtin, dc=ws, dc=loc

CN=Операторы печати, CN=Builtin, dc=ws, dc=loc

CN=Операторы архива, CN=Builtin, dc=ws, dc=loc

Сохранить Отменить

Рисунок 85. 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:

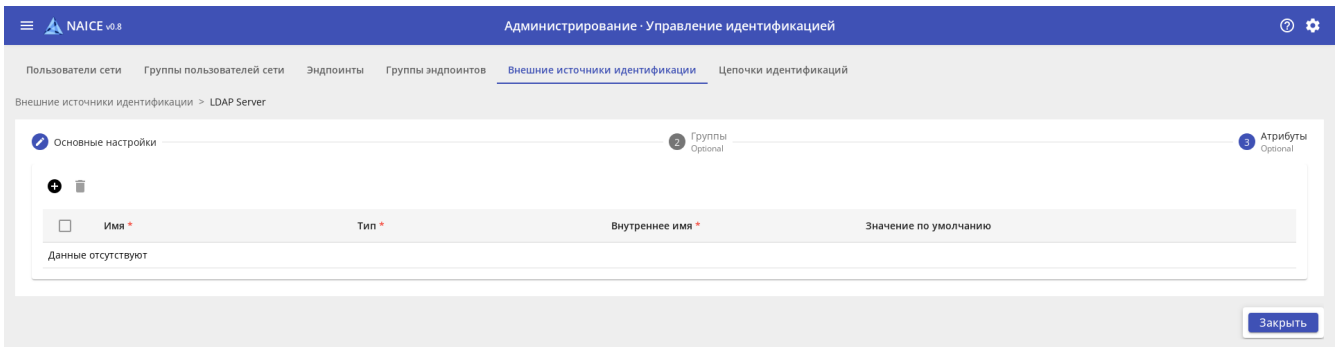






Рисунок 86. Добавление атрибутов

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 один атрибут).
-  - редактировать атрибуты (не отображается, пока не добавлен хотя бы один).
-  - сохранить атрибут после редактирования (не отображается, пока не начато редактирование).

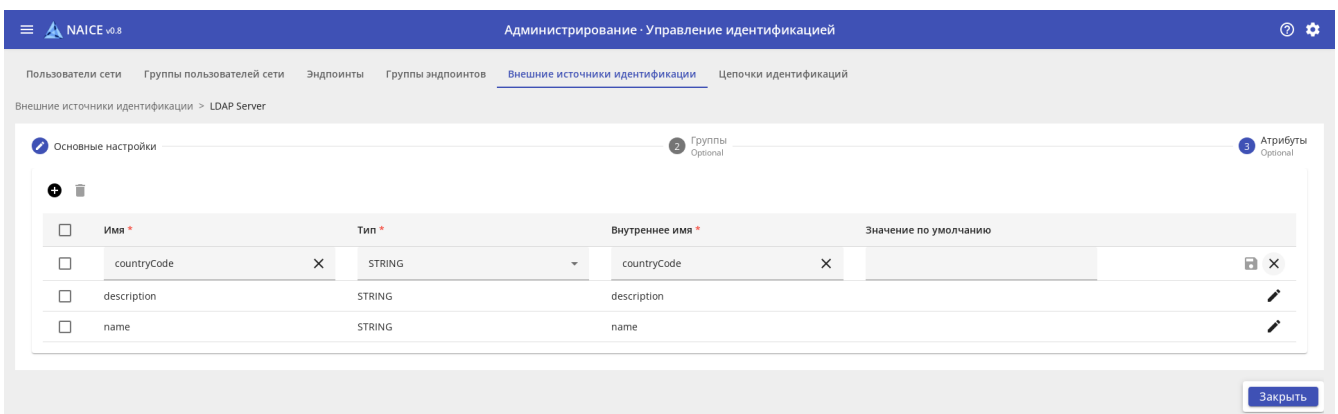


Рисунок 87. Таблица атрибутов в режиме редактирования

После нажатия на кнопку  откроется меню:

- **Добавить новый атрибут** - создать произвольный новый атрибут.
- **Выбрать атрибут из службы каталогов** - добавить атрибут из источника идентификации.

## Добавить новый атрибут

<input type="checkbox"/>	Имя *	Тип *	Внутреннее имя *	Значение по умолчанию	
<input type="checkbox"/>		STRING			
<input type="checkbox"/>	countryCode	STRING	countryCode		
<input type="checkbox"/>	description	STRING	description		
<input type="checkbox"/>	name	STRING	name		

Рисунок 88. 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.

<input type="checkbox"/>	Имя	Атрибут	Значение
Данные отсутствуют			

Рисунок 89. 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.
- **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 сущности. 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.

<input type="checkbox"/>	Имя	Атрибут	Значение
<input type="checkbox"/>	isCriticalSystemObject	STRING	TRUE
<input type="checkbox"/>	systemFlags	STRING	-1946157056
<input type="checkbox"/>	uSNCreated	STRING	5660
<input type="checkbox"/>	showInAdvancedViewOnly	STRING	FALSE
<input type="checkbox"/>	description	STRING	Default container for upgraded user accounts

Рисунок 90. 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.

### Добавление источника идентификации

Для добавления источника идентификации нажмите в правой части поля над таблицей, откроется следующая страница, на которой надо будет выбрать схему `CUSTOM`:

Администрирование · Управление идентификацией

Пользователи сети   Группы пользователей сети   Эндпоинты   Группы эндпоинтов   **Внешние источники идентификации**   Цепочки идентификаций

Внешние источники идентификации > Добавление

1 Основные настройки   2 Группы Optional   3 Атрибуты Optional

Имя\*

Описание

^ 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

^ Подключение

Admin dn\*   Admin password\*

Имя хоста (IP)\*   Port\*

^ Структура каталога

Subject search base\*   Group search base\*


Проверить связь с сервером

Добавить   Отменить

Рисунок 91. 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.
  - **Subject in group attribute** - атрибут, значение которого используется в значении атрибута "Group map attribute" при проверке принадлежности пользователя группе.
  - **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 (как правило, используется 389).
- Блок **Структура каталогов:**
  - Subject search base \* - контекст для поиска атрибутов записей 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),
- русские 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

После заполнения всех необходимых данных станет активна кнопка **Добавить и Проверить связь с сервером**.

Кнопка **Добавить** становится активной при условии добавления всех параметров и не зависит от успешности проверки связи с сервером.

При успешной проверки связи с сервером появится сообщение вида:

## Результат подключения

Привязка LDAP к "example.org:389" выполнена успешно:

кол-во предметов: "25",

кол-во групп: "25".

Макс. кол-во запрашиваемых предметов и групп - 25.

Аутентификация netlogon прошла успешно

[Заккрыть](#)

Рисунок 92. Привязка к LDAP выполнена успешно



При проверке соединения запрашивается не более 5 предметов и групп, что бы не вызывать лишнюю нагрузку на сервер, поэтому если реальных пользователей или групп больше будет показано число "5" - это не свидетельствует о проблеме.

## Добавление групп пользователей



Для возможности аутентификации через внешний источник идентификации добавление групп не является обязательным. Группы можно использовать в политиках авторизации пользователей.

После добавления источника идентификации кнопка **Добавить** примет значение "Далее". Так же можно выполнить переход нажав на надпись **(2) Группы**, откроется страница:

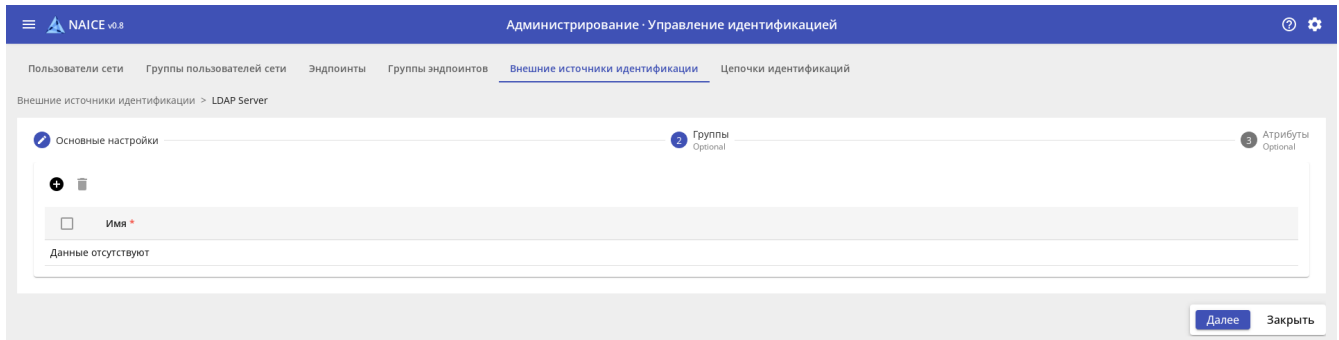


Рисунок 93. Пустая таблица групп

Элементы управления:

-  - добавить группу.
-  - удалить выбранные чекбоксом группы (неактивно, пока не выбрана хоть одна группа).

После нажатия на кнопку  откроется меню:

- **Добавить новую группу** - создать произвольную новую группу.
- **Выбрать группы из службы каталогов** - добавить группы из источника идентификации.

## Добавить новую группу



Рисунок 94. 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

### 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

Данные отсутствуют

Сохранить Отменить

Рисунок 95. 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

users

admins

guests

staff

workers

Сохранить Отменить

Рисунок 96. 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:

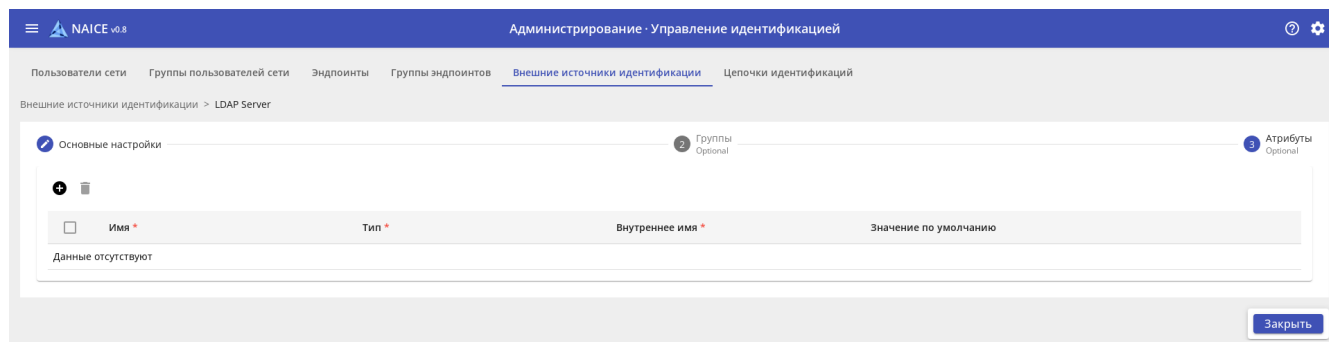




Рисунок 97. Добавление атрибутов

Элементы управления:

-  - добавить атрибуты.
-  - удалить выбранные чекбоксом атрибуты (неактивно, пока не выбран хоть один атрибут).

После нажатия на кнопку  откроется меню:

- **Добавить новый атрибут** - создать произвольный новый атрибут.
- **Выбрать атрибут из службы каталогов** - добавить атрибут из источника идентификации.

## Добавить новый атрибут

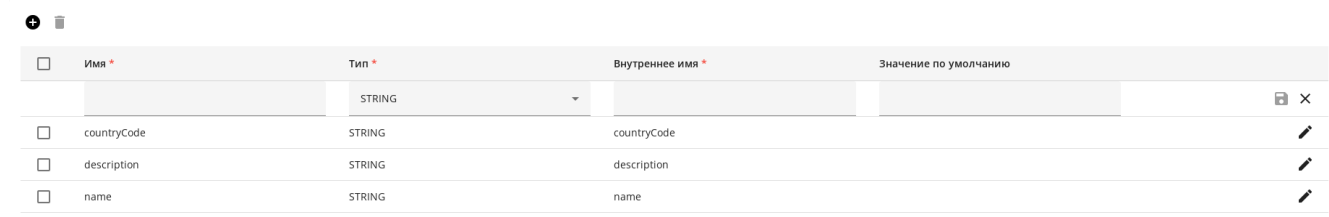


Рисунок 98. Добавить новый атрибут

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\*  
сп=\*

Получить данные

<input type="checkbox"/>	Имя	Атрибут	Значение
Данные отсутствуют			

Сохранить

Отменить

Рисунок 99. 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

<input type="checkbox"/>	Имя	Атрибут	Значение
<input type="checkbox"/>	isCriticalSystemObject	STRING	TRUE
<input type="checkbox"/>	systemFlags	STRING	-1946157056
<input type="checkbox"/>	uSNCreated	STRING	5660
<input type="checkbox"/>	showInAdvancedViewOnly	STRING	FALSE
<input type="checkbox"/>	description	STRING	Default container for upgraded user accounts

Сохранить Отменить

Рисунок 100. 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!

## 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.

## Редактирование источника идентификации

Для редактирования ранее добавленного источника идентификации на странице просмотра нажмите на имя источника в таблице.

<input type="checkbox"/>	Имя ↑
<input type="checkbox"/>	Active Directory
<input type="checkbox"/>	LDAP Server


Рисунок 101. Колонка имя

Откроется страница редактирования:

Рисунок 102. Страница редактирования источника

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

## Удаление источника идентификации

Для удаления одного или нескольких источников идентификации необходимо на странице просмотра через чекбокс  выбрать необходимые источники и в правом верхнем углу над таблицей нажать на  .

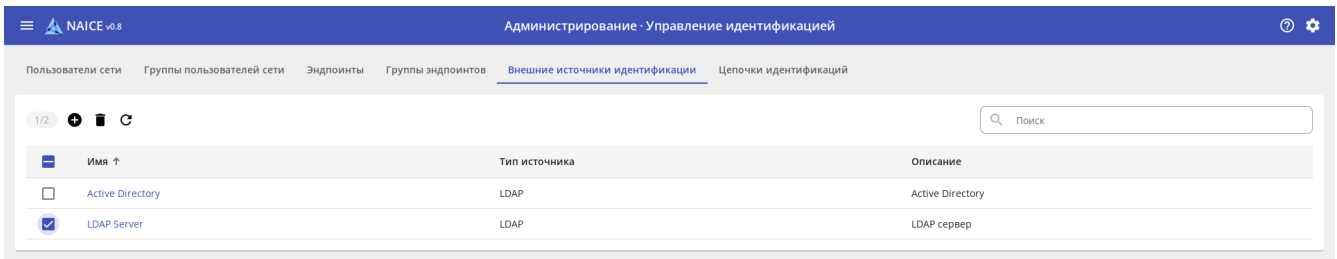


Рисунок 103. Выбор источников для удаления



Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.



### Подтверждение действия

Данные будут удалены. Вы уверены?

Да

Нет

Рисунок 104. Модальный диалог подтверждения

## Цепочки идентификаций

### Описание

Цепочки идентификаций (цепочки источников идентификаций) используются в политиках аутентификации при настройке [политик доступа](#). Они определяют, в каких источниках и в каком их порядке искать пользователей при аутентификации. В качестве источников пользователей поддерживаются [внутренняя база данных пользователей](#) и [внешние источники идентификации](#), такие как MS AD и OpenLDAP.

### Просмотр цепочек идентификаций

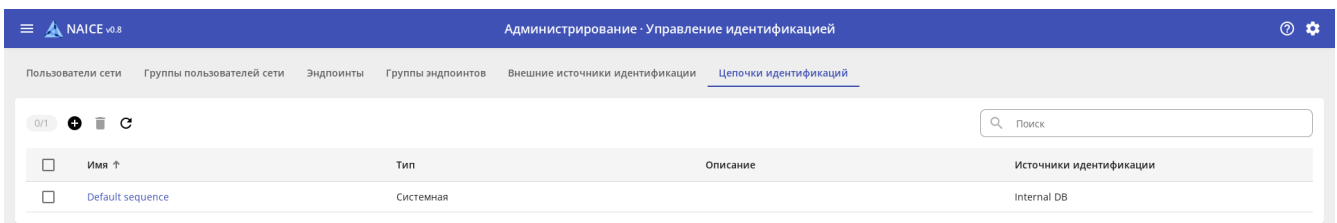


Рисунок 105. Просмотр цепочек идентификации

На данной странице содержится таблица со списком всех цепочек идентификаций.

Таблица содержит колонки:

- **Имя** - название цепочки.
- **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:

- **0/1** - Счетчик выбранных чекбоксом элементов / общего количества элементов.
- **+** - Добавить новый элемент.
- **🗑** - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- **↻** - Обновить данные таблицы.
- **🔍 Поиск** - Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
- **↑** - Изменить текущий порядок сортировки.
- **☐** - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).



Нельзя переименовать или удалить системные цепочки идентификации: "[Default sequence]"

## Добавление цепочки идентификаций

Для добавления цепочки идентификаций **+** в левой части поля над таблицей страницы просмотра, откроется следующая страница:

Рисунок 106. 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.

- **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.

<input type="checkbox"/>	Имя ↑
<input type="checkbox"/>	Default sequence
<input type="checkbox"/>	my_first_sequence

Рисунок 107. Гиперссылка на страницу редактирования цепочки идентификации

Откроется страница редактирования.

The screenshot shows the 'my\_first\_sequence' configuration page in the NAICE v0.8 administration interface. The page has a blue header with the NAICE logo and navigation tabs. The main content area includes a form with the following elements:

- Name:** my\_first\_sequence
- Type:** Создана администратором
- Description:** (empty text area)
- Authentication by certificate:** A checkbox labeled 'Использовать для идентификации атрибут сертификата' is unchecked. The 'Type' dropdown is set to 'Subject - Common Name'.
- List of authentication sources:** Two columns are shown: 'Доступные' (Available) containing 'Endpoints' and 'Используемые\*' (Used) containing 'Internal DB'. Between the columns are buttons for '➤' (Add) and '⏪' (Remove).
- Buttons:** 'Сохранить' (Save) and 'Отменить' (Cancel) buttons are located at the bottom right.

Рисунок 108. 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

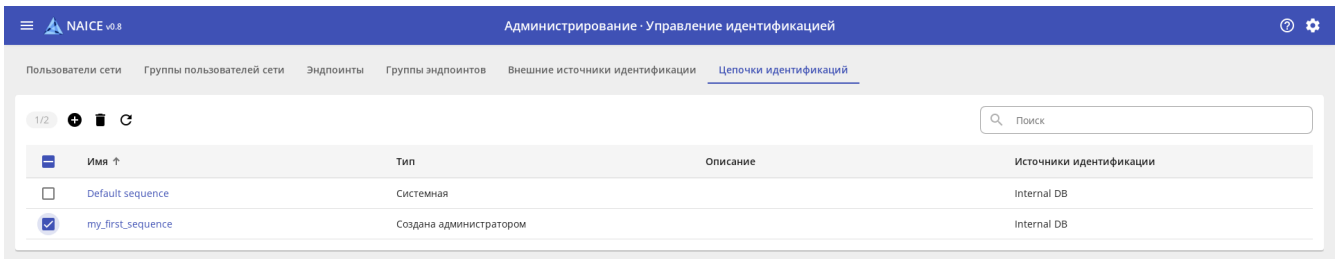


Рисунок 109. Выбор цепочек для удаления



Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.



### Подтверждение действия

Данные будут удалены. Вы уверены?

Да

Нет

Рисунок 110. Модальный диалог подтверждения



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.

# Контроль сетевых устройств



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](mailto:eltex@eltex-co.ru).

Раздел *Контроль сетевых устройств* содержит сущности 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 сетевых устройств](#) - 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

#### 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 [Политики доступа - Элементы - Условия](#), однако для создания условий доступны только атрибуты, которые могут использоваться в [:policy-sets/index.html](#).

## Просмотр списка логических условий

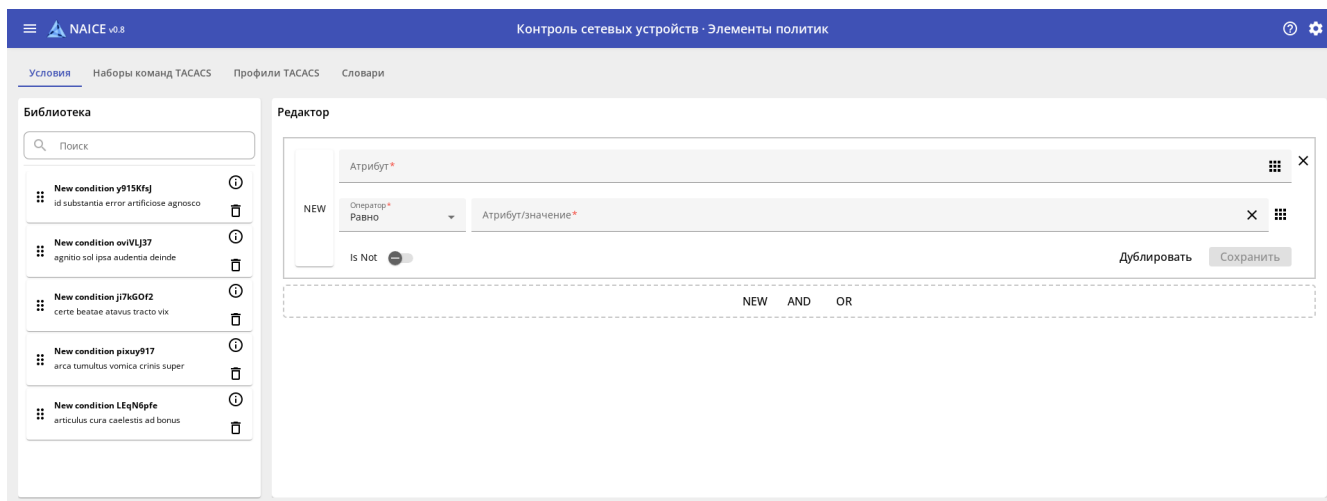


Рисунок 111. Библиотека логических условий

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)
- **Атрибут/значение \*** - атрибут/значение, которые используются для сопоставления с атрибутом логического условия в соответствие 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






🔍 Атрибут    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

Рисунок 112. 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+.

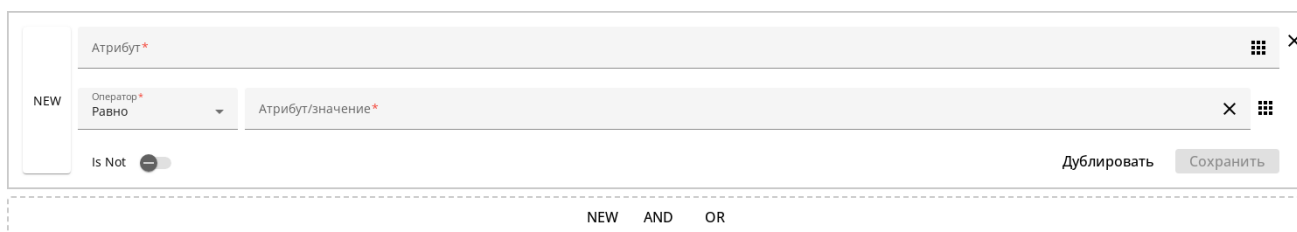
Ниже находятся колонки для фильтрации атрибутов.

- "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**.

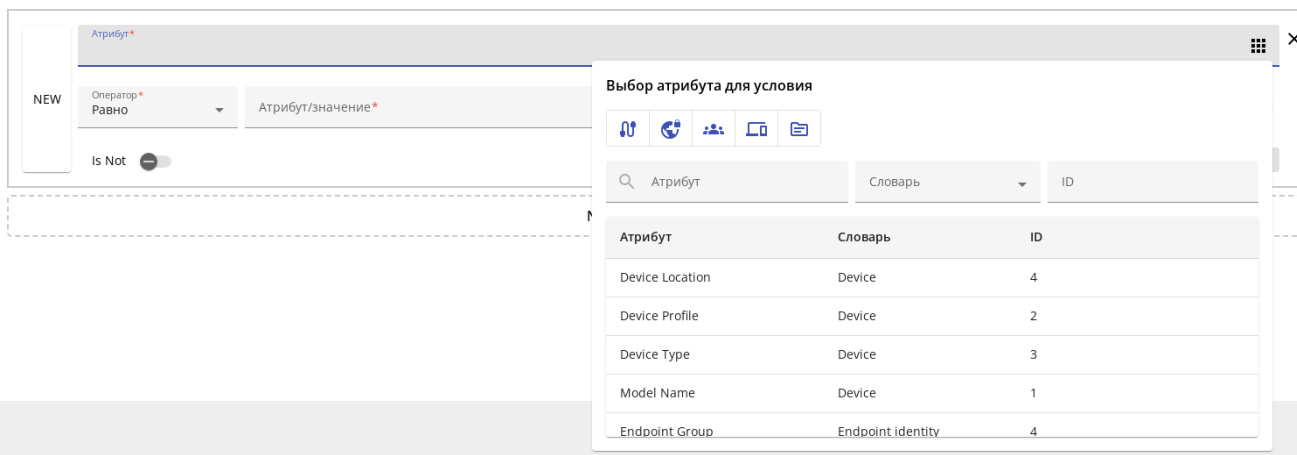


The screenshot shows the 'Condition Editor' interface. At the top, there is a field labeled 'Атрибут\*' with a grid icon and a close button. Below it, the 'Оператор\*' is set to 'Равно'. The 'Атрибут/значение\*' field is empty. There is a toggle for 'Is Not' and buttons for 'Дублировать' and 'Сохранить'. Below the editor, there are options for 'NEW AND OR'.

Рисунок 113. 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.



The screenshot shows the 'Condition Editor' with the 'Выбор атрибута для условия' menu open. The menu has search fields for 'Атрибут', 'Словарь', and 'ID'. Below the search fields is a table with the following data:

Атрибут	Словарь	ID
Device Location	Device	4
Device Profile	Device	2
Device Type	Device	3
Model Name	Device	1
Endpoint Group	Endpoint Identity	4

Рисунок 114. 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
Число	Больше или равно, Больше чем, Меньше или равно, Меньше чем, Равно, Не равно, Равно NULL, Не равно NULL
IPv4 адрес	Равно, Не равно, Равно NULL, Не равно NULL
MAC адрес	Равно, Не равно, Равно NULL, Не равно NULL, Начинается на, Не начинается на, Заканчивается на, Не заканчивается на, Содержит, Не содержит,
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.

The screenshot shows a configuration window for a condition. At the top, the attribute is set to "ТАСАС+Authen-Method". Below this, there are two dropdown menus: "Оператор" (Operator) set to "Равно" (Equal) and "Атрибут/значение" (Attribute/Value) set to "NotSet". There is a toggle switch for "Is Not" which is currently turned off. At the bottom right of the form, there are two buttons: "Дублировать" (Duplicate) and "Сохранить" (Save). Below the form, the logical operators "NEW AND OR" are displayed.

Рисунок 115. 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\*

Сохранить в библиотеку как новое условие

Имя\*

New condition u66Xnuwo

Описание

Сохранить

Отменить

Рисунок 116. Диалог сохранения условия в библиотеку

По умолчанию действие предполагает сохранение нового условия:

- "Наименование" \* - 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.

NEW AND OR

Рисунок 117. 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 118. 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.

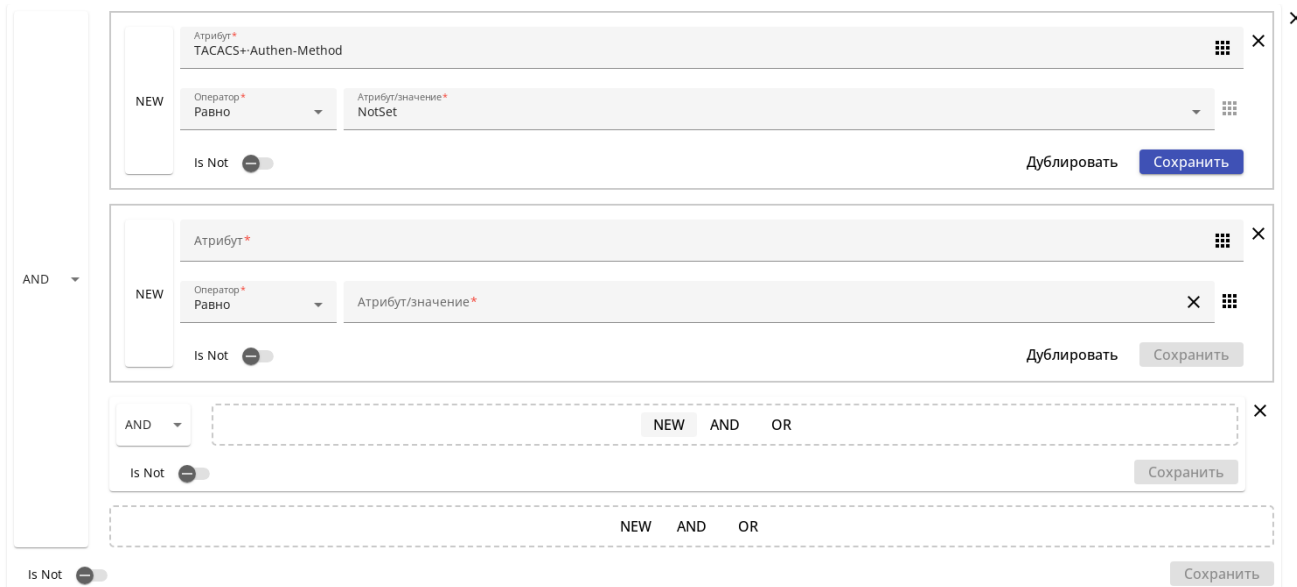


Рисунок 119. Условие, содержащее вложенные правила

Для сохранения всех условий надо нажать кнопку "Сохранить" в нижнем правом углу.

## Редактирование логического условия

Для редактирования логического условия необходимо его захватить курсором в библиотеке и перенести в поле редактора.

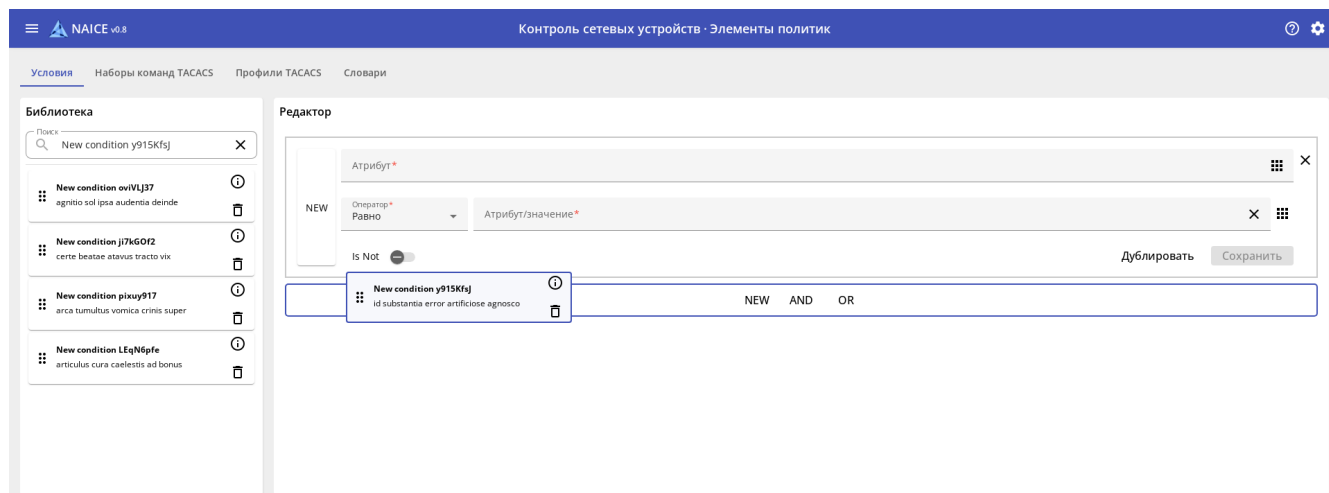


Рисунок 120. Выбор логического условия

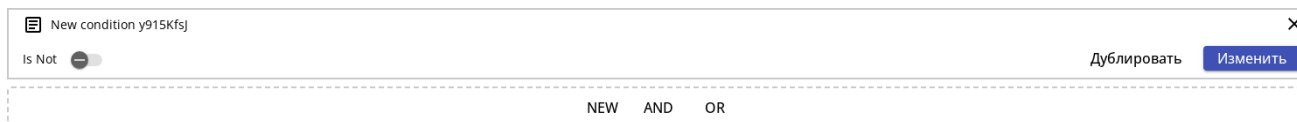



Рисунок 121. Редактирование логического условия

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.

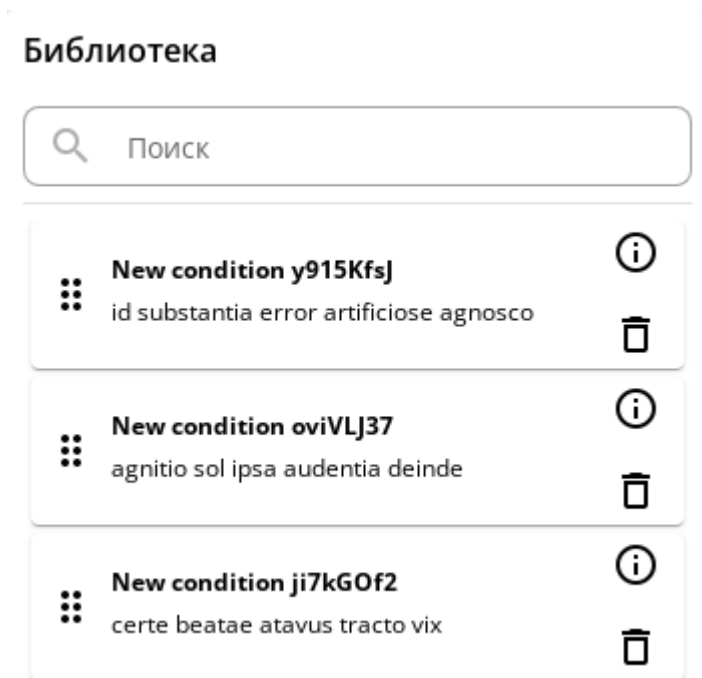


Рисунок 122. Выбор условия для удаления



Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.



### Подтверждение действия

Данные будут удалены. Вы уверены?

Да

Нет

Рисунок 123. Модальный диалог подтверждения



#### Ограничения:

- нельзя удалить 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

## 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 [Политиках сетевых устройств](#) при настройке политики авторизации.

## Просмотр наборов команд TACACS

На данной странице содержится таблица со списком всех наборов команд TACACS.

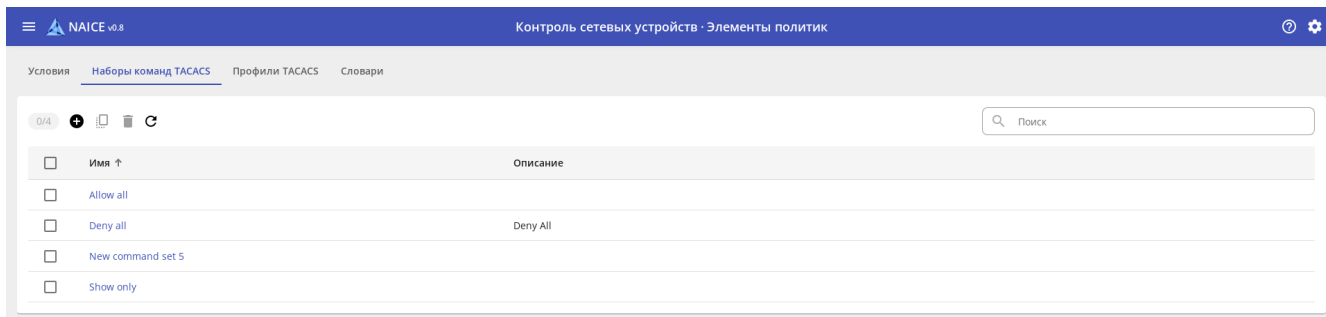


Рисунок 124. Таблица со списком наборов команд TACACS на странице просмотра

Таблица содержит колонки:

- **Имя** - название набора команд.
- **Описание** - произвольное описание.

Сортировка возможна только по полю "Имя" в прямом и обратном порядке. По умолчанию сортировка выполняется в прямом (алфавитном) порядке.

Элементы управления:

- **0/1** - Счетчик выбранных чекбоксом элементов / общего количества элементов.
- **+** - Добавить новый элемент.
- **🗑️** - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- **🔄** - Обновить данные таблицы.
- **🔍 Поиск** - Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
- **↑** - Изменить текущий порядок сортировки.
- - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).
- **📄** - Дублировать выбранный чекбоксом набор команд.

## Добавление нового набора команд

Для добавления набора команд нажмите **+** в левой верхней части поля над таблицей.

Рисунок 125. 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 сохранения созданного набора команд необходимо нажать на кнопку **Сохранить**, или отменить создание с помощью **Отменить**.

## Редактирование набора команд

Для редактирования набора команд TACACS необходимо на странице со списком нажать на его имя.

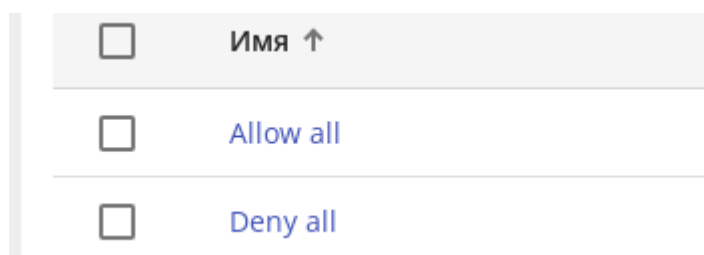



Рисунок 126. Гиперссылка на страницу редактирования набора команд

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.

После редактирования нажать на кнопку **Сохранить**. Кнопка остается неактивной, пока не будет изменено хотя бы одно поле.

## 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 1. 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 2. 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
show	(radius-servers) (tacacs)

### 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.

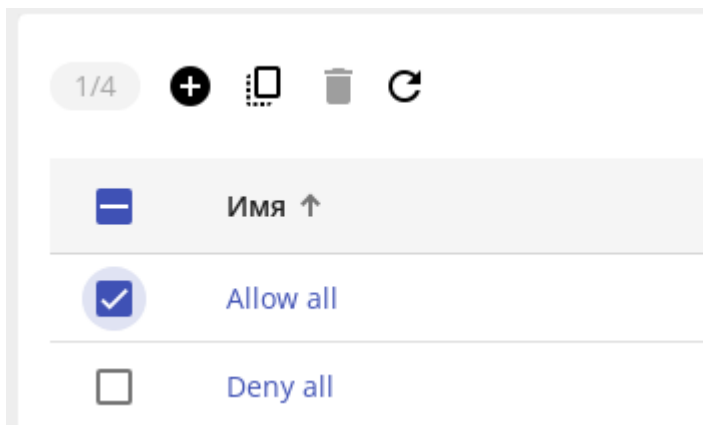


Рисунок 127. Выбор набора команд в таблице для удаления



Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.



### Подтверждение действия

Данные будут удалены. Вы уверены?

Да

Нет

Рисунок 128. Модальный диалог подтверждения



#### Ограничения:

- нельзя удалить наборы команд, которые используются в какой-либо политике сетевых устройств.
- нельзя удалить системные наборы команд `Allow all`, `Deny all` и `Show only`.

## Профили TACACS

### Описание

Профили TACACS предназначены для обобщения тонкой настройки уровней привилегий доступа к сетевым устройствам в отдельные сущности, 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

Имя ↑	Описание
<input type="checkbox"/> Both privilege	
<input type="checkbox"/> Deny all shell profile	Deny all shell profile
<input type="checkbox"/> Maximum privilege	
<input type="checkbox"/> Minimum privilege	
<input type="checkbox"/> New profile 8	

Рисунок 129. Таблица с перечнем профилей TACACS

На данной странице содержится таблица со списком профилей TACACS.

Таблица содержит колонки:

- **Имя** - наименование профиля;
- **Описание** - произвольное описание профиля.

Доступна сортировка по колонке **Имя**.

Элементы управления:

- **0/1** - Счетчик выбранных (отмеченных флажком), а так же общего количества профилей.
- **+** - Добавить профиль TACACS.
- **📄** - Дублировать профиль TACACS.
- **🗑** - Удалить выбранный (отмеченный флажком) профиль TACACS.
- **🔄** - Обновить список профилей.

## Добавление профиля TACACS

Имя\*

Описание

Атрибуты Передаваемые параметры

Уровень привилегий ⓘ

Уровень привилегий по умолчанию Значение\*

Максимальный уровень привилегий Значение\*

Пользовательские атрибуты

0/0 + 🗑

Имя\* Значение\*

Данные отсутствуют

Добавить Отменить

## Рисунок 130. Страница добавления профиля TACACS

Для добавления профиля устройства нажмите .

В открывшемся окне необходимо заполнить следующие параметры:

Параметры отмеченные символом \* - обязательны для заполнения.




**Имя \*** - Наименование профиля. **Описание** - Описание профиля в произвольной форме (будет отображаться в списке профилей). **Уровень привелегий по умолчанию** - Уровень привилегий доступный авторизуемому администратору сразу после авторизации. **Максимальный уровень привелегий** - Уровень привилегий доступный к повышению авторизованному администратору (данный уровень пользователь может включить при помощи авторизованных команд, например в процессе конфигурации сетевого устройства).



Если флажки включения параметров **Уровень привелегий по умолчанию** и **Максимальный уровень привелегий** сняты, авторизуемой учетной записи администратора будет назначен единственный доступный уровень привилегий "1" по умолчанию.

**Пользовательские атрибуты** илб 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:

-  - Счетчик выбранных (отмеченных флажком), а так же общего количества атрибутов.
-  - 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".

### 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".

# Политики сетевых устройств

## Описание

Политики сетевых устройств 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 политик сетевых устройств.

- 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 попыток	Действия	Настройка
✔	Policy set bdbbd5de-7bbc-6b6c-ce9c-addbbc181a7f	description	test condition f3P07KBJ	PAP/ASCII	1	⋮	»
✔	Default	Tacacs default policy set		PAP/ASCII	1	⋮	»




Рисунок 131. 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 попыток авторизации, подпадающих под указанные Условия.
- Действия - действия по добавлению/удалению набора политик.
- Настройка - переход к просмотру и редактированию политики.

Элементы управления:

- Поиск - регистронезависимый поиск по имени набора политик (найденные совпадения будут подсвечены желтым цветом).
- - обновить данные.
- Сбросить - сбросить счетчики количества срабатываний всех наборов политик (попыток).
- - добавить политику сетевых устройств (политика будет добавлена первой в списке).
- - Счетчик количества попыток авторизации, подпадающих под указанные Условия.

-  - действия:
  - Добавить сверху - добавить политику До выбранного;
  - Добавить снизу - добавить политику После выбранного;
  - Удалить - удалить выбранную политику.
-  - перейти к управлению выбранной политикой.
- Сохранить - сохранить изменения.
- Отменить - отменить изменения.
-  - Элемент для перетаскивания политик в списке.

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 желтым цветом, не скрывая их из списка.

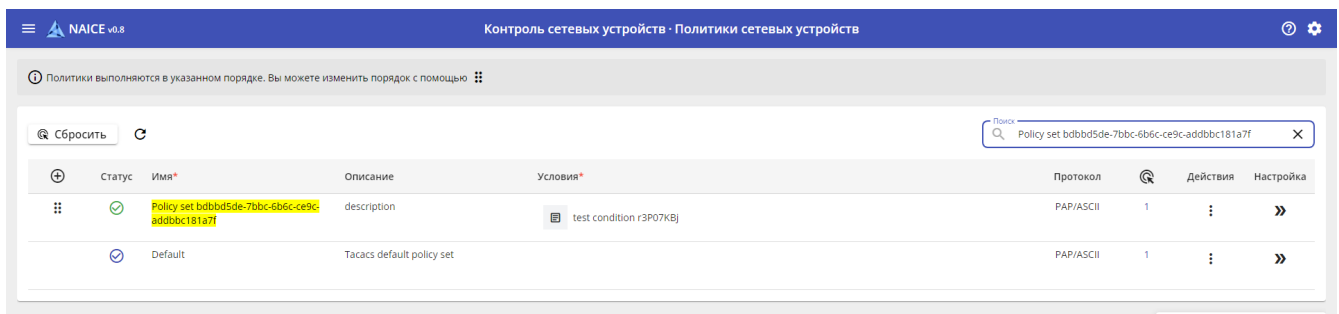



Рисунок 132. Поиск Политики.

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 в колонке Просмотр нажать  справа от выбранного набора политик.

## Редактирование политик

Для добавления политики в окне списка политик - можно нажать сверху слева кнопку  - новая политика будет добавлена первой в списке.

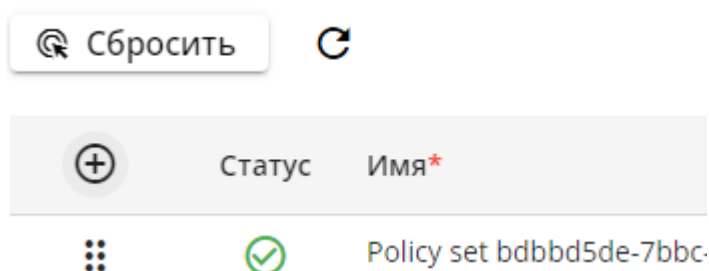



Рисунок 133. Иконка добавления политики.

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**.

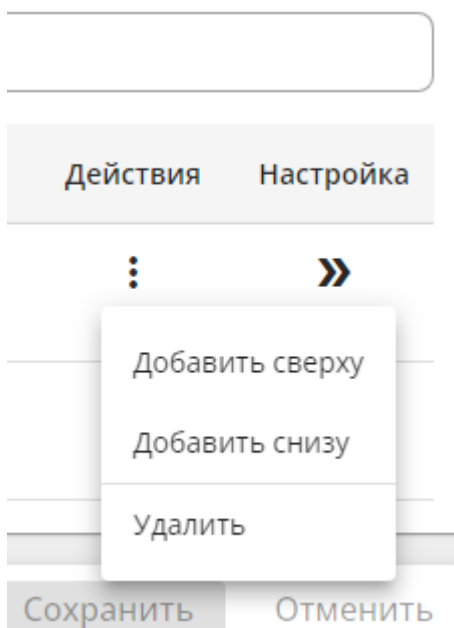






Рисунок 134. Отображение политики. Выпадающее меню с действиями.

Информация по Статусу :

-  **Включено** - разрешается обрабатывать запросы;
-  **Выключено** - исключить из обработки, не проверять Условие, не обрабатывать запросы;
-  **Монитор** - разрешается проверять Условие (и инкрементировать счётчик срабатываний), обрабатывать запросы - нет;
-  **По умолчанию** - используется только для политики по умолчанию `Default`.

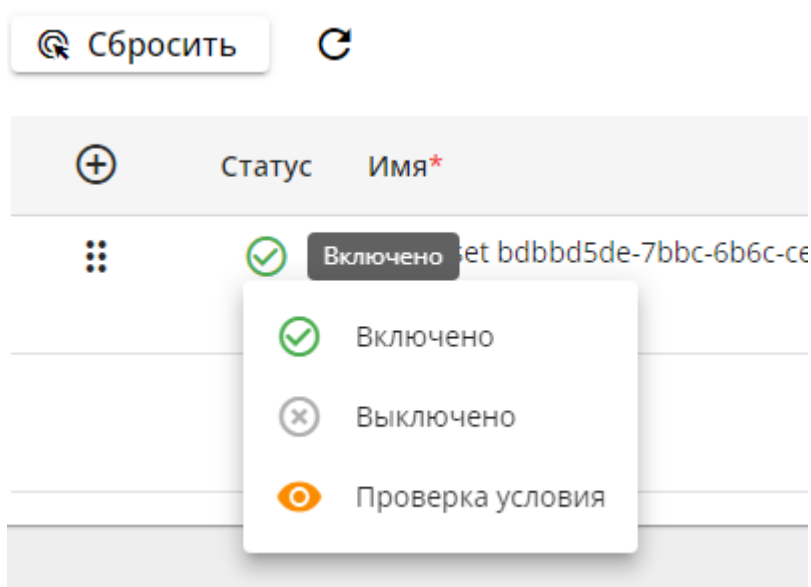


Рисунок 135. Изменение статуса политики.

Во вновь созданной политике в поле **Имя** ввести читаемое наименование или оставить неизменным автоматически сформированное название.

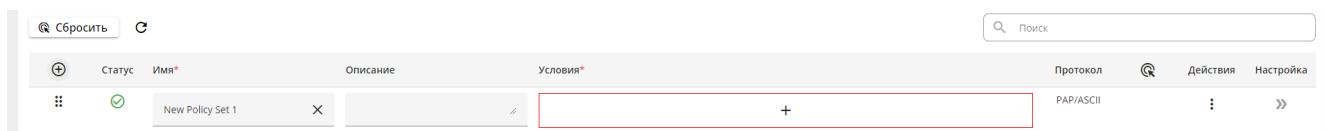


Рисунок 136. Отображение записи новой политики. Элементы обязательные для заполнения.

Для редактирования условия необходимо нажать **+** и откроется редактор условий.

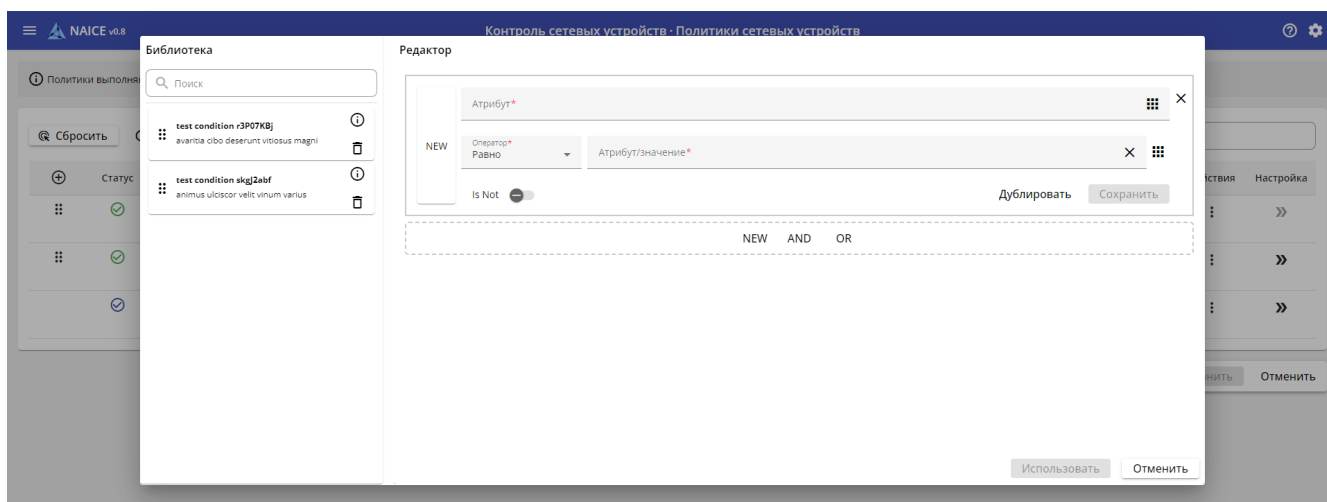


Рисунок 137. Редактор условий.

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 надо после настройки, не сохраняя условие, нажать кнопку **Использовать**.

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 в правиле, а в по умолчанию **Default**!

## Удаление политики

Удаление набора политик доступно в меню **Действия**. Доступно удаление только одного набора политик за раз.

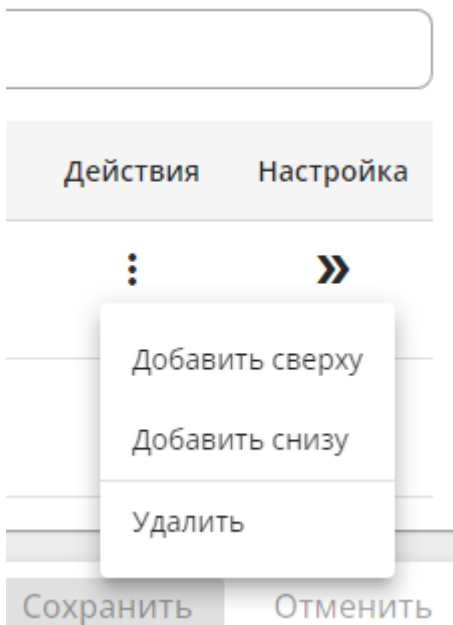



Рисунок 138. Выпадающее меню для удаления политики.

## Количество срабатываний политики

Счётчики в колонке  показывают, сколько попыток было обработано с использованием этой политики. Изменения значений свидетельствует, что **Условие** срабатывает.

## Настройка политики контроля сетевых устройств

### Просмотр списка политик аутентификации и авторизации в выбранном наборе политик контроля сетевых устройств

Для просмотра списка политик аутентификации и авторизации TACACS необходимо в колонке **Просмотр** нажать **>>** справа от выбранного [набора политик]. Откроется детальная страница по изменению правил политик аутентификации и авторизации.

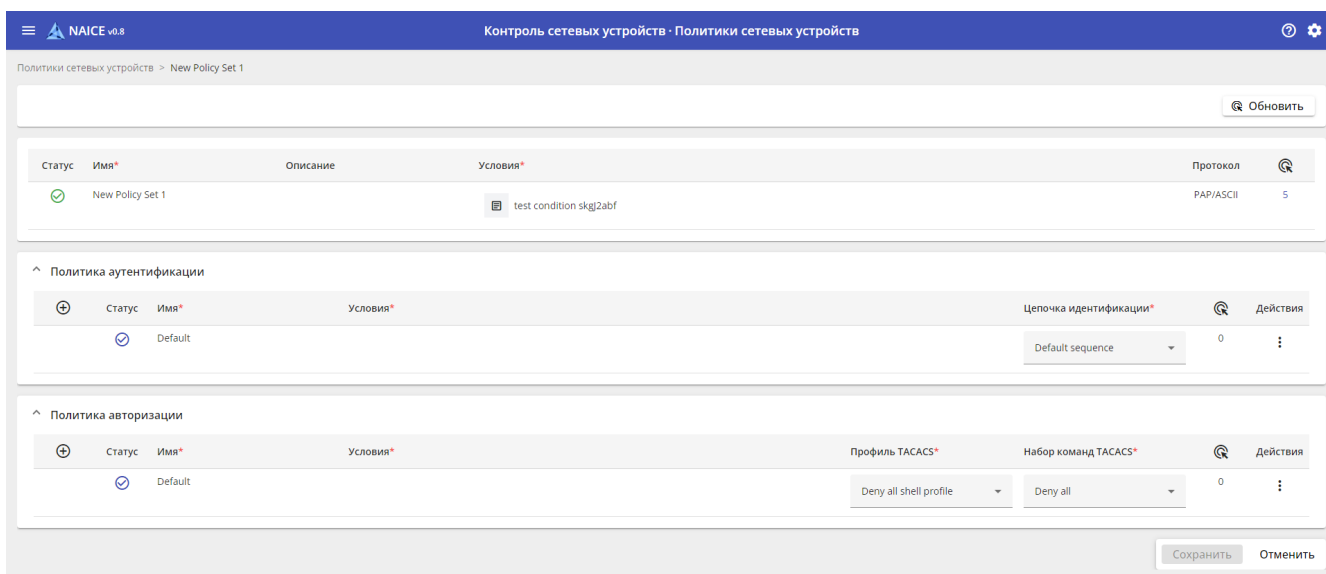


Рисунок 139. Страница просмотра и редактирования набора политик





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 [Наборы политик](#).
- **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:

-  **Обновить** - запрос актуального количества срабатываний 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 авторизации].
- **Набор команд TACACS \*** - выбор доступных [наборов команд].
- **⋮** - действия:
  - **Добавить сверху** - добавить политику *До* выбранного;
  - **Добавить снизу** - добавить политику *После* выбранного;
  - **Удалить** - удалить выбранную политику.
-  - количество попыток авторизации, подпадающих под указанные Условия. При нажатии на число срабатываний счётчик можно **Сбросить**.
- **Сохранить** - сохранить изменения.
- **Отменить** - отменить изменения.

Параметры, отмеченные звёздочкой \*, обязательны для заполнения.

Для изменения порядка Политик Аутентификации и Авторизации перетащите политику за элемент **⋮** в колонке **⊕** (становится видимым при наведении в эту область) аналогично разделу [Наборы](#)

## Редактирование политик аутентификации и авторизации внутри политик контроля сетевых устройств

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 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



Рисунок 140. Панель политик "Аутентификации".

Для настройки политики аутентификации в блоке **Политика аутентификации** необходимо нажать кнопку **+**. Появится новое правило.

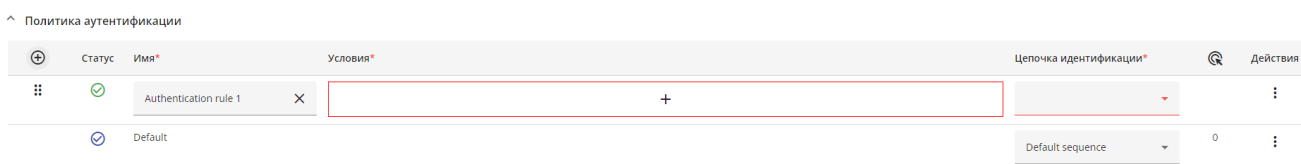


Рисунок 141. Новая политика "Аутентификации".

В поле **Имя** ввести наименование 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 надо после настройки, не сохраняя условие, нажать кнопку **Использовать**.

Кнопкой **⋮** справа от политики можно добавить новое правило выше или ниже, либо удалить текущее.

Выбрать в выпадающем меню **Цепочка идентификации** необходимую [цепочку]

По нажатию кнопки **Сохранить** изменения будут сохранены.

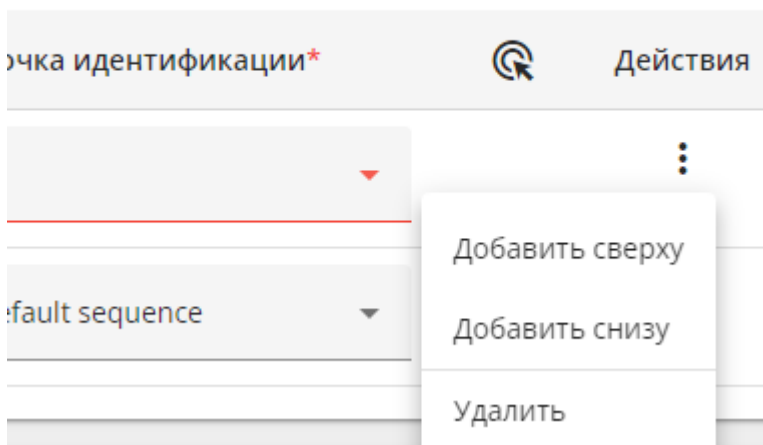


Рисунок 142. Политика аутентификации. Выпадающее меню. Действия.

Также можно изменить статус политики аналогично статусам в наборах политик.

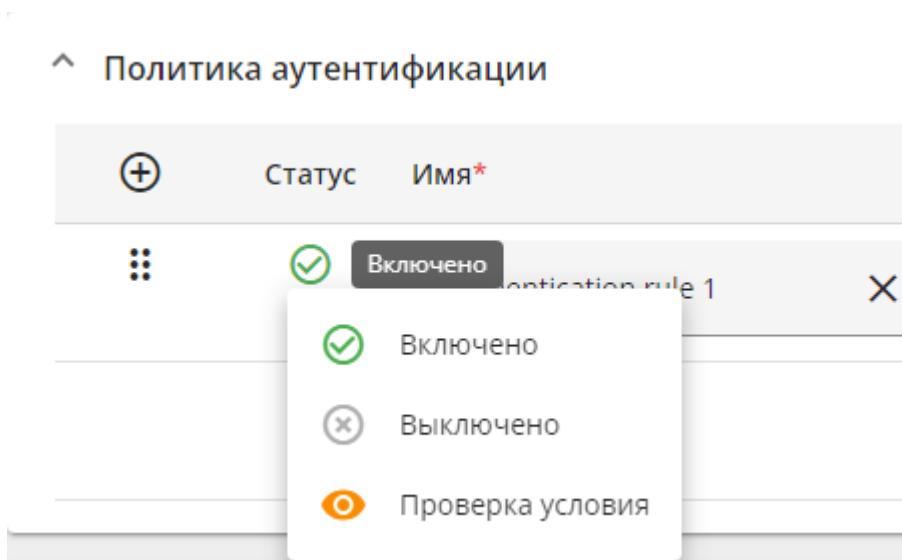


Рисунок 143. Политика аутентификации. Изменение статуса политики.

## Политика авторизации

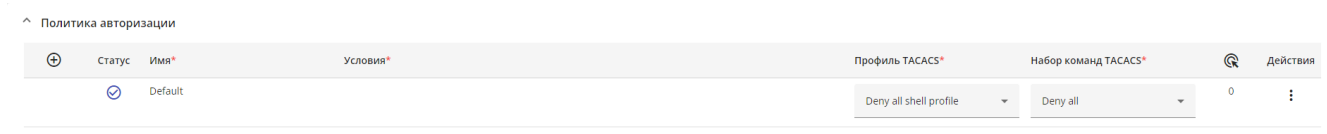


Рисунок 144. Панель политик "Авторизации".

Для настройки правила политики авторизации в блоке **Политики авторизации** нажать **+**. Появится новое правило.

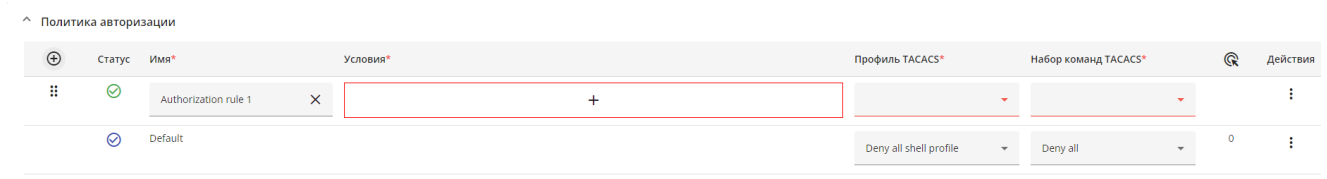


Рисунок 145. Новая политика "Авторизации".

В поле **Имя** ввести наименование правила политики.

Для редактирования условия необходимо нажать **+** - откроется редактор условий.


Редактирование условий выполняется аналогично описанному в [Условия](#).

При настройке политики авторизации можно использовать следующие словари: **LDAP**, **NETWORK\_ACCESS**, **TACACS\_PLUS**, **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].

Кнопкой  справа от политики можно добавить новое правило выше или ниже, либо удалить текущее.

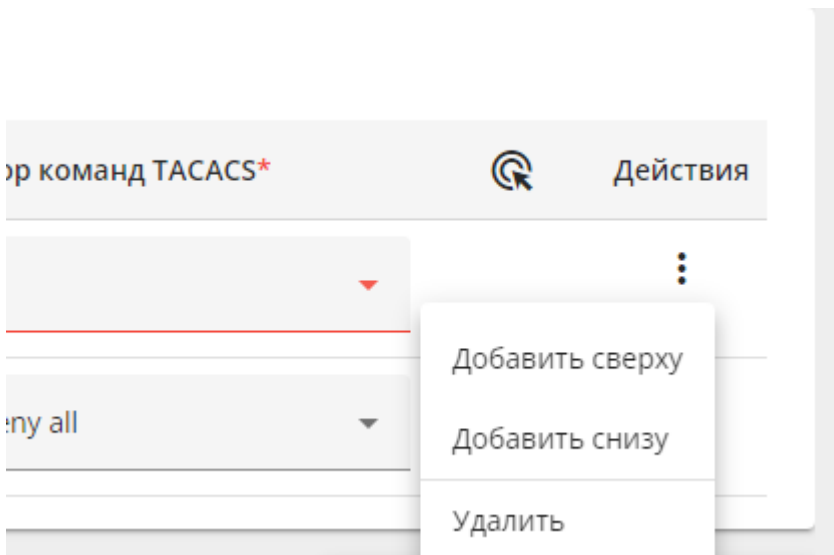


Рисунок 146. Политика авторизации. Выпадающие меню. Действия.

Также можно изменить статус политики аналогично статусам в наборах политик.

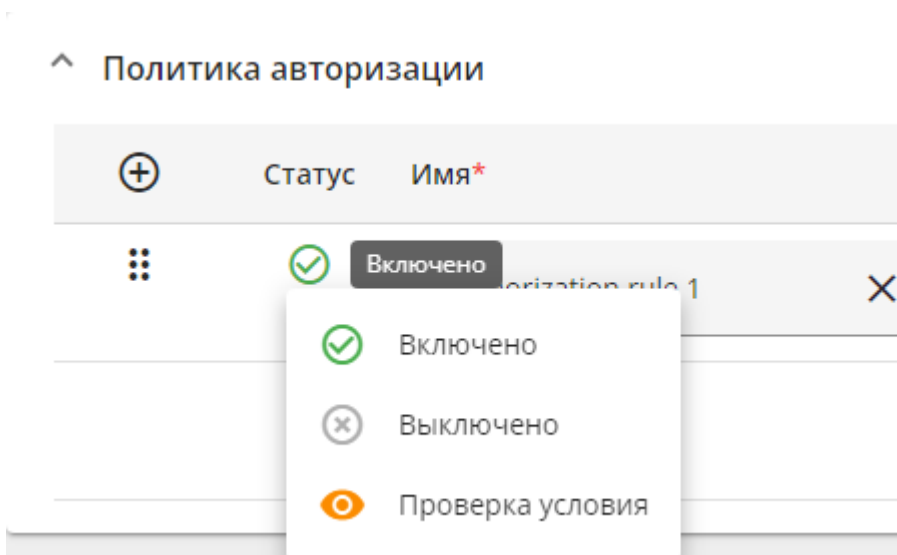


Рисунок 147. Политика авторизации. Изменение статуса политики.

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 путём нажатия кнопкой мыши на поле соответствующей настройки.

После этого необходимо нажать кнопку **Сохранить**.

## Удаление правил политик

Удаление выполняется нажатием на кнопку  и выбором действия **Удалить**.



Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.



### Подтверждение действия

Данные будут удалены. Вы уверены?

Да

Нет

Рисунок 148. Модальный диалог подтверждения

# Политики доступа

## Элементы

### 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** для каждого пользовательского сценария.

В данный момент поддерживаются следующие протоколы: PAP, MS-CHAPv2, EAP-PEAP, EAP-TLS.

Доступна настройка разрешения или запрета MAB авторизации.

#### Просмотр списков разрешенных протоколов

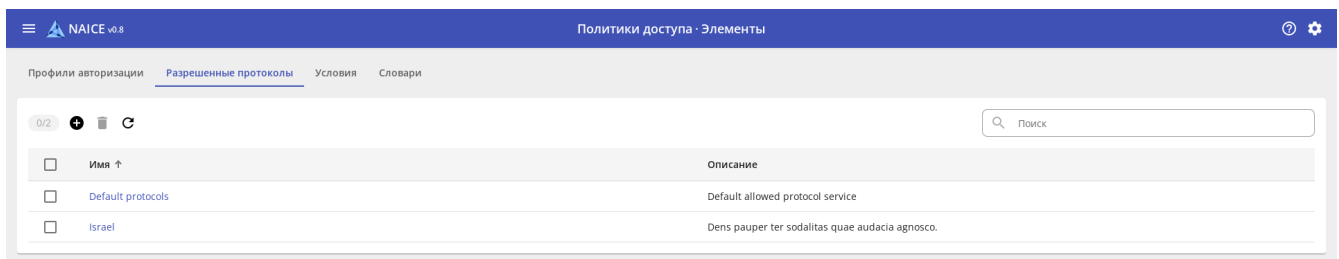


Рисунок 149. Таблица с перечнем списков разрешенных протоколов на странице просмотра

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 сервиса".

Элементы управления:

- **0/1** - Счетчик выбранных чекбоксом элементов / общего количества элементов.
- **+** - Добавить новый элемент.
- **🗑️** - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- **🔄** - Обновить данные таблицы.
- **🔍 Поиск** - Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
- **↑** - Изменить текущий порядок сортировки.
-

- Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).

## Добавление списка разрешенных протоколов

Для добавления списка разрешенных протоколов нажмите **+**, после чего откроется окно:

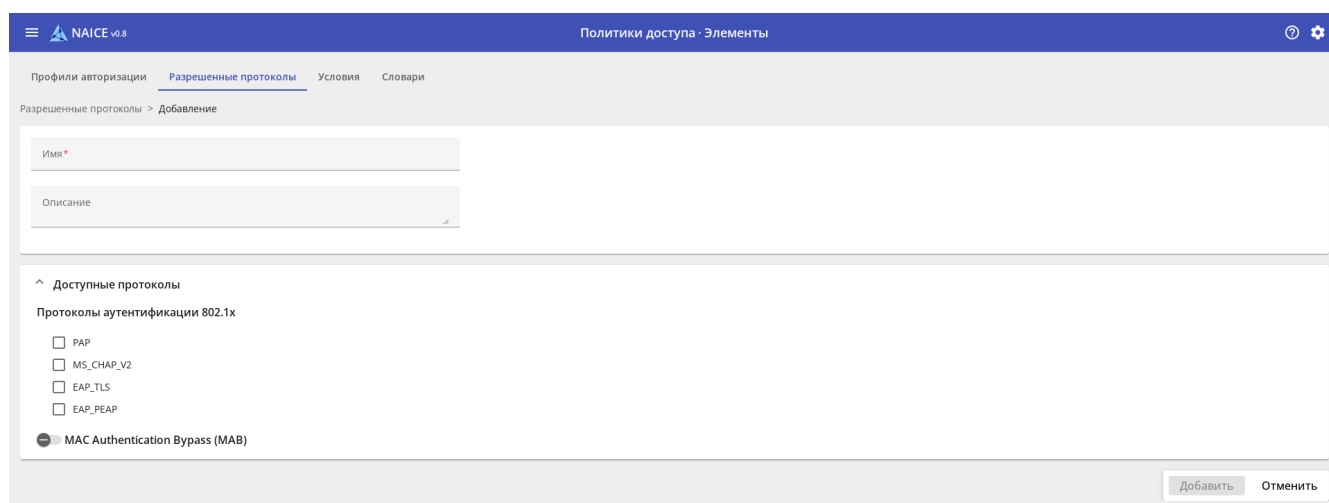


Рисунок 150. Окно добавления списка разрешенных протоколов

- **Имя \*** - наименование, должно быть уникально. Максимальная длина - 100 символов.
- **Описание** - произвольное описание. Максимальная длина - 200 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).
  - **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.

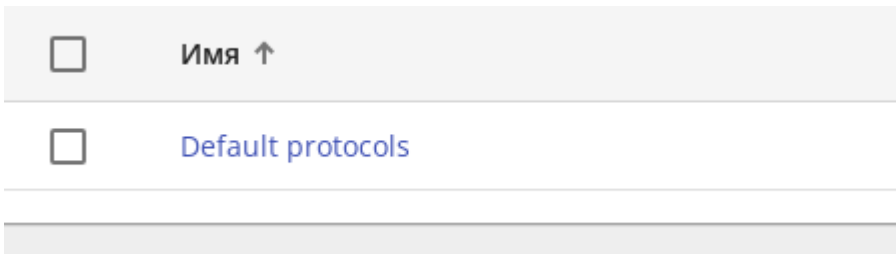


Рисунок 151. Гиперссылка на страницу редактирования списка разрешенных протоколов

После этого откроется окно редактирования, аналогичное окну добавления.

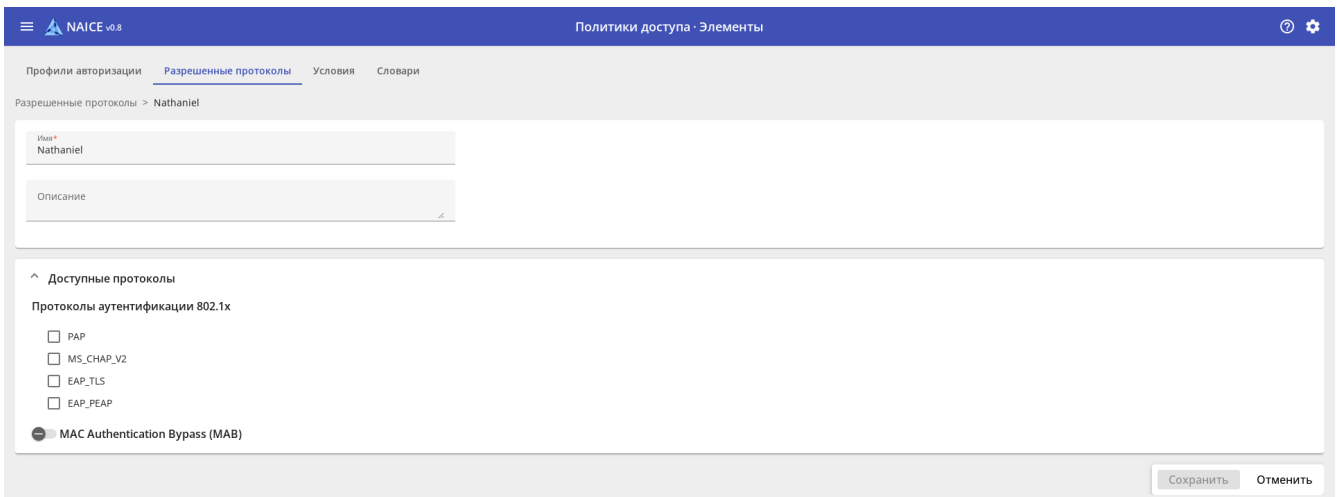



Рисунок 152. Окно редактирования списка разрешенных протоколов

После редактирования нажать на кнопку **"Сохранить"**. Кнопка остается неактивной, пока не будет изменено хотя бы одно поле.

## 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.

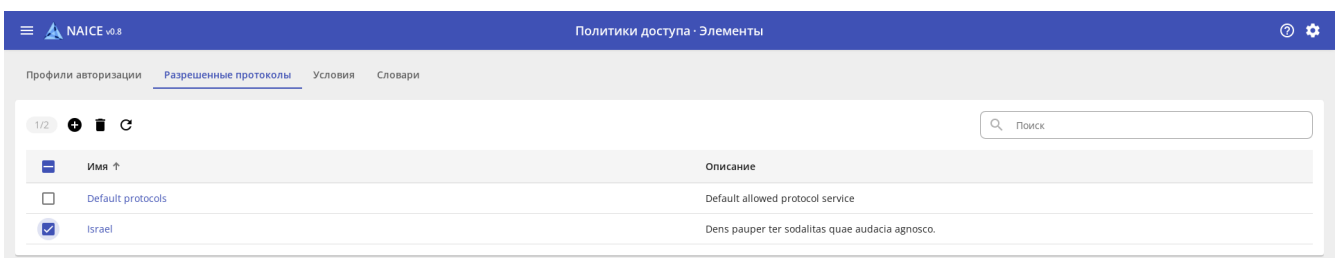


Рисунок 153. Выбор списков разрешенных протоколов в таблице для удаления



Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.



### Подтверждение действия

Данные будут удалены. Вы уверены?

Да

Нет

Рисунок 154. Модальный диалог подтверждения



**Ограничения:**

- нельзя удалить список разрешенных протоколов, которая используется в каком-либо наборе политик.

## Профили авторизации

### 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).
- Любой другой RADIUS-атрибут через Расширенные настройки атрибутов.

## Просмотр списка доступных профилей авторизации

The screenshot shows the NAICE v0.8 web interface. The top navigation bar includes 'Политики доступа · Элементы'. The main content area is titled 'Профили авторизации' and contains a table with the following data:

Имя ↑	Профиль сетевого устройства	Описание
<input type="checkbox"/> DenyAccess	DEFAULT	
<input type="checkbox"/> MES auth	Eltex MES23xx	
<input type="checkbox"/> PermitAccess	DEFAULT	
<input type="checkbox"/> Virgil	8tWYM7DY	Esse subnecto cursim curtus delicate.

Рисунок 155. 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:

- **0/1** - Счетчик выбранных чекбоксом элементов / общего количества элементов.
- **+** - Добавить новый элемент.

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

## Добавление профиля авторизации

Для добавления профиля авторизации нажмите , откроется окно добавления профиля авторизации.

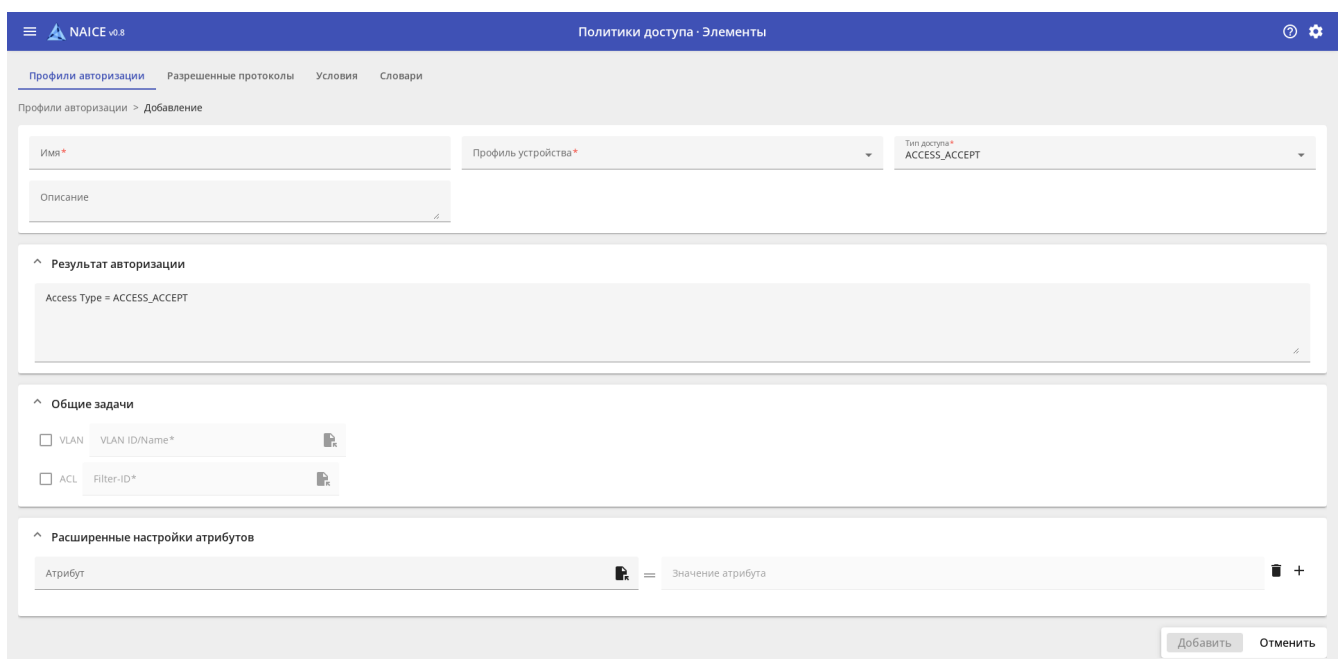


Рисунок 156. Окно добавления профиля авторизации

- **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. По умолчанию все сценарии отключены.
  - **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.
- **Расширенные настройки атрибутов** - ручная настройка выдачи RADIUS-атрибутов. Рекомендуется только в том случае, когда для определенного результата авторизации не доступен сценарий из списка **Общих задач**.

\* - поля, обязательные для заполнения.



Для динамического назначения пользователю при авторизации VLAN и ACL необходимо, чтобы данные действия были включены в [профиле сетевого устройства](#), который используется в профиле авторизации. В противном случае их настройка будет недоступна.

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.

<input type="checkbox"/>	Имя ↑
<input type="checkbox"/>	<a href="#">DenyAccess</a>
<input type="checkbox"/>	<a href="#">MES auth</a>
<input type="checkbox"/>	<a href="#">PermitAccess</a>

*Рисунок 157. Гиперссылка на страницу редактирования профиля авторизации*

После этого откроется окно редактирования, аналогичное окну добавления.

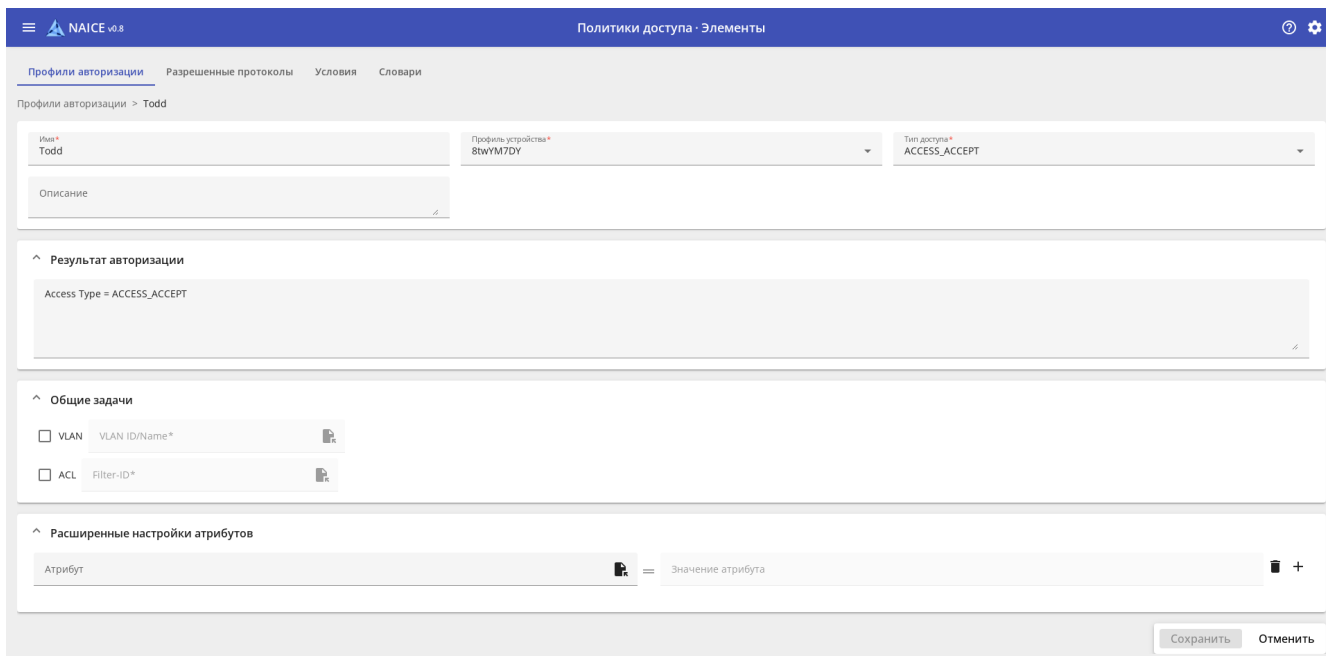



Рисунок 158. Окно редактирования профиля авторизации

После редактирования нажать на кнопку **"Сохранить"**. Кнопка остается неактивной, пока не будет изменено хотя бы одно поле.

## Удаление профиля авторизации

Для удаления в окне со списком необходимо выделить чекбокс слева от профилей авторизации, которые требуется удалить, и нажать кнопку  вверху слева.

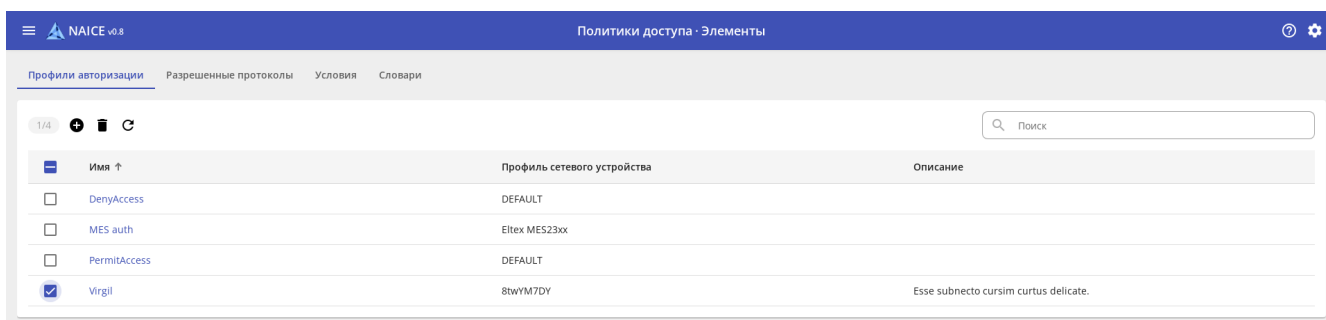


Рисунок 159. Выбор профиля авторизации в таблице для удаления



Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.



### Подтверждение действия

Данные будут удалены. Вы уверены?

Да

Нет

Рисунок 160. Модальный диалог подтверждения



### Ограничения:

- нельзя удалить профиль авторизации, который используется в какой-либо политике авторизации.

## Словари

### Описание

Базовым элементом при настройке [логического условия](#) являются атрибуты, сгруппированные по словарям. Помимо базовых и vendor-specific атрибутов RADIUS в NAICE доступно использование Non-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 верхней правой части окна.

### 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
Alteon	1872	Alteon 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

Рисунок 161. 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:

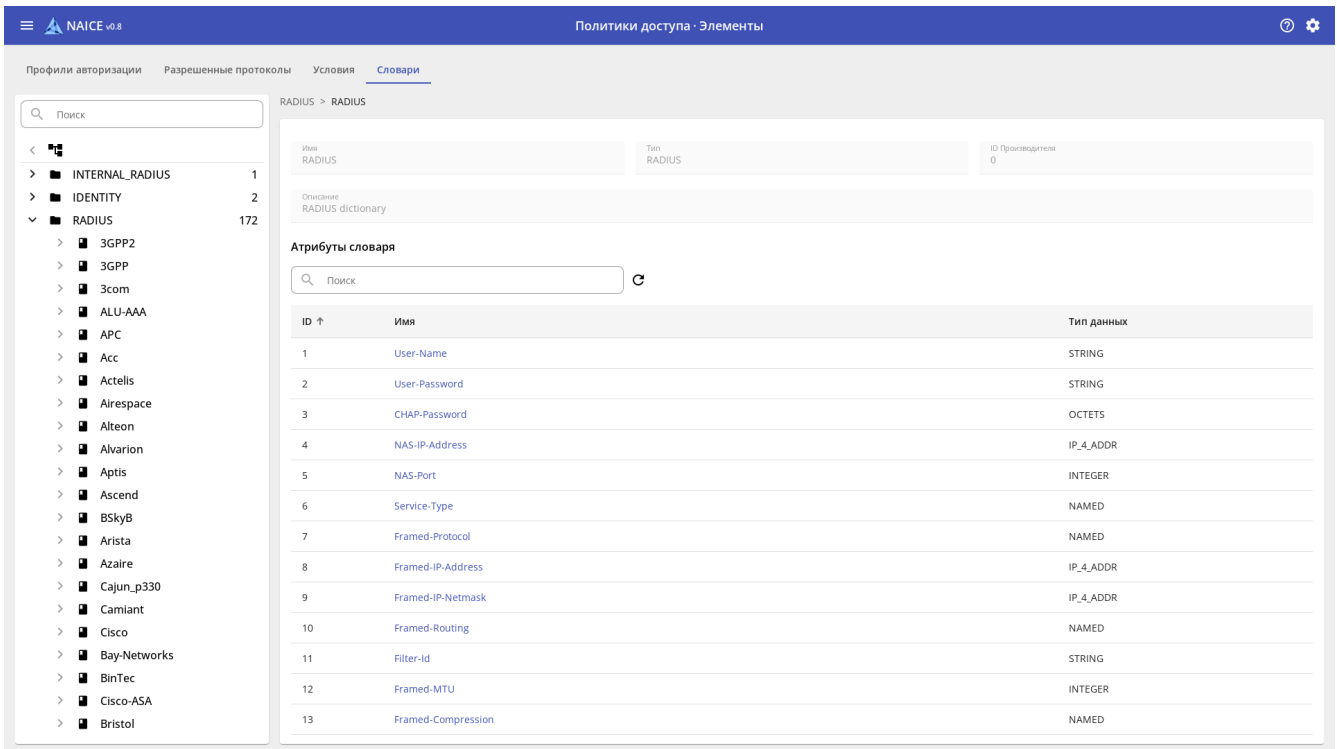


Рисунок 162. Просмотр атрибутов словаря

Для просмотра информации об атрибуте требуется нажать на имя атрибута в списке атрибутов:

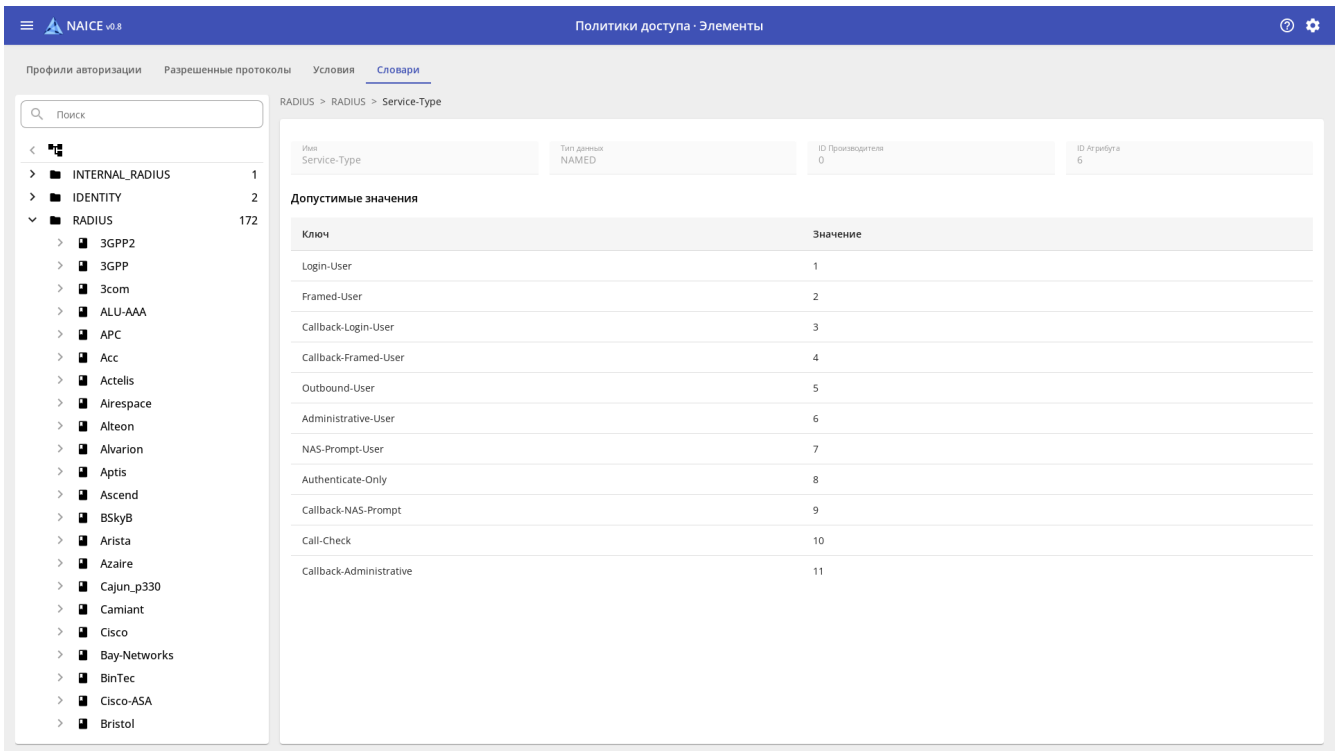


Рисунок 163. Просмотр информации об атрибуте

Для атрибутов, предполагающих конечный список допустимых значений, на данной странице будет перечислен список этих значений.

## 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

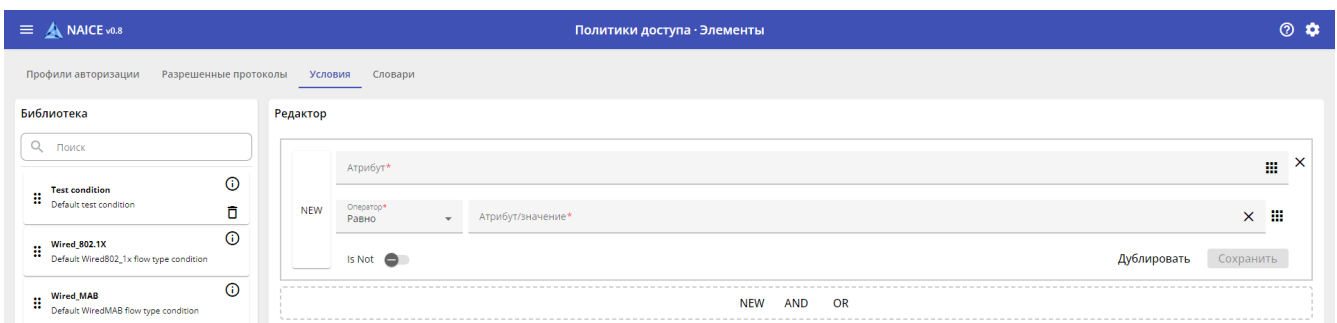


Рисунок 164. Библиотека логических условий





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)
- **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







Атрибут      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-	3GPP	14

Рисунок 165. 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 с 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.

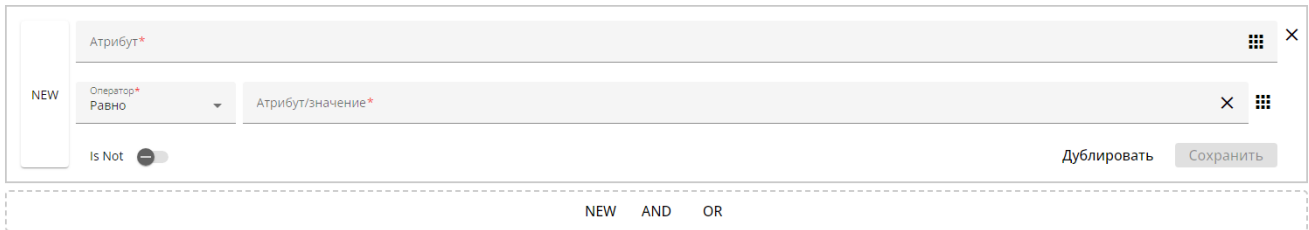



Рисунок 166. Исходное состояние редактора условия

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.

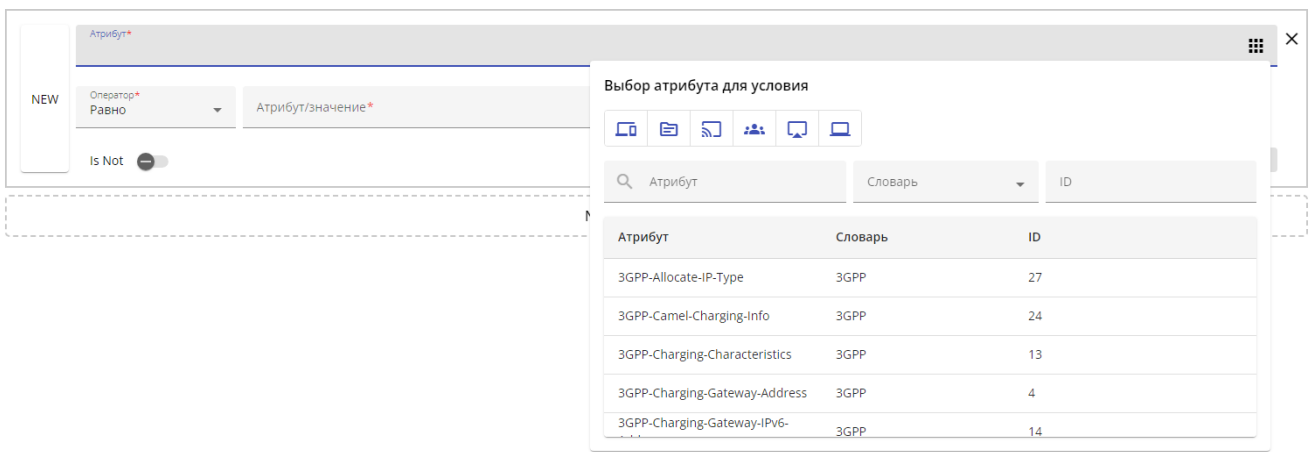


Рисунок 167. Выбор атрибута

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
Число	Больше или равно, Больше чем, Меньше или равно, Меньше чем, Равно, Не равно, Равно NULL, Не равно NULL
IPv4 адрес	Равно, Не равно, Равно NULL, Не равно NULL
MAC адрес	Равно, Не равно, Равно NULL, Не равно NULL, Начинается на, Не начинается на, Заканчивается на, Не заканчивается на, Содержит, Не содержит,
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.

NEW AND OR

Рисунок 168. 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\*

Сохранить в библиотеку как новое условие

Имя\*  
New condition

Описание

Сохранить

Отменить

Рисунок 169. 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.

NEW AND OR

Рисунок 170. 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 171. 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.

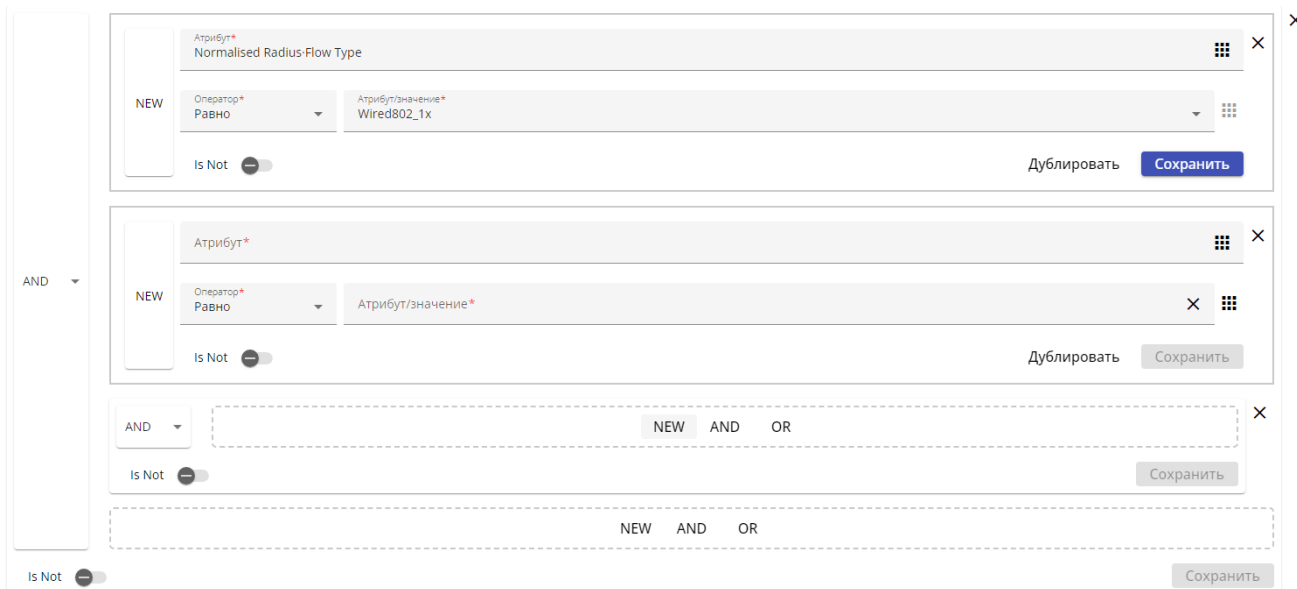


Рисунок 172. Условие, содержащее вложенные правила

Для сохранения всех условий надо нажать кнопку "Сохранить" в нижнем правом углу.

## Редактирование логического условия

Для редактирования логического условия необходимо его захватить курсором в библиотеке и перенести в поле редактора.

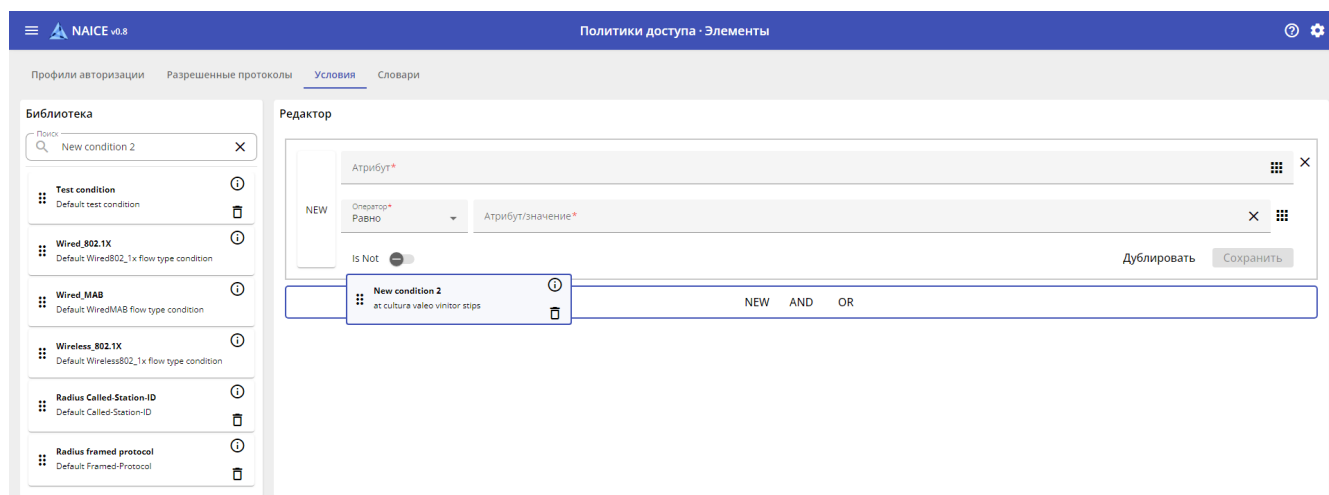


Рисунок 173. Выбор логического условия

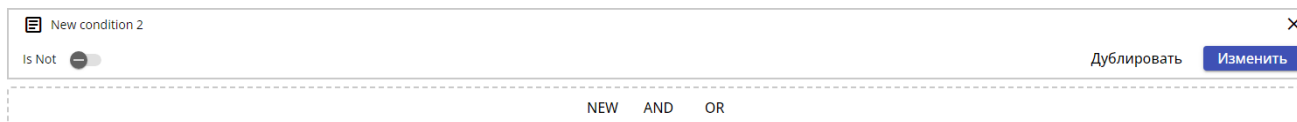



Рисунок 174. Редактирование логического условия

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.

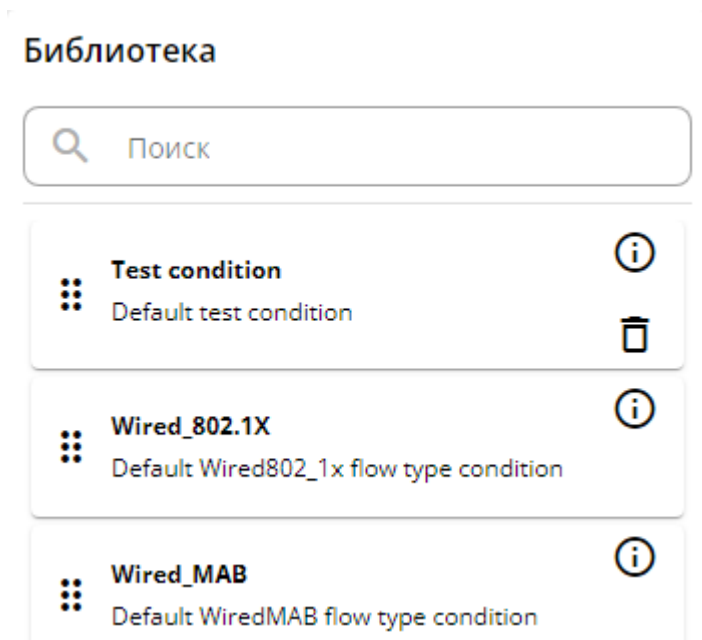


Рисунок 175. Выбор условия для удаления



Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.



### Подтверждение действия

Данные будут удалены. Вы уверены?

Да

Нет

Рисунок 176. Модальный диалог подтверждения



#### Ограничения:

- нельзя удалить 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 политик

## 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. Отключенные наборы политик не участвуют в проверке.
- 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`.

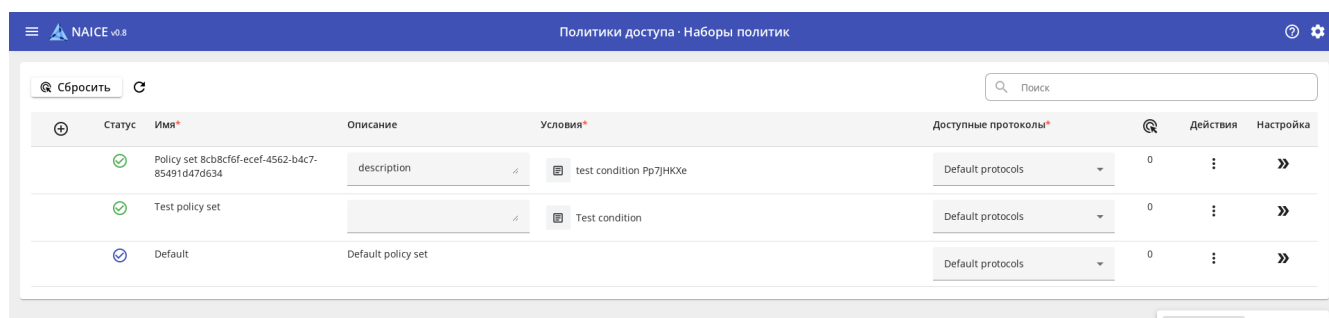
### 3. Обработка в рамках найденного набора политик:

- 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*	Действия	Настройка
✓	Policy set 8cb8cf6f-ecfe-4562-b4c7-85491d47d634	description	test condition Pp7JHXe	Default protocols	0	⋮ »
✓	Test policy set		Test condition	Default protocols	0	⋮ »
⊙	Default	Default policy set		Default protocols	0	⋮ »


Рисунок 177. Просмотр всех наборов политик.

В таблице отображаются наборы политик, 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 последней в списке, ниже которой расположить другие политики нельзя.

Описание колонок таблицы:

- **Статус** - статус набора политик.
- **Имя \*** - наименование набора политик.
- **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](#).
-  - 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 желтым цветом).
-  - обновить данные.
-  **Сбросить** - сбросить счетчики количества срабатываний всех наборов политик.
-  - добавить политику (политика будет добавлена первой в списке).
-  - 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 наборы политик проверяются по порядку, как на экране - сверху вниз. Потому на странице отображаются ВСЕ наборы политик сразу, а **Поиск** не скрывает записи из списка, а лишь подсвечивает их желтым цветом.

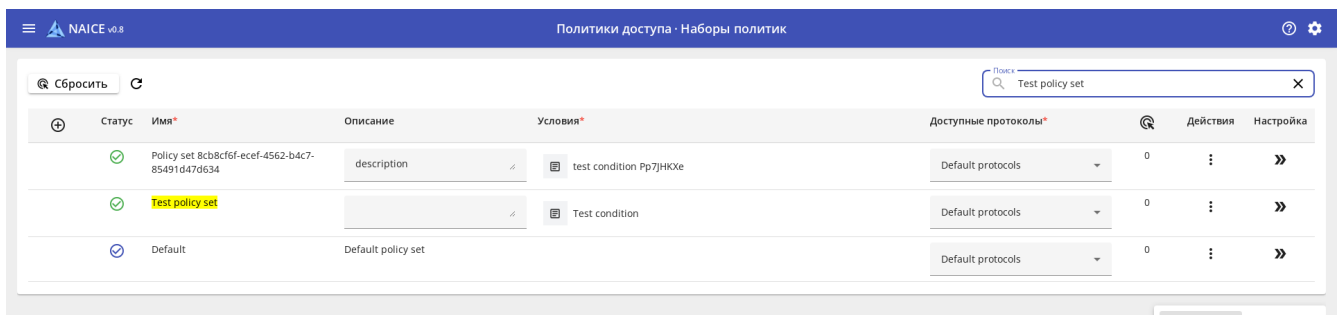




Рисунок 178. Поиск набора политик

Для изменения порядка перетащите политику за элемент  в колонке  (становится видимым при наведении в эту область).

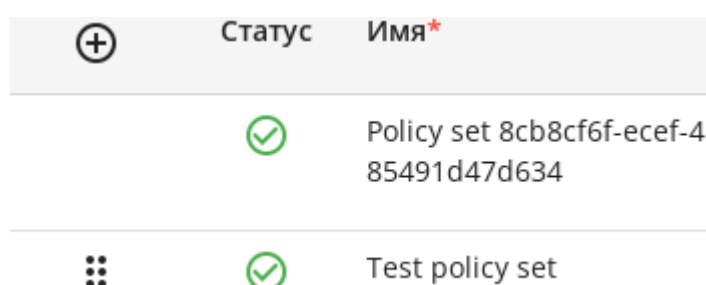


Рисунок 179. Иконка перетаскивания набора политик



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.

(+)	Статус	Имя*
	✓	Policy set 8cb8cf6f-ecef-485491d47d634
	✓	Test policy set

Рисунок 180. 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**.

Действия	Настройка
⋮	>>
⋮	>>
Добавить сверху	
Добавить снизу	
Удалить	
Сохранить	Отменить

Рисунок 181. Отображение политики. Выпадающие меню с действиями.

Информация по Статусу:

- ✓ Включено - разрешается обрабатывать запросы;
- ✗ Выключено - исключить из обработки, не проверять Условие, не обрабатывать запросы;
- 👁 Монитор - разрешается проверять Условие (и инкрементировать счётчик срабатываний), обрабатывать запросы - нет;
-

✓ По умолчанию - используется только для политики по умолчанию Default .

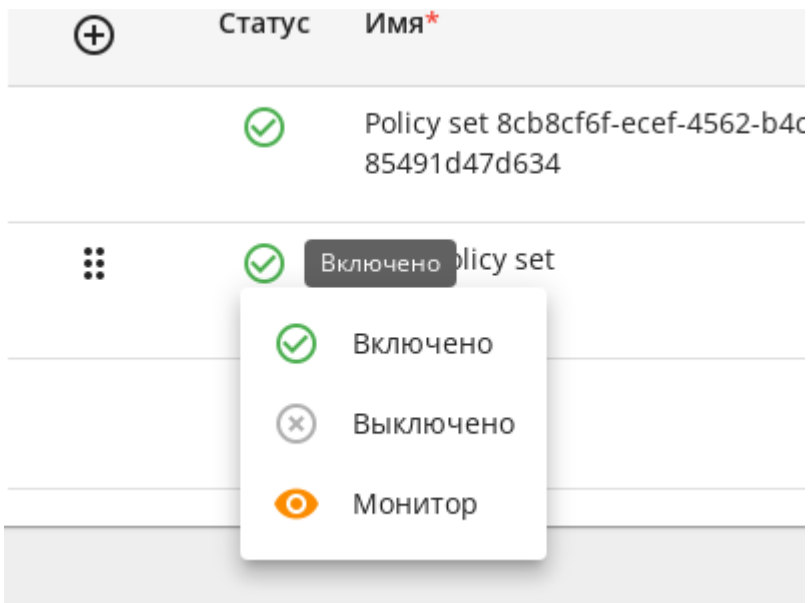


Рисунок 182. Изменение статуса политики.

Во вновь созданном наборе политик в поле Имя ввести наименование набора политик или оставить неизменным автоматически сформированное имя.

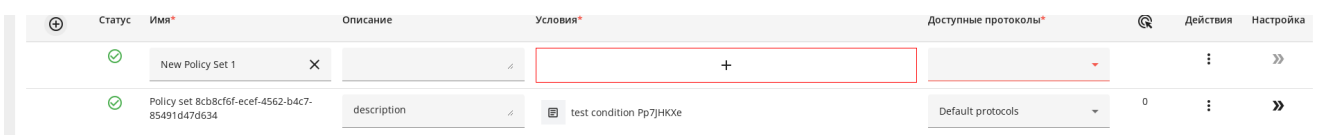


Рисунок 183. Отображение записи новой политики. Элементы обязательные для заполнения.

Для редактирования условия необходимо нажать + и откроется редактор условий.

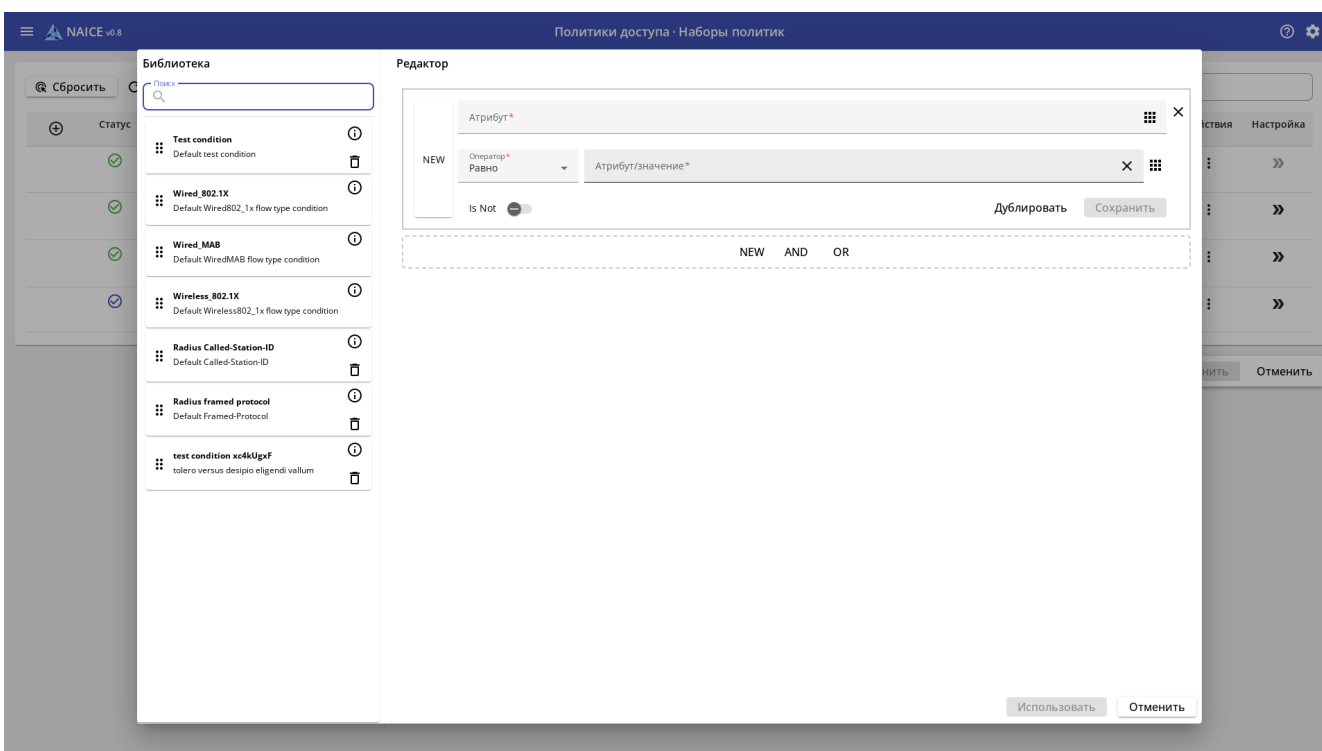


Рисунок 184. Редактор условий.

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.

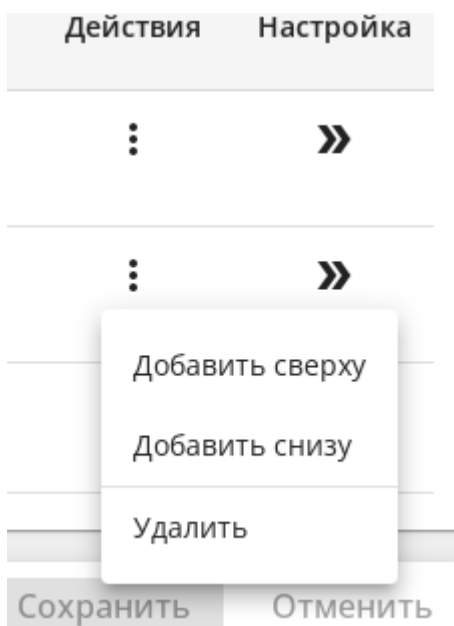


Рисунок 185. Выпадающее меню для удаления набора политик




Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.

## Подтверждение действия



Данные будут удалены. Вы уверены?

Рисунок 186. Модальный диалог подтверждения

## Количество срабатываний политики

Счётчики в колонке  показывают, сколько попыток авторизации было обработано с использованием этой политики. Изменения значений свидетельствует о том, что Условие срабатывает; нулевые значения, наоборот, говорят о несоответствии получаемых RADIUS-запросов отслеживаемому условию.



Используя статус  **Монитор** и наблюдая за счётчиками срабатывания, можно сначала подобрать и отладить условие, а лишь потом включать политику в работу, переведя её в статус  **Включено**.

## 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.

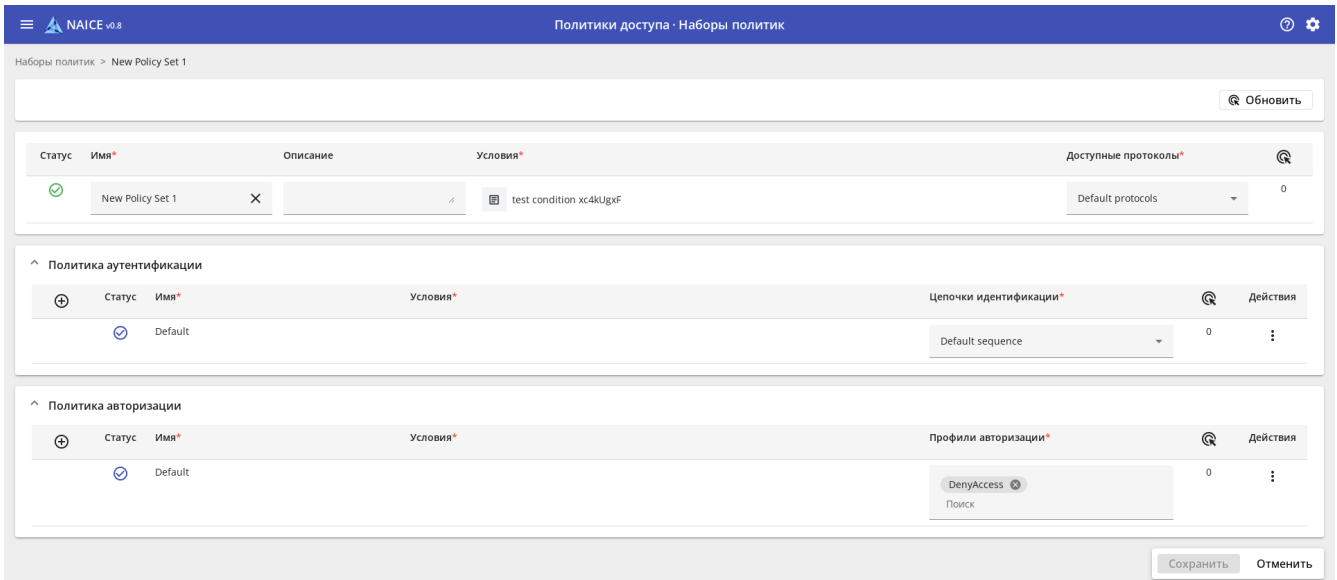


Рисунок 187. Страница просмотра и редактирования набора политик





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 [Наборы политик](#).
- **Политика аутентификации** - управление аутентификацией пользователей.
- **Политика авторизации** - управление авторизацией пользователей.

Элементы управления:

-  **Обновить** - запрос актуального количества срабатываний 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 попыток авторизации, подпадающих под указанные Условия. При нажатии на число срабатываний счетчик можно **Сбросить**.
- **Сохранить** - сохранить изменения.
- **Отменить** - отменить изменения.

Параметры, отмеченные звездочкой \*, обязательны для заполнения.

Для изменения порядка Политик Аутентификации и Авторизации перетащите политику за элемент  в колонке  (становится видимым при наведении в эту область) аналогично разделу [Наборы политик](#).

## 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

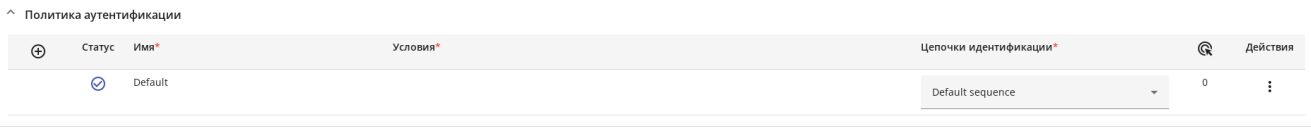


Рисунок 188. Панель политик "Аутентификации".

Для настройки политики аутентификации в блоке **Политика аутентификации** необходимо нажать кнопку **+**. Появится новое правило.

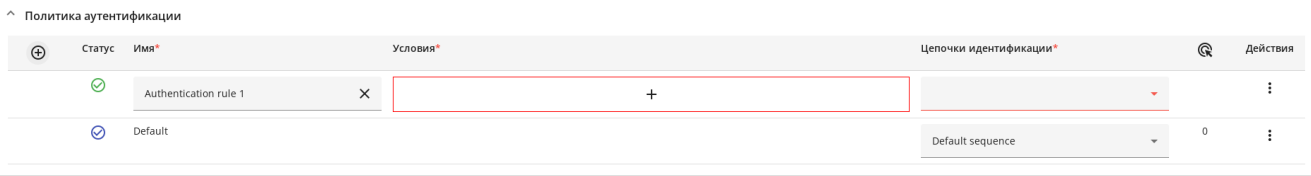


Рисунок 189. Новая политика "Аутентификации".

В поле **Имя** ввести наименование политики.

Для редактирования условия необходимо нажать **+** - откроется редактор условий.

Редактирование условий выполняется аналогично описанному в [Условия](#).

При настройке политики аутентификации есть ограничение по используемым типам словарей. Можно использовать словари: `DEVICE`, `RADIUS`, `NORMALISED_RADIUS`, `INTERNAL_RADIUS`.

При редактировании условий непосредственно в политике добавляется возможность использовать настроенное условие без сохранения его в Библиотеке условий. Для этого надо после настройки не сохраняя условие нажать кнопку **Использовать**.

Выбрать в выпадающем меню **Цепочки идентификации** [цепочку идентификаций](#).

Кнопкой **⋮** справа от политики можно добавить новое правило выше или ниже, либо удалить текущее.

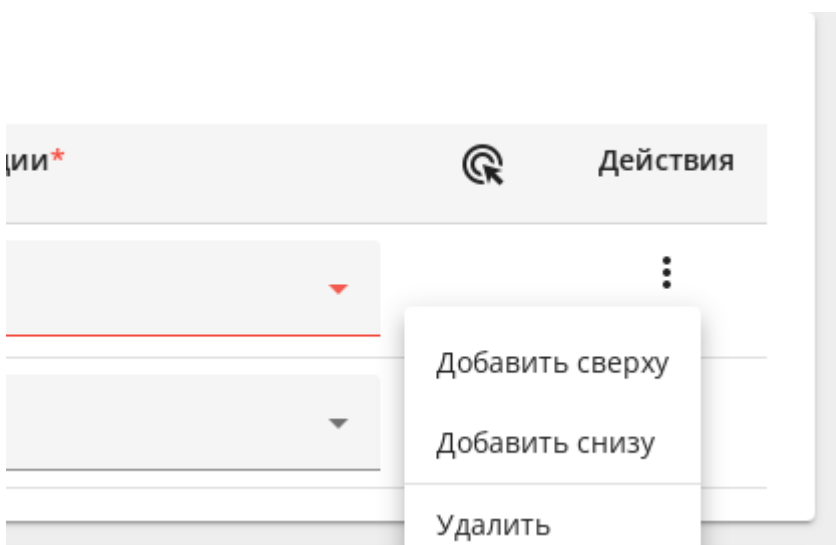


Рисунок 190. Политика аутентификации. Выпадающее меню. Действия.

Также можно изменить статус политики аналогично статусам в наборах политик.

## ^ Политика аутентификации

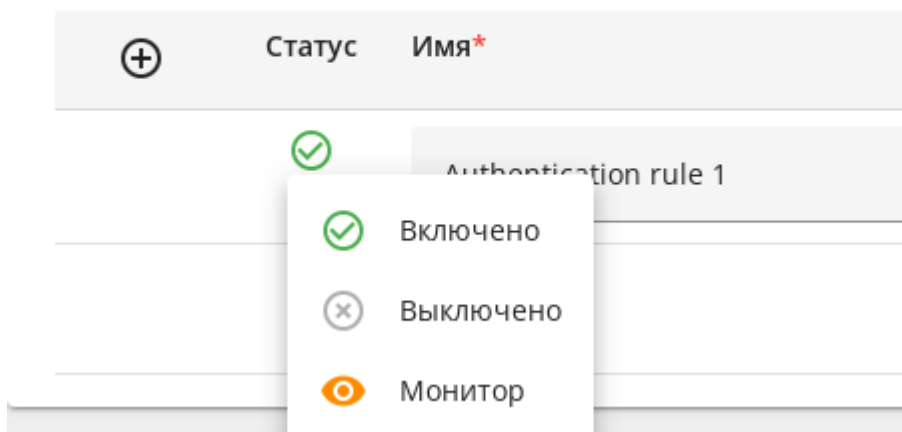


Рисунок 191. Политика аутентификации. Изменение статуса политики.

## Политика авторизации

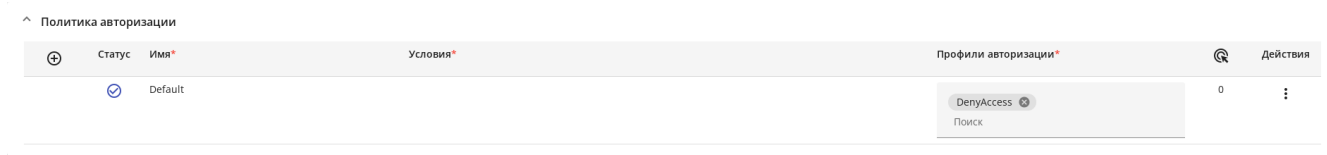



Рисунок 192. Панель политик "Авторизации".

Для настройки правила политики авторизации в блоке **Политики авторизации** нажать . Появится новое правило.

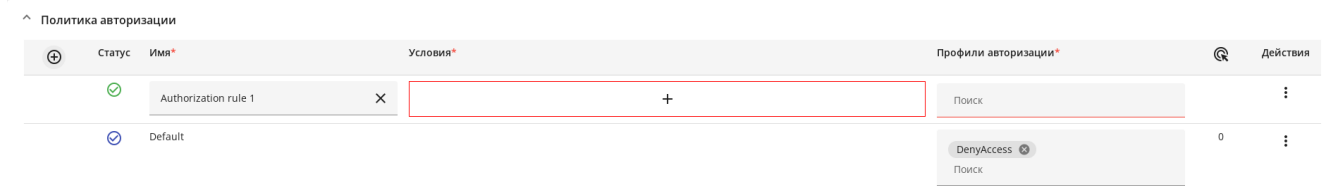


Рисунок 193. Новая политика "Авторизации".

В поле **Имя** ввести наименование правила политики.

Для редактирования условия необходимо нажать  - 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 одной Политике авторизации можно привязать несколько Профилей авторизации. Однако при обработке запроса будут учитываться только те, которые соответствуют текущему Профилю устройства.

Кнопкой  справа от политики можно добавить новое правило выше или ниже, либо удалить текущее.

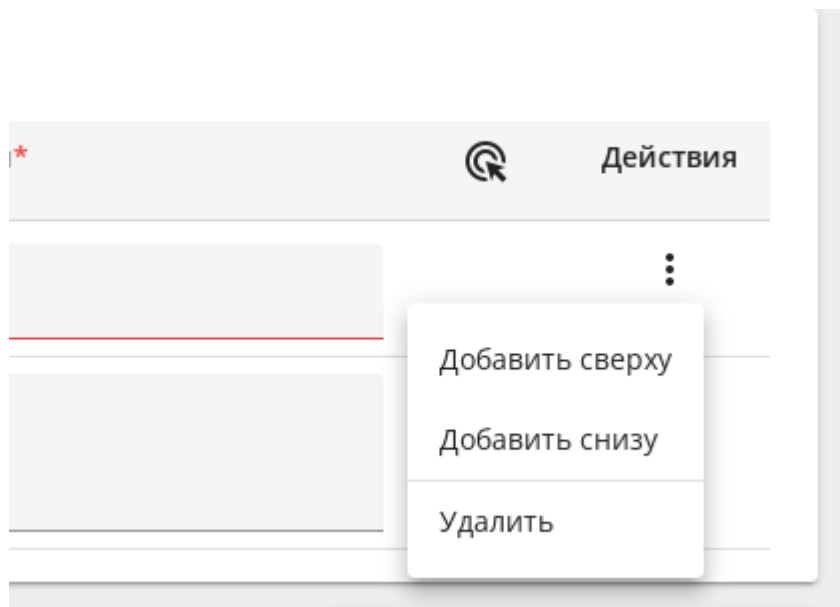


Рисунок 194. Политика авторизации. Выпадающее меню. Действия.

Также можно изменить статус политики аналогично статусам в наборах политик.

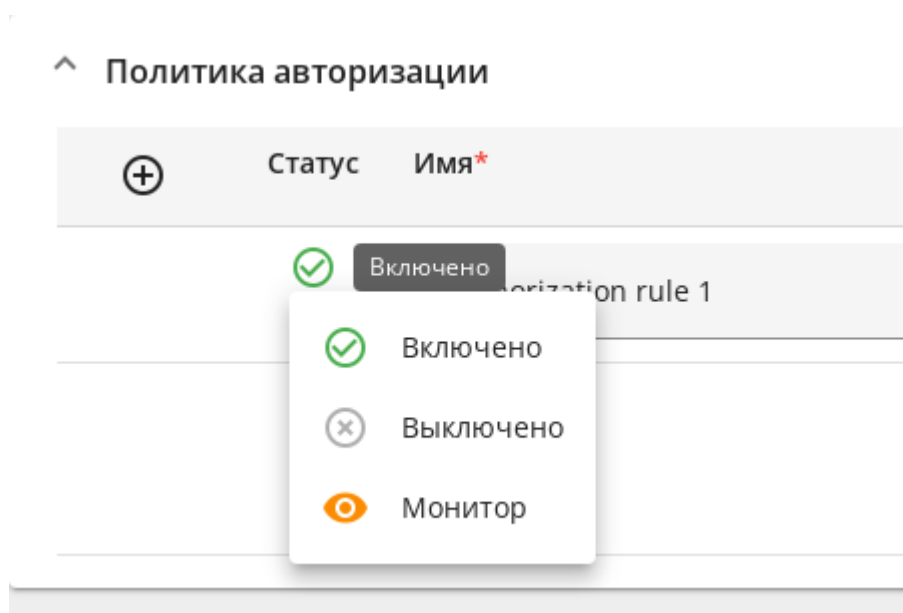


Рисунок 195. Политика авторизации. Изменение статуса политики.

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 выполняется нажатием на кнопку  и выбором действия **Удалить**.



Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.



### Подтверждение действия

Данные будут удалены. Вы уверены?

Да

Нет

Рисунок 196. Модальный диалог подтверждения

## 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

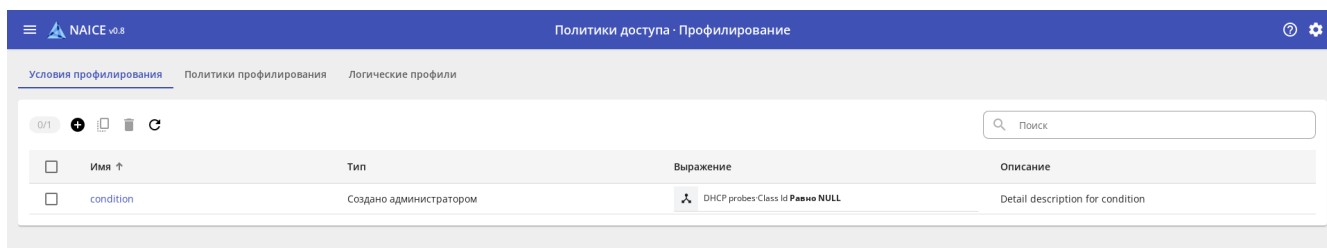
### Описание

*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
<input type="checkbox"/> condition	Создано администратором	<input type="checkbox"/> DHCP probes Class Id равно NULL	Detail description for condition

Рисунок 197. 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:

- **0/1** - Счетчик выбранных чекбоксом элементов / общего количества элементов.
- **+** - Добавить новый элемент.
- **🗑** - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- **↻** - Обновить данные таблицы.
- **🔍 Поиск** - Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
- **↑** - Изменить текущий порядок сортировки.
- - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).
- - Чекбокс, который отвечает за копирование выбранного элемента. Становится активным, если выбран только один элемент в списке.

## Добавление условия профилирования

Для добавления условия профилирования нажмите **+** в левой верхней части поля над таблицей.


The screenshot shows the 'Условия профилирования > Добавление' page. At the top, there are navigation tabs: 'Условия профилирования', 'Политики профилирования', and 'Логические профили'. The main form contains three input fields: 'Имя\*' (Name), 'Тип' (Type) with a dropdown menu showing 'Создано администратором', and 'Описание'. Below this is a section titled '^ Условие' (Condition) containing three fields: 'Атрибут' (Attribute), 'Оператор\*' (Operator) with a dropdown menu, and 'Значение\*' (Value). At the bottom right, there are two buttons: 'Сохранить' (Save) and 'Отменить' (Cancel).

Рисунок 198. 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 predetermined values, selection of values is produced from the list.

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

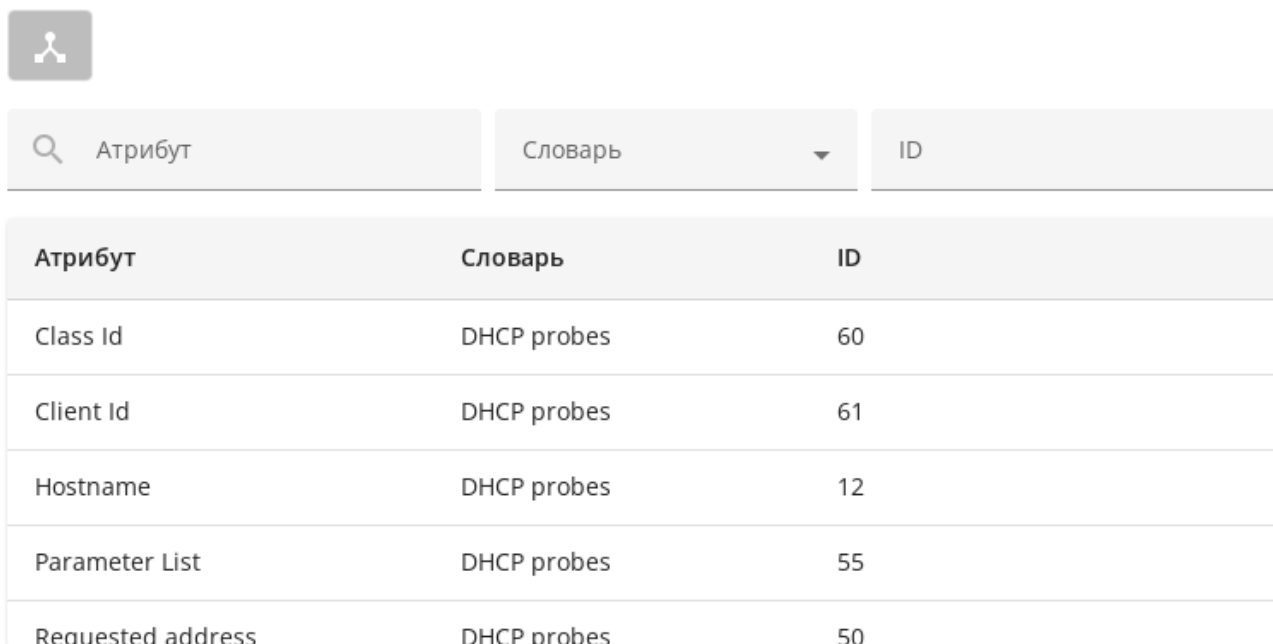



Рисунок 199. Меню выбора атрибута

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.

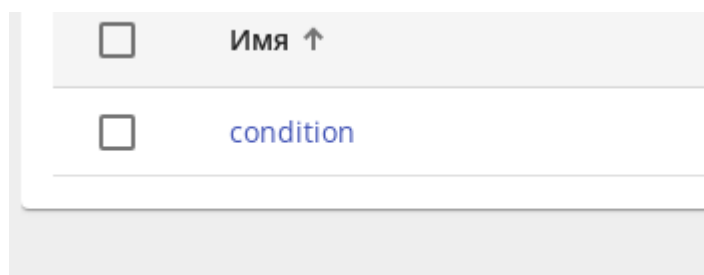


Рисунок 200. Гиперссылка на страницу редактирования условия

После этого откроется окно редактирования.

Рисунок 201. Форма редактирования условия профилирования

После редактирования нажать на кнопку "Сохранить". Кнопка остается неактивной, пока не будет изменено хотя бы одно поле.

## 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 "\_copy". Можно выбрать любое другое имя, которое еще не используется в системе.

Рисунок 202. 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.




<input type="checkbox"/>	Имя ↑	Тип	Выражение	Описание
<input type="checkbox"/>	condition	Создано администратором	 DHCP probes'Class Id <b>Равно NULL</b>	Detail description for condition
<input type="checkbox"/>	condition_copy	Создано администратором	 DHCP probes'Class Id <b>Равно NULL</b>	Detail description for condition

Рисунок 203. 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.


Имя ↑	Тип	Выражение	Описание
<input checked="" type="checkbox"/> condition	Создано администратором	 DHCP probes/Class Id <b>Равно NULL</b>	Detail description for condition

Рисунок 204. Выбор условий для удаления



Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.



### Подтверждение действия

Данные будут удалены. Вы уверены?

Да

Нет

Рисунок 205. Модальный диалог подтверждения

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.

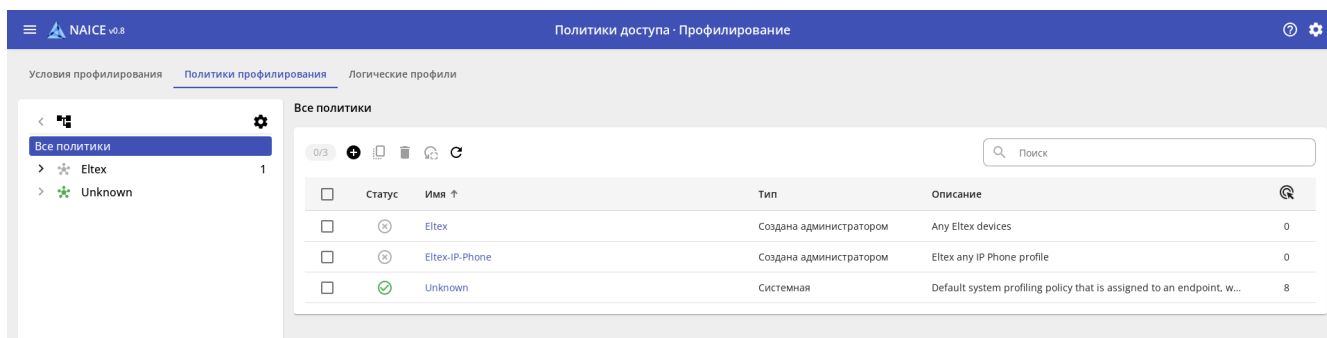


Рисунок 206. Просмотр политик профилирования.

## 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.

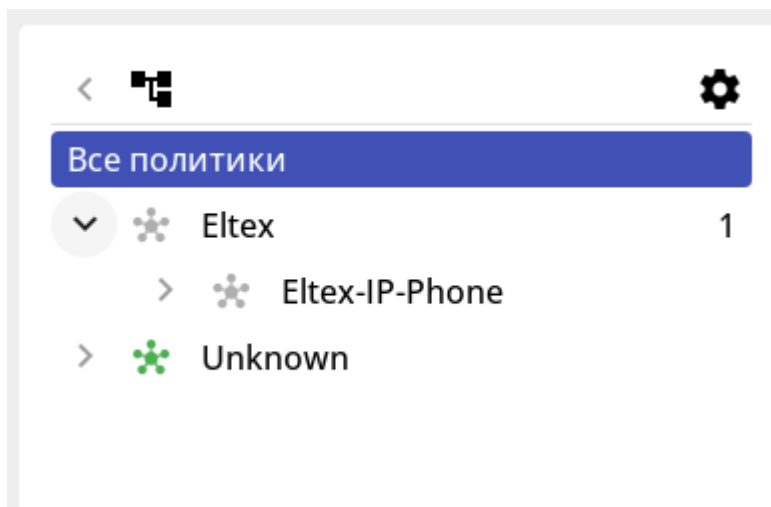



Рисунок 207. Дерево политик профилирования.

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.

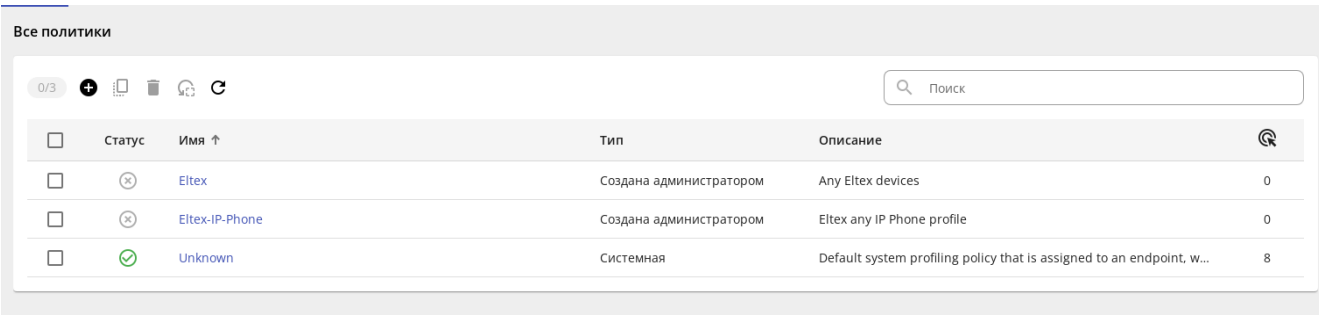
- ✓ - в режиме древовидной структуры отображается слева от наименования политик профилирования имеющих дочерние элементы, если список раскрыт.
-  - элемент для обозначения политики профилирования.

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.










<input type="checkbox"/>	Статус	Имя ↑	Тип	Описание	
<input type="checkbox"/>		Eltex	Создана администратором	Any Eltex devices	0
<input type="checkbox"/>		Eltex-IP-Phone	Создана администратором	Eltex any IP Phone profile	0
<input type="checkbox"/>		Unknown	Системная	Default system profiling policy that is assigned to an endpoint, w...	8

Рисунок 208. Таблица со списком всех политик профилирования.








Таблица содержит колонки:

- Статус - текущий статус политики профилирования: может принимать значения  (включено) или  (выключено).
- Имя - наименование политики профилирования.
- Тип - тип политики профилирования. Возможны значения "Создана администратором" или "Системная".
- Описание - описание политики профилирования.
-  - 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:

-  - Счетчик выбранных чекбоксом элементов / общего количества элементов.


-  - Добавить новый элемент.
-  - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
-  - Обновить данные таблицы.
-  Поиск - Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
-  - Изменить текущий порядок сортировки.
- - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).
-  - Копировать выбранный элемент. Становится активным, если выбран только один элемент в списке.
-  - Сбросить счётчик попаданий в политику профилирования. Становится активным, если выбран хотя бы один элемент в списке и количество срабатываний политики больше 0.



Порядок политик профилирования крайне важен!  
Обращение к политикам профилирования для проверки соответствия эндпоинта политике профилирования происходит сверху вниз списка.

## 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.

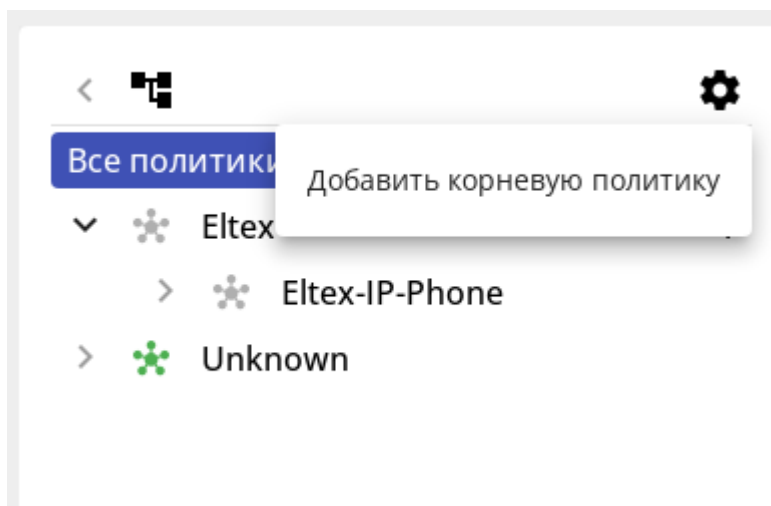



Рисунок 209. Добавление политики профилирования. Действия.

- 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.

Рисунок 210. 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.

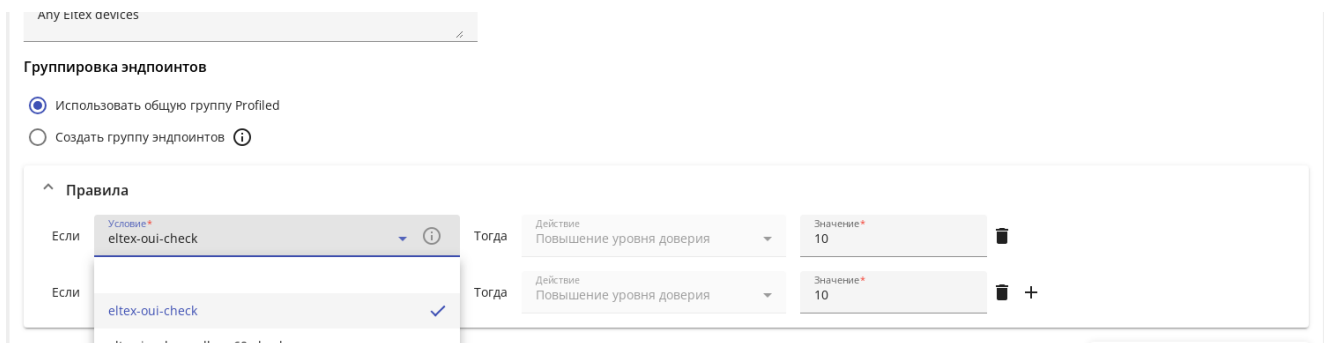


Рисунок 211. Добавление правил в политику профилирования.

Параметры, отмеченные звездочкой \*, обязательны для заполнения.



Политика профилирования должна содержать минимум одно правило.



Для одной политики профилирования может быть добавлено несколько правил.



Запрещено добавлять одно и тоже условие профилирования в политику несколько раз.

Для добавления политики нажмите кнопку **Добавить**. Кнопка станет активной после заполнения всех необходимых полей политики профилирования.

## Принцип проверки соответствия эндпоинта политике профилирования

При профилировании эндпоинта выполняются следующие действия:

- Для первого условия профилирования, указанного в правилах политики профилирования, выполняется проверка на соответствие эндпоинта указанному условию:

Если эндпоинт соответствует условию профилированию, то к текущему уровню доверия прибавляется соответствующее правилу значение;


- Если эндпоинт не соответствует условию, то уровень доверия остается неизменным.
- Действие повторяется для каждого правила в политике.
- Когда эндпоинт был проверен на соответствие всем правилам политики, суммарный уровень доверия сравнивается с минимальным уровнем доверия политики:
  - Если суммарный уровень доверия равен или больше минимального, то эндпоинт соответствует политике профилирования;
  - Если суммарный уровень доверия меньше минимального, то эндпоинт не соответствует политике профилирования.
- Так как политики вложены друг в друга, работает обход дерева вглубь:
  - Обнаруживается первая совпавшая корневая политика.
  - Если у корневой политики есть дочерние, то происходит их обход на предмет совпадения.
  - Возвращается самая "глубокая" политика из дерева.
  - Как только одна из политик текущего уровня подошла, обход этого уровня прекращается, поиск продолжается только среди дочерних политик.

## 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.

Условия профилирования | Политики профилирования | Логические профили

Все политики > Eitex

Статус: Выключено | Тип: Создана администратором | Количество срабатываний политики: 0

Имя: Eitex | Родительская политика

Минимальный уровень доверия: 10

Описание: Алу Eitex devices

Группировка эндпоинтов

Использовать общую группу Profiled

Создать группу эндпоинтов

Правила

Если: Условие: eitex-oui-check | Тогда: Действие: Повышение уровня доверия | Значение: 10

Сохранить | Отменить

Рисунок 212. Редактирование политики профилирования.





Редактирование системной политики профилирования "Unknown" недоступно.

После редактирования нажать на кнопку "Сохранить". Кнопка остается неактивной, пока не будет изменено хотя бы одно поле.

## 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 выбрать любое другое имя, которое еще не используется в системе.

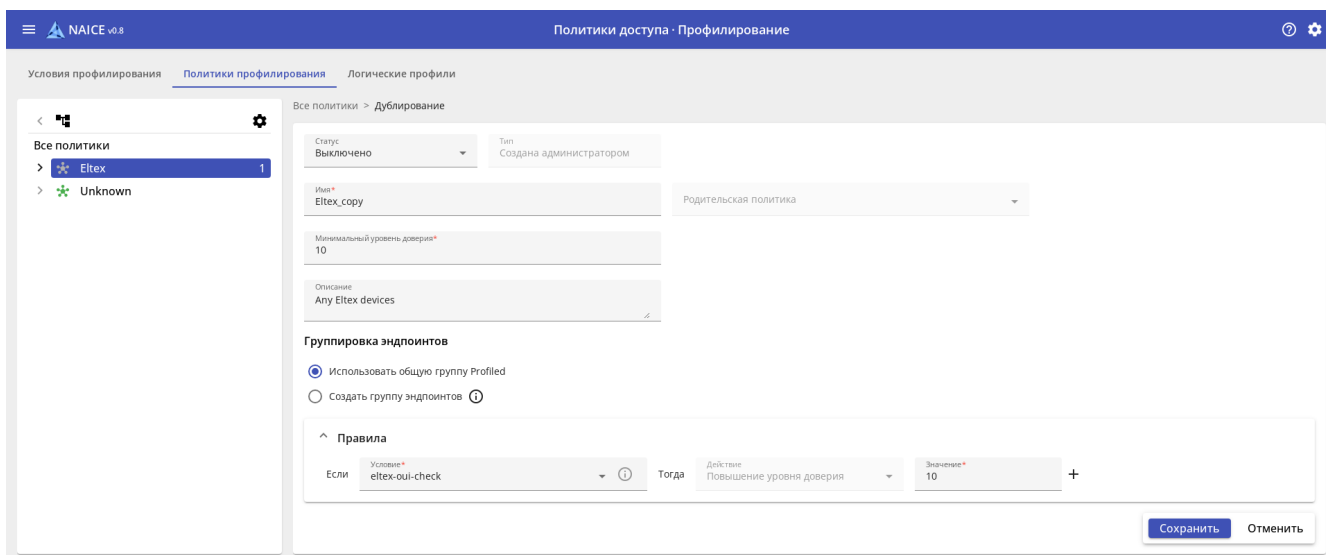




Рисунок 213. Дублирование политики профилирования.

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 требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.



### Подтверждение действия

Данные будут удалены. Вы уверены?

Да

Нет

Рисунок 214. Модальный диалог подтверждения



#### 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".

## 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.

Имя ↑	Тип	Описание
IP-Phone_UbiUBbz	Создан администратором	Profile for all ip phones

Рисунок 215. 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:

- **0/1** - Счетчик выбранных чекбоксом элементов / общего количества элементов.
- **+** - Добавить новый элемент.
- **🗑** - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- **↻** - Обновить данные таблицы.

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

- **↑** - Изменить текущий порядок сортировки.
- - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).

## Добавление логического профиля

Для добавления логического профиля нажмите **+** в левой верхней части поля над таблицей.

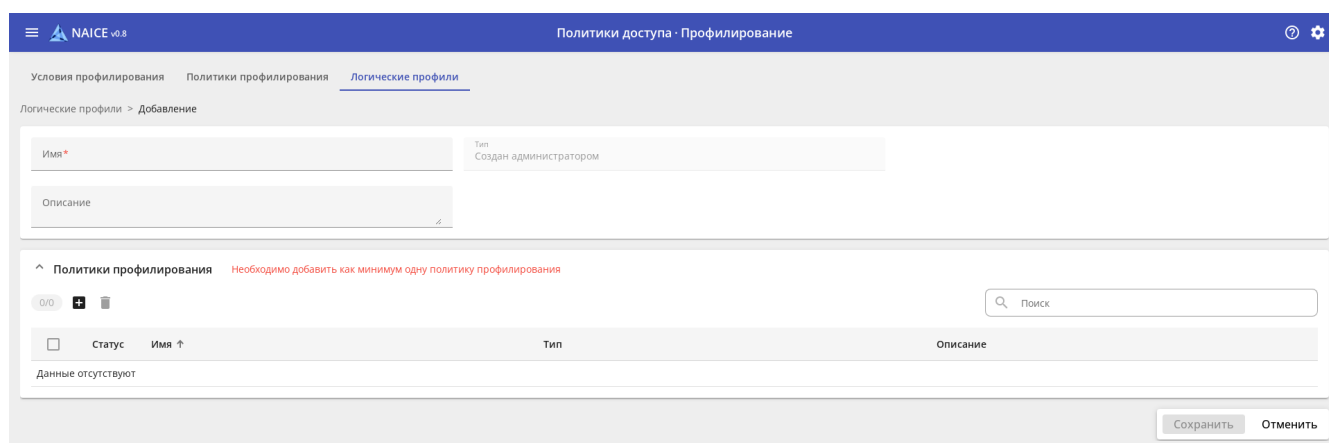


Рисунок 216. Форма добавления логического профиля

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.
- **0/1** - Счетчик выбранных чекбоксом элементов / общего количества элементов.
- **+** - 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**.

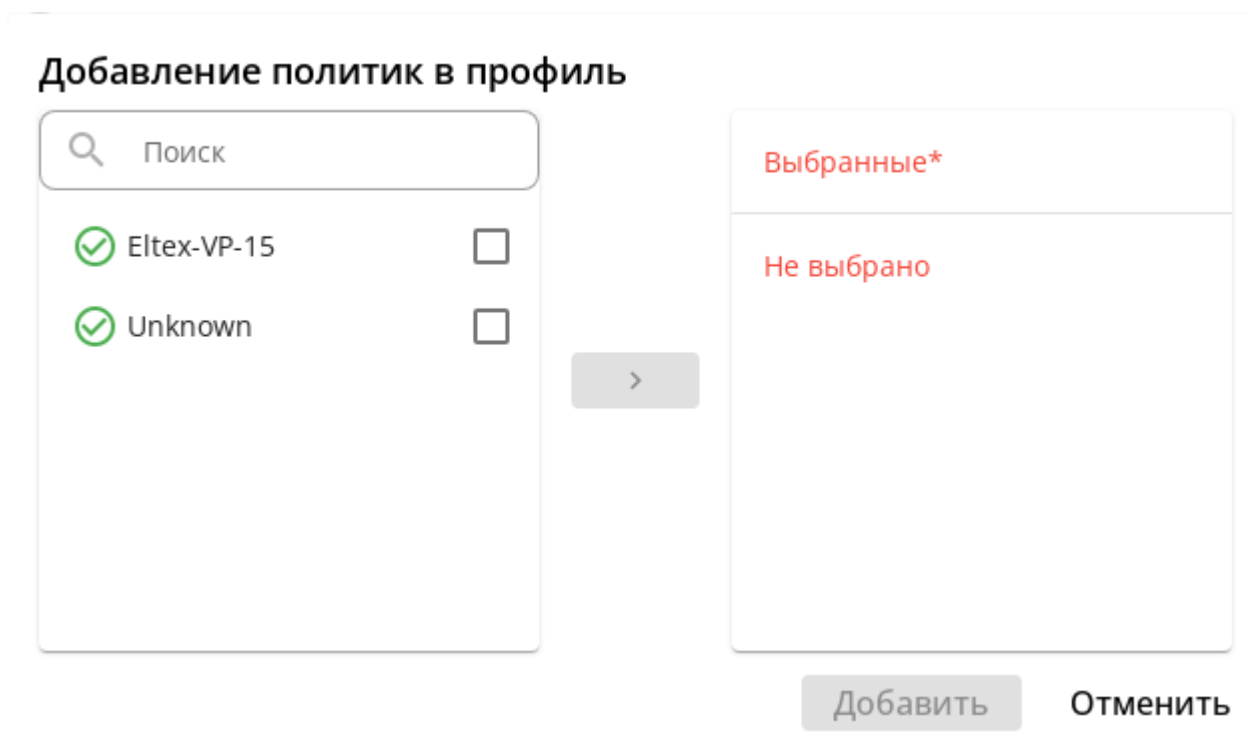




Рисунок 217. Модальный диалог добавления политик профилирования

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.

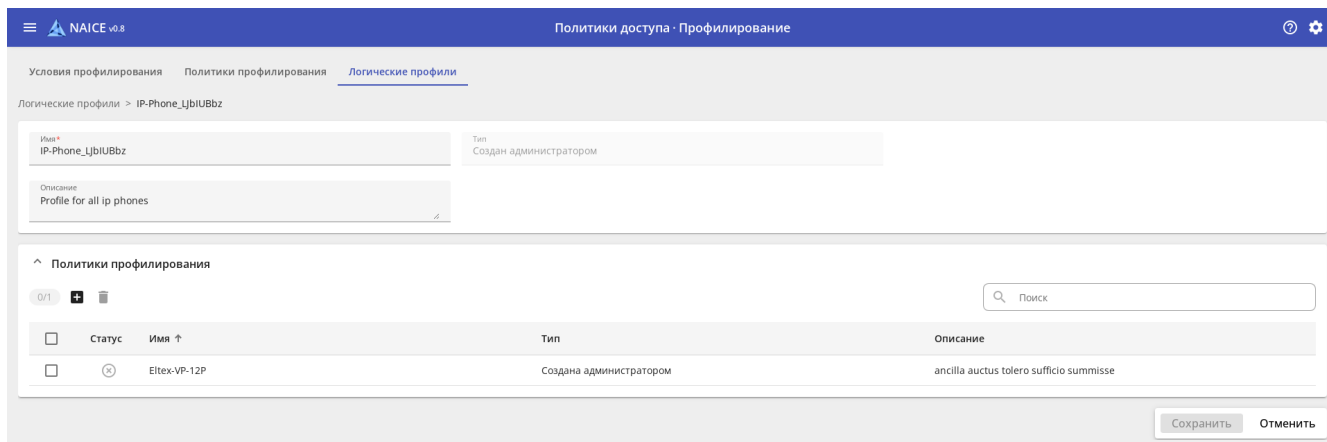



Рисунок 218. Форма редактирования логического профиля

После редактирования нажать на кнопку "Сохранить". Кнопка остается неактивной, пока не будет изменено хотя бы одно поле или изменен набор политик профилирования.

## 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.

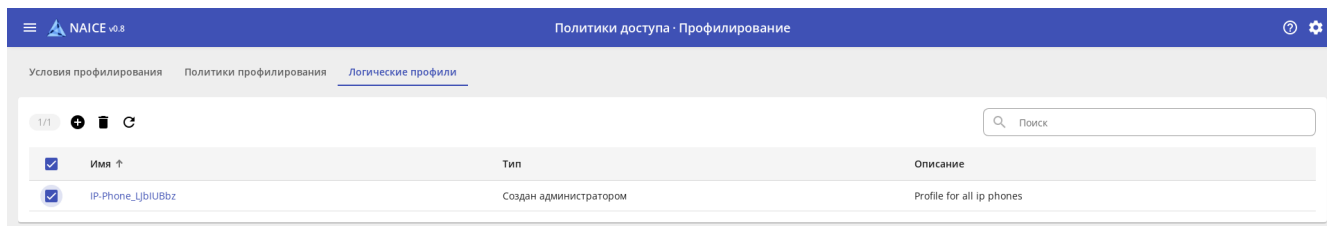


Рисунок 219. Выбор логических профилей для удаления



Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.



### Подтверждение действия

Данные будут удалены. Вы уверены?

Да

Нет

Рисунок 220. Модальный диалог подтверждения



### Ограничения:

- Нельзя удалить логический профиль, который используется в какой-либо политике авторизации.

# Мониторинг

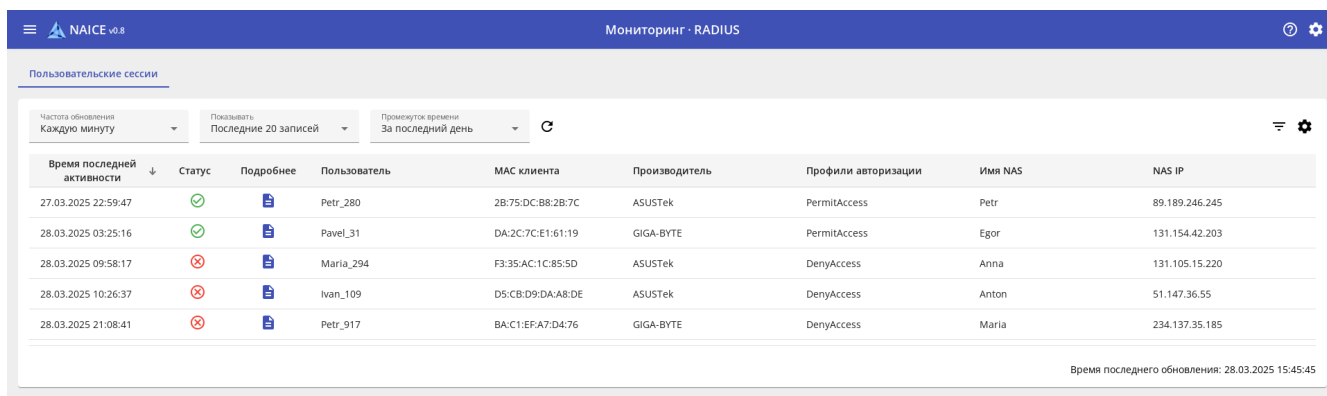
## RADIUS

### Пользовательские сессии

#### 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



The screenshot shows the NAICE v0.8 interface for monitoring RADIUS sessions. It features a table with columns for session time, status, user, MAC address, manufacturer, authorization profiles, NAS name, and NAS IP. The table contains five rows of session data with various statuses (green checkmark, red X, and hourglass).

Время последней активности	Статус	Подробнее	Пользователь	MAC клиента	Производитель	Профили авторизации	Имя NAS	NAS IP
27.03.2025 22:59:47	✓		Petr_280	28:75:DC:B8:2B:7C	ASUSTek	PermitAccess	Petr	89.189.246.245
28.03.2025 03:25:16	✓		Pavel_31	DA:2C:7C:E1:61:19	GIGA-BYTE	PermitAccess	Egor	131.154.42.203
28.03.2025 09:58:17	✗		Maria_294	F3:35:AC:1C:85:5D	ASUSTek	DenyAccess	Anna	131.105.15.220
28.03.2025 10:26:37	✗		Ivan_109	D5:CB:D9:DA:A8:DE	ASUSTek	DenyAccess	Anton	51.147.36.55
28.03.2025 21:08:41	🕒		Petr_917	BA:C1:EF:A7:D4:76	GIGA-BYTE	DenyAccess	Maria	234.137.35.185

Время последнего обновления: 28.03.2025 15:45:45

Рисунок 221. 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:
  - - CREATED - сессия была создана, однако по какой-то причине авторизация не была завершена;
  - - ACCEPTED - авторизация была пройдена успешно;
  - - REJECTED - авторизация была отклонена;
  - - EXPIRED - сессия была завершена по истечении определенного времени.
- **Подробнее** - ссылка для открытия детальной страницы сессии, на которой содержится подробная информация о сессии.
- **Пользователь** - логин пользователя, с которым проходила авторизация.
- **MAC клиента** - идентификатор авторизуемого клиента, который указан в RADIUS-атрибуте Calling-Station-Id.
- **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).



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

Элементы управления:

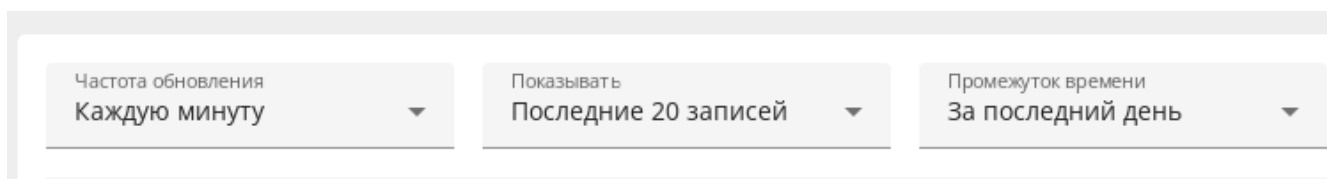





Рисунок 222. Настройки отображения активности пользователей

- **Частота обновления** - настройка частоты автоматического перечитывания пользовательских сессий.
- **Показывать** - настройка количества записей для отображения в таблице.
- **Промежуток времени** - выбор временного периода, в который происходила активность по пользовательским сессиям для отображения.
-  - обновить данные таблицы вручную.
-  - открыть окно настройки фильтрации.
-  - открыть окно настройки отображаемых колонок таблицы.

Фильтрация настраивается в следующем окне:

## Фильтр





Пользователь	MAC клиента 	Статус 
Тип подключения 	Протокол аутентификации... 	
		<input type="button" value="Применить"/> <input type="button" value="Закреть"/>

Рисунок 223. Окно настройки фильтрации записей

Фильтрация записей доступна по параметрам "MAC клиента", "Пользователь", "Статус", "Тип подключения" 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.

В настройках таблицы  можно сменить состав отображаемых колонок.

Кнопка  выбирает или снимает выбор всех колонок для отображения.

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

## Настройки таблицы



Время последней активности

Статус

Подробнее

Пользователь


MAC клиента

Сохранить

Отменить

Рисунок 224. 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.

☰ NAICE v0.8 Мониторинг · RADIUS ? ⚙

Пользовательские сессии

**Общая информация**

Session status	ACCEPTED
Event	SUCCESS
Username	tester
Calling-Station-Id	22:FA:8D:2E:F3:23
Vendor	TP-Link
Authentication policy	Default
Authorization policy	Test Authorization rule
Authorization profile	common_acl

**Детали аутентификации**

Event	SUCCESS
Username	tester
Calling-Station-Id	22:FA:8D:2E:F3:23
Vendor	TP-Link
Session creation timestamp	2025-03-28 15:45:46.0
Session updating timestamp	2025-03-28 15:45:46.0
Identity source	Internal DB
Authentication protocol	PAP
Authorization profile	common_acl
Network device	Egor:BE2EE753
Service Type	Framed-User

**Прочие атрибуты** ^

```
[
  {
    "name": "Service-Type",
    "type": "integer",
    "value": [
      "Framed-User"
    ]
  }
]
```

**Результат** ^

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

Рисунок 225. Детальная информация о сессии

Информация на странице разделена на 4 блока:

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

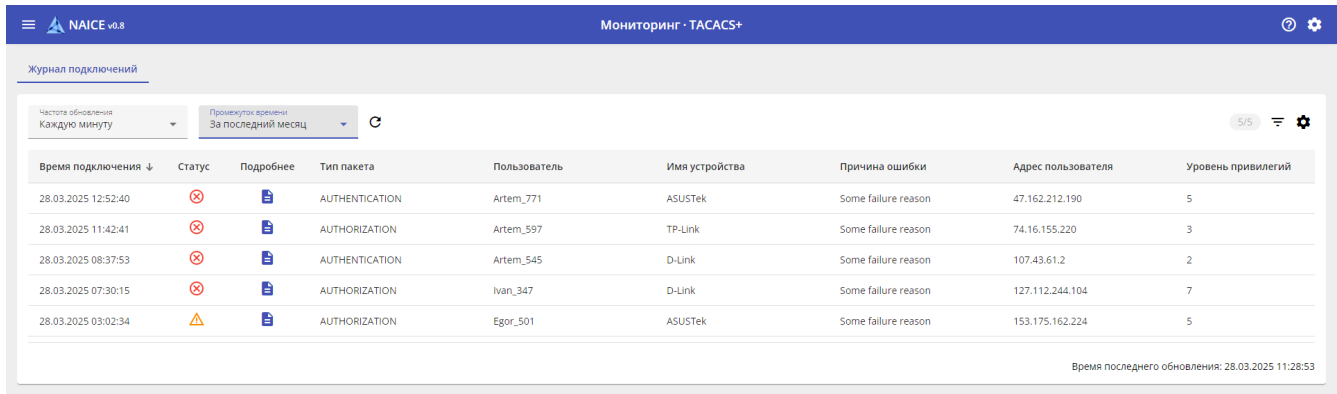
## TACACS

### Журнал подключений

## 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+







The screenshot shows the 'Журнал подключений' (Connection Log) interface. At the top, there are filters for 'Частота обновления' (Update frequency) set to 'Каждую минуту' (Every minute) and 'Период времени' (Time period) set to 'За последний месяц' (Last month). The table has 9 columns: 'Время подключения' (Connection time), 'Статус' (Status), 'Подробнее' (More details), 'Тип пакета' (Packet type), 'Пользователь' (User), 'Имя устройства' (Device name), 'Причина ошибки' (Error reason), 'Адрес пользователя' (User address), and 'Уровень привилегий' (Privilege level). The table contains 5 rows of data, all with a status of 'FAIL' (red X icon) and a reason of 'Some failure reason'. The last row has a status of 'EXPIRED' (yellow triangle icon). The bottom right corner shows the last update time: 'Время последнего обновления: 28.03.2025 11:28:53'.

Время подключения ↓	Статус	Подробнее	Тип пакета	Пользователь	Имя устройства	Причина ошибки	Адрес пользователя	Уровень привилегий
28.03.2025 12:52:40	❌	📄	AUTHENTICATION	Artem_771	ASUSTek	Some failure reason	47.162.212.190	5
28.03.2025 11:42:41	❌	📄	AUTHORIZATION	Artem_597	TP-Link	Some failure reason	74.16.155.220	3
28.03.2025 08:37:53	❌	📄	AUTHENTICATION	Artem_545	D-Link	Some failure reason	107.43.61.2	2
28.03.2025 07:30:15	❌	📄	AUTHORIZATION	Ivan_347	D-Link	Some failure reason	127.112.244.104	7
28.03.2025 03:02:34	⚠️	📄	AUTHORIZATION	Egor_501	ASUSTek	Some failure reason	153.175.162.224	5

Рисунок 226. 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:
  -  - PASS - авторизация/аутентификация была пройдена успешно;
  -  - FAIL - авторизация/аутентификация была отклонена;
  -  - EXPIRED - сессия была завершена по истечении определенного времени;
- **Подробнее**  - ссылка для открытия детальной страницы, на которой содержится подробная информация о подключении.
- **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:

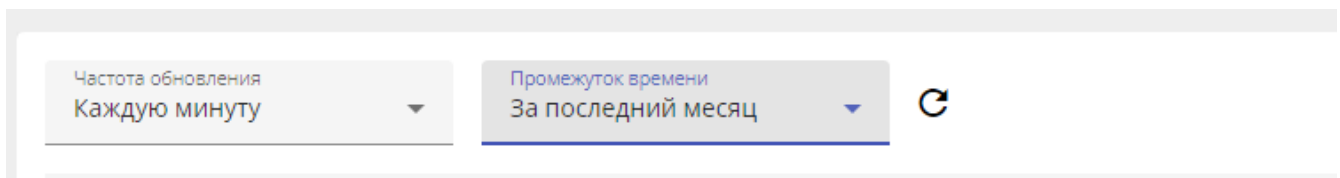






Рисунок 227. Настройки отображения подключений в журнале

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



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:

Фильтр

Тип пакета    Пользователь    Статус

IP устройства    Имя устройства    Адрес пользователя

Порт    Команда

Применить    **Заккрыть**


Рисунок 228. Окно настройки фильтрации записей

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



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

В настройках таблицы  можно сменить состав отображаемых колонок.

Кнопка  выбирает или снимает выбор всех колонок для отображения.

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

Настройки таблицы

Время подключения

Статус

Подробнее


Тип пакета

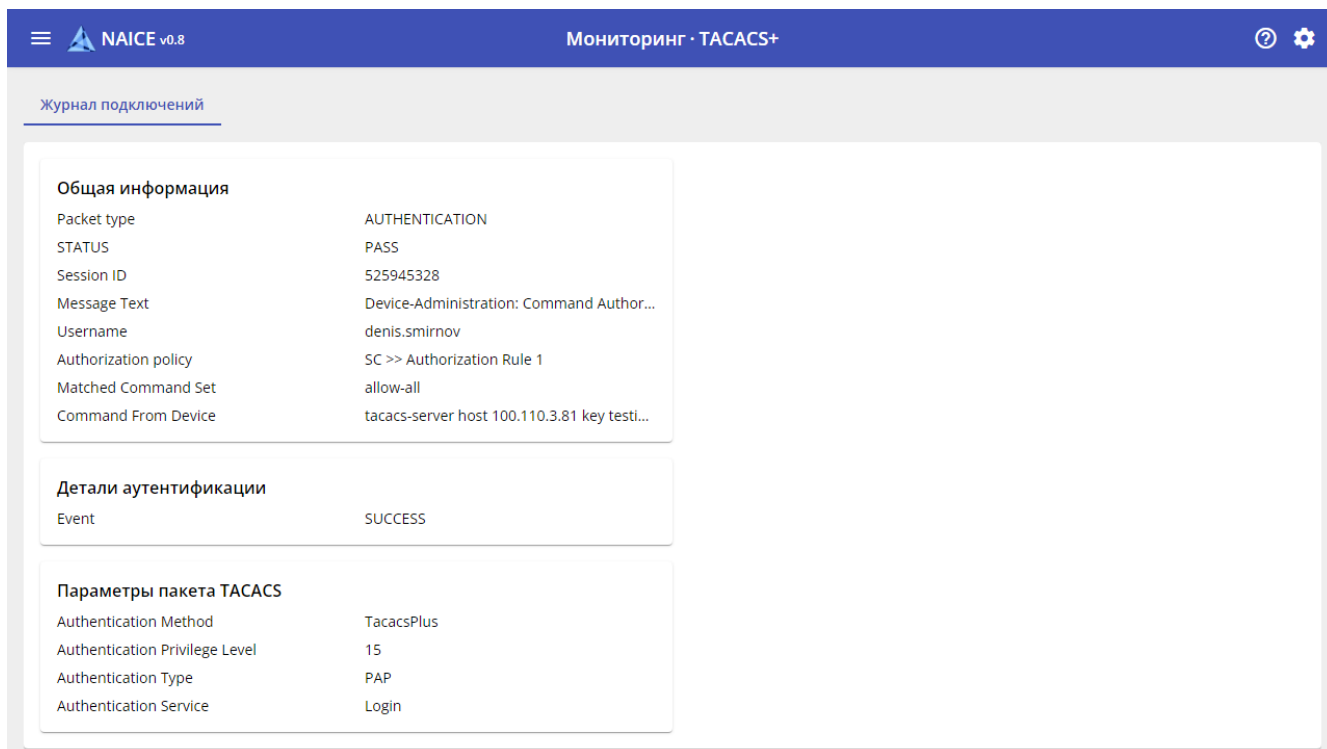
Пользователь

Сохранить    Отменить

Рисунок 229. 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.



The screenshot shows the 'Журнал подключений' (Connection Log) page in the NAICE v0.8 interface. The page title is 'Мониторинг · TACACS+'. The main content area displays detailed information for a selected session, organized into three sections:

- Общая информация** (General Information):
  - Packet type: AUTHENTICATION
  - STATUS: PASS
  - Session ID: 525945328
  - Message Text: Device-Administration: Command Author...
  - 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 testi...
- Детали аутентификации** (Authentication Details):
  - Event: SUCCESS
- Параметры пакета TACACS** (TACACS Packet Parameters):
  - Authentication Method: TacacsPlus
  - Authentication Privilege Level: 15
  - Authentication Type: PAP
  - Authentication Service: Login

Рисунок 230. 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.

# Лицензирование

## Описание

Лицензирование NAICE обеспечивается с помощью сервера лицензий **Eltex License Manager** (далее - ELM), осуществляющего функцию лицензирования программных и аппаратных продуктов компании «Элтекс». Для лицензирования может использоваться сервер ELM компании «Элтекс» (далее - Online ELM) или сервер ELM, установленный на стороне клиента (далее - Offline ELM). В обоих случаях адрес ELM сервера указывается при установке NAICE и на момент активации лицензии он должен быть доступен.

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 активации лицензии*, уникальный для каждого экземпляра NAICE. Для разблокировки функционала NAICE, соответствующего данной лицензии, файл необходимо загрузить в систему на странице *Лицензирование*.

## Уровни лицензии и лицензируемый функционал

В текущей версии реализован единственный уровень лицензирования **BASIC**. На этом уровне 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 авторизовывать 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](mailto:eltex@eltex-co.ru).

Для приобретения также доступен дополнительный модуль **NAICE-TACACS**, активирующий TACACS-сервер в составе NAICE. Модули приобретаются дополнительно для основной лицензии

любого уровня.

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](mailto:eltex@eltex-co.ru).

## Демонстрационный режим

После установки NAICE находится в демонстрационном режиме (деморезим). 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.



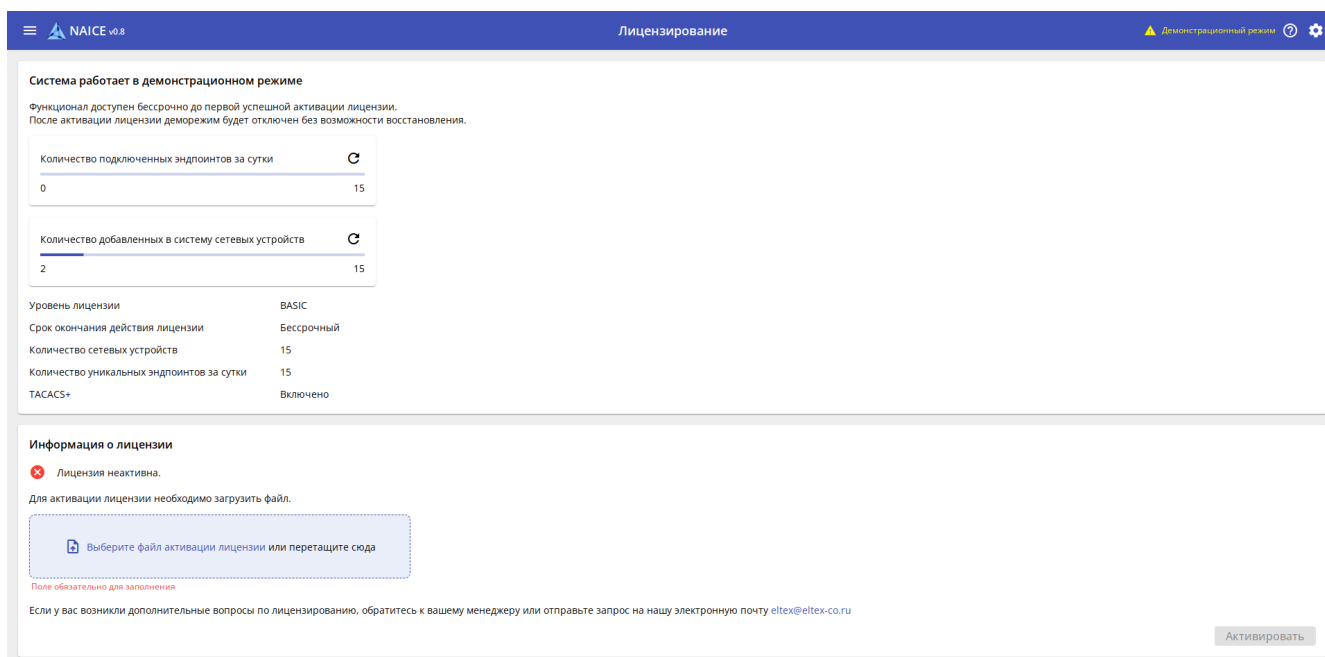
Демонстрационный режим не ограничен во времени, однако он доступен только **до первой успешной активации лицензии**. После активации лицензии деморезим будет отключен без возможности восстановления.

О том, что система находится в демонстрационном режиме, сигнализирует соответствующее предупреждение в верхней правой части страницы.

### Демонстрационный режим

Рисунок 231. Предупреждение о демонстрационном режиме

При нажатии на предупреждение будет осуществлен переход на страницу *Лицензирование*, содержащей актуальные параметры и лимиты деморезима. Также на этой странице отображается информация о лицензии.




Система работает в демонстрационном режиме  
Функционал доступен бессрочно до первой успешной активации лицензии.  
После активации лицензии деморезим будет отключен без возможности восстановления.


Количество подключенных эндпоинтов за сутки	0	15
Количество добавленных в систему сетевых устройств	2	15

Уровень лицензии	BASIC
Срок окончания действия лицензии	Бессрочный
Количество сетевых устройств	15
Количество уникальных эндпоинтов за сутки	15
TASACS+	Включено

**Информация о лицензии**

 Лицензия неактивна.

Для активации лицензии необходимо загрузить файл.

 Выберите файл активации лицензии или перетащите сюда

Поле обязательно для заполнения

Если у вас возникли дополнительные вопросы по лицензированию, обратитесь к вашему менеджеру или отправьте запрос на нашу электронную почту [eltex@eltex-co.ru](mailto:eltex@eltex-co.ru)

Активировать

Рисунок 232. Страница Лицензирование в демонстрационном режиме

## Первичная активация лицензии



Для активации лицензии необходимо иметь *файл активации*, полученный от Вашего менеджера при приобретении системы.



Формат имени файла активации - **NICENNNNNNN.txt**, например - NICE1111111.txt.

Активация лицензии осуществляется на странице *Лицензирование*, изображение которой приведено выше.

Страница в демонстрационном режиме, помимо актуальных параметров деморежима, содержит следующие элементы управления:

- Лицензия неактивна - текущий статус лицензии.
- Поле для загрузки файла активации лицензии. Файл активации лицензии можно выбрать из проводника или перетащить в данное поле.
- **Активировать** - кнопка для активации лицензии из загруженного файла активации.

Для загрузки лицензии перетащите файл в поле активации лицензии или выберите его в проводнике при клике на *"Выберите файл активации лицензии"*. При необходимости до нажатия на кнопку **Активировать** файл можно заменить, кликнув на в правой части поля загрузки.



Рисунок 233. Загрузка файла активации



Валидный файл активации лицензии не может быть пустым или иметь размер более 1 Мб.

Для активации лицензии нажмите кнопку **Активировать**.



Активация лицензии может занять до нескольких минут. Не предпринимайте никаких действий до завершения процесса.

## Успешная активация лицензии

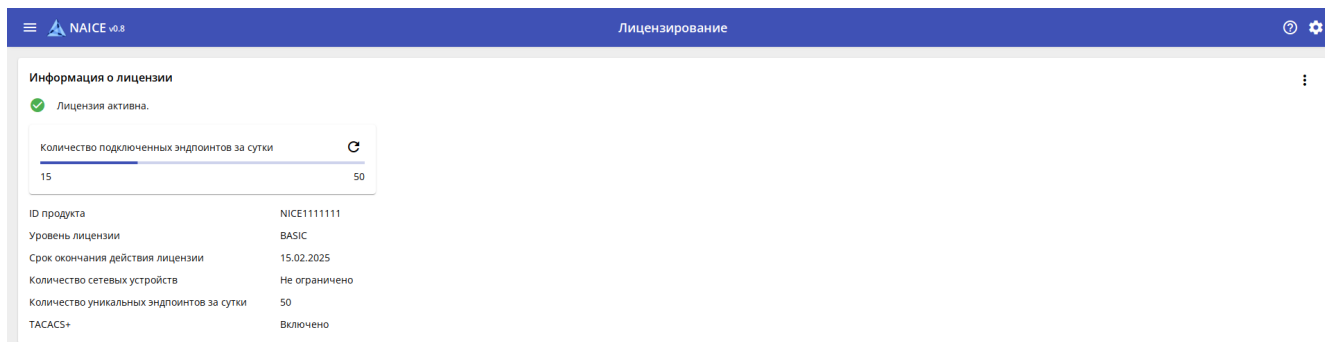



Рисунок 234. Лицензия активна

При успешной активации статус лицензии сменится на  **Лицензия активна** и отобразятся параметры текущей лицензии. Подробнее о параметрах лицензии описано [далее](#).

## Ошибки при активации лицензии

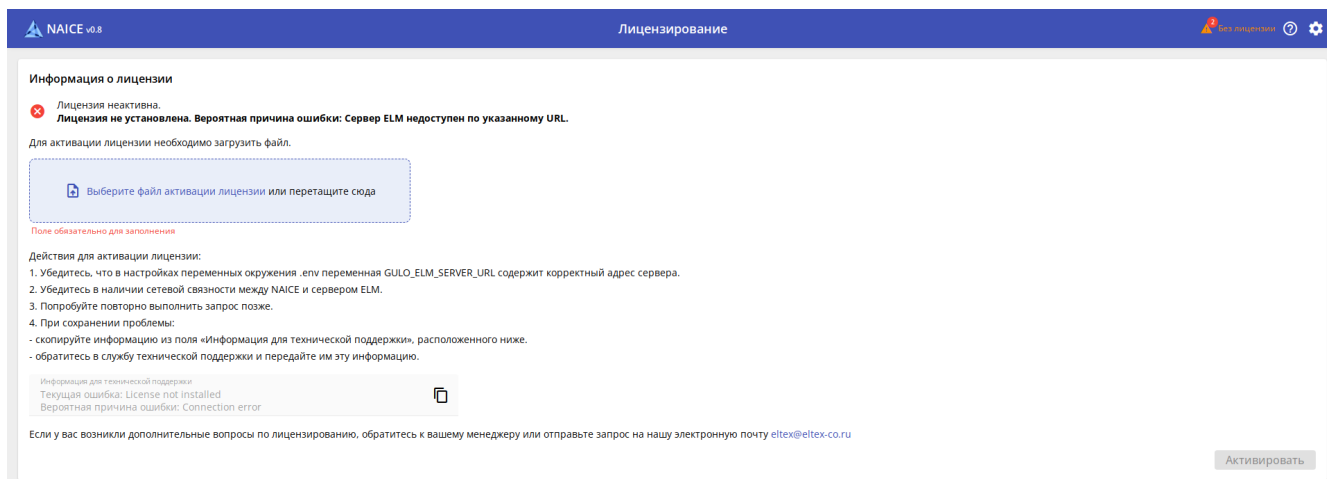


Рисунок 235. Ошибка при активации лицензии

При возникновении ошибок при активации лицензии на странице под статусом лицензии отобразится ошибка, возникшая в процессе активации. Как правило, ошибки при активации лицензии связаны либо с проблемами с доступом к серверу ELM (некорректный адрес ELM в конфигурации NAICE, отсутствие сетевой связности и т.п.), либо с ошибками самой лицензии (не наступивший или истекший срок лицензии).

Под полем для загрузки файла активации указаны рекомендации для устранения возникшей ошибки. В случае, если предложенные действия не оказали нужного воздействия, обратитесь в службу технической поддержки, приложив информацию из поля «Информация для технической поддержки» под рекомендациями.

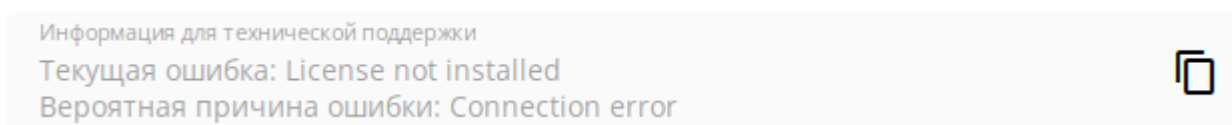




Рисунок 236. Информация для технической поддержки



Не рекомендуется выполнять действия, отличные от обозначенных в рекомендациях или указанных технической поддержкой. В некоторых ситуациях это может привести к блокировке экземпляра NAICE в ELM.

На данном этапе при необходимости файл активации лицензии можно заменить. Для этого нужно кликнуть на  в правой части поля загрузки файла активации и нажать на кнопку **Активировать**.

## Мониторинг состояния лицензии

После успешной активации лицензии ее состояние можно отслеживать на странице *Лицензирование*. Для перехода на страницу из любого раздела NAICE в правом верхнем углу необходимо выбрать , в открывшемся меню выбрать "Лицензирование".

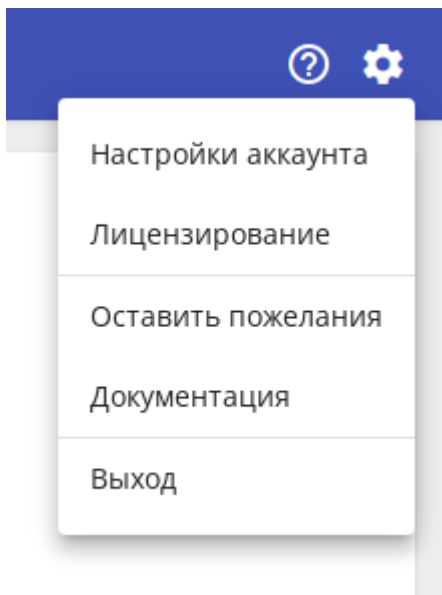


Рисунок 237. Меню системных настроек

После этого откроется страница с информацией о лицензии.

## Информация о лицензии

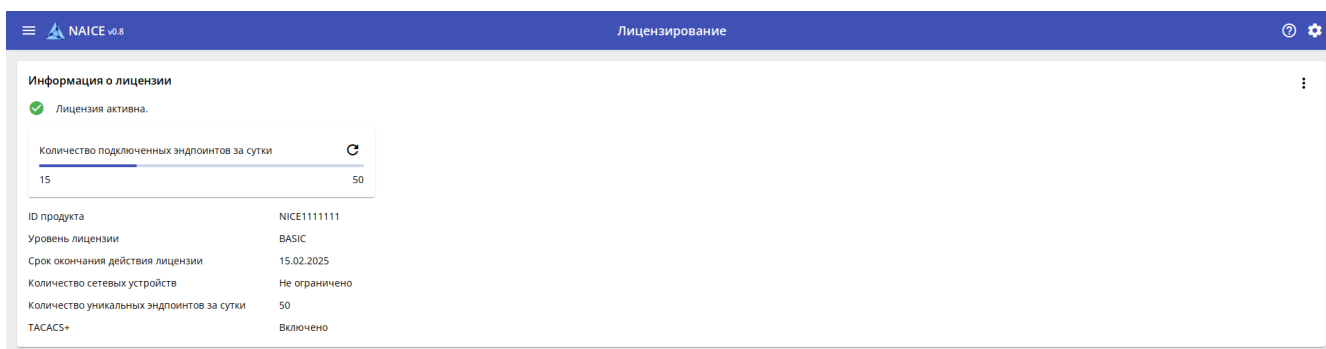


Рисунок 238. Информация о лицензии

Страница содержит следующие элементы:

- **Лицензия активна** - текущий статус лицензии.
- Счетчик текущего количества подключенных эндпоинтов за сутки. Автоматически обновляется раз в 5 минут.
- **↻** - ручное обновление счетчика.
- Параметры лицензии:
  - **ID продукта** - уникальный идентификатор экземпляра NAICE.
  - **Уровень лицензии** определяет доступный для настройки и использования функционал NAICE.
  - **Срок окончания действия лицензии** - дата, при наступлении которой текущая срочная лицензия истекает. Не распространяется на бессрочную лицензию.




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.

- TACACS+ - наличие или отсутствие дополнительного модуля NAICE-TACACS в лицензии.
-  - меню, за которым находятся кнопки **Обновить лицензию** и **Заменить файл активации**. Подробнее об этих действиях описано [далее](#).

## Особенности подсчета количества подключенных устройств за сутки

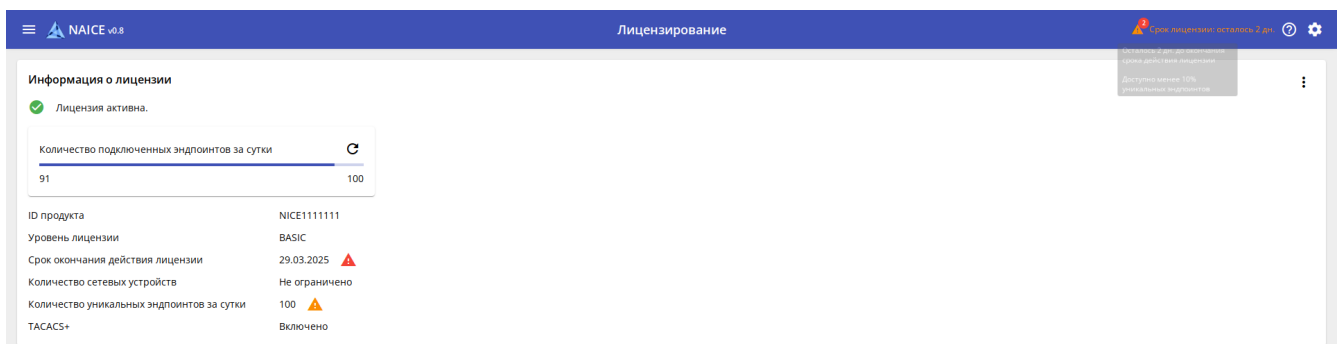
- Счетчик подключенных эндпоинтов увеличивается только при подключении **уникального** эндпоинта, то есть эндпоинта, который не был успешно авторизован NAICE в последние 24 часа.
- Для определения уникальности эндпоинта необходимо, чтобы в RADIUS-запросе передавался RADIUS-атрибут **Calling-Station-Id**, содержащий MAC-адрес конечного устройства.
- Устройство считается активным ровно 24 часа с момента последнего подключения. При переавторизации в эти сутки 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 переавторизовано 10 июня в 20:20:10, то время сдвинется до 11 июня в 20:20:11.

## Предупреждения о достижении лимитов



The screenshot shows the NAICE v0.8 interface with the following details:

- Header:** NAICE v0.8 | Лицензирование | Срок лицензии остался 2 дн.
- Information Section:**
  - Лицензия активна.
  - Количество подключенных эндпоинтов за сутки: 91 / 100
- License Details Table:**


ID продукта	NICE1111111
уровень лицензии	BASIC
Срок окончания действия лицензии	29.03.2025 ⚠
Количество сетевых устройств	Не ограничено
Количество уникальных эндпоинтов за сутки	100 ⚠
TACACS+	Включено

Рисунок 239. Предупреждения о достижении лимитов

При приближении к лимиту лицензии или демонстрационного режима по количеству подключенных эндпоинтов или при приближении к дате истечения лицензии в верхней правой части любой страницы NAICE будут отображаться предупреждения о приближении или достижении лимитов. При клике на предупреждение осуществляется переход на страницу Лицензирования.

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 верхней части страниц, данные предупреждения отображаются на странице Лицензирование напротив соответствующего параметра в виде .

## Недоступность сервера ELM

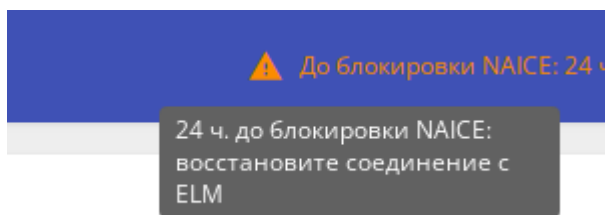


Рисунок 240. Предупреждение о недоступности ELM

NAICE периодически должен актуализировать параметры текущей 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 верхней правой части страницы 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.

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"}
```

## Обновление параметров лицензии



Выполняйте ручное обновление параметров лицензии только в случаях, когда это действительно необходимо - например, если был изменен уровень лицензирования и необходимо ускорить процесс применения новых параметров.

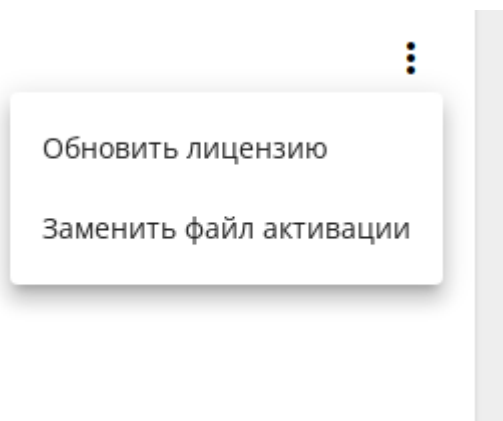



Рисунок 241. Меню дополнительных действий

Как было указано выше, NAICE периодически актуализирует параметры текущей лицензии на сервере ELM. В случае, если необходимо вручную обновить параметры лицензии, не дожидаясь автоматического обновления, то на странице Лицензирования нажмите на  и выберите **Обновить лицензию** в меню. Появится уведомление вида:

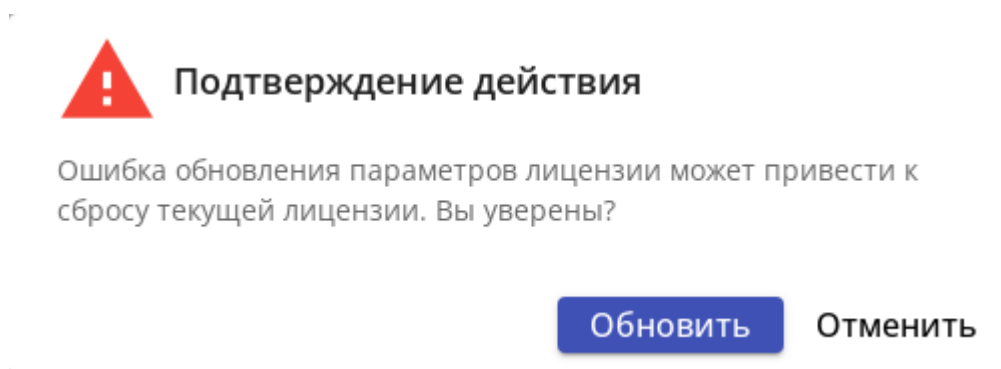


Рисунок 242. Подтверждение обновления параметров лицензии

Нажмите **Обновить**.

В случае успешного обновления параметров лицензии на странице отобразятся соответствующее уведомление и новые параметры лицензии.

Ручное обновление параметров доступно раз в 30 секунд. До истечения 30-секундной паузы кнопка будет заблокирована.

## Замена лицензии



Одному экземпляру NAICE соответствует одна лицензия. При необходимости изменения лицензии правки вносятся сотрудниками «Элтекс» в *текущую* лицензию, после чего ее параметры автоматически обновляются. Замена лицензии действительно необходима в редких случаях. Выполняйте замену лицензии **только** по указанию технической поддержки или вашего менеджера.

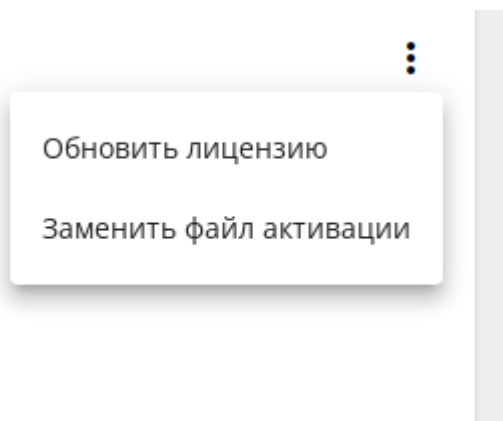

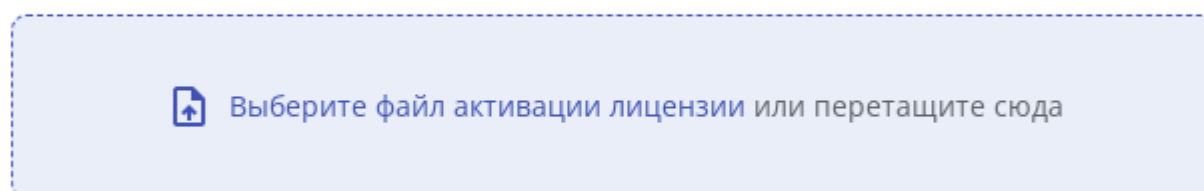


Рисунок 243. Меню дополнительных действий

Для замены файла активации на странице Лицензирования в правом верхнем углу страницы нажмите на  и выберите **Заменить файл активации** в меню.

## Замена файла активации лицензии

Замена файла активации приведет к сбросу текущей лицензии и обновлению параметров.



Поле обязательно для заполнения

Заменить

Отменить

Рисунок 244. Замена файла активации лицензии

В открывшемся окне выберите через проводник или перетащите в поле загрузки новый файл активации и нажмите **Заменить**.

При успешной замене файла откроется страница Лицензирование с параметрами новой лицензии.

При ошибках замены файла предыдущая лицензия будет сброшена, а возникшая ошибка отобразится на странице. Для устранения ошибок следуйте рекомендациям по активации лицензии, указанным на странице.