ГАЗИНФОРМ СЕРВИС

# Программный комплекс по защите системно-технической инфраструктуры «Efros Defence Operations»

## Руководство пользователя
## Часть 3

## Контроль доступа

Санкт-Петербург, 2024

# Аннотация

Руководство содержит описание настройки и конфигурирования модуля «Efros Network Access Control» (модуль «Efros NAC») в рамках разделов «Контроль доступа» и «Агенты».

Для работы с данным модулем необходимо убедиться в установке соответствующей лицензии в программном комплексе по защите системно-технической инфраструктуры «Efros Defence Operations» (ПК «Efros DO» или комплекс).

Для перехода в требуемый раздел необходимо выбрать в панели главного меню раздел «Контроль доступа» или «Агенты». Если панель свернута, навести курсор на пиктограмму «  » или «  » соответственно, панель автоматически раскроется и отобразятся все подразделы.

Руководство состоит из следующих частей:

- часть 1 – содержит сведения, необходимые для настройки доступа пользователей ПК «Efros DO» к сетевым ресурсам и функциям, а также описание выполнения функций контроля работы объектов сети с использованием веб-интерфейса;
- часть 2 – содержит сведения, необходимые для настройки и конфигурирования модулей ПК «Efros DO»: «Efros Network Assurance» («Efros NA»), «Efros Firewall Assurance» («Efros FA»), «Efros Integrity Check Compliance» («Efros ICC») и «Efros Vulnerability Control» («Efros VC»);
- часть 3 (данный документ) – содержит сведения, необходимые для настройки и конфигурирования функций контроля доступа;
- часть 4 – содержит сведения, необходимые для настройки возможностей контроля целостности функционального модуля «Efros Integrity Check Compliance» («Efros ICC»);
- часть 5 – содержит сведения, необходимые для настройки агента «Efros Defence Operations».

Степени важности примечаний:

Важная информация
Указания, требующие особого внимания.

Дополнительная информация
Информация, позволяющая упростить работу с ПК «Efros DO».

Представленные в документе снимки экрана могут отличаться для различных версий поставляемого комплекса и предназначены для демонстрации работы комплекса.

# Содержание

# 1 Предварительные настройки

Общие вопросы администрирования комплекса рассмотрены в первой части руководства пользователя (см. документ «Руководство пользователя. Часть 1. Администрирование»). Для работы с модулем «Efros NAC» необходимо произвести подготовительные действия:

- настроить подключение к AD (LDAP);
- добавить сертификаты для установки доверенного соединения при доступе устройств в сеть;
- при необходимости, вручную добавить конечные точки сети;
- добавить учетные записи сетевых пользователей (более подробно об этом написано в п. 3.3.1).

В ПК «Efros DO» в качестве сетевых пользователей поддерживаются локальные – учетные записи непосредственно заведены в комплексе – и сетевые пользователи из внешних систем.

При настройке доступа пользователей из внешних систем необходимо выполнить подключение в подразделе «Настройки/Источники данных» комплекса. Подробнее данный вопрос рассмотрен в документе «Руководство пользователя. Часть 1. Администрирование».

Предварительно необходимо провести работы на сетевом оборудовании: указать сетевой адрес комплекса, протокол взаимодействия TACACS+ и (или) RADIUS и разделяемый ключ.

При наличии в комплексе настроенной иерархии и, если пользователю назначены права доступа к различным серверам иерархии, то перед выполнением действий по контролю доступа пользователю необходимо выбрать в главном меню сервер, к которому подключено контролируемое оборудование (подробнее см. документ «Руководство пользователя. Часть 1. Администрирование»).

# 2 Работа со списком сущностей. Общие сведения

Списки сущностей в программном комплексе: устройства, сетевые пользователи, группы устройств и сетевых пользователей, а также наборы политик, профилей, наборов команд, отображающиеся в рабочей области, выполнены в виде таблицы. В качестве примера приведен подраздел «Сетевое оборудование», вкладка «Устройства» (рис. 1).

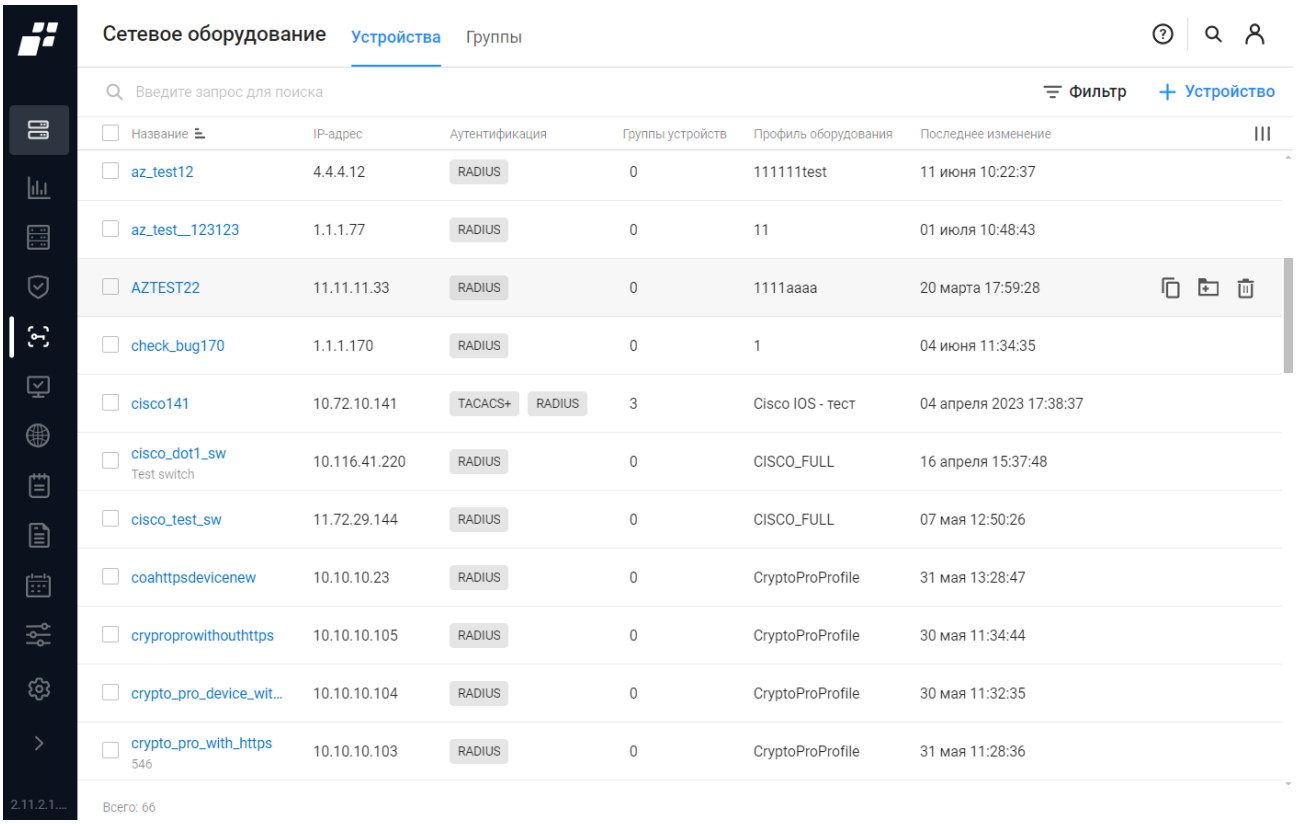



Рисунок 1 – Подраздел «Сетевое оборудование»

Над таблицей в зависимости от типа сущности могут быть доступны:

- поле поиска ( Введите запрос для поиска ) для поиска записи в списке. Поиск выполняется по мере ввода символов;
- кнопка «Устройство» ( + Устройство ) для перехода на страницу создания сущности[1];
- кнопка «Фильтр» ( Фильтр или ) для фильтрации списка сущностей;
- кнопка «Колонки» ( ) для изменения отображения колонок на странице
- индивидуальные для записей списка кнопки (подробнее описание кнопок приведено в разделах документа ниже).

[1] Название кнопки зависит от типа создаваемой сущности

Таблицы, кроме колонок с данными сущностей, содержат столбец с полями для флага.

После установки флага в одной или несколькими строками над таблицей отображается выбор операций, выполняемых с одной или несколькими сущностями (рис. 2, 3).

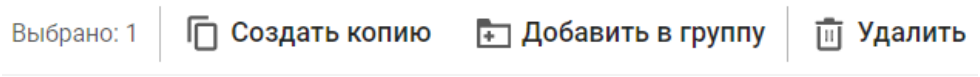



Рисунок 2 – Строка выбора операции, выполняемой с одной сущностью

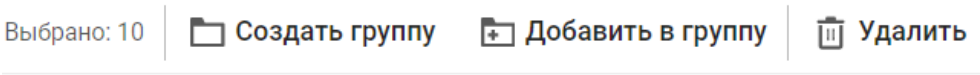



Рисунок 3 – Строка выбора операции, выполняемой с несколькими сущностями

Пользователь имеет возможность:

- в списках устройств, сетевых пользователей – создать копию сущности, создать группу сущностей, добавить в группу сущность, удалить выбранные сущности;
- в списках групп сетевого оборудования, групп сетевых пользователей – создать копию группы сущностей, удалить выбранные группы сущностей;
- в списках набора политик, профилей оборудования, профилей авторизации, набора команд – создать копию сущности, удалить выбранные сущности.
- в списках разрешенных MAC-адресов – удалить выбранные сущности.

## 2.1 Выбор сортировки записей таблиц

По умолчанию список сущностей отсортирован в порядке убывания даты и времени внесения последних изменений в данные сущности. Записи списка профилей оборудования, профилей авторизации – в алфавитном порядке.

Пользователь имеет возможность задать другой тип сортировки, выбрав заголовок требуемого столбца таблицы. В заголовке отобразится знак « », сортировка всех строк таблицы выполнена по убыванию значений выбранного столбца. Для изменения направления сортировки необходимо повторно выбрать заголовок столбца. В заголовке отобразится знак « ».

## 2.2 Поиск данных в таблицах списков сущностей

Для поиска в списке сущностей требуемых записей необходимо ввести в поле поиска последовательность символов из искомой записи. Поиск выполняется по мере ввода символов, в списке отобразятся записи сущностей, в данных которых содержатся введенные символы.

Для отмены заданного правила поиска и отображения в таблице всех записей необходимо нажать в поле поиска кнопку «Очистить» ( ).

## 2.3 Фильтрация данных в таблицах сущностей

Для фильтрации данных в списках сущностей по параметрам элементов таблицы необходимо:

- нажать кнопку « Фильтр » или « ». Откроется окно фильтрации. Состав полей окна для разных подразделов раздела «Контроль доступа» отличается. На рис. 4 приведен пример окна фильтрации списка активного сетевого оборудования (АСО);
- задать требуемые параметры фильтрации. Для раскрывающихся списков доступен множественный выбор значений параметра;
- нажать кнопку «Применить». Окно фильтрации закроется, на странице отобразятся данные, соответствующие заданным параметрам фильтрации.

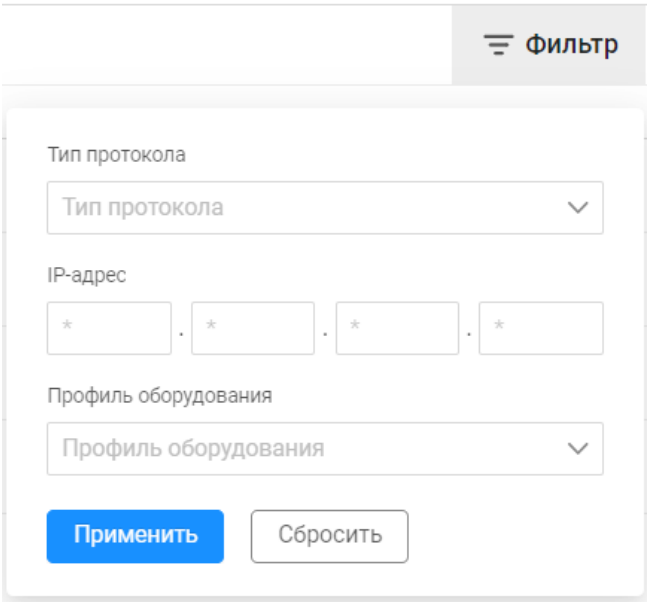



Рисунок 4 – Окно фильтрации списка АСО

Для внесения изменений в заданные правила фильтрации необходимо повторно открыть окно фильтрации, задать новые правила и нажать кнопку «Применить». Для очищения поля параметра – нажать в поле кнопку «Очистить» ( ✕).

Для отмены заданных правил фильтрации и отображения на странице всех данных необходимо повторно открыть окно фильтрации и нажать кнопку «Сбросить».

## 2.4 Настройка отображаемых колонок в таблицах списков сущностей

Для настройки состава отображаемых колонок в списках сущностей необходимо нажать кнопку «Колонки» ( ). Откроется окно выбора колонок таблицы. На рис. 5 приведено окно для списка устройств.

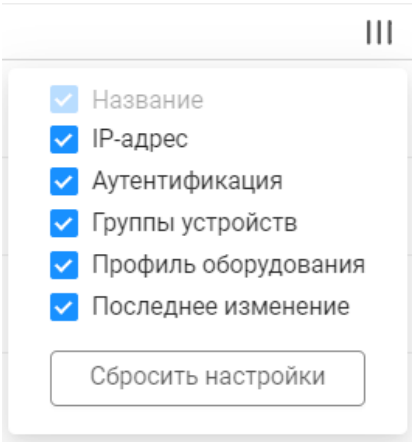



Рисунок 5 – Окно выбора колонок списка устройств

В окне отображаются строки с наименованиями всех колонок таблицы. Им соответствуют поля для флага. Наличие в поле флага означает, что столбец выбран для отображения в таблице. Колонка, строка которого неактивна, не доступен для изменения его видимости в таблице.

Для настройки состава отображаемых в списке колонок необходимо установить/отменить флаг. Состав колонок изменяется по мере установки/отмены флагов.

В окне выбора колонок пользователь может настроить последовательность расположения колонок в таблице. При наведении курсора на строку с названием колонки слева от поля для флага отображается символ «⠿». Перетаскиванием символа выбирается требуемое положение в списке колонок.

Для отмены изменений необходимо нажать на кнопку «Сбросить настройки».

## 2.5 Копирование/изменение параметров сущностей

Копирование сущности в списке может быть выполнено одним из следующих способов:

1) Способ 1:
   - навести курсор на строку с сущностью;
   - в правой части строки копируемой записи нажать кнопку «Создать копию» ( );
   - в открывшемся окне отредактировать необходимые параметры и нажать кнопку «Создать».

2) Способ 2:
   - установить флаг в строке копируемой записи;
   - нажать в строке операций над таблицей (см. рис. 2) кнопку «Создать копию» ( Создать копию );
   - в открывшемся окне отредактировать необходимые параметры и нажать кнопку «Создать».

Изменение параметров сущностей выполняется следующим способом:

1) навести курсор в таблице на название сущности;
2) нажать на сущность. Откроется страница с параметрами сущности;
3) внести требуемые изменения;
4) нажать кнопку «Сохранить».

После копирования или внесения изменений и нажатия кнопки «Создать» или «Сохранить» автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности копируемой/изменяемой сущности.

При обнаружении недопустимых значений под полем появится подсказка красного цвета с информацией для корректного заполнения поля и кнопка «Создать»/«Сохранить» будет недоступна. При дублировании информации в верхней части страницы появится сообщение, что поле должно содержать уникальную информацию. Пользователю необходимо корректно заполнить поля страницы, кнопка «Создать»/«Сохранить» станет доступной.

## 2.6 Затемнение символов введенного пароля или ключа

При вводе пароля или ключа символы в поле заменяются знаком «•». Для просмотра введенного значения необходимо нажать в поле ввода кнопку «Просмотр» ( ).

## 2.7 Просмотр предварительно настроенных параметров

При создании или изменении параметров сущности рядом с полем выбора предварительно настроенных сущностей может присутствовать кнопка «Просмотр» ( ). При нажатии на кнопку выводятся основные параметры выбранной предварительно настроенной сущности (рис. 6).

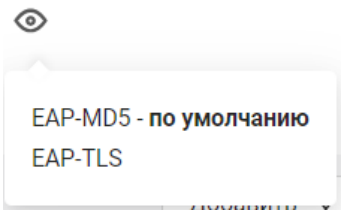


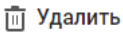

Рисунок 6 – Просмотр предварительно настроенных параметров

## 2.8 Удаление сущностей

Удаление сущностей выполняется вручную. Для удаления доступны только те записи списков ПК «Efros DO», которые не использованы в карточках других. При попытке удаления таких сущностей, удаление выполнено не будет, отобразится соответствующее сообщение.

Удаление одной сущности из списка может быть выполнено двумя способами:

1) Способ 1:
   - навести курсор на строку с сущностью;
   - нажать в строке удаляемой записи кнопку «Удалить» (  );
   - нажать в открывшемся окне подтверждения кнопку «Удалить».

2) Способ 2:
   - установить флаг в строке или нескольких строках удаляемых записей;
   - нажать в строке операций над списком сущностей (см. рис. 2) кнопку «Удалить» (  );
   - нажать в открывшемся окне подтверждения кнопку «Удалить».

В результате будет запущен процесс удаления сущности.

В случае возникновения ошибки в процессе удаления сущность из списка не будет удалена.

## 2.9 Аудит основных событий

После успешного завершения процесса создания, изменения или удаления сущностей в журнале событий ПК «Efros DO» вносится сообщение соответствующего типа. Просмотр событий доступен в разделе «События»:

- подраздел «Аудит действий пользователя»;
- подраздел «Системные события» → вкладка «Контроль доступа».

# 3 Раздел «Контроль доступа»

## 3.1 Настройка политик доступа

Управление сетевым доступом с использованием сервера RADIUS осуществляется на основе сформированных политик, которые представляют собой набор условий, а также результат срабатывания правил аутентификации и авторизации. В качестве условий могут выступать различные протоколы (проводной/беспроводной доступ с использованием 802.1x, MAB и т.п.), атрибуты словарей RADIUS, источники идентификации (локальные сетевые пользователи, пользователи подключенного LDAP, зарегистрированные конечные точки и т.п.).

Для управления доступом с использованием сервера TACACS+ необходимо настроить предустановленные наборы команд (создать пользовательский набор команд) и сделать привязку пользователя либо групп пользователей к оборудованию/группе оборудования. Для некоторых сценариев, связанных с проверкой доменных пользователей, требуется дополнительная настройка политик доступа.

Политики доступа определяют основные правила, по которым будет осуществляться разграничение доступа в сеть. Наборы политик позволяют сгруппировать политики аутентификации и авторизации в рамках одного набора правил.

Созданные политики срабатывают последовательно, начиная с расположенных вверху списка, до первого совпадения.

При формировании нового набора политики указывается основное правило, правила аутентификации и правила авторизации.

При составлении правил, используемых в наборах политик, рекомендуется использовать правила доступа к сети из предустановленных шаблонов (таблица 1).

Таблица 1 – Предустановленные шаблоны, используемые в условиях набора политик

| Название шаблона условий | Описание |
|---|---|
| RemoteAccessVPN | Удаленный доступ (VPN) |
| DeviceAdministration | Управление сетевыми устройствами |
| WiredWebAuth | Проводная аутентификация |
| WirelessWebAuth | Беспроводная аутентификация |
| Wired802_1X | Проводная аутентификация по стандарту 802.1x |
| Wireless802_1X | Беспроводная аутентификация по стандарту 802.1x |
| WiredMab | Проводная аутентификация по MAC-адресам |
| WirelessMab | Беспроводная аутентификация по MAC-адресам |

Конкретные параметры, определяющие используемый сценарий доступа, могут отличаться для разных производителей оборудования и указываются в профиле

оборудования, более подробно см. подраздел 3.5 «Профили оборудования» данного документа.

После срабатывания условий, указанных в настройках набора политик, происходит проверка на соответствие условиям, указанным в правилах аутентификации.

Правила аутентификации позволяют обеспечить аутентификацию для сеанса входа пользователя с использованием различных стандартных протоколов аутентификации. Комплекс определяет допустимый протокол(ы), который доступен для сетевых устройств, на которых пользователь пытается пройти аутентификацию, и проверяет наличие учетных данных субъекта, запрашивающего доступ к сети, в выбранном источнике данных (локальные сетевые пользователи, пользователи подключенного LDAP, конечные точки, профили сертификатов и т.п.).

Каждый набор политик может содержать несколько правил аутентификации, которые настраиваются отдельно для каждого набора.

В случае ошибки аутентификации, дальнейшее поведение будет зависеть от действий, указанных в правилах:

- «Отклонить» – аутентификация не считается пройденной;
- «Продолжить» – осуществляется дальнейшая проверка по включенным правилам.

Основные условия, используемые при формировании правил аутентификации, указаны в таблице 2.

Таблица 2 – Основные условия, используемые при формировании правил аутентификации

| **Протокол, используемый при доступе к сети** | **Логическая операция** | **Выбранные значения** | | | |
|---|---|---|---|---|---|
| EAP-MD5 | | Gazinformservice | GisEapType | равно | MD5 |
| EAP-TLS | | Gazinformservice | GisEapType | равно | TLS |
| PAP | | Gazinformservice | GisAuthType | равно | PAP |
| PEAP_EAP-GTC | И | Gazinformservice | GisEapType | равно | PEAP |
| | | Gazinformservice | GisEapAuthType | равно | GTC |
| PEAP_EAP-MSCHAPv2 | И | Gazinformservice | GisEapType | равно | PEAP |
| | | Gazinformservice | GisEapAuthType | равно | MSCHAPv2 |
| PEAP_EAP-TLS | И | Gazinformservice | GisEapType | равно | PEAP |
| | | Gazinformservice | GisEapAuthType | равно | TLS |
| TTLS_PAP | И | Gazinformservice | GisEapType | равно | TTLS |
| | | Gazinformservice | GisAuthType | равно | PAP |
| TTLS_CHAP | И | Gazinformservice | GisEapType | равно | TTLS |
| | | Gazinformservice | GisAuthType | равно | CHAP |

| Протокол, используемый при доступе к сети | Логическая операция | Выбранные значения | | | |
|---|---|---|---|---|---|
| TTLS_MSCHAPv2 | И | Gazinformservice | GisEapType | равно | TTLS |
| | | Gazinformservice | GisAuthType | равно | MS-CHAP |
| TTLS_EAP-MD5 | И | Gazinformservice | GisEapType | равно | TTLS |
| | | Gazinformservice | GisEapAuthType | равно | MD5 |
| TTLS_EAP-GTC | И | Gazinformservice | GisEapType | равно | TTLS |
| | | Gazinformservice | GisEapAuthType | равно | GTC |
| TTLS_EAP-MSCHAPv2 | И | Gazinformservice | GisEapType | равно | TTLS |
| | | Gazinformservice | GisEapAuthType | равно | MSCHAPv2 |
| TTLS_EAP-TLS | И | Gazinformservice | GisEapType | равно | TTLS |
| | | Gazinformservice | GisEapAuthType | равно | TLS |

После успешной аутентификации будет осуществлена проверка на соответствие условиям правил авторизации и назначен соответствующий профиль авторизации. Для выбора профиля авторизации при создании правил авторизации в наборе политик, необходимый профиль должен быть создан заранее.

Ниже приведена рекомендуемая последовательность действий при настройке типового сценария взаимодействия по RADIUS\TACACS+. В зависимости от решаемых задач и используемого протокола сетевого доступа, последовательность может различаться.

Предварительно необходимо провести конфигурацию сетевого оборудования: указать сетевой адрес комплекса, протокол взаимодействия TACACS+ и (или) RADIUS и разделяемый ключ.

Более подробно о рекомендуемой последовательности действий для настройки типового сценария взаимодействия с использованием протоколов RADIUS и TACACS+ написано в приложении А.

## 3.2 Сетевое оборудование

Данный подраздел позволяет зарегистрировать в базе данных ПК «Efros DO» новое АСО и закрепить за ним сетевых пользователей/группу сетевых пользователей. Если сетевых пользователей нет в базе данных ПК «Efros DO», то закрепить АСО за ними можно позже.

Страница содержит отдельные вкладки списков АСО (вкладка «Устройства») и групп АСО (вкладка «Группы»). По умолчанию активной является вкладка «Устройства», содержащая список всего АСО, контролируемого ПК «Efros DO» (рис. 7). АСО добавляется, редактируется или удаляется в списке вручную пользователем комплекса. Также АСО можно добавить с помощью импорта данных из внешних систем (более подробно см. документ «Руководство пользователя. Часть 1. Администрирование»).

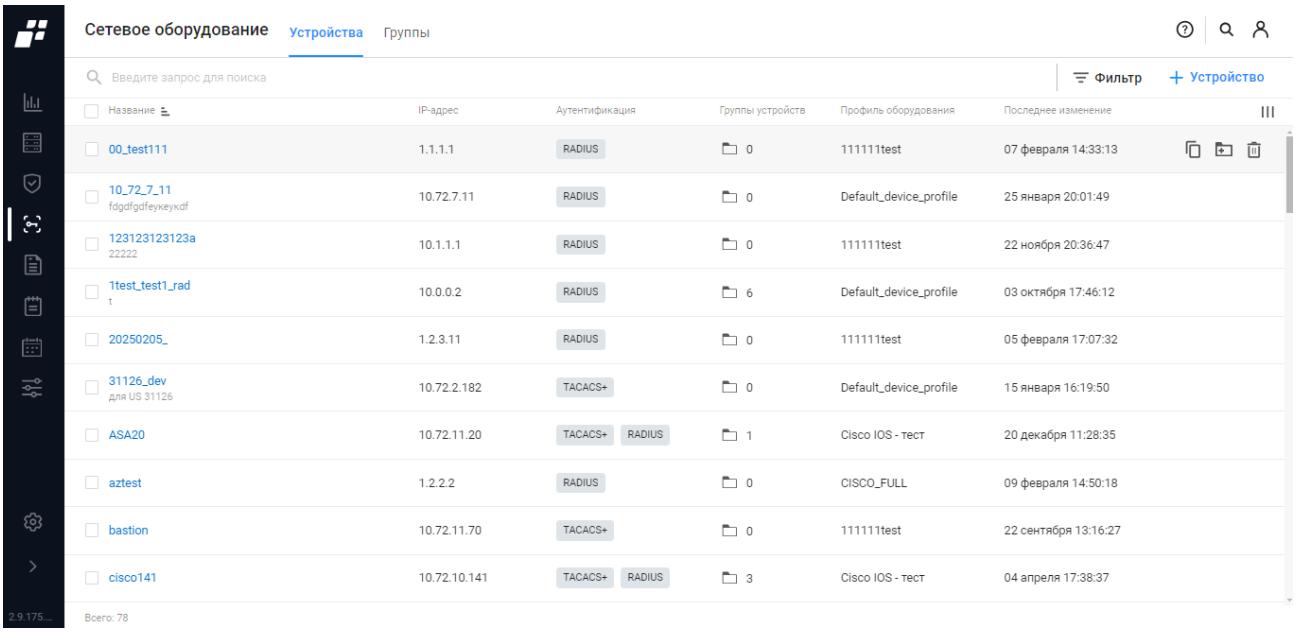



Рисунок 7 – Подраздел «Сетевое оборудование»

### 3.2.1 Вкладка «Устройства»

На странице список АСО реализован в виде таблицы (см. рис. 7). Для каждой записи списка отображаются следующие данные:

- поле для флага;
- название – является ссылкой, при переходе открывается окно редактирования устройства;
- IP-адрес устройства;
- используемый тип протокола доступа к сетевому оборудованию (RADIUS/TACACS+);
- количество групп, в которые входит устройство;
- профиль оборудования;
- дата и время последнего изменения параметров устройства.

Над списком АСО располагаются:

— поле поиска ( Введите запрос для поиска );
— кнопка «Фильтр» ( Фильтр );
— кнопка «Устройство» ( Устройство );
— кнопка «Колонки» ( ).

При установке флага в строке с необходимым АСО над списком появляются следующие кнопки:

— кнопка «Создать копию» ( Создать копию );
— кнопка «Добавить в группу» ( Добавить в группу );
— кнопка «Удалить» ( Удалить ).

Аналогичные кнопки появляются в правой части экрана в строке с выбранным АСО.

### 3.2.1.1 Добавление нового устройства

Для ручного добавления АСО пользователю необходимо выполнить следующие шаги:

1) Нажать на странице кнопку «Устройство» ( Устройство ).
2) Откроется страница «Создание устройства», приведенная на рис. 8. Заполнить поля вкладки требуемыми параметрами. Состав и описание полей вкладки «Свойства» приведены в таблице 3.

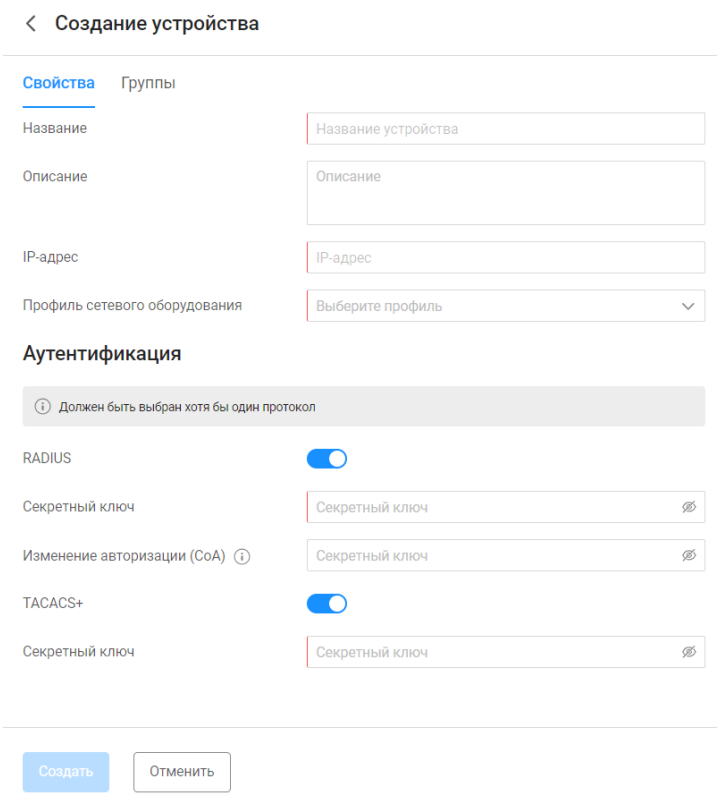



Рисунок 8 – Страница «Создание устройства»

Таблица 3 – Состав и описание полей вкладки «Свойства»

| Поле | Описание |
|---|---|
| Поле «Название» | Текстовое поле для ввода имени устройства.<br>Параметры ввода текста: от 1 до 250 символов.<br>Допустимые символы: буквы латинского алфавита, цифры, «_», «–» |
| Поле «Описание» | Текстовое поле для ввода описания устройства.<br>Параметры ввода текста: от 1 до 4000 любых символов |
| Поле «IP-адрес» | Текстовое поле для ввода IP-адреса устройства.<br>Параметры ввода текста: формат от 0.0.0.0 до 255.255.255.255, кроме 0.0.0.0 и 255.255.255.255, |
| Поле «Профиль сетевого оборудования» | Раскрывающийся список заранее созданных профилей сетевого оборудования (см. подраздел 3.5) |
| Блок полей «Аутентификация» | Переключатели:<br>«RADIUS»;<br>«TACACS+».<br>Активация переключателя означает, что устройство работает с использованием соответствующего протокола.<br>Должен быть выбран хотя бы один протокол.<br>Для активированного протокола необходимо ввести заданный на устройстве секретный ключ. |
| Элементы управления | |
| Создать | При нажатии кнопки выполняется создание устройства |
| Отменить | При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных |

3) Перейти на вкладку «Группы» (рис. 9). Заполнить поля необходимыми параметрами. Состав и описание полей вкладки приведены в таблице 4.

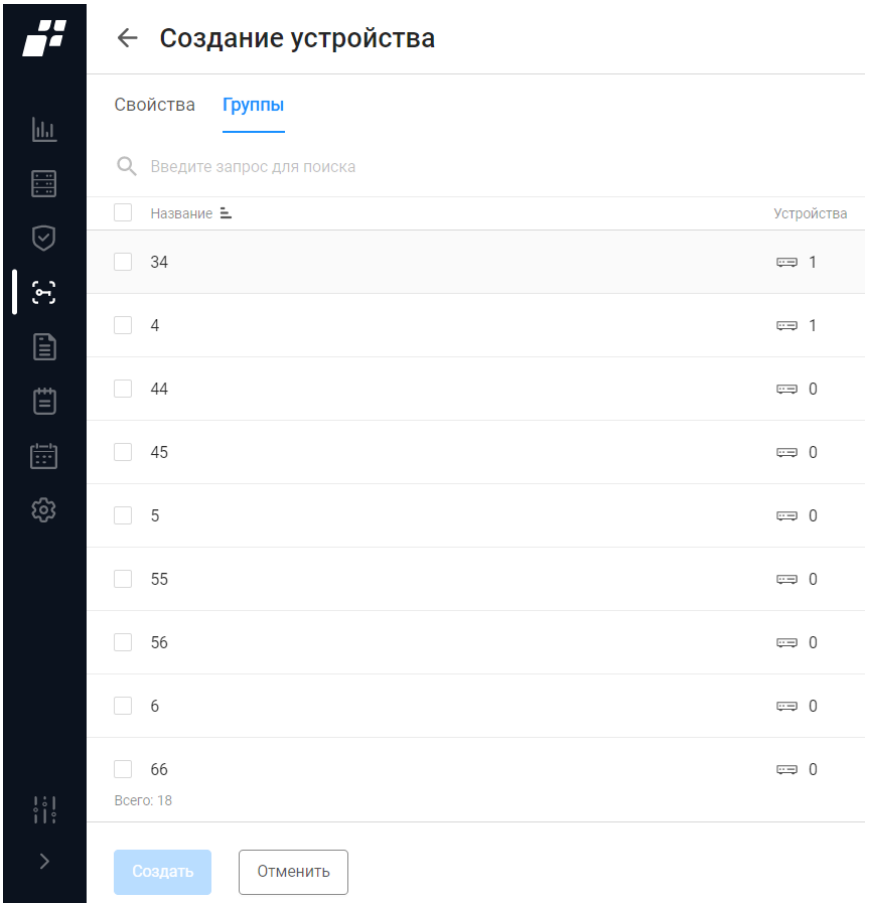



Рисунок 9 – Вкладка «Группы» страницы «Создание устройства»

Таблица 4 – Состав и описание полей вкладки «Группы»

| Поле | Описание |
|---|---|
| Поле для флага | Поле для выбора требуемых групп устройств |
| Поле «Название» | Содержит следующую информацию:<br>— название группы устройств;<br>— описание |
| Поле «Устройства» | Поле содержит информацию о количестве устройств в группе |
| Элементы управления | |
| Поле «Поиск» | Поле для ввода последовательности символов из искомой записи |
| Создать | При нажатии кнопки выполняется создание устройства |
| Отменить | При нажатии кнопки выполняется переход на страницу «Сетевое оборудование», вкладка «Устройства» без сохранения внесенных изменений |

4) Добавить, при необходимости, устройство в группу устройств, установив флаг в нужной строке.

### 3.2.2 Вкладка «Группы»

На странице список групп АСО реализован в виде таблицы (рис. 10).

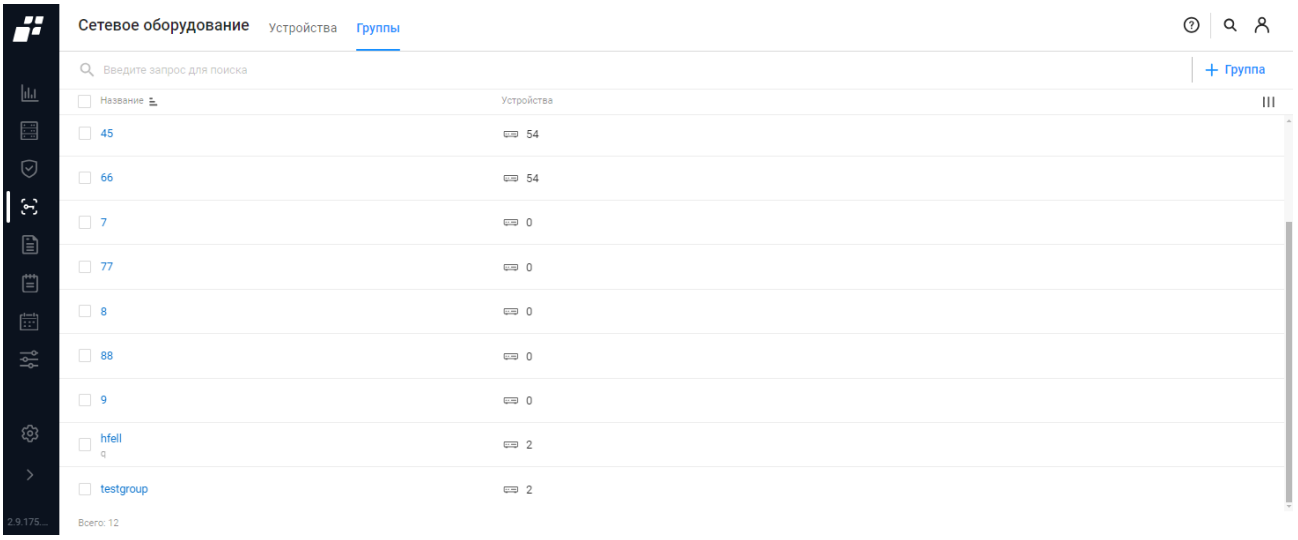



Рисунок 10 – Вкладка «Группы» подраздела «Сетевое оборудование»

Для каждой записи списка отображаются следующие данные:

- поле для флага;
- название – является ссылкой, при переходе открывается окно редактирования группы;
- количество устройств, входящих в группу.

Над списком групп располагаются:

- поле поиска ( Введите запрос для поиска );
- кнопка «Группа» ( + Группа );
- кнопка «Колонки» ( ).

При установке флага в строке с необходимой группой устройств над списком групп появляются следующие кнопки:

- кнопка «Удалить» ( );
- кнопка «Создать копию» ( ).

Аналогичные кнопки появляются в правой части экрана в строке с выбранной группой.

#### 3.2.2.1 Добавление группы устройств

Для ручного добавления новой группы устройств пользователю необходимо выполнить следующие шаги:

1) Нажать на кнопку «Группа» ( + Группа ) (рис. 10).

2) Откроется страница «Создание группы устройств» (рис. 11). Заполнить поля необходимыми параметрами. Состав и описание полей страницы приведены в таблице 5.

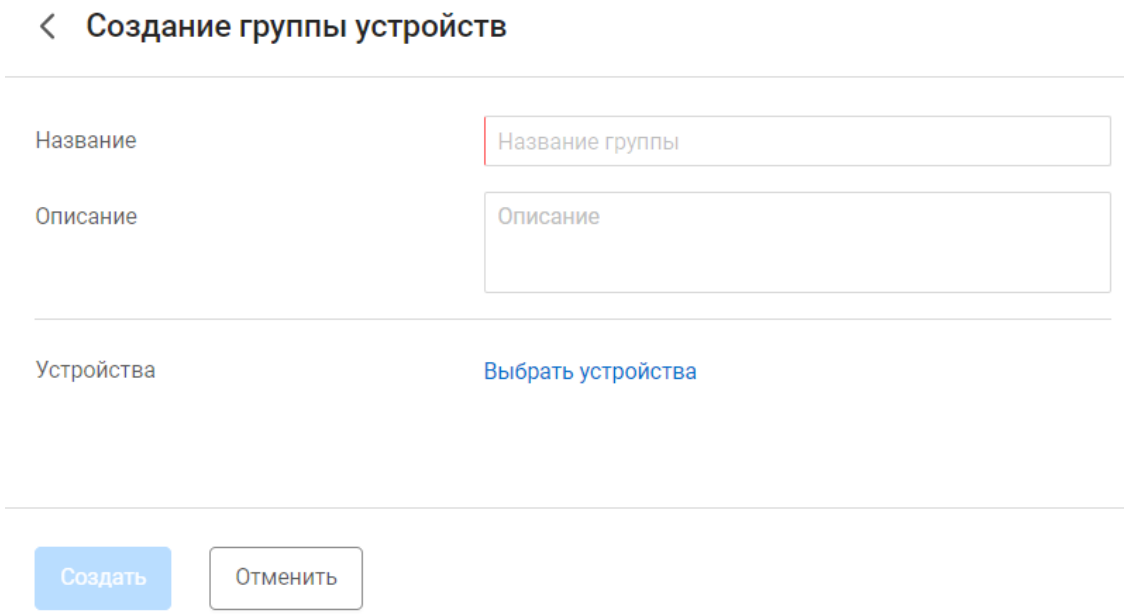



Рисунок 11 – Страница «Создание группы устройств»

Таблица 5 – Состав и описание полей страницы «Создание группы устройств»

| Поле | Описание |
|---|---|
| Поле «Название» | Текстовое поле для ввода названия группы устройств.<br>Параметры ввода текста: от 1 до 250 символов.<br>Допустимые символы: буквы латинского и кириллического алфавитов, цифры, знак «пробел», «_», «–» |
| Поле «Описание» | Текстовое поле для ввода описания группы устройств.<br>Параметры ввода текста: от 1 до 4000 любых символов |
| Поле «Устройства» | При нажатии на кнопку «Выбрать устройства» открывается окно со списком устройств, заведенных в ПК «Efros DO». Для добавления устройств в группу необходимо установить флаг в строке устройства и нажать кнопку «Выбрать» |
| Элементы управления | |
| Создать | При нажатии кнопки выполняется создание группы |
| Отменить | При нажатии кнопки выполняется переход без сохранения внесенных данных |

## 3.3 Сетевые пользователи

Подраздел «Сетевые пользователи» позволяет зарегистрировать в базе данных ПК «Efros DO» сетевых пользователей для настройки доступа к АСО либо ресурсам сети (гостевой портал).

Страница содержит отдельные вкладки пользователей и групп пользователей и вкладку «Настройки безопасности». Сетевые пользователи добавляются, редактируются или удаляются в списке вручную пользователем ПК «Efros DO» с соответствующей привилегией. По умолчанию активной является вкладка «Пользователи» (рис. 12).

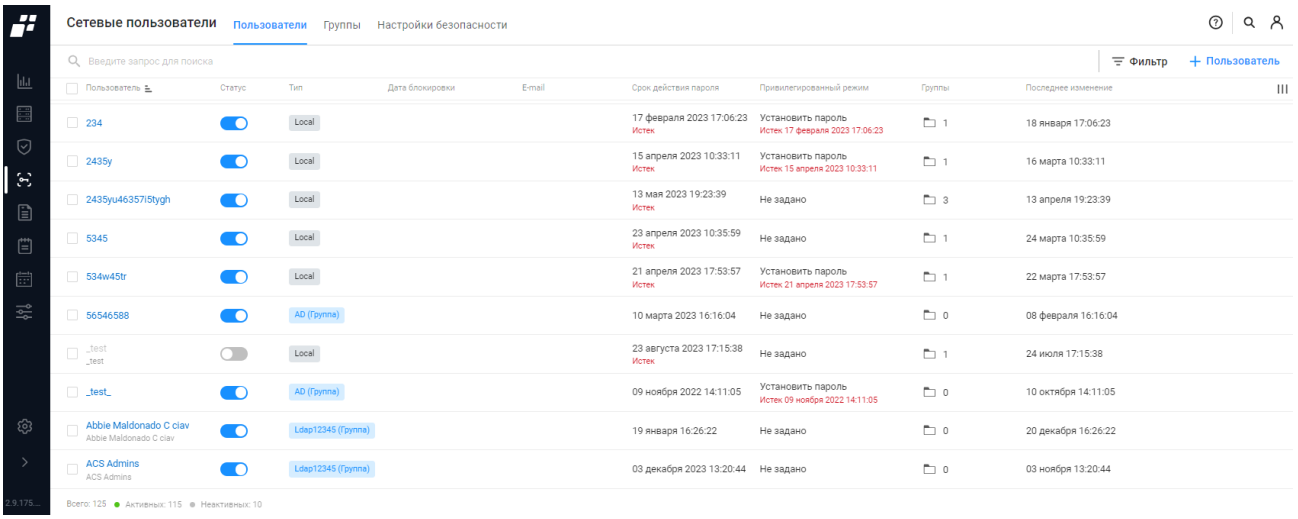



Рисунок 12 – Вкладка «Пользователи»

### 3.3.1 Вкладка «Пользователи»

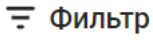
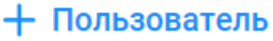
На странице вкладки «Пользователи» список сетевых пользователей реализован в виде таблицы (см. рис. 12). Для каждой записи списка отображаются следующие данные:

- поле для флага;
- пользователь – является ссылкой, при переходе по которой открывается окно для редактирования данных сетевого пользователя (более подробно см. п.п. 3.3.1.1);
- статус (активен/неактивен);
- тип – содержит информацию об учетной записи сетевого пользователя:
  - « Local » – учетная запись сетевого пользователя создана локально в базе данных ПК «Efros DO»;
  - « AD » – используется доменная учетная запись[2].

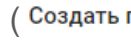
[2] Для доменных пользователей кнопка отображает название домена

- дата блокировки – дата окончания действия учетной записи сетевого пользователя;
- E-mail, указанный при создании пользователя;
- срок действия пароля;
- привилегированный режим;
- количество групп, в которые входит сетевой пользователь;
- дата внесения последних изменений в параметры учетной записи сетевого пользователя.

Над списком с сетевыми пользователями располагаются:

- поле поиска (  );
- кнопка «Фильтр» (  );
- кнопка «Пользователь» (  );
- кнопка «Колонки» (  ).

При установке флага в строке с необходимым локальным сетевым пользователем над списком появляются следующие кнопки:

- кнопка «Создать копию» (  ) – для одного выбранного локального пользователя;
- кнопка «Создать группу» (  ) – для нескольких, выбранных локальных пользователей;
- кнопка «Добавить в группу» (  );
- кнопка «Удалить» (  ).

При наведении курсора на локального сетевого пользователя в правой части экрана появляются следующие кнопки:

- кнопка «Сменить пароль» (  ).
- кнопка «Создать копию» (  ) – для одного выбранного локального пользователя;
- кнопка «Добавить в группу» (  );
- кнопка «Удалить» (  ).

При установке флага в строке с необходимым доменным сетевым пользователем над списком появляется кнопка «Удалить» (  ). При наведении курсора на доменного сетевого пользователя в правой части экрана также появляется кнопка «Удалить» (  ).

### 3.3.1.1 Добавление сетевого пользователя

Для добавления доменных сетевых пользователей предварительно необходимо произвести настройку соединения к источнику данных LDAP («Настройки» → «Источники данных»).

Для добавления сетевого пользователя пользователю ПК «Efros DO» необходимо выполнить следующие действия:

1) Нажать кнопку «Пользователь» ( + Пользователь ).
2) Откроется страница «Создание сетевого пользователя». При изменении значения поля «Тип» можно выбрать добавление локального пользователя, доменного пользователя или группы доменных пользователей. Для различных типов выводится различный состав полей для заполнения (рис. 13-15). Необходимо заполнить поля требуемыми параметрами и нажать кнопку «Создать». Состав и описание полей страницы приведены в таблицах 6.

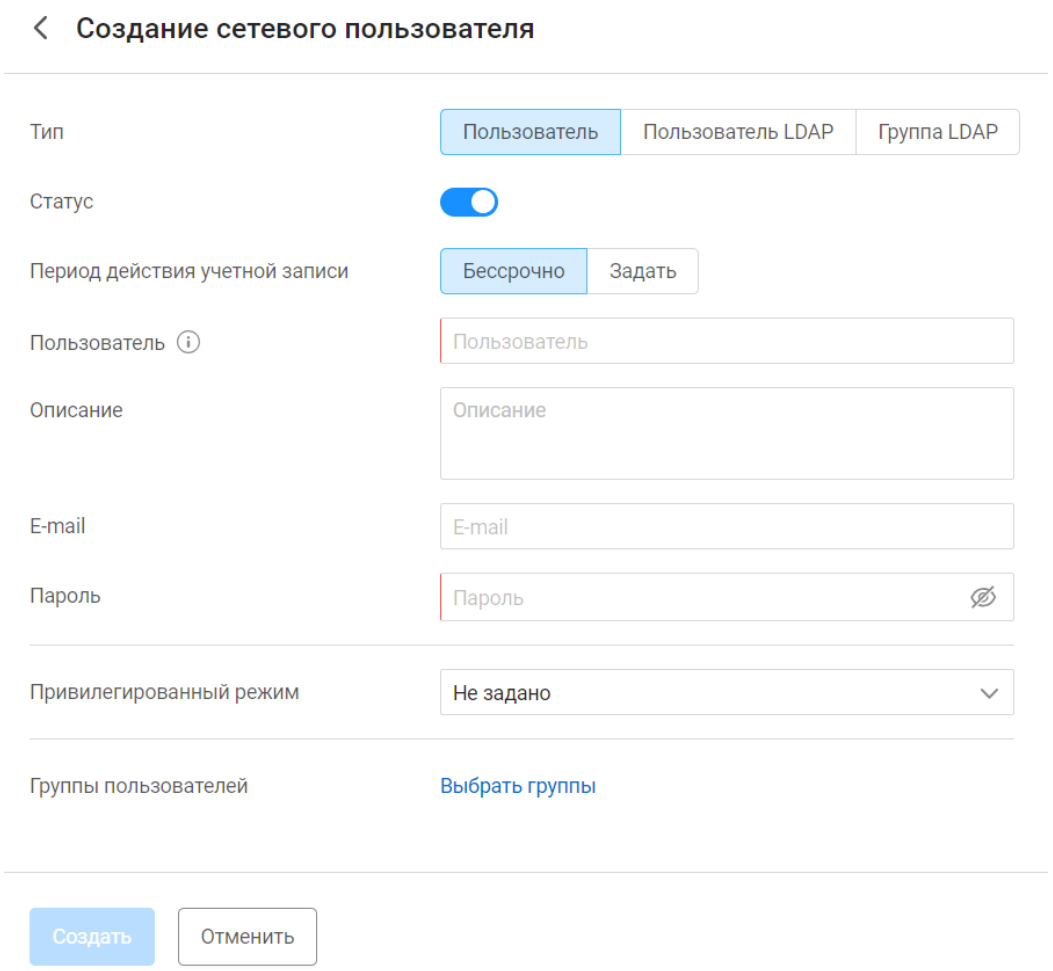



Рисунок 13 – Страница «Создание сетевого пользователя». Добавление локального типа пользователя

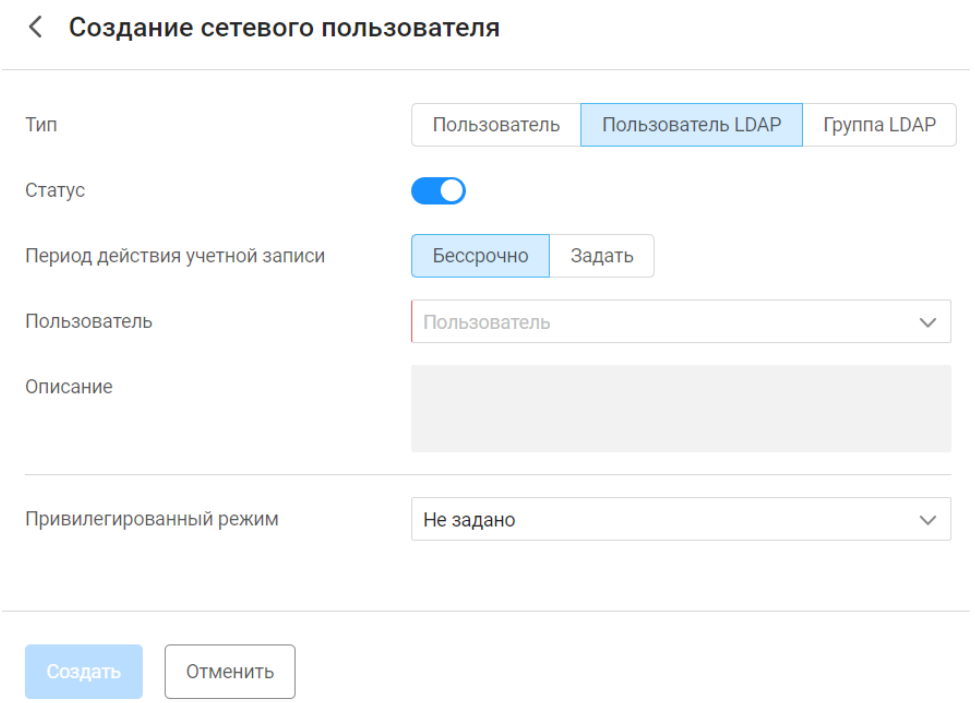



Рисунок 14 – Страница «Создание сетевого пользователя». Добавление доменного типа пользователя

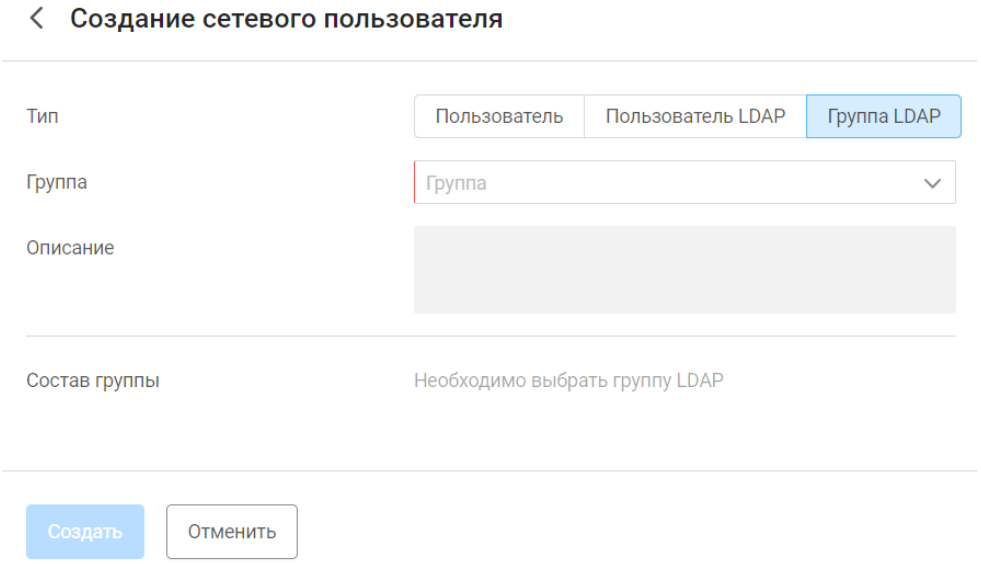



Рисунок 15 – Страница «Создание сетевого пользователя». Добавление доменной группы пользователей

Таблица 6 – Состав и описание полей страницы «Создание сетевого пользователя»

| Поле | Описание |
|---|---|
| Поле «Тип» | Переключатель:<br>— «Пользователь»;<br>— «Пользователь LDAP»;<br>— «Группа LDAP». |

| Поле | Описание |
|---|---|
| | От выбранного в поле значения зависит состав полей страницы создания сетевого пользователя |
| Поле «Статус» | Переключатель:<br>— «Активен» (  ) – сетевому пользователю разрешен доступ к устройствам;<br>— «Неактивен» (  ) – сетевому пользователю закрыт доступ к устройствам.<br><br>По умолчанию переключатель установлен в положение «Активен» |
| Поле «Период действия учетной записи» | Переключатель:<br>— «Бессрочно» – учетная запись сетевого пользователя действует на устройстве без ограничений;<br>— «Задать» – учетная запись сетевого пользователя действует на устройстве определенный период времени.<br><br>При выборе значения «Задать» появляется поле «Дата блокировки» для ввода даты блокировки учетной записи сетевого пользователя |
| Группа полей при выборе типа «Пользователь» | |
| Поле «Пользователь» | Текстовое поле для ввода уникального логина сетевого пользователя для доступа в сеть или на оборудование по настроенным политикам.<br>Параметры ввода текста: от 1 до 50 символов.<br>Допустимые символы: буквы латинского алфавита, цифры, «_», «–».<br>Поддерживается ввод специальных логинов $enable$ и $enab<n>$, где <n> – требуемый уровень доступа от 0 до 15 |
| Поле «Описание» | Текстовое поле для ввода описания сетевого пользователя.<br>Параметры ввода текста: от 1 до 250 любых символов |
| Поле «E-mail» | Текстовое поле для ввода почтового адреса сетевого пользователя для привязки к почте аккаунта |
| Поле «Пароль» | Текстовое поле для ввода пароля сетевого пользователя. Только для локальных сетевых пользователей.<br>Параметры для ввода текста настраиваются на вкладке «Настройки безопасности» (см. п. 3.3.3) |
| Поле «Привилегированный режим» | Поле с раскрывающимся списком типов привилегированного режима работы с АСО. Содержит значения:<br>— «Не задано» – привилегированный режим не задан;<br>— *«Установить пароль» – привилегированный режим доступен по заданному паролю для привилегированного доступа (см. ниже поле «Пароль»). Поле «Пароль» отображается при выборе значения «Установить пароль»; |

| Поле | Описание |
|---|---|
| | — «Использовать пароль пользователя» – привилегированный режим доступен по паролю пользователя от учетной записи пользователя;<br>— «Разрешить без пароля» – привилегированный режим доступен без пароля;<br>— «Запретить» – установка принудительного запрета на использование привилегированного режима пользователем.<br><br>*При выборе значения «Установить пароль» появляется поле «Привилегированный режим» для ввода пароля авторизации сетевого пользователя в привилегированном режиме |
| Поле «Группы пользователей» | По умолчанию поле содержит кнопку «Выбрать группы» для перехода на страницу выбора одной или нескольких групп. Для выбора группы необходимо установить флаг в соответствующей строке и нажать кнопку «Выбрать».<br><br>Локального пользователя можно добавить в группу после создания. Для этого необходимо перейти на вкладку «Группы» |
| Группа полей при выборе типа «Пользователь LDAP» | |
| Поле «Пользователь» | Поле заполняется путем выбора логина пользователя из списка пользователей LDAP |
| Поле «Описание» | Поле заполняется автоматически после выбора логина пользователя в поле «Пользователь» |
| Поле «Привилегированный режим» | Поле заполняется так же, как для типа «Пользователь» |
| Группа полей при выборе типа «Группа LDAP» | |
| Поле «Группа» | Раскрывающийся список групп LDAP. Необходимо начать вводить имя группы (минимум 2 символа), содержащейся в подключенном источнике данных LDAP. В результате поиска будет выведен список групп для выбора с указанием источников данных, в которых были найдены совпадения |
| Поле «Описание» | Поле заполняется автоматически после выбора группы в поле «Группа» |
| Поле «Состав группы» | Раскрывающийся список с пользователями в составе группы. Поле становится доступно только после выбора имени группы в поле «Группа» |
| Элементы управления | |
| Создать | При нажатии кнопки выполняется создание пользователя |
| Отменить | При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных |

### 3.3.2 Вкладка «Группы»

На странице вкладки «Группы» список групп сетевых пользователей реализован в виде таблицы (рис. 16).

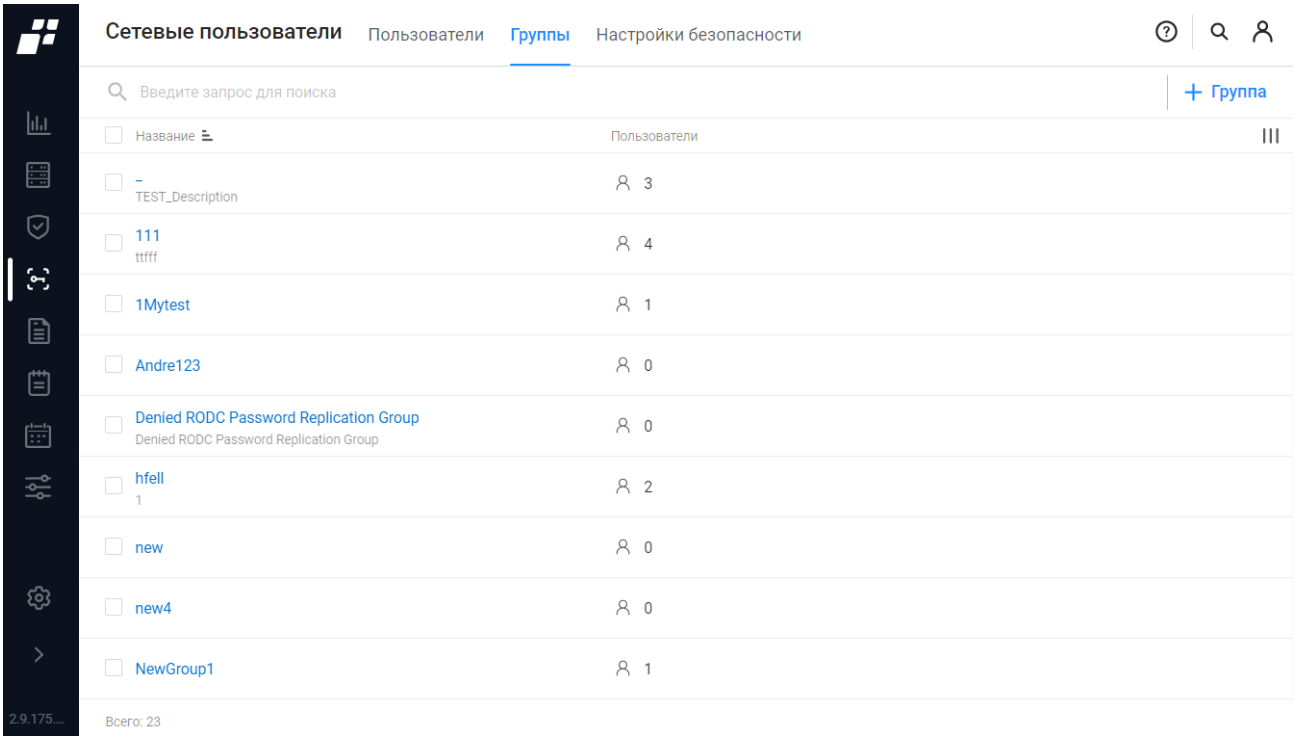



Рисунок 16 – Вкладка «Группы»

Для каждой записи списка отображаются следующие данные:

- поле для флага;
- название – является ссылкой, при переходе по которой открывается окно для редактирования данных группы;
- количество пользователей, входящих в группу.

Над списком групп сетевых пользователей располагаются:

- поле поиска ( Введите запрос для поиска );
- кнопка «Группа» ( + Группа );
- кнопка «Колонки» ( ).

При установке флага в строке с необходимой группой сетевых пользователей над списком групп появляются следующие кнопки:

- кнопка «Удалить» ( );
- кнопка «Создать копию» ( ).

Аналогичные кнопки появляются в правой части экрана в строке с выбранной группой.

### 3.3.2.1 Добавление группы сетевых пользователей

Для добавления группы сетевых пользователей пользователю ПК «Efros DO» необходимо:

1) Нажать кнопку «Группа» ( + Группа ).
2) Откроется страница «Создание группы сетевых пользователей», приведенная на рис. 17. Заполнить поля необходимыми параметрами. Состав и описание полей страницы приведены в таблице 7.

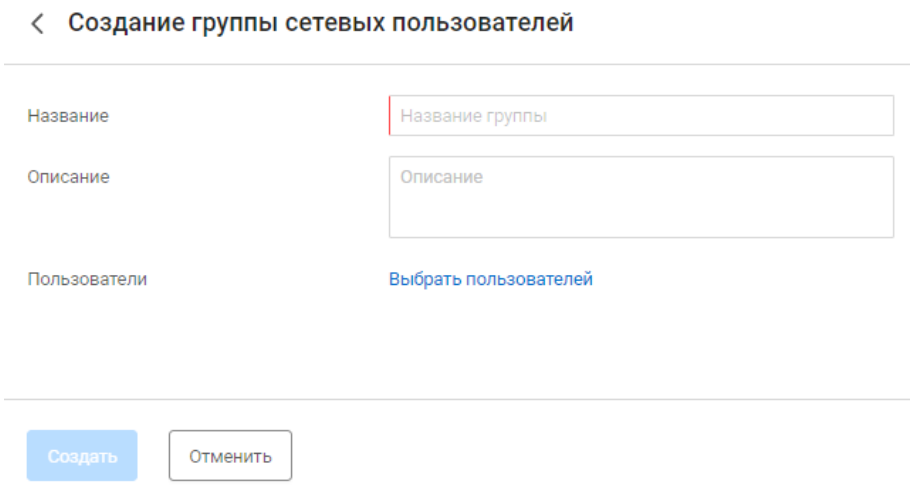



Рисунок 17 – Страница «Создание группы сетевых пользователей»

Таблица 7 – Состав и описание полей окна «Создание группы сетевых пользователей»

| Поле | Описание |
|---|---|
| Поле «Название» | Текстовое поле для ввода названия группы пользователей.<br>Параметры ввода текста: от 1 до 50 символов.<br>Допустимые символы: буквы латинского алфавита, цифры, «_», «–» |
| Поле «Описание» | Текстовое поле для ввода описания группы пользователей.<br>Параметры ввода текста: от 1 до 250 любых символов |
| Поле «Пользователи» | Поле содержит кнопку «Выбор пользователей» для перехода в окно выбора одного или нескольких сетевых пользователей. Для выбора сетевого пользователя необходимо установить флаг в соответствующей строке и нажать кнопку «Выбрать». |
| Элементы управления | |
| Создать | При нажатии кнопки выполняется создание устройства |
| Отменить | При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных |

### 3.3.3 Вкладка «Настройки безопасности»

Вкладка «Настройки безопасности» содержит список параметров парольной политики для сетевых пользователей (рис. 18). Состав и описание полей вкладки приведены таблице 8.

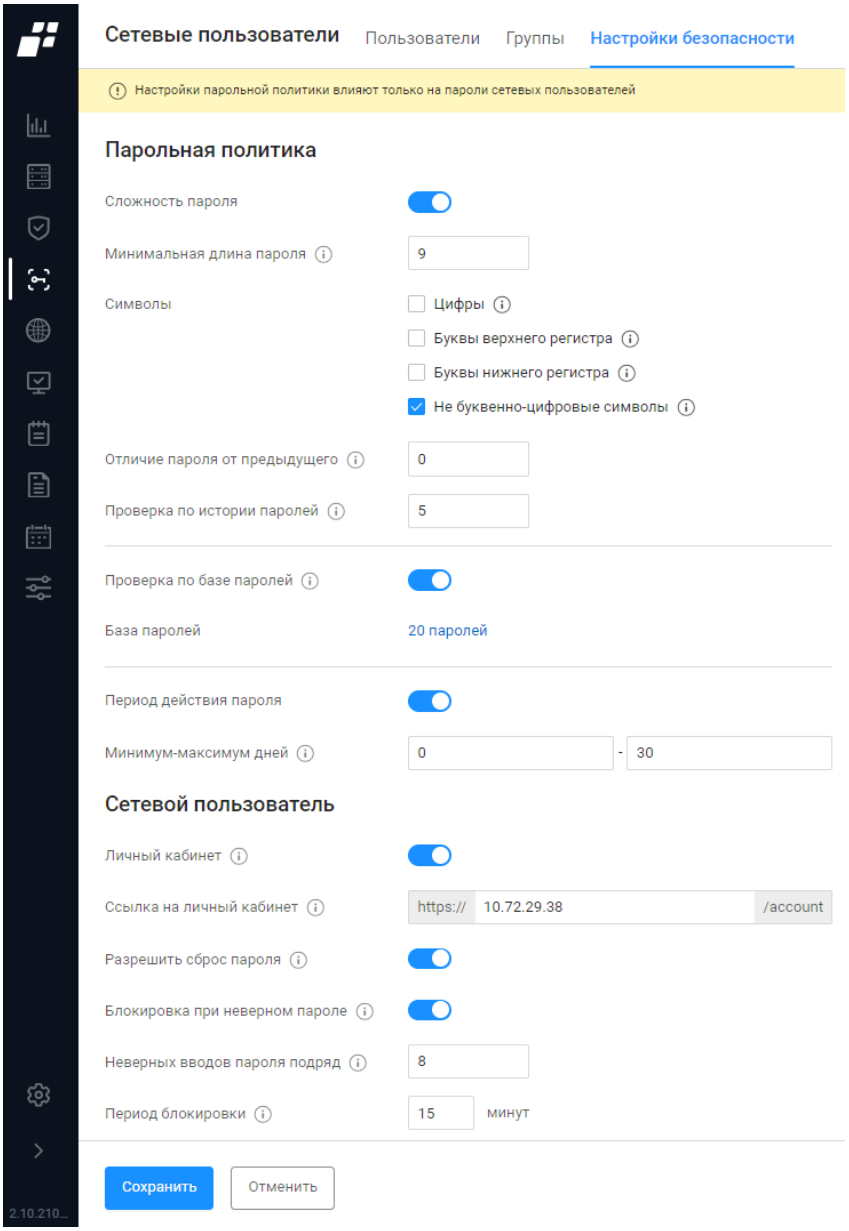



Рисунок 18 – Вкладка «Настройки безопасности»

Таблица 8 – Состав и описание полей вкладки «Настройки безопасности»

| Поле | Описание |
|---|---|
| Блок полей «Парольная политика» | |
| Поле «Сложность пароля» | Переключатель:<br>— «Активен» ( ) – применить настройки сложности для паролей сетевых пользователей; |

| Поле | Описание |
|---|---|
| | — «Неактивен» ( ) – настройки сложности для паролей сетевых пользователей не применяются.<br>При активации переключателя появляются дополнительные поля |
| Поле «Минимальная длина пароля» | Числовое поле для ввода минимального количества знаков, которые должны содержаться в пароле сетевого пользователя.<br>Допустимые значения: от 8 до 30.<br>Значение по умолчанию: 9 |
| Поле «Символы» | Поле для выбора обязательных символов, которые должны содержаться в пароле:<br>— «Цифры» – пароль должен содержать хотя бы одну цифру;<br>— «Буквы верхнего регистра» – пароль должен содержать хотя бы одну латинскую заглавную букву (от A до Z);<br>— «Буквы нижнего регистра» – пароль должен содержать хотя бы одну латинскую строчную букву (от a до z);<br>— «Не буквенно-цифровые символы» – пароль должен содержать хотя бы один не буквенно-цифровой символ: @!"#$%*&()+,-./:;<=>?[ ]\^_`{}\|~ |
| Поле «Отличие пароля от предыдущего» | Числовое поле для ввода количества знаков пароля, которые должны отличаться от предыдущего.<br>Допустимые значения: от 0 до 3.<br>Значение по умолчанию: 0 |
| Поле «Проверка по истории паролей» | Числовое поле для ввода количества новых уникальных паролей до повторного использования сохраненного ранее пароля.<br>Допустимые значения: от 1 до 10.<br>Значение по умолчанию: 5 |
| Поле «Проверка по базе паролей» | Переключатель:<br>— «Активен» ( ) – применить проверку по базе паролей;<br>— «Неактивен» ( ) – проверка по базе паролей не применяется.<br>При активации переключателя появляется дополнительное поле «База паролей» |
| Поле «База паролей» | Содержит ссылку. При переходе открывается окно «Изменение списка пароля». Пароль не должен содержать слова из заданного списка |
| Поле «Период действия пароля» | Переключатель:<br>— «Активен» ( ) – применить настройки параметров периода действия паролей;<br>— «Неактивен» ( ) – настройки параметров периода действия паролей не применяются.<br>При активации переключателя появляется дополнительное поле |

| Поле | Описание |
|---|---|
| | «Минимум-максимум дней» |
| Поле «Минимум-максимум дней» | Числовое поле для ввода следующих значений:<br>— «Минимум» – период времени (в днях), в течение которого пользователь не может изменять пароль. Чтобы разрешить изменять пароль сразу, установите первое значение 0. Допустимые значения: от 0 до 60;<br>— «Максимум» – период времени (в днях), в течение которого пароль будет действительным. Допустимые значения: от 1 до 90 |
| Блок полей «Сетевой пользователь» | |
| Поле «Личный кабинет» | Переключатель:<br>— «Активен» ( ) – включить отображение страницы входа в личный кабинет сетевого пользователя;<br>— «Неактивен» ( ) – страницу входа в личный кабинет сетевого пользователя не отображать.<br><br>При активации переключателя появляются дополнительные поля |
| Поле «Ссылка на личный кабинет» | Поле для ввода адреса страницы входа в личный кабинет и сброса пароля сетевого пользователя.<br>Допустимые значения: FQDN или IP-адрес сервера Defence Operations |
| Поле «Разрешить сброс пароля» | Переключатель:<br>— «Активен» ( ) – разрешить сброс забытого пароля на странице входа в личный кабинет;<br>— «Неактивен» ( ) – запретить сброс забытого пароля |
| Поле «Блокировка при неверном пароле» | Переключатель:<br>— «Активен» ( ) – включить временную блокировку входа в личный кабинет при превышении заданного количества неверных попыток ввода пароля;<br>— «Неактивен» ( ) – запретить временную блокировку входа |
| Поле «Неверных вводов пароля подряд» | Числовое поле для ввода количества неуспешных попыток ввода пароля.<br>Допустимые значения: от 3 до 8<br>После превышения указанного количества неуспешных попыток авторизации пользователь блокируется на время, указанное в параметре «Период блокировки» |
| Поле «Период блокировки» | Числовое поле для ввода интервала времени (в минутах), на который блокируется учетная запись пользователя после превышения разрешенного количества неуспешных попыток авторизации.<br>Допустимые значения: от 3 до 30 |

| Поле | Описание |
|---|---|
| Элементы управления | |
| Сохранить | При нажатии кнопки введенные изменения применяются |
| Отменить | При нажатии кнопки настройки остаются без применения изменений |

## 3.4 Наборы политик

ПК «Efros DO» позволяет задавать настройки для управления доступом в сеть / на оборудование на основе политик – списка наборов политик сетевого доступа и/или доступа на оборудование (рис. 19). Наборы политик позволяют логически группировать политики аутентификации и авторизации в одном наборе. Допустимо создавать несколько наборов политик на основе местоположения, типа доступа и других категорий. При создании наборов политик настраиваются правила для выбора служб доступа к сети на уровне набора атрибутов, источников идентификации на уровне политики аутентификации. Поддерживается определение условий, используя RADIUS-словари различных производителей (см. подраздел 3.11).

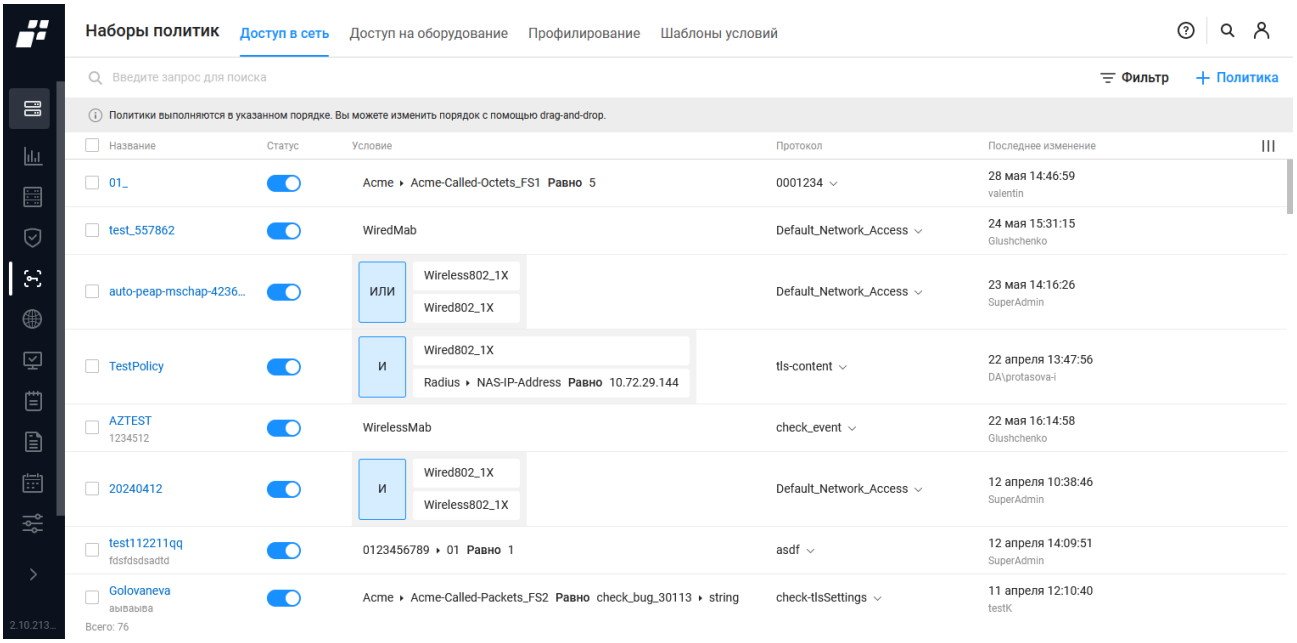



Рисунок 19 – Подраздел «Наборы политик», вкладка «Доступ в сеть»

Страница содержит вкладки:

- «Доступ в сеть»;
- «Доступ на оборудование»;
- «Профилирование»;
- «Шаблоны условий».

### 3.4.1 Вкладка «Доступ в сеть»

Вкладка «Доступ в сеть» содержит список политик, которыми управляет пользователь комплекса. Данный список позволяет контролировать доступ в сеть для сетевого пользователя.

На странице список политик реализован в виде таблицы (см. рис. 19). Для каждой записи списка отображаются следующие данные:

- поле для флага;
- название и описание;
- статус политики – переключатель режима «Активен» / «Неактивен»;
- условие – шаблон или набор условий, входящих в данную политику.

Над списком располагаются:

- поле поиска ( Введите запрос для поиска );
- кнопка «Политика» ( + Политика );
- кнопка «Фильтр» ( Фильтр );
- кнопка «Колонки» ( ).

При установке флага в строке с необходимым набором политики над списком появляются следующие кнопки:

- кнопка «Создать копию» ( );
- кнопка «Удалить» ( ).

Аналогичные кнопки появляются в правой части экрана в строке с выбранным набором политик.

После срабатывания условий, указанных в настройках набора политик, происходит проверка на соответствие условиям, указанным в правилах аутентификации (например, PAP, EAP–TLS, PEAP_EAP–TLS, TTLS_EAP–TLS, TTLS_EAP–MSCHAPv2 и т.п.), а также на наличие учетных данных субъекта, запрашивающего доступ к сети в выбранном источнике данных (локальные сетевые пользователи, пользователи подключенного LDAP, конечные точки, профили сертификатов и т.п.).

#### 3.4.1.1 Создание политик «Доступ в сеть»

Для добавления в список новой политики типа «Доступ в сеть» необходимо:

1) Нажать над списком политик доступа кнопку «Политика» ( + Политика ).
2) Откроется страница «Создание политики (Доступ в сеть)», приведенная на рис. 20. Состав и описание полей страницы приведены в таблице 9.

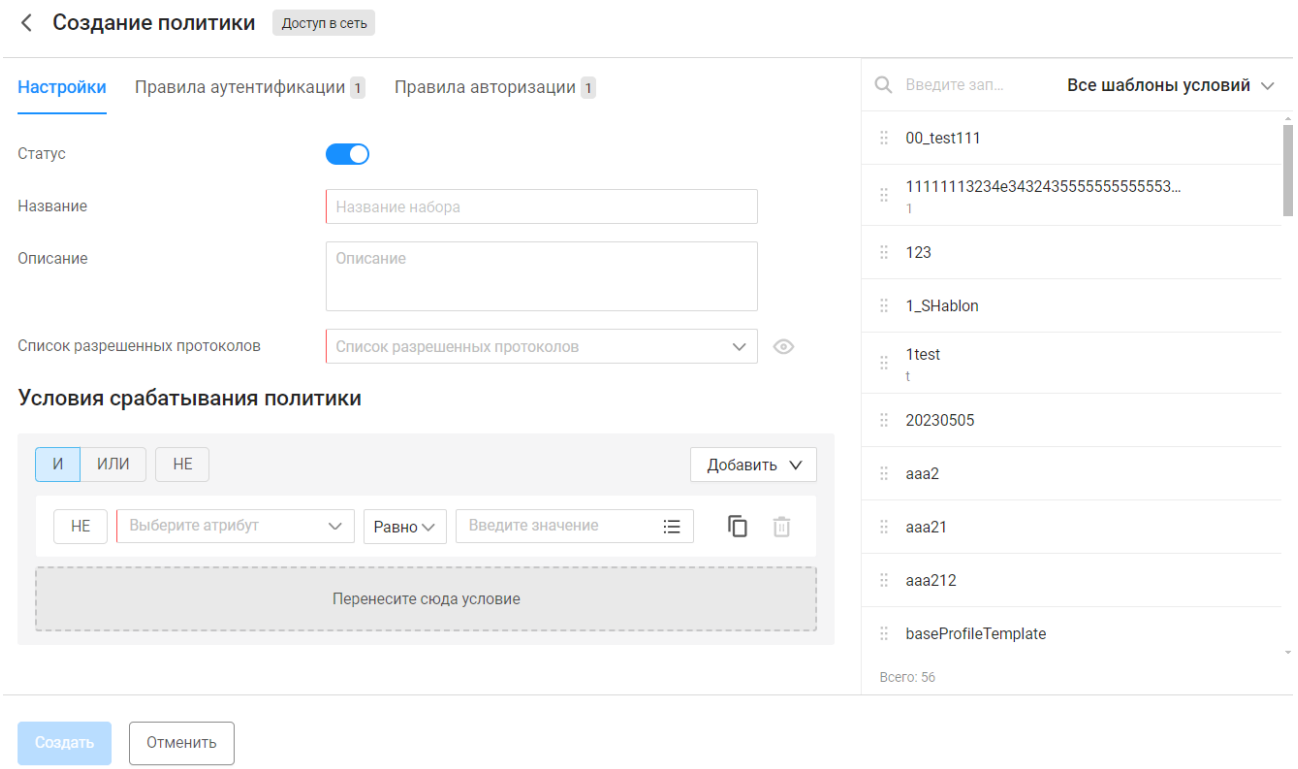



Рисунок 20 – Страница «Создание политики (Доступ в сеть)»

Таблица 9 – Состав и описание полей страницы «Создание политики (Доступ в сеть)»

| Поле | Описание |
|---|---|
| Поле «Статус» | Переключатель:<br>— «Активен»;<br>— «Неактивен» |
| Поле «Название» | Текстовое поле для ввода названия политики.<br>Параметры ввода текста: от 1 до 50 символов.<br>Допустимые символы: буквы латинского алфавита, цифры, «_», «–» |
| Поле «Описание» | Текстовое поле для ввода описания политики.<br>Параметры ввода текста: от 1 до 250 любых символов |
| Поле «Список разрешенных протоколов» | Раскрывающийся список существующих списков разрешенных протоколов<br>Предварительно необходимо создать созданных список разрешенных протоколов (см. подраздел 3.9) |
| Условия срабатывания политики | |
| Формирование основного правила условия срабатывания политики происходит на основе созданных правил аутентификации и авторизации на вкладках «Правила аутентификации» и «Правила авторизации» или стандартных шаблонов условий. | |

| Поле | Описание |
|---|---|
| Для использования стандартных или ранее сформированных шаблонов условий необходимо перенести шаблон из перечня шаблонов в поле «Перенесите сюда условие» | |
| Элементы управления | |
| Создать | При нажатии на кнопку окно создания политики закрывается, политика отображается в списке |
| Отменить | При нажатии на кнопку окно закрывается без сохранения данных |

3) Заполнить поля страницы соответствующими данными добавляемой политики.
4) Сформировать основное правило или воспользоваться заранее сформированными шаблонами условий.
5) Перейти на вкладку «Правила аутентификации» для определения правил аутентификации в рамках данного набора политик (рис. 21). По умолчанию вкладка содержит одно предустановленное в комплексе правило аутентификации «Default», правило по умолчанию включено и не доступно для смены статуса. Добавление нового правила аутентификации описано в п.п. 3.4.1.2.

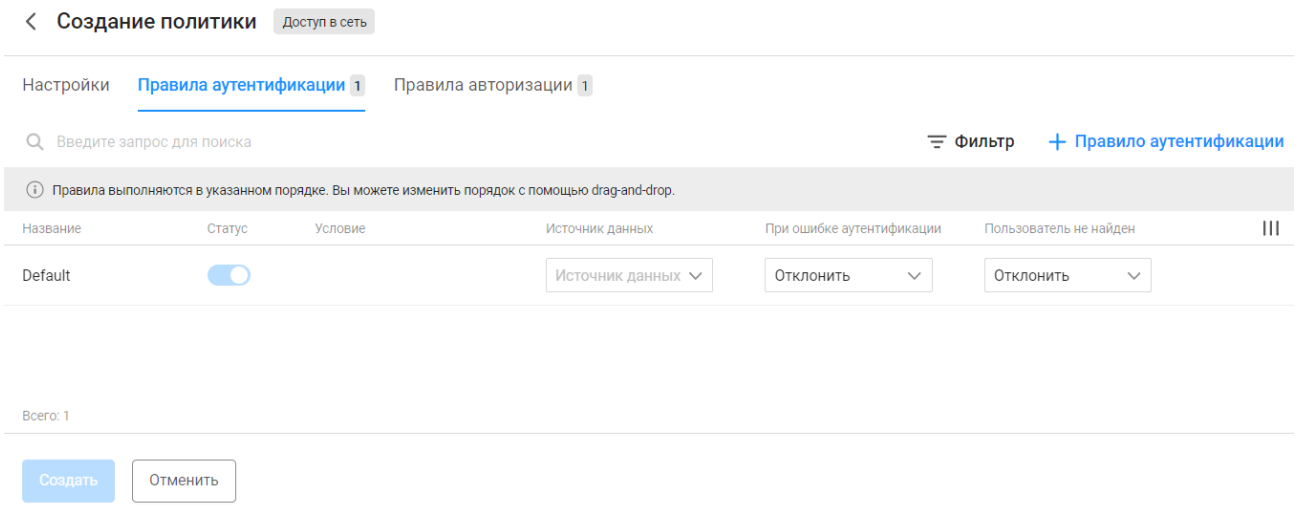



Рисунок 21 – Вкладка «Правила аутентификации»

6) Перейти на вкладку «Правила авторизации» для определения правил авторизации в рамках данного набора политик (рис. 22). По умолчанию вкладка содержит одно предустановленное в комплексе правило авторизации «Default», правило по умолчанию включено и не доступно для смены статуса. Добавление нового правила авторизации описано в п.п. 3.4.1.3.

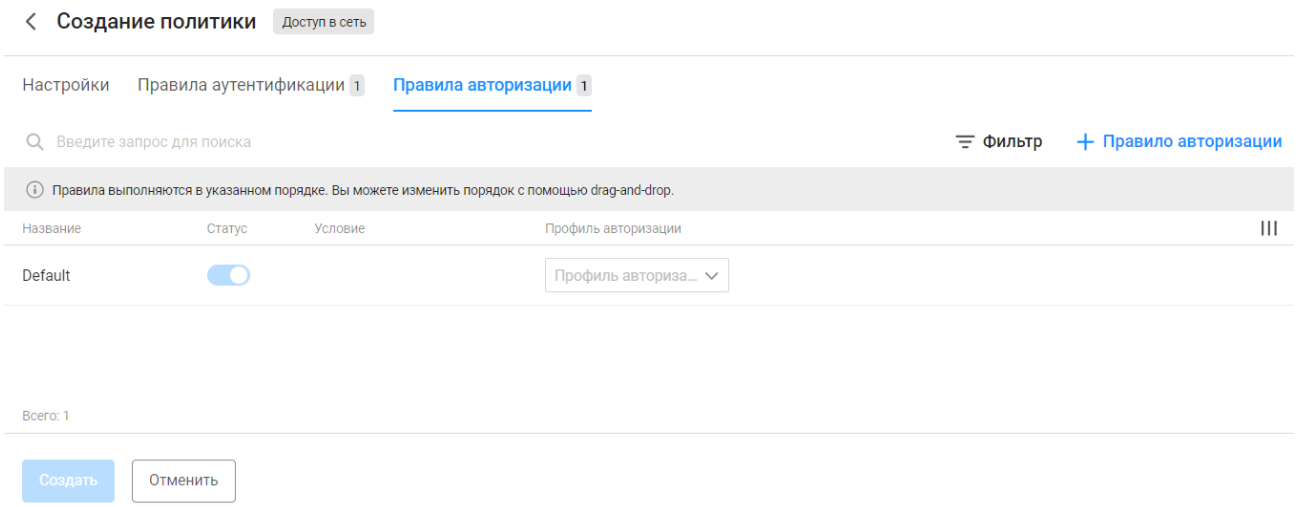



Рисунок 22 – Вкладка «Правила авторизации»

7) Настроить требуемые правила аутентификации и авторизации.

### 3.4.1.2 Добавление нового правила аутентификации

Аутентификация – процедура проверки подлинности субъекта по его идентификационным данным, например, проверка пользователя по логину и паролю, сертификату и т.п.

Каждый набор политик может содержать несколько правил аутентификации, при этом каждое правило настраивается отдельно друг от друга. Созданные правила аутентификации срабатывают последовательно, начиная с расположенных вверху списка до первого совпадения с указанными в них условиями, далее происходит проверка на наличие учетных данных субъекта, запрашивающего доступ к сети, в выбранном источнике данных (локальные сетевые пользователи, пользователи подключенного LDAP, конечные точки, профили сертификатов и т.п.).

После установки комплекса доступно к использованию предустановленное правило аутентификации «Default». По умолчанию правило активировано. Для данного правила рекомендуется использовать следующие значения:

- «Источник данных» – «DenyAccess»;
- «При ошибке аутентификации» – «Отклонить»;
- «Пользователь не найден» – «Отклонить».

Данное правило запрещает доступ в сеть устройству (пользователю) в случае, если ни одно из указанных выше правил аутентификации не пройдено успешно.

Для добавления в список нового правила аутентификации пользователю

ПК «Efros DO» необходимо выполнить следующее:

1) Перейти на вкладку «Правила аутентификации» страницы «Создание политики (Доступ в сеть)».
2) Нажать над списком правил аутентификации кнопку «Правило аутентификации» ( + Правило аутентификации ).
3) Откроется страница добавления правила, приведенная на рис. 23. Состав и описание полей страницы приведены в таблице 10.

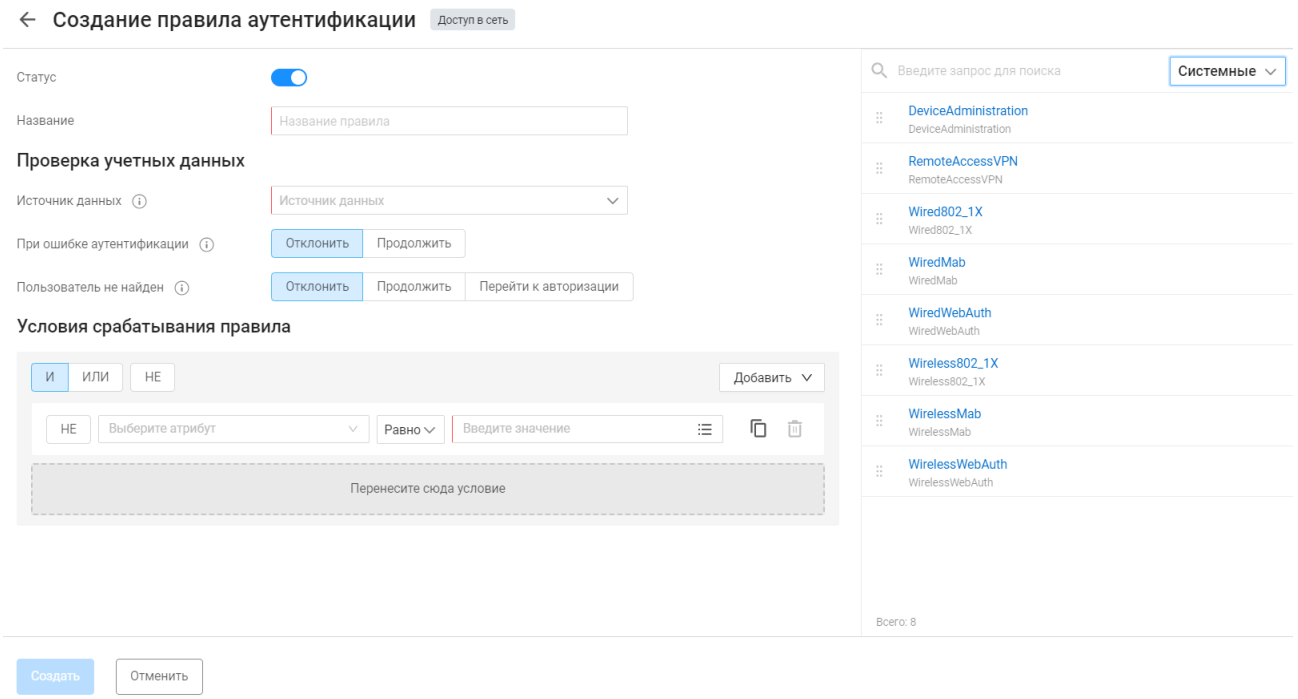



Рисунок 23 – Страница «Создание правила аутентификации (Доступ в сеть)»

Таблица 10 – Состав и описание полей страницы «Создание правила аутентификации (Доступ в сеть)»

| Поле | Описание |
|---|---|
| Поле «Статус» | Переключатель: «Активен», «Неактивен» (статус может быть изменен как в окне редактирования параметров, так и непосредственно на вкладке «Правила аутентификации» у созданного правила).<br><br>В случае выбора статуса «Неактивен», проверка на совпадение с условиями, заданными в данном правиле, осуществляться не будет |
| Поле «Название» | Текстовое поле для ввода названия правила аутентификации.<br>Параметры ввода текста: от 1 до 50 символов.<br>Допустимые символы: буквы латинского алфавита, цифры, |

| Поле | Описание |
|---|---|
| | «_», «–» |
| Группа полей «Проверка учетных данных» | |
| Поле «Источник данных» | Поле со списком источников данных для аутентификации |
| Поле «При ошибке аутентификации» | Выполняемое при ошибке аутентификации действие: отклонить запрос устройства на аутентификацию или продолжить процесс аутентификации |
| Поле «Пользователь не найден» | Переключатель:<br>— «Отклонить»;<br>— «Продолжить»;<br>— «Перейти к авторизации» |
| Условие срабатывания правила | |
| Формирование основного правила происходит на основе выбранного шаблона условий или созданного вручную правила. Для использования стандартных или ранее сформированных шаблонов условий необходимо перенести шаблон из перечня шаблонов в поле «Перенесите сюда условие» | |
| Элементы управления | |
| Создать | При нажатии кнопки создается правило аутентификации |
| Отменить | При нажатии кнопки страница закрывается без сохранения внесенных данных |

4) Заполнить поле страницы соответствующими значениями.
5) Сформировать условия, определяющие правило аутентификации, или воспользоваться заранее сформированными шаблонами условий.
6) После настройки правила аутентификации нажать в окне добавления кнопку «Создать».

### 3.4.1.3 Добавление нового правила авторизации

Авторизация — процедура проверки прав на выполнение определенных действий, а также процесс проверки данных прав при попытке выполнения этих действий. Права задаются при создании профиля авторизации.

Каждый набор политик может содержать несколько правил авторизации, при этом каждое правило настраивается отдельно друг от друга. Созданные правила авторизации срабатывают последовательно, начиная с расположенных вверху списка до первого совпадения с указанными в них условиями, далее происходит проверка по профилю авторизации, назначенному устройству или пользователю.

После установки комплекса доступно к использованию предустановленное правило авторизации «Default». По умолчанию правило активировано. Для данного правила необходимо выбрать заранее созданный профиль авторизации.

Данное правило запрещает доступ в сеть устройству (пользователю) в случае, если ни одно из указанных выше правил авторизации не пройдено успешно.

Для добавления в список нового правила авторизации пользователю необходимо выполнить следующее:

1) Перейти на вкладку «Правила авторизации» страницы «Создание политики (Доступ в сеть)».
2) Нажать кнопку «Правило авторизации» ( + Правило авторизации ).
3) Откроется страница «Создание правила авторизации (Доступ в сеть)», приведенное на рис. 24. Состав и описание полей страницы приведены в таблице 11.

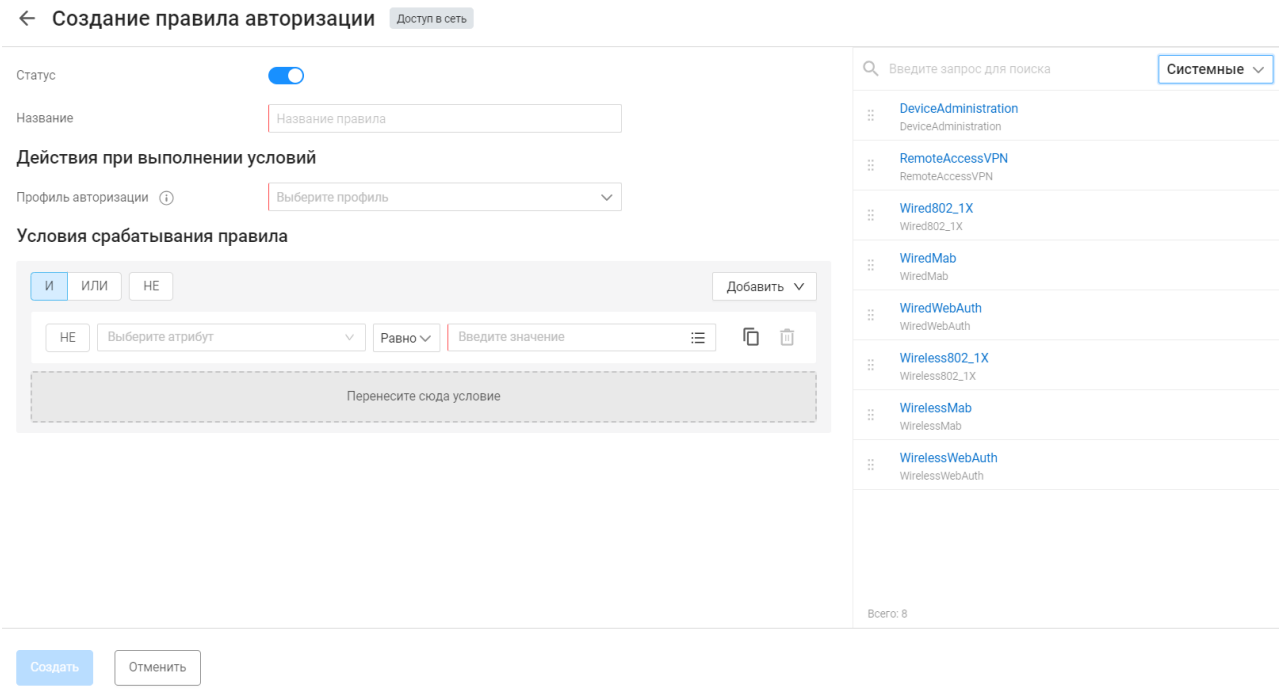



Рисунок 24 – Страница «Создание правила авторизации (Доступ в сеть)»

Таблица 11 – Состав и описание страницы «Создание правила авторизации (Доступ в сеть)»

| Поле | Описание |
|---|---|
| Поле «Статус» | Переключатель: «Активен», «Неактивен» (статус может быть изменен как в окне редактирования параметров, так и непосредственно на вкладке «Правила авторизации» у созданного правила) |
| Поле «Название» | Текстовое поле для ввода названия правила авторизации. |

| Поле | Описание |
|---|---|
| | Параметры ввода текста: от 1 до 50 символов.<br>Допустимые символы: буквы латинского алфавита, цифры, «_», «–» |
| Группа поле «Действия при выполнении условий» | |
| Поле «Профиль авторизации» | Раскрывающийся список существующих профилей авторизации<br><br>Предварительно необходимо создать профиль авторизации (см. подраздел 3.6) |
| Условие срабатывания правила | |
| Формирование основного правила происходит на основе выбранного шаблона условий или созданного вручную правила. Для использования стандартных или ранее сформированных шаблонов условий необходимо перенести шаблон из перечня шаблонов в поле «Перенесите сюда условие» | |
| Элементы управления | |
| Создать | При нажатии кнопки открывается список правил авторизации страницы создания/редактирования набора политик |
| Отменить | При нажатии кнопки выполняется переход на страницу создания/редактирования списка набора политик, вкладка Правила авторизации без сохранения внесенных данных |

4) Заполнить поле страницы соответствующими значениями.
5) Сформировать условия, определяющие правило авторизации, или воспользоваться заранее сформированными шаблонами условий.
6) После настройки правила аутентификации нажать в окне добавления кнопку «Создать».

### 3.4.2 Вкладка «Доступ на оборудование»

Вкладка «Доступ на оборудование» содержит список наборов политик, которыми управляет пользователь комплекса для контроля аутентификации и авторизации сетевого пользователя на устройстве по протоколу TACACS+.

На странице список политик реализован в виде таблицы (рис. 25). Для каждой записи списка отображаются следующие данные:

- поле для флага;
- название и описание;
- статус политики (активен/неактивен);
- условие – шаблон или набор шаблонов условий, входящих в данную политику;
- разрешенные протоколы;
- срабатывание – количество срабатываний политики.

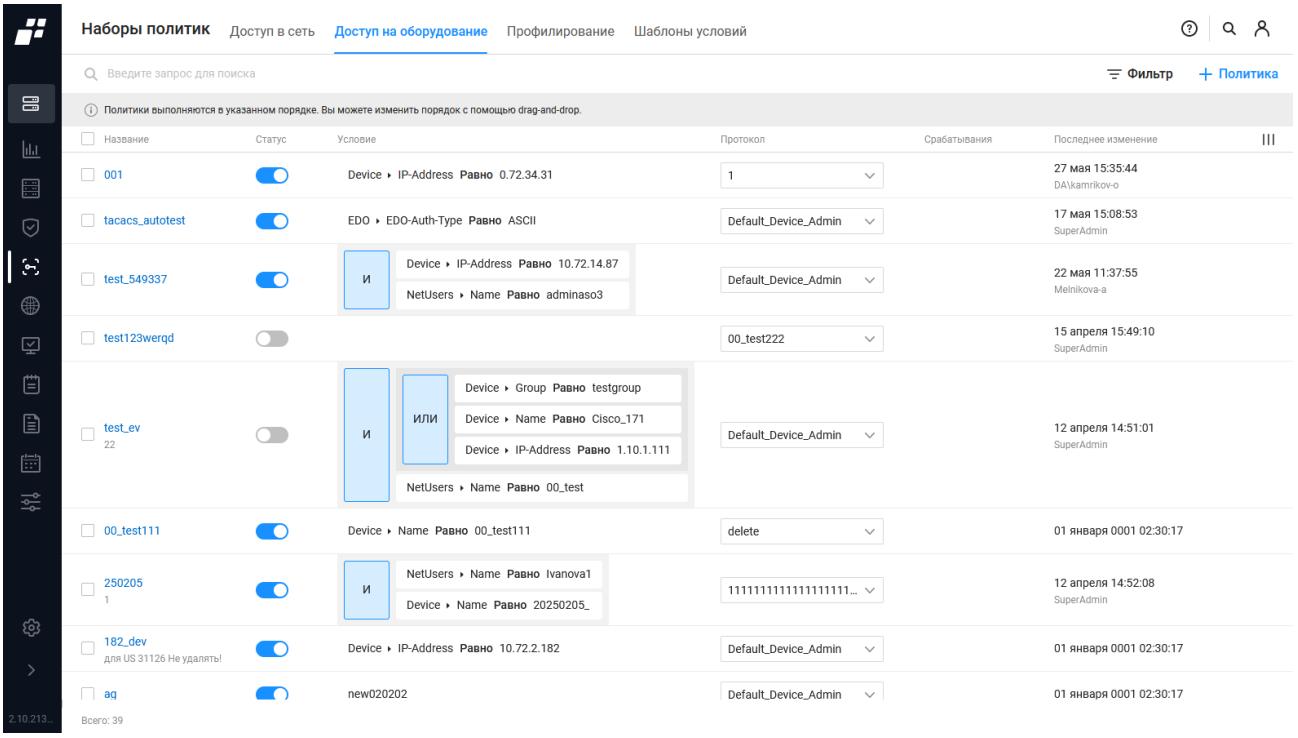



Рисунок 25 – Вкладка «Доступ на оборудование»

Над списком располагаются:

— поле поиска ( Введите запрос для поиска );
— кнопка «Политики» ( + Политика );
— кнопка «Фильтр» ( Фильтр );
— кнопка «Колонки» ( ).

При установке флага в строке с необходимым набором политики над списком появляются следующие кнопки:

— кнопка «Сбросить срабатывания» ( Сбросить срабатывания );
— кнопка «Создать копию» ( );
— кнопка «Удалить» ( ).

Аналогичные кнопки появляются в правой части экрана в строке с выбранным набором политик.

После срабатывания условий, указанных в настройках набора политик, происходит проверка на соответствие условиям, указанным в правилах аутентификации, проверка разрешенных протоколов, а также проверка на наличие учетных данных субъекта, запрашивающего доступ к сети, в выбранном

источнике данных (локальные сетевые пользователи, пользователи подключенного LDAP и т.п.).

### 3.4.2.1 Создание политик «Доступ на оборудование»

Для добавления в список новой политики типа «Доступ на оборудование» необходимо:

1) Нажать над списком политик доступа кнопку «Политика» ( + Политика ).
2) Откроется страница «Создание политики (Доступ на оборудование)», приведенная на рис. 26. Состав и описание полей вкладки приведены в таблице 12.

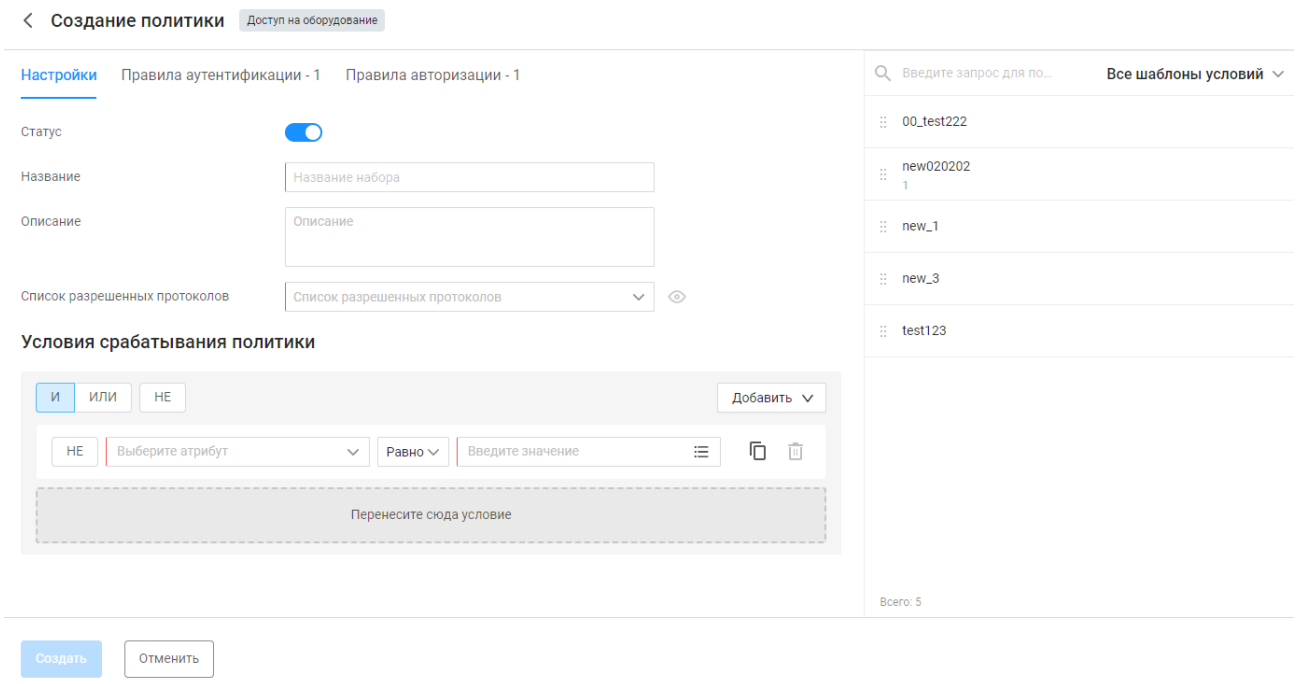



Рисунок 26 – Страница «Создание политики (Доступ на оборудование)»

Таблица 12 – Состав и описание полей страницы «Создание политики (Доступ на оборудование)»

| Поле | Описание |
|---|---|
| Поле «Статус» | Переключатель:<br>— «Активен»;<br>— «Неактивен» |
| Поле «Название» | Текстовое поле для ввода названия политики.<br>Параметры ввода текста: от 1 до 50 символов.<br>Допустимые символы: буквы латинского алфавита, цифры, «_», «–» |
| Поле «Описание» | Текстовое поле для ввода описания политики.<br>Параметры ввода текста: от 1 до 250 любых символов |
| Поле «Список | Раскрывающийся список протоколов, которые будут |

| Поле | Описание |
|---|---|
| разрешенных протоколов» | использоваться во время проверки аутентификации (см. подраздел 3.9) |
| Условия срабатывания политики | |
| Формирование основного правила происходит на основе созданных правил аутентификации и авторизации на вкладках «Правила аутентификации» и «Правила авторизации» или стандартных шаблонов условий.<br>Для использования стандартных или ранее сформированных шаблонов условий необходимо перенести шаблон из перечня шаблонов в поле «Перенесите сюда шаблон» | |
| Элементы управления | |
| Создать | При нажатии кнопки создается политика доступа |
| Отменить | При нажатии кнопки страница закрывается без сохранения внесенных данных |

3) Заполнить поля страницы соответствующими данными добавляемой политики.
4) Сформировать основное правило или воспользоваться заранее сформированными шаблонами условий.
5) Перейти на вкладку «Правила аутентификации» для определения правил аутентификации в рамках данного набора политик (рис. 27). По умолчанию вкладка содержит одно предустановленное в комплексе правило аутентификации «Default», правило по умолчанию включено и не доступно для выключения (кнопка в графе «Статус» неактивна). Добавление нового правила аутентификации описано в п.п. 3.4.2.2.

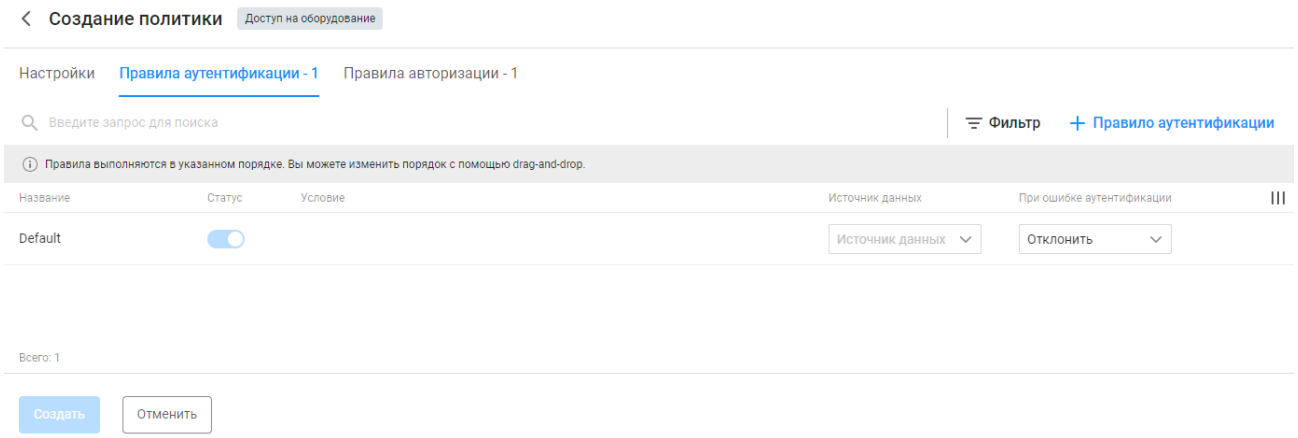



Рисунок 27 – Вкладка «Правила аутентификации»

6) Перейти на вкладку «Правила авторизации» для определения правил авторизации в рамках данного набора политик (рис. 28). По умолчанию вкладка содержит одно предустановленное в комплексе правило авторизации

«Default», правило по умолчанию включено и не доступно для выключения (кнопка в графе «Статус» неактивна). Добавление нового правила авторизации описано в п.п. 3.4.2.3.

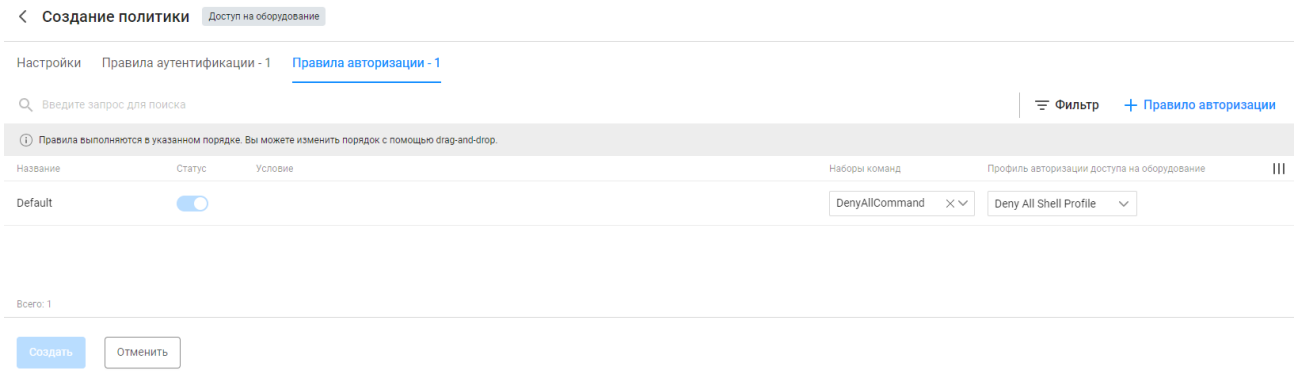



Рисунок 28 – Вкладка «Правила авторизации»

7) После настройки правил аутентификации и авторизации нажать в окне добавления набора политик кнопку «Создать».

### 3.4.2.2 Добавление нового правила аутентификации

После установки комплекса доступно к использованию предустановленное правило аутентификации «Default». По умолчанию правило активировано. Для данного правила рекомендуется использовать следующие значения:

— «Источник данных: DenyAccess»;
— «При ошибке аутентификации: Отклонить».

Для добавления в список нового правила аутентификации пользователю ПК «Efros DO» необходимо выполнить следующее:

1) Перейти на вкладку «Правила аутентификации» страницы «Создание политики (Доступ на оборудование)».
2) Нажать над списком правил аутентификации кнопку «Правило аутентификации» ( + Правило аутентификации ).
3) Откроется страница добавления правила, приведенное на рис. 29. Состав и описание полей страницы приведены в таблице 13.
4) Заполнить поле страницы соответствующими значениями.
5) Сформировать условия, определяющие правило аутентификации, или воспользоваться заранее сформированными шаблонами условий.
6) После настройки правила аутентификации нажать в окне добавления кнопку «Создать».

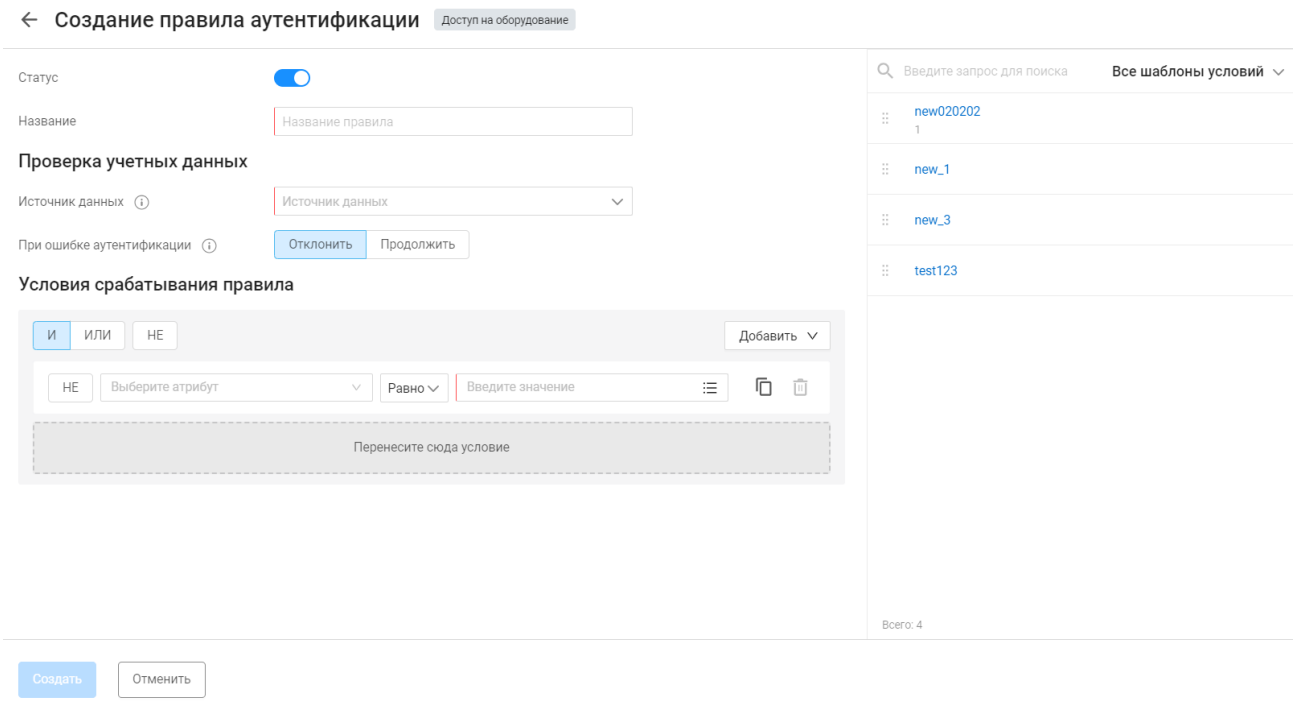



Рисунок 29 – Страница «Создание правила аутентификации (Доступ на оборудование)»

Таблица 13 – Состав и описание полей страницы «Создание правила аутентификации (Доступ на оборудование)»

| Поле | Описание |
|---|---|
| Поле «Статус» | Переключатель: «Активен», «Неактивен» (статус может быть изменен как в окне редактирования параметров, так и непосредственно на вкладке «Правила аутентификации» у созданного правила).<br><br>В случае выбора статуса «Неактивен», проверка на совпадение с условиями, заданными в данном правиле, осуществляться не будет |
| Поле «Название» | Текстовое поле для ввода названия политики.<br>Параметры ввода текста: от 1 до 50 символов.<br>Допустимые символы: буквы латинского алфавита, цифры, «_», «–» |
| Группа полей «Проверка учетных данных» | |
| Поле «Источник данных» | Поле со списком источников данных для аутентификации |
| Поле «При ошибке аутентификации» | Выполняемое при ошибке аутентификации действие – отклонить запрос устройства на аутентификацию или продолжить процесс аутентификации |

| Поле | Описание |
|---|---|
| Условия срабатывания правила | |
| Формирование основного правила происходит на основе выбранного шаблона условий или созданного вручную правила.<br>Для использования стандартных или ранее сформированных шаблонов условий необходимо перенести шаблон из перечня шаблонов в поле «Перенесите сюда условие» | |
| Элементы управления | |
| Создать | При нажатии кнопки создается правило аутентификации |
| Отменить | При нажатии кнопки страница закрывается без сохранения внесенных данных |

### 3.4.2.3 Добавление нового правила авторизации

После установки комплекса доступно к использованию предустановленное правило авторизации «Default». По умолчанию правило активировано. Для данного правила необходимо выбрать заранее созданный профиль авторизации и набор команд.

Данное правило запрещает доступ на оборудование в случае, если ни одно из указанных выше правил авторизации не пройдено успешно.

Для добавления в список нового правила авторизации пользователю необходимо выполнить следующее:

1) Перейти на вкладку «Правила авторизации» страницы «Создание политики (Доступ на оборудование)».
2) Нажать кнопку «Правило авторизации» ( + Правило авторизации ).
3) Откроется страница «Создание правила авторизации (Доступ на оборудование)», приведенное на рис. 30. Состав и описание полей страницы приведены в таблице 14.
4) Заполнить поле страницы соответствующими значениями.
5) Сформировать условия, определяющие правило авторизации, или воспользоваться заранее сформированными шаблонами условий.
6) После настройки правила авторизации нажать в окне добавления кнопку «Создать».

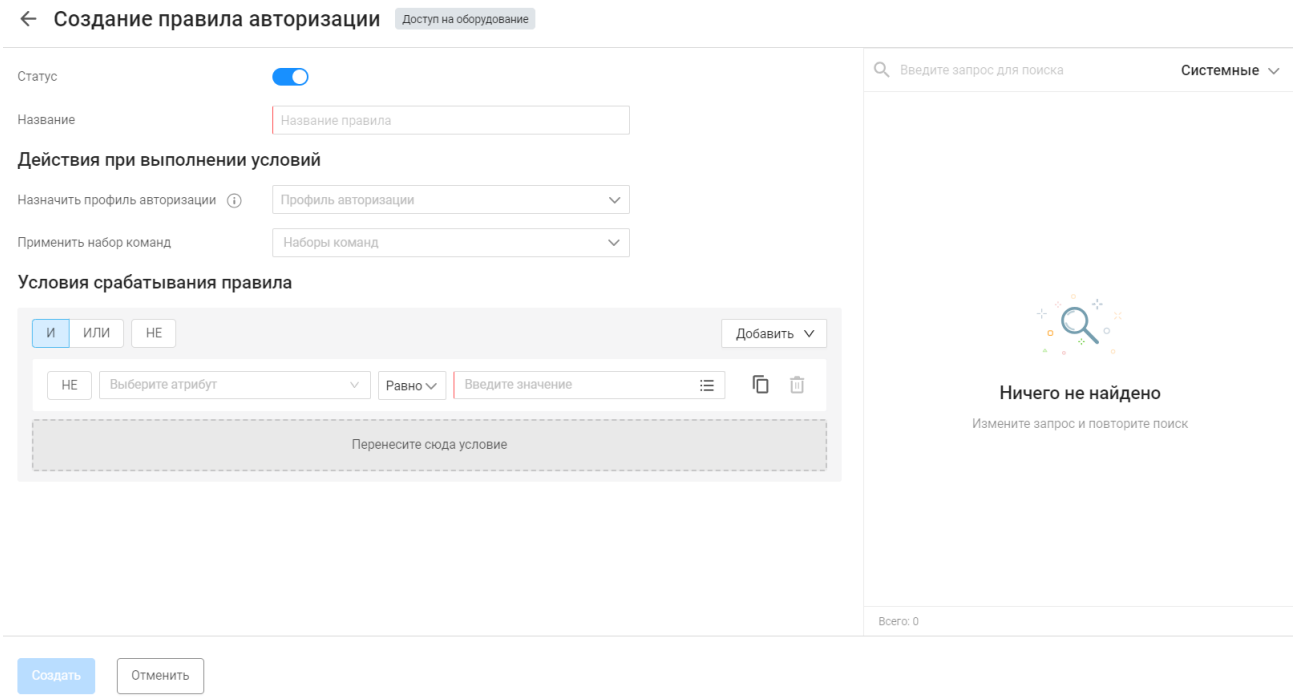



Рисунок 30 – Страница «Создание правила авторизации (Доступ на оборудование)»

Таблица 14 – Состав и описание полей страницы «Создание политики (Доступ на оборудование)»

| Поле | Описание |
|---|---|
| Поле «Статус» | Переключатель: «Активен», «Неактивен» (статус может быть изменен как в окне редактирования параметров, так и непосредственно на вкладке «Правила авторизации» у созданного правила).<br><br>В случае выбора статуса «Неактивен», проверка на совпадение с условиями, заданными в данном правиле, осуществляться не будет |
| Поле «Название» | Текстовое поле для ввода названия политики.<br>Параметры ввода текста: от 1 до 50 символов.<br>Допустимые символы: буквы латинского алфавита, цифры, «_», «–» |
| Группа полей «Действия при выполнении условий» | |
| Поле «Назначить профиль авторизации» | Раскрывающийся список существующих профилей авторизации<br><br>Предварительно необходимо создать профиль авторизации (см. подраздел 3.6) |
| Поле «Применить | Раскрывающийся список существующих наборов команд |

| Поле | Описание |
|---|---|
| набор команд» | Предварительно необходимо создать набор команд (см. подраздел 3.8) |
| Условия срабатывания политики | |
| Формирование основного правила происходит на основе выбранного шаблона условий или созданного вручную правила. Для использования стандартных или ранее сформированных шаблонов условий необходимо перенести шаблон из перечня шаблонов в поле «Перенесите сюда условие» | |
| Создать | При нажатии кнопки открывается список правил авторизации страницы создания/редактирования набора политик |
| Отменить | При нажатии кнопки выполняется переход на вкладку «Правила авторизации» без сохранения внесенных данных |

### 3.4.3 Вкладка «Профилирование»

Профилирование устройств (конечных точек) позволяет собрать информацию о производителе, типе устройства, используемом браузере и операционной системе (ОС) путем проверки атрибутов, отправляемых этими устройствами в сети. Например, можно определить, что устройство является принтером, сетевым оборудованием или IP-телефоном.

В результате профилирования конечным точкам может быть присвоен профиль (один или несколько) или метки, которые можно использовать при настройке политик доступа в сеть (более подробно о наборе политик доступа по источнику профилирования написано в приложении Б).

В ПК «Efros DO» поддерживаются следующие источники профилирования:

- CDP;
- DHCP;
- Edo-Agent;
- LLDP;
- RADIUS;
- SNMP;
- UserAgent.

Значения, полученные от источника, отображаются разделе «Объекты сети» → «Конечные точки». При нажатии на MAC-адрес конечной точки открывается страница с описанием конечной точки. На вкладке «Дополнительные атрибуты» отображаются полученные значения по источникам профилирования.

При получении или обновлении параметров от источников профилирования конечной точки, осуществляется проверка на соответствие данных условиям политик, заданным

в политиках профилирования. В случае совпадения с условиями одной или нескольких политик – конечной точке назначается один или несколько профилей, которые соответствуют названию сработавших активных политик.

Если в политике профилирования задана метка, то она автоматически будет добавлена к конечной точке при срабатывании политики. Если была изменена сама политика профилирования, то происходит автоматическая проверка всех конечных точек на соответствие новым условиям согласно заданным атрибутам.

На странице вкладки «Профилирование» список политик профилирования реализован в виде таблицы (рис. 31).

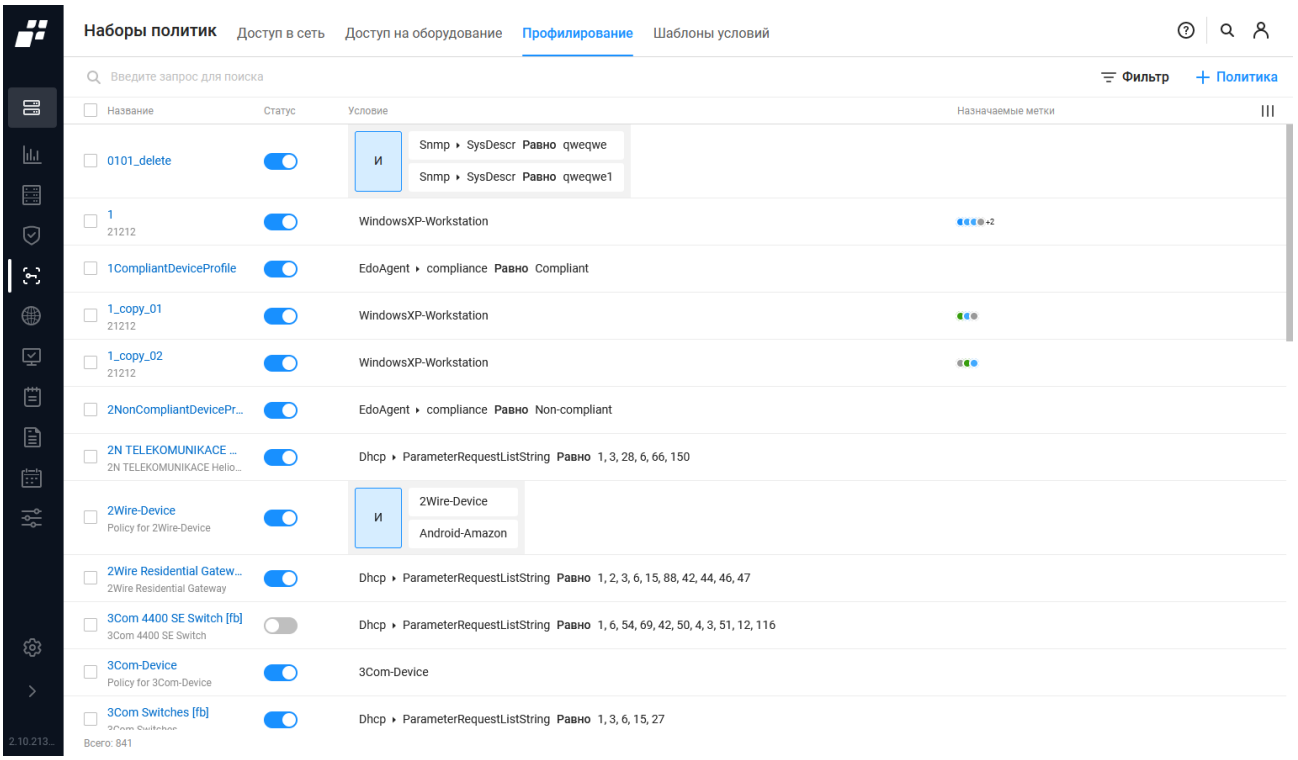



Рисунок 31 – Страница вкладки «Профилирование»

Для каждой записи списка отображаются следующие данные:

- поле для флага;
- название политики профилирования;
- статус (активен/неактивен). Если переключатель в положении «Неактивен», то проверка атрибутов конечных точек не осуществляется и профиль не назначается;
- условие, входящее в политику профилирования;
- назначаемые метки.

Над списком располагаются:

- поле поиска ( Введите запрос для поиска );
- кнопка «Политика профилирования» ( + Политика профилирования );

— кнопка «Фильтр» ( Фильтр );
— кнопка «Колонки» ( ).

При установке флага в строке с необходимым профилем над списком появляются следующие кнопки:

— кнопка «Создать копию» ( Создать копию );
— кнопка «Удалить» ( Удалить ).

Аналогичные кнопки появляются в правой части экрана в строке с выбранной политикой.

### 3.4.3.1 Создание новой политики профилирования

Для добавления в список новой политики профилирования необходимо:

1) Нажать на странице кнопку «Политика профилирования» ( + Политика профилирования ).
2) Откроется страница «Создание политики профилирования», приведенная на рис. 32. Состав и описание полей вкладки приведены в таблице 15.

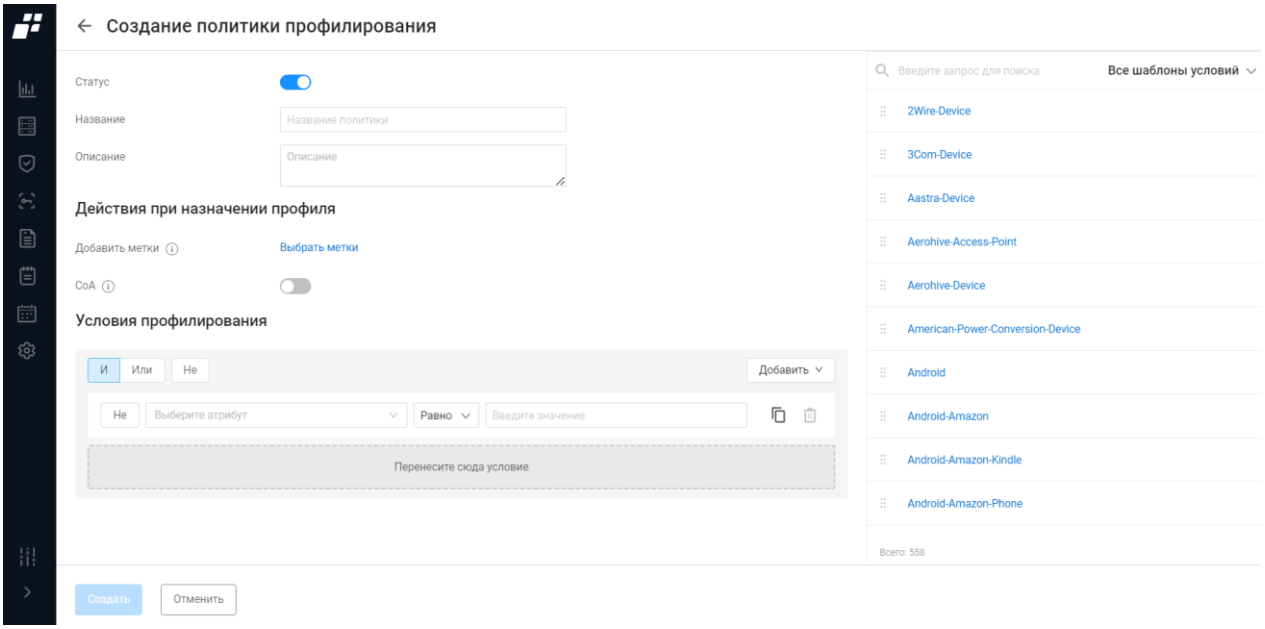



Рисунок 32 – Страница «Создание политики профилирования»

Таблица 15 – Состав и описание полей страницы «Создание политики профилирования»

| Поле | Описание |
|---|---|
| Поле «Статус» | Переключатель:<br>— «Активен»;<br>— «Неактивен» |

| Поле | Описание |
|---|---|
| Поле «Название» | Текстовое поле для ввода названия политики.<br>Параметры ввода текста: от 1 до 50 символов.<br>Допустимые символы: буквы латинского алфавита, цифры, «_», «–» |
| Поле «Описание» | Текстовое поле для ввода описания политики.<br>Параметры ввода текста: от 1 до 250 любых символов |
| Группа полей «Действия при назначении профиля» | |
| Поле «Добавить метки» | Ссылка «Выбрать метки», которые будут добавляться на конечные точки при назначении профиля в результате срабатывания политики профилирования |
| Поле «CoA» | Повторная аутентификация при назначении профиля конечной точке в результате срабатывания политики профилирования. Переключатель:<br>— «Активен»;<br>— «Неактивен» |
| Условия профилирования | |
| Формирование основного правила происходит на основе выбранного шаблона условий или созданного вручную правила. Для использования стандартных или ранее сформированных шаблонов условий необходимо перенести шаблон из перечня шаблонов в поле «Перенесите сюда условие» | |
| Элементы управления | |
| Создать | При нажатии кнопки выполняется переход на страницу списка политик с сохранением внесенных данных |
| Отменить | При нажатии кнопки выполняется переход на страницу списка без сохранения внесенных данных |

3) Заполнить поля страницы соответствующими данными добавляемой политики.
4) Сформировать основное условие или воспользоваться заранее сформированными шаблонами условий.

### 3.4.4 Вкладка «Шаблоны условий»

Конструктор условий используется для создания и управления шаблонами условий. Данные шаблоны можно применять как часть правил, настроенных для конкретных политик, или сохранения в шаблоне для дальнейшего использования. Список шаблонов ведется во вкладке «Шаблоны условий» (рис. 33).

Созданный шаблон условий поддерживает до трех уровней вложенности условий (правил), которые могут быть построены с любым уровнем сложности.

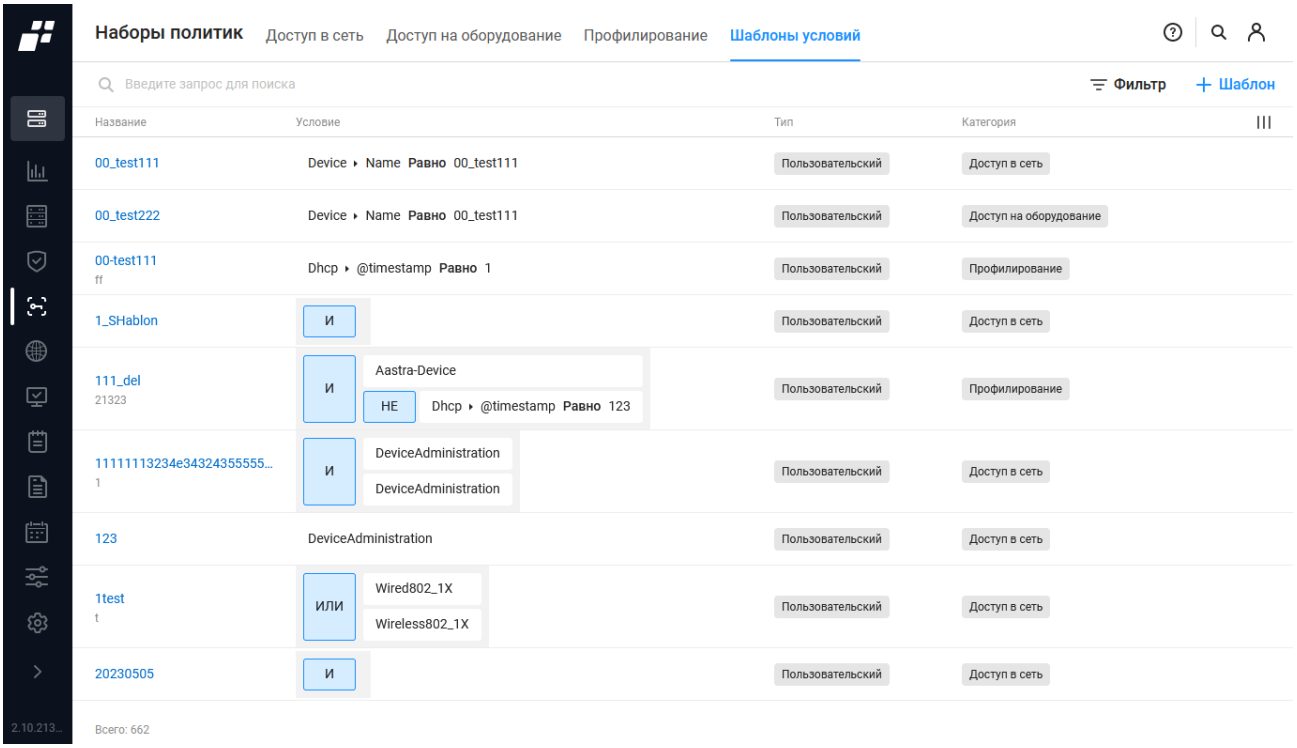



Рисунок 33 – Вкладка «Шаблоны условий»

На странице содержатся следующие данные:

- название шаблона условий – является ссылкой, при переходе по которой можно отредактировать шаблон условий;
- условие;
- тип условия;
- категория условия.

Над списком располагаются:

- поле поиска ( Введите запрос для поиска );
- кнопка «Шаблон» ( + Шаблон );
- кнопка «Фильтр» ( Фильтр );
- кнопка «Колонки» ( ).

При установке флага в строке с необходимым шаблоном над списком появляются следующие кнопки:

- кнопка «Создать копию» ( );
- кнопка «Удалить» ( ).

Аналогичные кнопки появляются в правой части экрана в строке с выбранным шаблоном условий.

### 3.4.4.1 Добавление нового шаблона условий

Для добавления в список нового шаблона условий пользователю необходимо:

1) Нажать кнопку «+ Шаблон». Из раскрывающегося окна выбрать тип шаблона.
2) Заполнить поля страницы необходимыми параметрами. На рис. 34 приведен пример создания шаблона «Доступ в сеть».

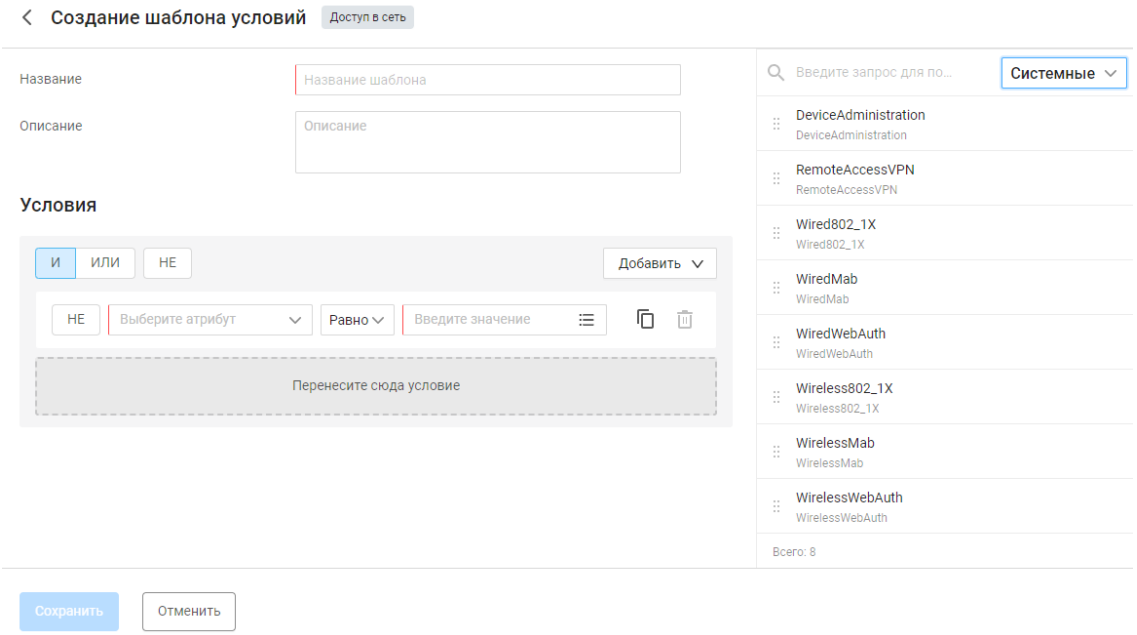



Рисунок 34 – Страница создания шаблона условий «Доступ в сеть»

Новое условие можно создать самостоятельно, с помощью ручного выбора атрибута из предлагаемого списка словарей атрибутов по типам производителей устройств (более подробно см. подраздел 3.11) и присваивания соответствующего значения, либо путем перетаскивания соответствующих условий из набора шаблонов. Для добавления нового условия в рамках одного уровня иерархии необходимо воспользоваться кнопкой «Добавить» → «Новое условие» (рис. 35). Для копирования условия в рамках одного уровня необходимо воспользоваться значком «Копировать» ( ), для удаления – «Удалить» ( ).

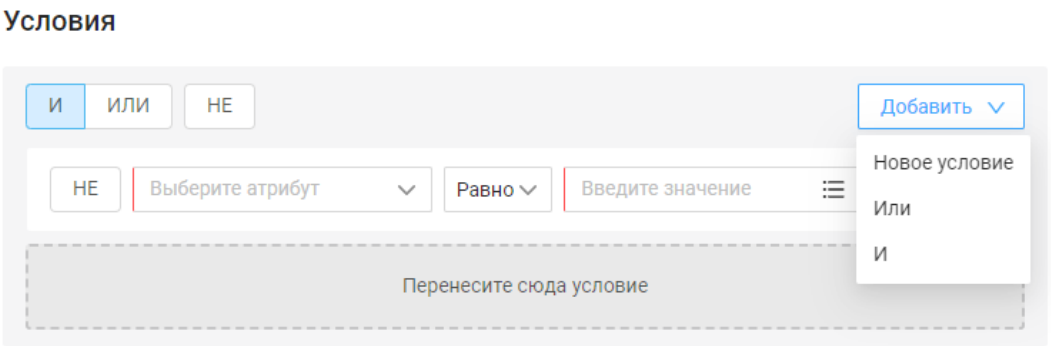



Рисунок 35 – Поле для добавления нового условия в рамках одного уровня

Для добавления нового уровня вложенности необходимо нажать кнопку «Добавить». Из контекстного меню выбрать один из вариантов: «ИЛИ» или «И» (рис. 36).

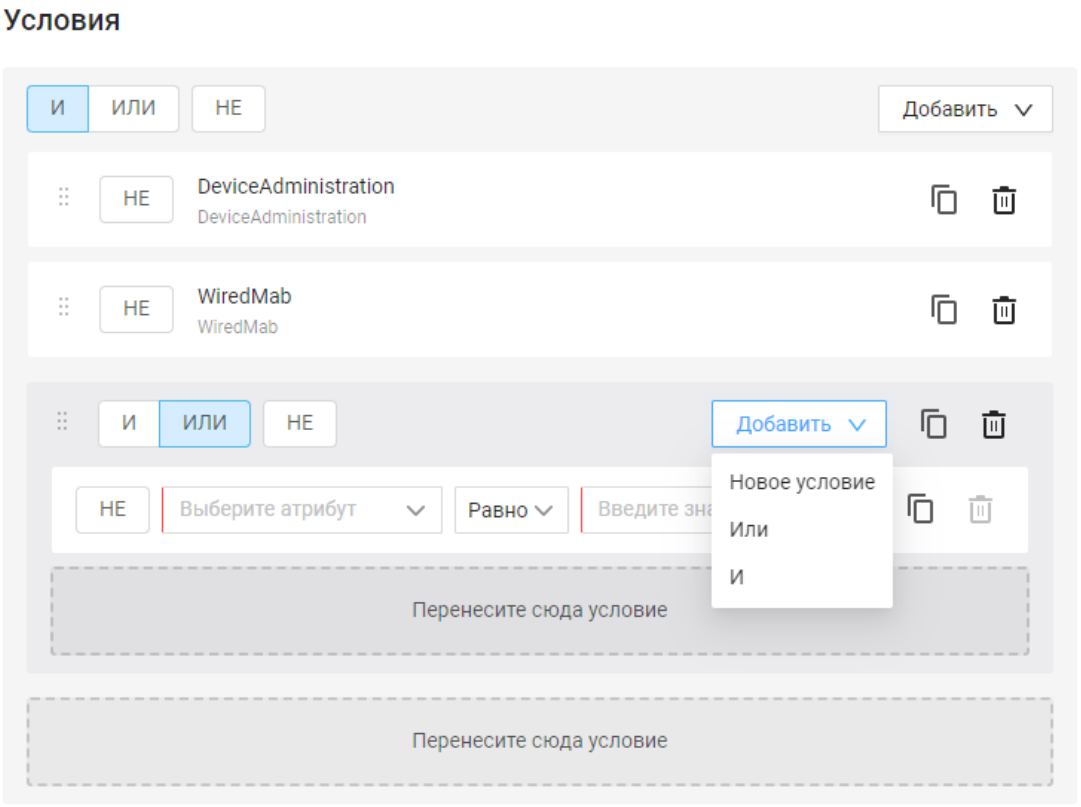



Рисунок 36 – Добавление условий с новым уровнем вложенности

Строки с добавляемыми новыми уровнями имеют отступ, основанный на его положении в иерархии. Чтобы изменить уровень, необходимо захватить условие за левый край и переместить выше.

Созданный шаблон будет добавлен в набор условий.

## 3.5 Профили оборудования

Подраздел «Профили оборудования» (рис. 37) предназначен для формирования профилей сетевого оборудования и назначения общих правил аутентификации и авторизации на оборудовании для сетевых пользователей. В дальнейшем созданный профиль применяется как шаблон при регистрации/заведении сетевого оборудования в базу данных ПК «Efros DO».

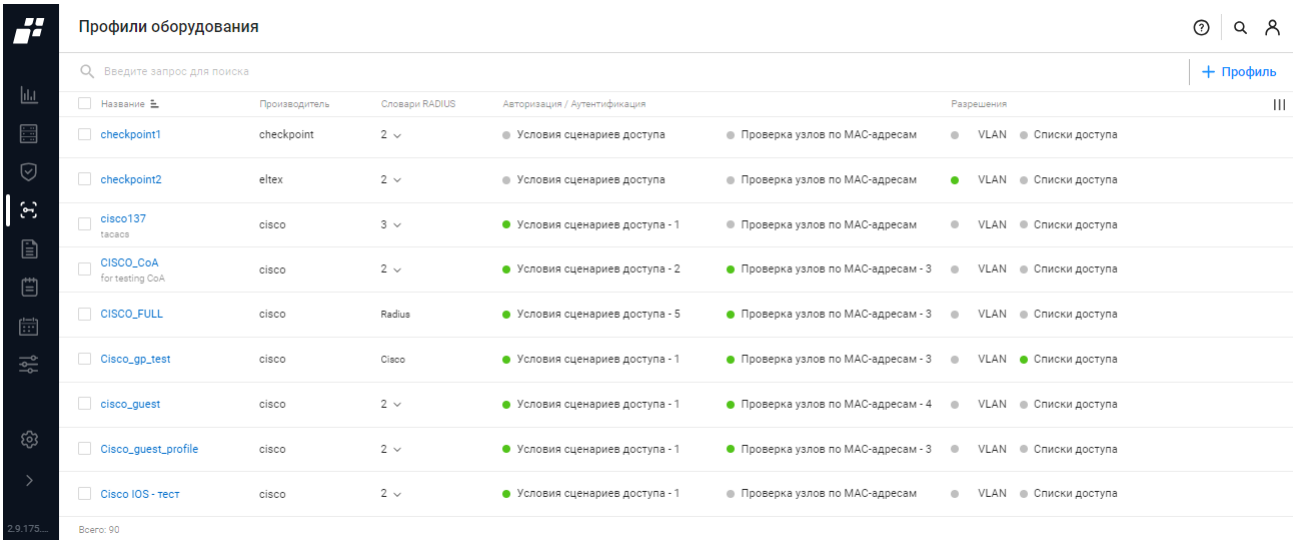



Рисунок 37 – Подраздел «Профили оборудования»

Для каждой записи списка отображаются:

- поле для флага;
- название – является ссылкой, при переходе открывается страница профиля оборудования;
- производитель оборудования;
- RADIUS-словари – списки атрибутов и разрешенных значений для атрибутов, которые используются для определения политик доступа (в виде раскрывающегося списка);
- авторизация/аутентификация – отображение условий сценариев доступа и проверок по MAC-адресам;
- разрешения (VLAN, списки доступов ACL).

Над списком располагаются:

- поле поиска ( Введите запрос для поиска );
- кнопка «Профиль» ( + Профиль );
- кнопка «Колонки» ( ).

При установке флага в строке с необходимым профилем оборудования над списком появляются следующие кнопки:

- кнопка «Создать копию» ( );
- кнопка «Удалить» ( ).

Аналогичные кнопки появляются в правой части экрана в строке с профилем оборудования.

### 3.5.1 Добавление профиля сетевого оборудования

Для добавления нового профиля сетевого оборудования необходимо:

1) Нажать на странице кнопку «Профиль» (+ Профиль).
2) Откроется страница «Создание профиля сетевого оборудования», приведенная на рис. 38. Состав и описание полей страницы приведены в таблице 16.

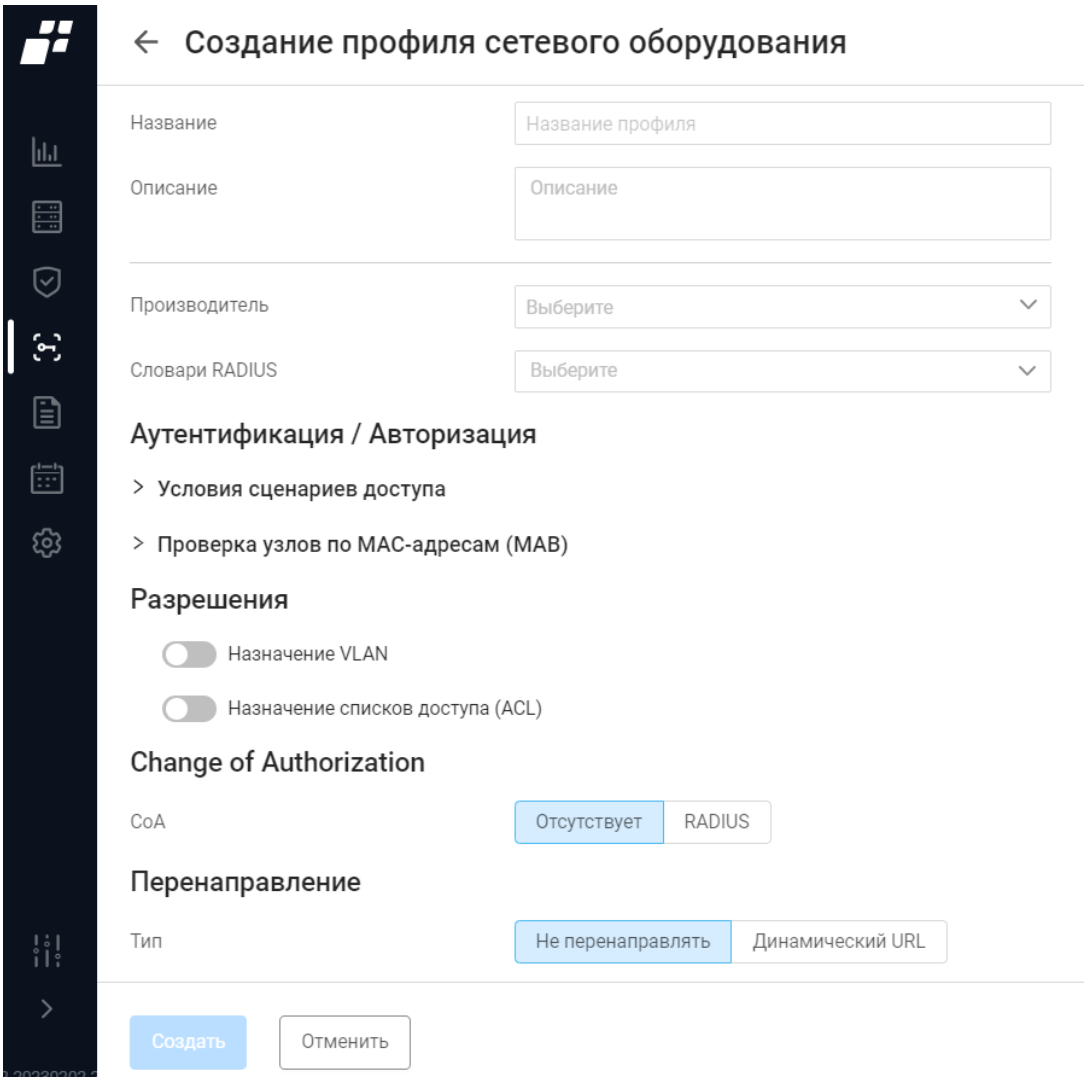



Рисунок 38 – Страница «Создание профиля сетевого оборудования»

Таблица 16 – Состав и описание полей страницы «Создание профиля сетевого оборудования»

| Поле | Описание |
|---|---|
| Поле «Название» | Текстовое поле для ввода названия профиля сетевого оборудования.<br>Параметры ввода текста: от 1 до 50 любых символов |
| Поле «Описание» | Текстовое поле для ввода описания профиля сетевого оборудования. |

| Поле | Описание |
|---|---|
| | Параметры ввода текста: от 1 до 250 любых символов |
| Поле «Производитель» | Раскрывающийся список для выбора производителя.<br>В случае создания универсального профиля предлагается выбрать Efros ACS |
| Поле «Словари RADIUS» | Текстовое поле для выбора системных словарей и правил политик аутентификации и авторизации.<br><br>Не влияет на настройки сценария доступа по протоколу TACACS+. Выбирается любой |
| Блок полей «Аутентификация/Авторизация»<br>Данный блок полей предназначен для определения разрешенных сценариев доступа с указанием необходимых атрибутов и их значений (стандартные шаблоны условий, используемые при формировании набора политик).<br><br>Атрибуты, определяющие используемый сценарий доступа, могут различаться для разных производителей и типа оборудования (более подробно см. п. 3.11) | |
| Группа полей «Условия сценариев доступа» | |
| Проводная аутентификация по MAC-адресам (Wired MAB) | Данные поля предназначены для определения фиксированных атрибутов, поддерживаемых словарями, которые можно использовать в условиях набора политик.<br><br>Для выбранного типа аутентификации формируется условие проверки, выбранному из списка атрибуту присваивается соответствующее значение |
| Беспроводная аутентификация по MAC-адресам (Wireless MAB) | |
| Проводная аутентификация по стандарту 802.1X (Wired 802.1X) | |
| Беспроводная аутентификация по стандарту 802.1X (Wireless 802.1X) | |
| Управление сетевыми устройствами (Device Administration) | |
| Удаленный доступ (VPN) | |
| Группа полей «Проверка узлов по MAC-адресам (MAB)» | |
| Переключатель «Метод проверки узлов» | При включении отображаются три переключателя:<br>— «С использованием PAP/ASCII»;<br>— «С использованием CHAP»;<br>— «С использованием EAP–MD5» |
| Блок полей «Разрешения» | |

| Поле | Описание |
|---|---|
| Поле «Назначение VLAN» | Переключатель:<br>— «Активен» ( ) – разрешить использование VLAN;<br>— «Неактивен» ( ) – запретить использование VLAN.<br><br>По умолчанию переключатель установлен в положение «Неактивен».<br>При включении переключателя появляются следующие переключатели:<br>— «Атрибуты IETF 802.1X»;<br>— «Пользовательские атрибуты». При выборе данного поля необходимо указать атрибуты из раскрывающегося списка |
| Поле «Назначение списков доступа (ACL)» | Переключатель:<br>— «Активен» ( ) – разрешить использование ACL;<br>— «Неактивен» ( ) – запретить использование ACL.<br><br>По умолчанию переключатель установлен в положение «Неактивен».<br>При активации появляется поле для выбора атрибутов |
| Блок полей «Change of Authorization»<br><br>Для производителя «Crtpto-pro» нет возможности настройки параметров изменения авторизации (CoA) в профиле сетевого оборудования. Изменение авторизации (CoA) настраивается для каждого сетевого устройства производителя «Crtpto-pro» в разделе «Контроль доступа» → «Сетевое оборудование» | |
| Поле «CoA» | Содержит два переключателя:<br>— «Отсутствует» – механизм «Change of Authorization» не применяется;<br>— «RADIUS» – механизм «Change of Authorization» применяется с использованием сервера RADIUS.<br><br>При активации переключателя «RADIUS» появляются дополнительные поля |
| Поле «Порт CoA» | Порт для обмена CoA сообщениями между ПК «Efros DO» и сетевым оборудованием |
| Поле «Отправлять Message-Authentificator» | Переключатель:<br>— «Активен» ( );<br>— «Неактивен» ( ).<br><br>Message-Authenticator – атрибут (сетевого пакета), обеспечивающий дополнительную проверку подлинности при взаимодействии сервера RADIUS и сетевого оборудования |
| Группа полей «Отключение» | |

| Поле | Описание |
|---|---|
| Переключатель «RFC 5176» | Завершение сессии |
| Переключатель «Port Bounce» | Завершение сессии и перезагрузка |
| Переключатель «Port Shutdown» | Завершение сессии и отключение порта |
| Группа полей «Повторная аутентификация» | |
| Переключатель «Basic» | При активации переключателя необходимо указать атрибуты сообщения CoA-Request для инициирования сеанса аутентификации |
| Переключатель «Rerun» | При активации переключателя необходимо указать атрибуты для перезапуска процесса аутентификации при запросе повторной аутентификации CoA |
| Переключатель «Last» | При активации переключателя необходимо указать атрибуты для повторной аутентификации, которая была успешна в сеансе |
| Блок полей «Перенаправление» | |
| Поле «Тип» | Содержит следующие переключатели:<br>— «Не перенаправлять» – перенаправление не используется;<br>— «Динамический URL» – задать для пользователя, осуществляющего попытку доступа к сети, тип перенаправления на URL-адрес.<br><br>При активации переключателя «Динамический URL», в профиле авторизации при выборе данного профиля сетевого оборудования появляется поле для выбора атрибута |
| Элементы управления | |
| Создать | При нажатии кнопки выполняется переход на страницу списка профилей с сохранением внесенных данных |
| Отменить | При нажатии кнопки выполняется переход на страницу списка без сохранения внесенных данных |

Перечень атрибутов словаря RADIUS, их описание и возможные принимаемые значения приведены в документе «RFC 2865 Remote Authentication Dial In User Service (RADIUS)».

## 3.6 Профили авторизации

Подраздел «Профили авторизации» (рис. 39) позволяет создавать профили авторизации, формируя общие правила авторизации для сетевых пользователей на оборудовании и правила для доступа в сеть. В дальнейшем созданные профили

применяются для настройки правил авторизации при создании набора политик доступа на оборудование и доступа в сеть.

Отображение доступных параметров для настройки зависит от выбранного профиля оборудования. В случае, если поля основных настроек недоступны для редактирования, необходимо проверить, что для требуемых полей включены и заданы соответствующие настройки выбранного профиля оборудования.

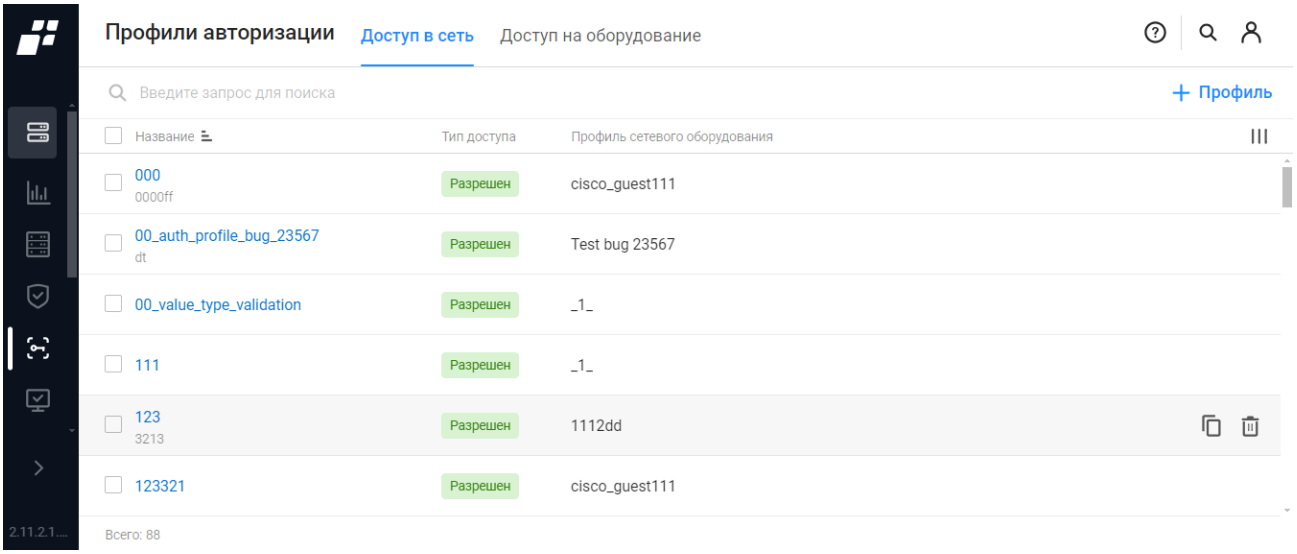



Рисунок 39 – Подраздел «Профили авторизации»

Страница состоит из вкладок:

- «Доступ в сеть»;
- «Доступ на оборудование».

### 3.6.1 Вкладка «Доступ в сеть»

На странице вкладки «Доступ в сеть» список профилей реализован в виде таблицы (см. рис. 39). Для каждой записи списка отображаются данные:

- поле для флага;
- название – является ссылкой, при переходе по которой открывается страница редактирования профиля;
- тип доступа (разрешен/запрещен);
- профиль сетевого оборудования.

Над списком располагаются:

- поле поиска ( Введите запрос для поиска );
- кнопка «Профиль» ( + Профиль );
- кнопка «Колонки» ( ).

При установке флага в строке с необходимым профилем над списком появляются следующие кнопки:

— кнопка «Создать копию» ( );
— кнопка «Удалить» ( ).

Аналогичные кнопки появляются в правой части экрана в строке с профилем доступа в сеть.

### 3.6.1.1 Создание профиля авторизации доступа в сеть

Для ручного добавления нового профиля авторизации пользователю ПК «Efros DO» необходимо:

1) Нажать кнопку «Профиль» ( Профиль ).
2) Откроется страница «Создание профиля авторизации доступа в сеть» (рис. 40). Заполнить поля необходимыми параметрами. Состав и описание полей страницы приведены в таблице 17.

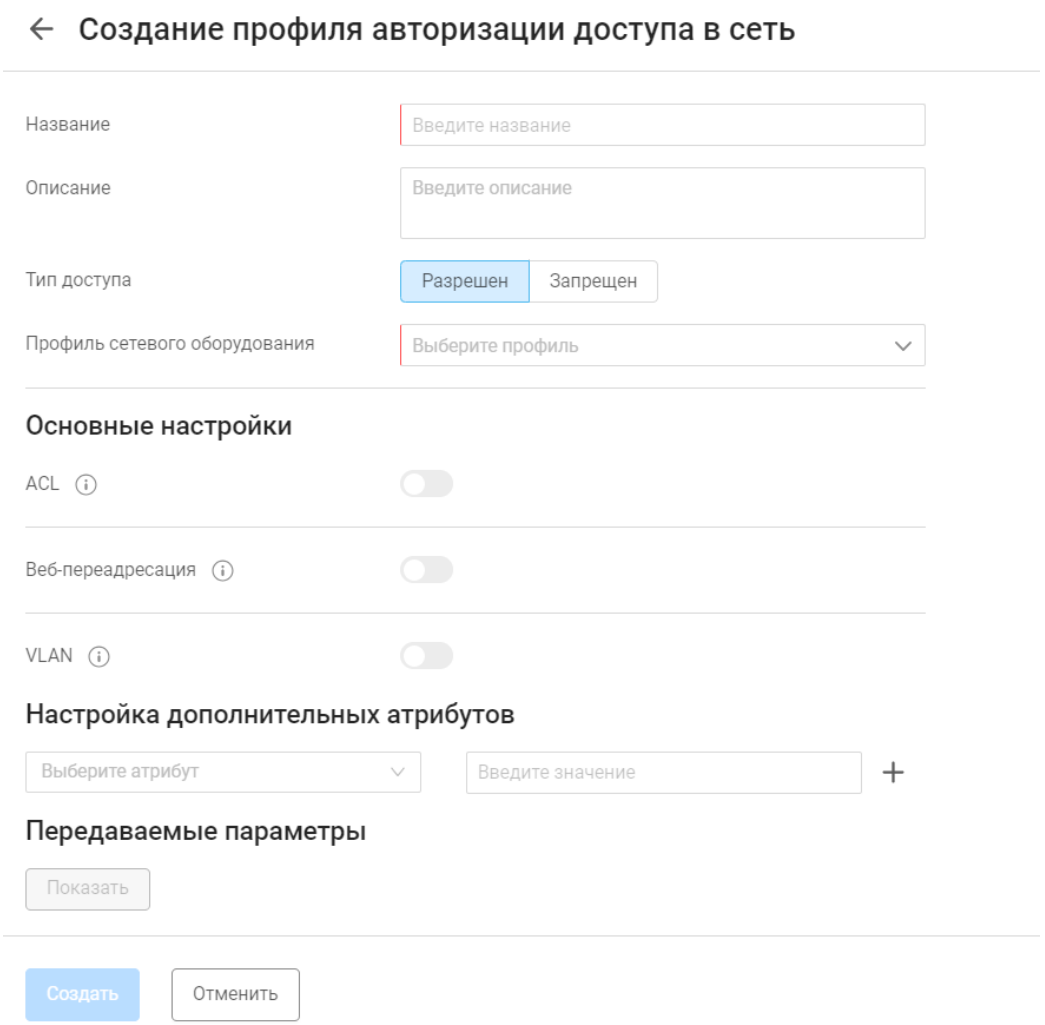



Рисунок 40 – Страница «Создание профиля авторизации доступа в сеть»

Таблица 17 – Состав и описание полей страницы «Создание профиля авторизации доступа в сеть»

| Поле | Описание |
|---|---|
| Поле «Название» | Текстовое поле для ввода названия профиля авторизации.<br>Параметры ввода текста: от 1 до 50 символов.<br>Допустимые символы: буквы латинского алфавита, цифры, «_», «–» |
| Поле «Описание» | Текстовое поле для ввода описания профиля авторизации.<br>Параметры ввода текста: от 1 до 250 любых символов |
| Переключатель «Тип доступа» | Переключатель:<br>— «Разрешен»;<br>— «Запрещен» |
| Поле «Профиль сетевого оборудования» | Поле содержит список созданных профилей сетевого оборудования (более подробно описано в подразделе 3.5) |
| Группа полей «Основные настройки[3]» | |
| Переключатель «Загружаемый ACL» | Содержит список созданных загружаемых ACL. Позволяет загрузить и применить на сетевом оборудовании ACL, сформированные в ПК «Efros DO» (более подробно описано в подразделе 3.7) |
| Переключатель «ACL» | Поле для указания названия списка контроля доступа, определяющего правила использования ресурсов сети, который будет применен на сетевом оборудовании (ACL предварительно должен быть создан локально на сетевом оборудовании).<br><br>Название поля необходимо указывать с **.in** на конце |
| Переключатель «ACL контроллера точек доступа» | В поле указывается список контроля доступа, который будет применен для пользователя в случае его успешной аутентификации при сценарии доступа с использованием гостевого портала. (ACL предварительно должен быть создан локально на контроллере точек доступа). Применимо для оборудования Cisco |
| Переключатель «Веб-переадресация» | Используется для сценария доступа пользователей к сетевым ресурсам с использованием гостевого портала. При активации становятся доступны поля «Гостевой портал», «Название ACL», «Статический IP / Имя хоста / FQDN» |

[3] Состав полей зависит от выбранного профиля сетевого оборудования

| Поле | Описание |
|---|---|
| Поле «Гостевой портал» | Содержит список созданных гостевых порталов. Указывается портал, на который необходимо переадресовать пользователя при попытке подключения к сети |
| Поле «Название ACL» | В поле указывается список контроля доступа, который будет применен на контроллере точек доступа для пользователя, при попытке подключения к сети до прохождения им аутентификации на гостевом портале. ACL предварительно должен быть создан локально на оборудовании доступа. |
| Поле «Статический IP / Имя хоста / FQDN» | Содержит адрес сервера ПК «Efros DO», на котором создан выбранный ранее гостевой портал. По умолчанию используется порт 5802. (Например, https://192.168.1.1:5802/) |
| Поле «Настройка дополнительных атрибутов» | Поле с раскрывающимся списком словарей RADIUS. Параметр специфичен для конкретного устройства, значение зависит от производителя |
| Элементы управления | |
| Показать (поле «Передаваемые параметры») | Параметры, которые будут переданы на устройство по результату авторизации |
| Создать | При нажатии кнопки выполняется переход на страницу списка профилей с сохранением внесенных данных |
| Отменить | При нажатии кнопки выполняется переход на страницу списка без сохранения внесенных данных |

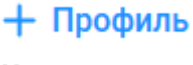
### 3.6.2 Вкладка «Доступ на оборудование»

На странице вкладки «Доступ на оборудование» список профилей реализован в виде таблицы (рис. 41).

Для каждой записи списка отображаются:

- поле для флага;
- название – является ссылкой, при переходе по которой открывается страница редактирования профиля;
- тип настроек.

Над списком располагаются:

- поле поиска (  );
- кнопка «Профиль» (  );
- кнопка «Колонки» (  ).

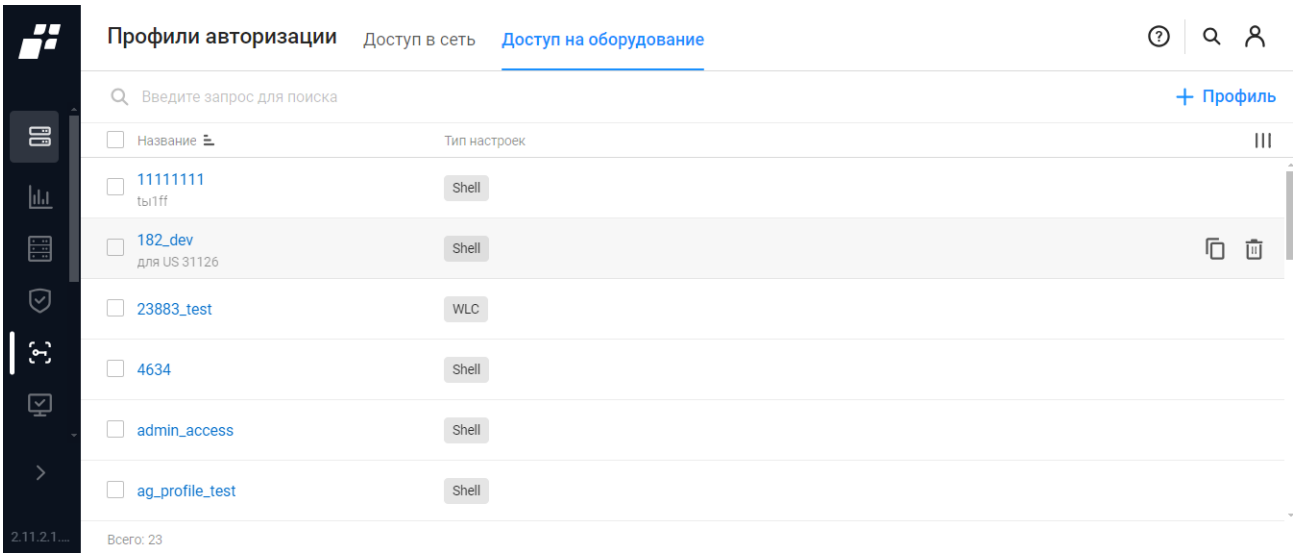



Рисунок 41 – Вкладка «Доступ на оборудование»

При установке флага в строке с необходимым профилем над списком появляются следующие кнопки:

— кнопка «Создать копию» ( );

— кнопка «Удалить» ( ).

Аналогичные кнопки появляются в правой части экрана в строке с профилем доступа в сеть.

### 3.6.2.1 Создание профиля авторизации доступа на оборудование

Для ручного добавления нового профиля авторизации пользователю необходимо:

1) Нажать кнопку «Профиль» ( + Профиль ).
2) Откроется страница «Создание профиля авторизации доступа на оборудование» (рис. 42). Заполнить поля необходимыми параметрами. Состав и описание полей страницы приведены в таблице 18.

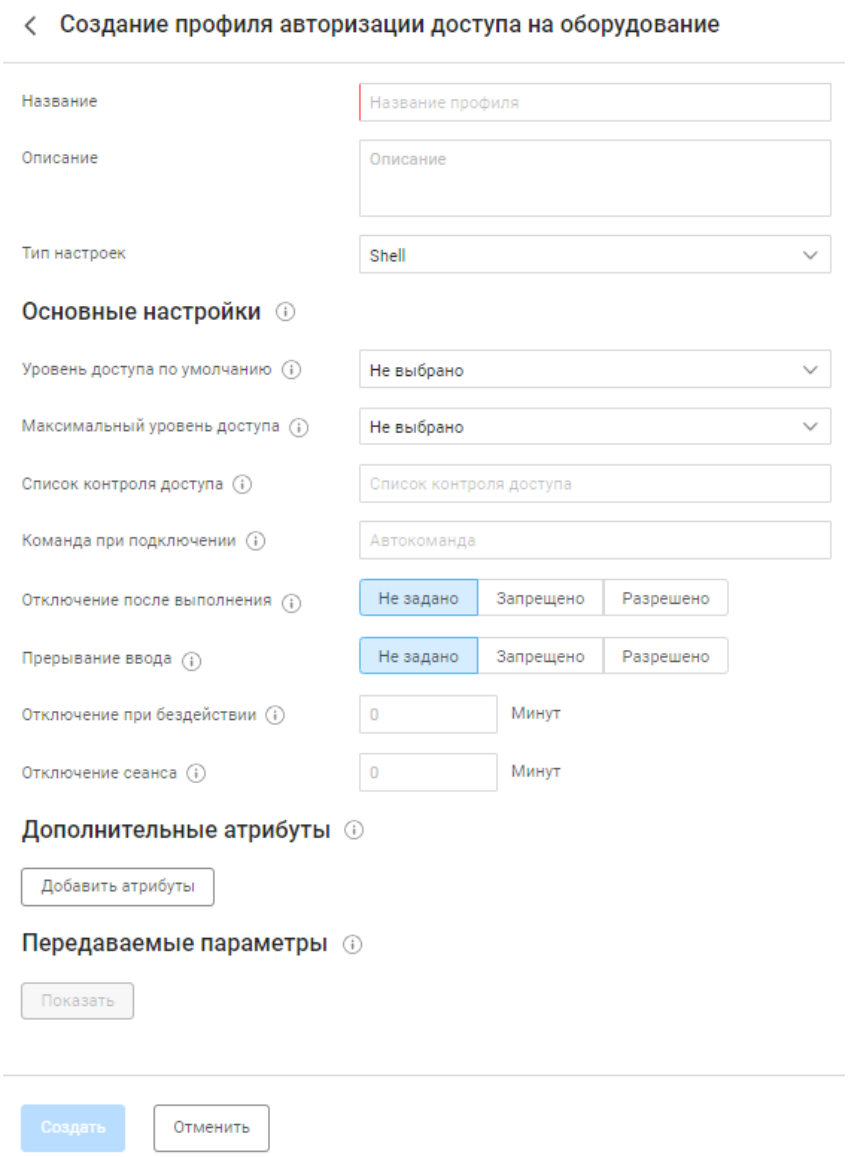



Рисунок 42 – Страница «Создание профиля авторизации доступа на оборудование»

Таблица 18 – Состав и описание полей страницы «Создание профиля авторизации доступа на оборудование»

| Поле | Описание |
|---|---|
| Поле «Название» | Текстовое поле для ввода названия профиля авторизации.<br>Параметры ввода текста: от 1 до 50 символов.<br>Допустимые символы: буквы латинского алфавита, цифры, «_», «–» |
| Поле «Описание» | Текстовое поле для ввода описания профиля авторизации.<br>Параметры ввода текста: от 1 до 250 любых символов |
| Поле «Тип настроек» | Раскрывающийся список:<br>— «Shell» – базовый профиль, применимый к большинству сетевых устройств;<br>— «WLC» – применим для беспроводных LAN-контроллеров (Wireless LAN Controller); |

| Поле | Описание |
|---|---|
| | — «Nexus» – используется для коммутаторов Cisco Nexus;<br>— «Generic» – полностью настраиваемый профиль без предустановленных значений |
| Группа полей «Основные настройки» при выборе типа настроек «Shell» | |
| Поле «Уровень доступа по умолчанию» | Раскрывающийся список значений уровня доступа, с которым будет осуществлен вход пользователя на оборудование.<br>Допустимые значения: «Не выбрано», от 0 до 15.<br>Передается в атрибуте «priv-lvl»<br><br>Необходимо убедиться, что конкретная модель оборудования поддерживает выбранное значение |
| Поле «Максимальный уровень доступа» | Раскрывающийся список значений максимально разрешенного уровня при запросе на повышение прав доступа<br>Допустимые значения: «Не выбрано», от 0 до 15.<br>Передается в атрибуте «max_priv_lvl»<br><br>Необходимо убедиться, что конкретная модель оборудования поддерживает выбранное значение |
| Поле «Список контроля доступа» | Поле для ввода названия ACL, который будет применен на интерфейсе сетевого оборудования.<br>Передается в атрибуте «acl»<br><br>ACL предварительно должен быть создан локально на сетевом оборудовании |
| Поле «Команда при подключении» | Поле для ввода команды, которая автоматически выполнится при входе пользователя на оборудование.<br><br>Необходимо убедиться, что введенная команда поддерживается оборудованием. Передается в атрибуте «autocmd» |
| Поле «Отключение после выполнения» | Завершать сессию после автоматического выполнения команды при подключении. Переключатель:<br>— «Не задано» –- действие по умолчанию;<br>— «Запрещено» – запретить автоматическое отключение;<br>— «Разрешено» – разрешить автоматическое отключение.<br>Передается в атрибуте «nohangup». |
| Поле «Прерывание ввода» | Запрет использования символа прерывания ввода. Переключатель:<br>— «Не задано» –- действие по умолчанию;<br>— «Запрещено» – запретить прерывание ввода;<br>— «Разрешено» – разрешить прерывание ввода.<br>Передается в атрибуте «noescape» |
| Поле «Отключение | Числовое поле для ввода значения времени в минутах, после |

| Поле | Описание |
|---|---|
| при бездействии» | которого неактивный сеанс будет завершен.<br>Допустимые значения: от 0 до 9999, где 0 – отсутствие таймаута.<br>Передается в атрибуте «idletime» |
| Поле «Отключение сеанса» | Числовое поле для ввода значения времени в минутах, после которого сеанс будет завершен.<br>Допустимые значения: от 0 до 9999, где 0 – отсутствие таймаута. Передается в атрибуте «timeout» |
| Группа полей «Основные настройки» при выборе типа настроек «WLC» | |
| Поле «Выбор роли» | Переключатель:<br>— «All» – полный доступ ко всем вкладкам приложений WLC. Передается в атрибуте "role1";<br>— «Monitor» – доступ только для чтения к вкладкам приложения WLC. Передается в атрибуте "role1";<br>— «Lobby» – только ограниченные права на настройку. Передается в атрибуте "role1";<br>— «Selected» – доступ только к определенным вкладкам (необходимо проставить флаги напротив раскрывающегося списка вкладок) |
| Группа полей «Основные настройки» при выборе типа настроек «Nexus» | |
| Поле «Установить атрибут как» | Поле определяет обязательность атрибутов. Переключатель:<br>— «Обязательный»;<br>— «Опциональный» |
| Поле «Роль для NX-OS» | Предустановленные роли для управления устройством NX-OS. Переключатель:<br>— «Нет» – нет привилегий;<br>— «Оператор» – доступ только для чтения;<br>— «Администратор» – полный доступ для чтения и записи |
| Поле «Роль для VDC» | Предустановленные роли для управления VDC (только на Nexus серии 7000). Переключатель:<br>— «Нет» – нет привилегий;<br>— «Оператор» – доступ только для чтения;<br>— «Администратор» – полный доступ для чтения и записи |
| Элементы управления | |
| Добавить атрибуты (поле «Дополнительные атрибуты») | При нажатии кнопки появляются поля для ввода признаков и значений атрибутов, которые будут переданы на оборудование, дополнительно к заданным в блоке «Основные настройки» |
| Показать (поле «Передаваемые параметры») | При нажатии кнопки выполняется вывод списка параметров в том виде, как он будет передан на устройство.<br>Для обязательных значений используется знак равенства (=), а для необязательных звездочка (*) |
| Создать | При нажатии кнопки выполняется переход на страницу списка профилей авторизации с сохранением внесенных данных |

| Поле | Описание |
|---|---|
| Отменить | При нажатии кнопки выполняется переход на страницу списка без сохранения внесенных данных |

## 3.7 Загружаемые ACL

Загружаемые ACL работают только с оборудованием Cisco.

В подразделе «Загружаемые ACL» (рис. 43) осуществляется настройка загружаемого списка управления доступом непосредственно на ПК «Efros DO» для дальнейшей передачи на порт коммутатора в виде атрибутов RADIUS, специфичных для поставщика cisco-av-pair.

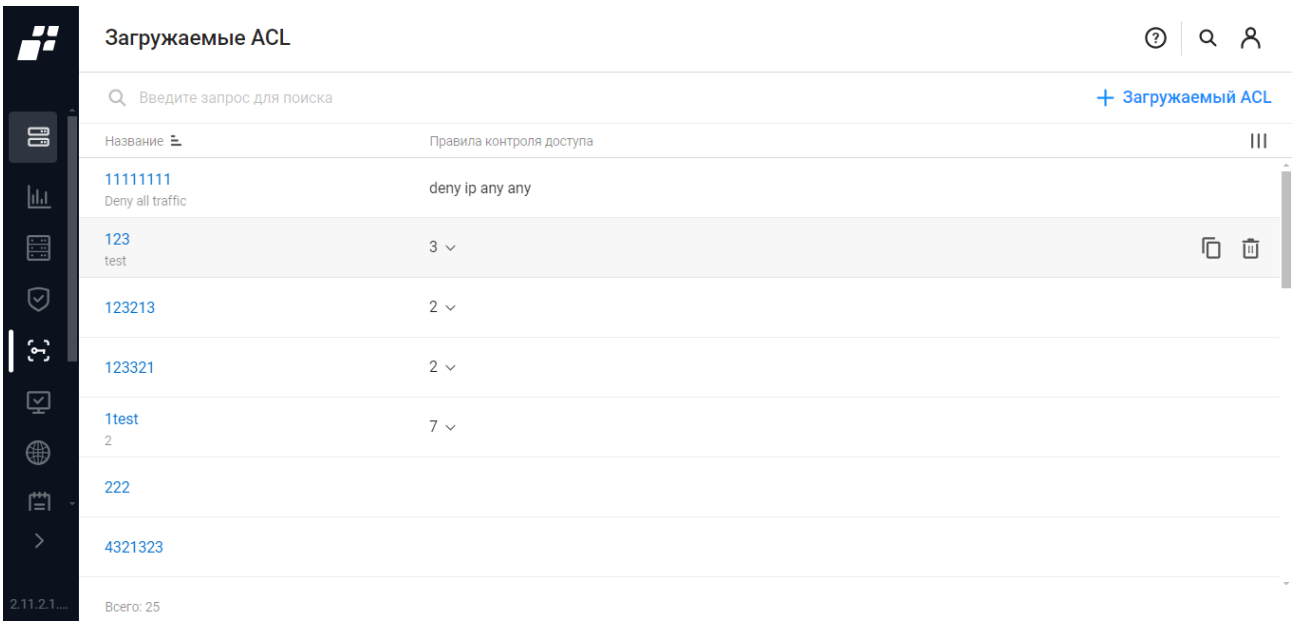



Рисунок 43 – Страница «Загружаемые ACL»

Загружаемые ACL добавляются, редактируются или удаляются в списке вручную пользователями с соответствующими привилегиями.

Для каждой записи списка отображаются данные:

- название – является ссылкой, при выборе которой раскрывается страница с возможностью редактирования текущего загружаемого ACL;
- правила контроля доступа – правила доступа, загружаемые на оборудование.

Над списком располагаются:

- поле поиска ( Введите запрос для поиска );
- кнопка «Загружаемый ACL» ( + Загружаемый ACL );
- кнопка «Колонки» ( ).

При установке флага в строке с необходимым ACL над списком появляются следующие кнопки:

— кнопка «Создать копию» ( );

— кнопка «Удалить» ( ).

Аналогичные кнопки появляются в правой части экрана в строке с ACL.

### 3.7.1 Создание загружаемых ACL

Для добавления нового ACL пользователю необходимо:

1) Нажать кнопку «Загружаемый ACL» ( + Загружаемый ACL ).
2) Откроется страница «Создание загружаемого ACL», приведенная на рис. 44. Заполнить поля необходимыми параметрами. Состав и описание полей страницы приведены в таблице 19.

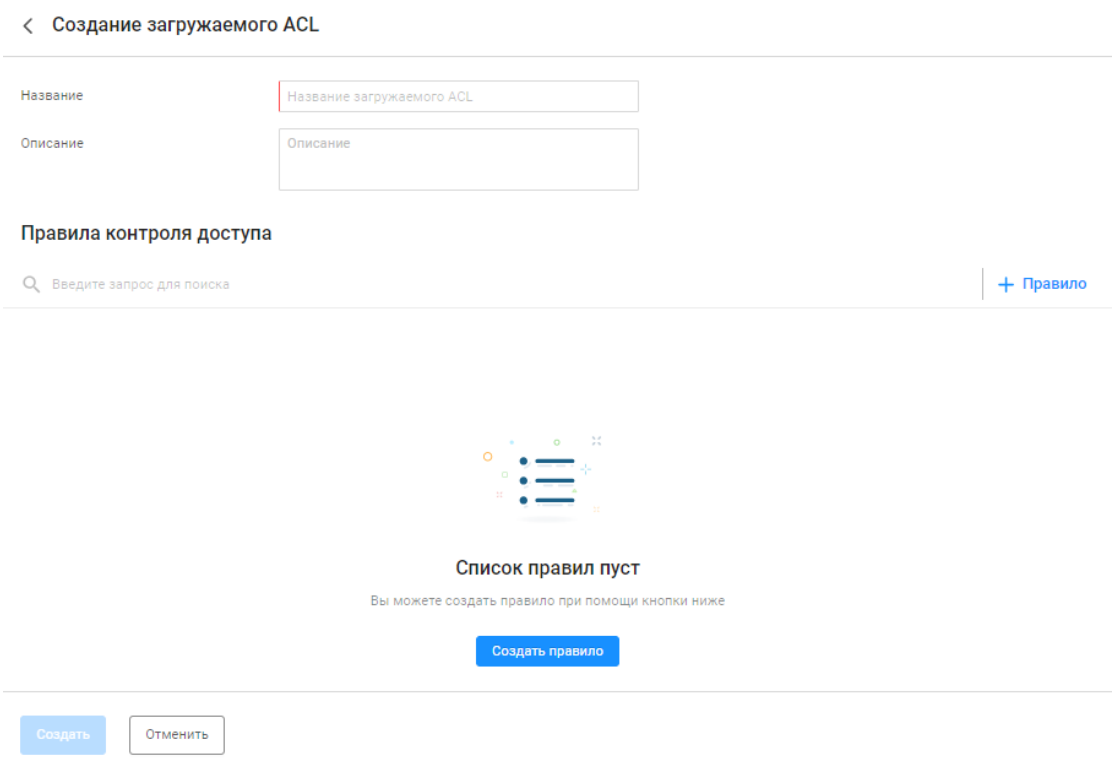



Рисунок 44 – Страница «Создание загружаемого ACL»

Таблица 19 – Состав и описание полей страницы создания загружаемого ACL

| Поле | Описание |
|---|---|
| Поле «Название» | Текстовое поле для ввода названия ACL.<br>Параметры ввода текста: от 1 до 50 символов.<br>Допустимые символы: буквы латинского алфавита, цифры, «_», «–» |

| Поле | Описание |
|---|---|
| Поле «Описание» | Текстовое поле для ввода описания ACL.<br>Параметры ввода текста: от 1 до 250 любых символов |
| Поле «Правила контроля доступа» | Поле для заполнения правил доступа. После установки комплекса список правил отсутствует, на странице отображается сообщение «Список правил пуст. Вы можете создать правило при помощи кнопки ниже» и кнопка «Создать правило» (Создать правило). Создание правила описано в п. 3.7.2<br><br>Список представляет собой набор текстовых выражений, в каждом правиле определяется действие над пакетом: permit (разрешить) или deny (запретить).<br><br>Проверка осуществляется по очередности приведенных выражений. В конце списка стоит неявный запрет на весь трафик (deny any), используется ограничивающий контроль доступа: запрещено все, что явно не разрешено выражениями |
| Элементы управления | |
| Показать | Позволяет осуществить проверку корректности введенных аргументов |
| Создать | При нажатии кнопки выполняется переход на страницу списка ACL с сохранением внесенных данных |
| Отменить | При нажатии кнопки выполняется переход на страницу списка без сохранения внесенных данных |

### 3.7.2 Создание правила доступа для загружаемого ACL

Для создания нового правила доступа необходимо выполнить следующие действия:

1) Нажать кнопку «Создать правило» (Создать правило) или кнопку «Правило» (+ Правило).
2) В открывшемся окне «Создание правила» (рис. 45) заполнить необходимые поля и нажать кнопку «Создать». Состав и описание полей страницы приведено в таблице 20.

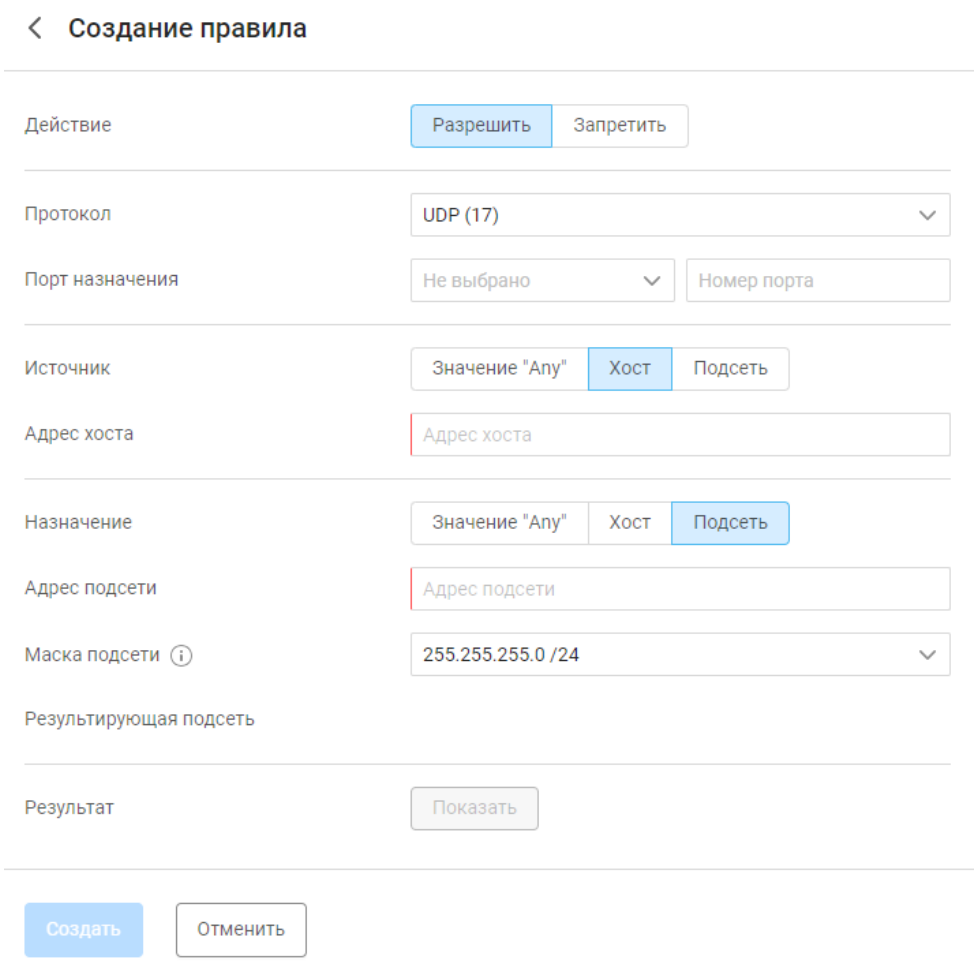



Рисунок 45 – Окно «Создание правила»

Таблица 20 – Состав и описание полей окна «Создание правила»

| Поле | Описание |
|---|---|
| Поле «Действие» | Переключатель:<br>— «Разрешить»;<br>— «Запретить» |
| Поле «Протокол» | Раскрывающийся список с протоколами |
| Группа полей, зависящих от типа протокола в поле «Протокол» | |
| Поле «Порт назначения» | Раскрывающийся список со значениями:<br>— «Не выбрано»;<br>— «Равен»;<br>— «Неравен»;<br>— «Диапазон»;<br>— «Больше»;<br>— «Меньше» |
| Поле «Номер порта» | Поле для ввода номера порта |

| Поле | Описание |
|---|---|
| Поле «Established» | Переключатель:<br>— «Вкл.»;<br>— «Выкл.» |
| Поле «Дополнительные параметры» | Переключатель:<br>— «Отсутствует»;<br>— «Сообщение»;<br>— «Тип» |
| Поле «Источник» | Переключатель:<br>— «Все адреса»;<br>— *«Хост»;<br>— **«Подсеть».<br>*При выборе переключателей «Хост» появляется поле «Адрес хоста».<br>**При выборе переключателя «Подсеть» появляются поля «Адрес подсети», «Маска подсети», «Результирующая подсеть» |
| Поле «Назначение» | Переключатель:<br>— «Все адреса»;<br>— *«Хост»;<br>— **«Подсеть».<br>*При выборе переключателей «Хост» появляется поле «Адрес хоста».<br>**При выборе переключателя «Подсеть» появляются поля «Адрес подсети», «Маска подсети», «Результирующая подсеть» |
| Элементы управления | |
| Показать (поле «Результат») | Показывает результат срабатывания правила |
| Создать | При нажатии кнопки выполняется переход на страницу создаваемого ACL с сохранением внесенных данных |
| Отменить | При нажатии кнопки выполняется переход на страницу списка без сохранения внесенных данных |

## 3.8 Наборы команд

С помощью подраздела «Наборы команд» (рис. 46) можно создать список набора команд для пользователей, работающих с оборудованием. Это позволяет контролировать выполняемые действия с оборудованием. Создать список команд можно как до регистрации оборудования в ПК, так и после регистрации.

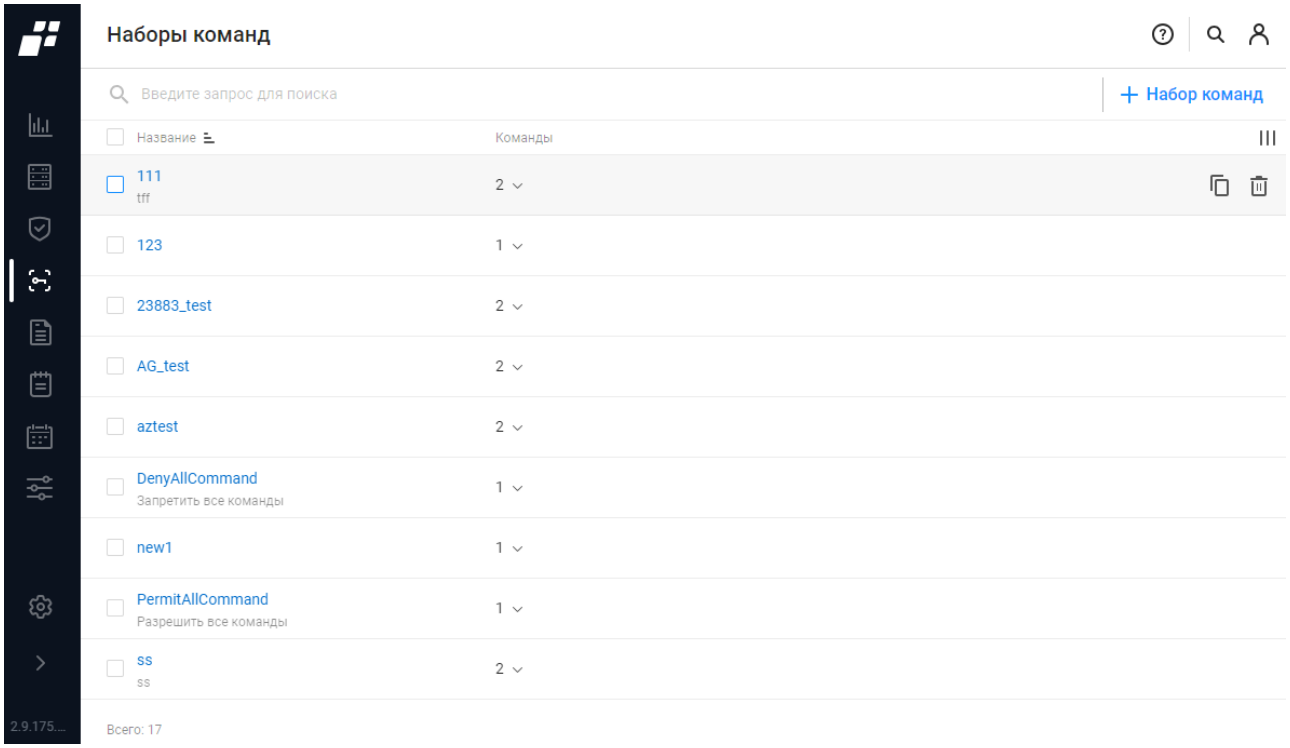



Рисунок 46 – Страница подраздела «Наборы команд»

Для каждой записи списка отображаются:

- поле для флага;
- название – является ссылкой, при нажатии откроется страница редактирования набора команд;
- количество входящих в набор команд – является раскрывающимся окном со списком соответствующих действий и аргументов.

Над списком располагаются:

- поле поиска ( Введите запрос для поиска );
- кнопка «Набор команд» ( Набор команд );
- кнопка «Колонки» ( ).

При установке флага в строке с необходимым профилем оборудования над списком появляются следующие кнопки:

- кнопка «Создать копию» ( Создать копию );
- кнопка «Удалить» ( Удалить ).

Аналогичные кнопки появляются в правой части экрана в строке с набором команд.

### 3.8.1 Создание набора команд

Для создания нового набора команд пользователю ПК «Efros DO» необходимо:

1) Нажать кнопку «Набор команд» ( + Набор команд ). Откроется страница «Создание набора команд», приведенная на рис. 47. Заполнить поля необходимыми параметрами. Состав и описание полей страницы приведены в таблице 21.

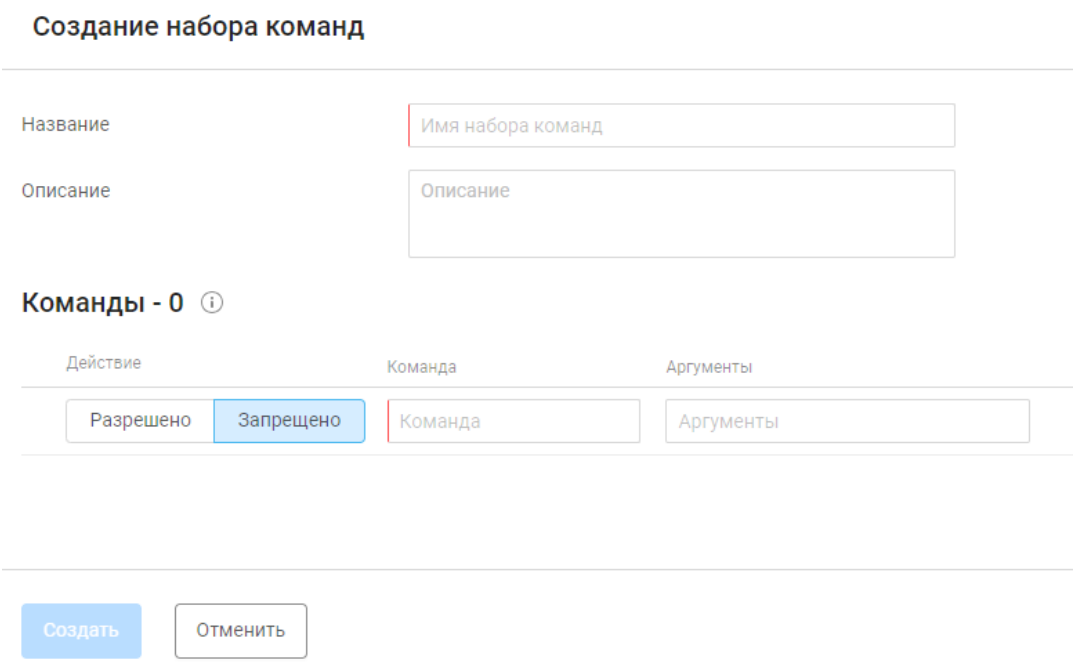



Рисунок 47 – Страница «Создание набора команд»

Таблица 21 – Состав и описание полей страницы «Создание набора команд»

| Поле | Описание |
|---|---|
| Поле «Название» | Текстовое поле для ввода названия набора команд.<br>Параметры ввода текста: от 1 до 50 символов.<br>Допустимые символы: буквы латинского алфавита, цифры, «_», «–» |
| Поле «Описание» | Текстовое поле для ввода описания набора команд.<br>Параметры ввода текста: от 1 до 250 любых символов |
| Таблица команд | После для ввода разрешенных и запрещенных команд для выполнения сетевым пользователем на оборудовании.<br>Параметры ввода команды:<br>— наименование команды не должно содержать пробелов;<br>— регистр не учитывается;<br>— «*» соответствует любому количеству символов, в том числе их отсутствию; |

| Поле | Описание |
|---|---|
| | — «?» соответствует любому отдельному символу;<br>— «all» соответствует любой команде.<br><br>Аргументы задаются в виде регулярных выражений.<br>Параметры ввода аргумента:<br>— допустимо отсутствие аргумента;<br>— «*» соответствует любому количеству символов, в том числе их отсутствию;<br>— «.*» соответствует любому количеству символов, но не менее одного;<br>— числа от 0 до 9.<br><br>Суммарное количество символов в наименовании команды и значении аргумента не должно превышать 512 символов.<br><br>Необходимо убедиться, что введенные значения поддерживаются на используемой модели оборудования |
| Элементы управления | |
| Создать | При нажатии кнопки выполняется переход на страницу с наборами команд с сохранением внесенных данных |
| Отменить | При нажатии кнопки выполняется переход на страницу списка без сохранения внесенных данных |

Для работы с набором команд на странице создания или редактирования (см. рис. 47) необходимо:

1) Выбрать в поле «Действия» одно из действий: «Разрешено» или «Запрещено».
2) Ввести в поле «Команда» наименование команды. В строке добавляемой команды отобразятся кнопки:

— «Принять» ( ) – для сохранения внесенных изменений;

— «Отменить» ( ) – для удаления внесенных данных.

3) Ввести в поле «Аргументы» значение аргумента, с которым команда соответственно разрешена или запрещена к выполнению.
4) Нажать « » или « » для разрешения выполнения команды или ее запрета.
5) Порядок команд можно менять, захватив курсором за начало строки с командой.

После сохранения внесенных изменений в таблице в соответствии с рис. 48 добавится строка с новой командой, в строке добавленной команды отобразятся кнопки:

— «Копировать» ( ⧉ );

— «Удалить» ( 🗑 ).

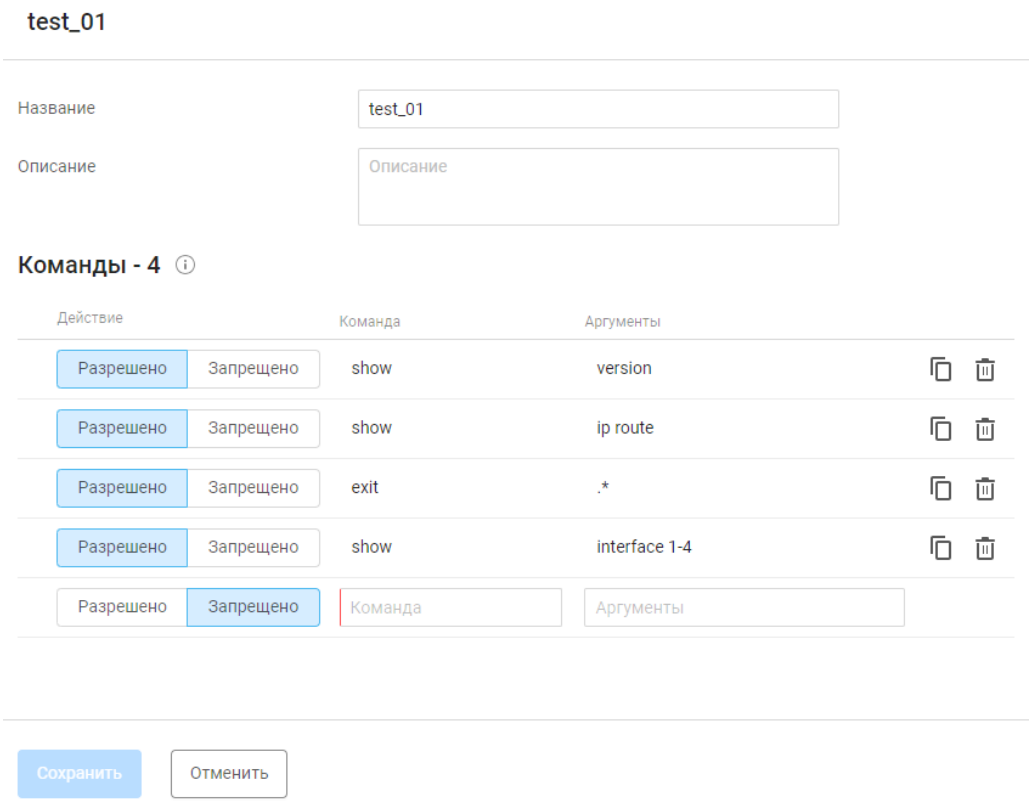



Рисунок 48 – Таблица команд

Пользователь имеет возможность добавить требуемые команды следующим образом:

— заполняя новые строки;

— копируя имеющиеся команды.

Скопированные команды должны быть отредактированы, поскольку в списке не допускаются дубликаты сочетания значений «Команда», «Аргумент».

Если в наборе команд для команды с аргументом задано значение «Разрешено», то разрешено будет выполнять только эту команду с таким аргументом. Остальные аргументы – запрещены.

Если в наборе команд для команды с аргументом задано значение «Запрещено», то правило будет наложено. Чтобы разрешить выполнение этой же команды с другими аргументами необходимо в одной из строк ниже в списке команд указать действие «Разрешено» с аргументом «.*».

## 3.9 Разрешенные протоколы

Подраздел «Разрешенные протоколы» (рис. 49) обеспечивает настройку протоколов, которые будут использоваться во время проверки аутентификации при доступе:

- в сеть
- на оборудование.

Раздел так же обеспечивает управление списком «Настройки TLS», необходимых для организации доступа в сеть.

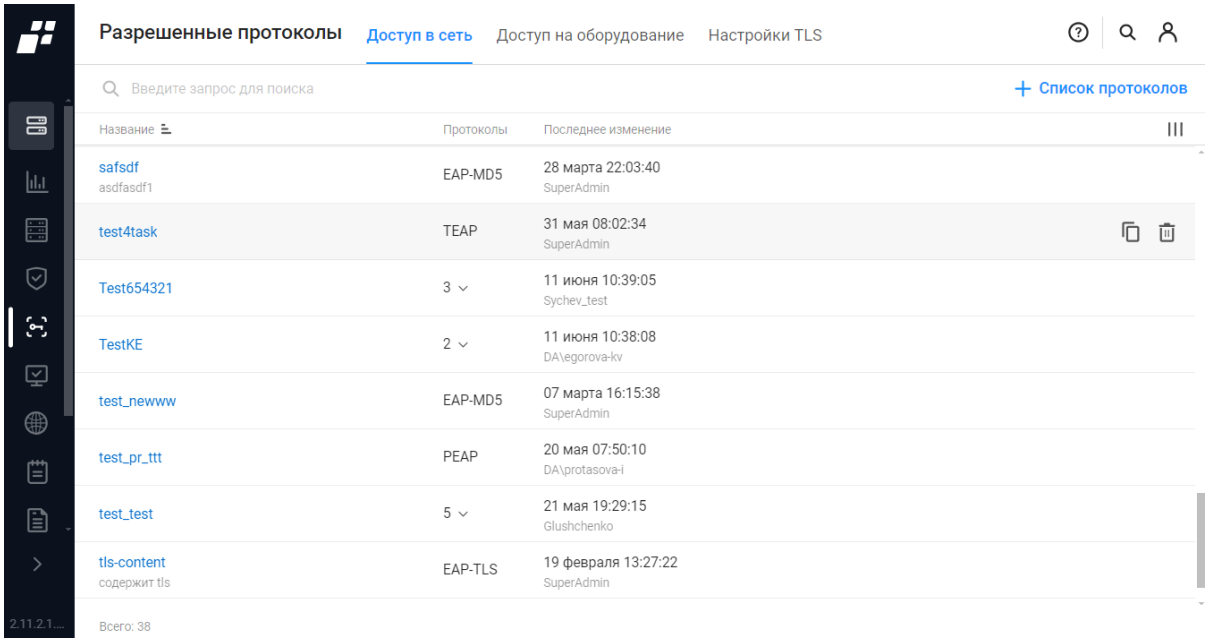



Рисунок 49 – Подраздел «Разрешенные протоколы»

Страница раздела состоит из следующих вкладок:

- «Доступ в сеть»;
- «Доступ на оборудование»;
- «Настройки TLS».

### 3.9.1 Вкладка «Доступ в сеть»

Данная вкладка содержит список разрешенных протоколов доступа в сеть, которые поддерживаются комплексом во время аутентификации через RADIUS-сервер (см. рис. 49).

Разрешенные протоколы необходимо определить перед настройкой политик аутентификации.

Разрешенные протоколы доступа в сеть содержат выбранные протоколы для конкретного варианта использования.

При установке комплекса по умолчанию добавлен один список разрешенных протоколов «Default_Network_Access». Пользователь имеет возможность вносить изменения в список протоколов по умолчанию. Удалить список протоколов невозможно.

Для каждой записи списка отображаются данные:

- название – является ссылкой, при нажатии откроется страница редактирования протоколов;
- количество протоколов – является раскрывающимся списком протоколов;
- дата, время и логин пользователя, внесшего последние изменения.

Над списком располагаются:

- поле поиска ( Введите запрос для поиска );
- кнопка «Список протоколов» ( + Список протоколов );
- кнопка «Колонки» ( ).

Кнопки, появляющиеся в правой части экрана в строке списка протоколов:

- кнопка «Создать копию» ( );
- кнопка «Удалить» ( ).

#### 3.9.1.1 Создание списка разрешенных протоколов «Доступ в сеть»

Для создания нового списка разрешенных протоколов необходимо:

1) Нажать на вкладке «Доступ в сеть» кнопку «Список протоколов» ( + Список протоколов ).
2) Откроется страница «Создание списка разрешенных протоколов «Доступ в сеть» (рис. 50). Заполнить поля страницы необходимыми параметрами. Состав и описание полей страницы приведены в таблице 22.

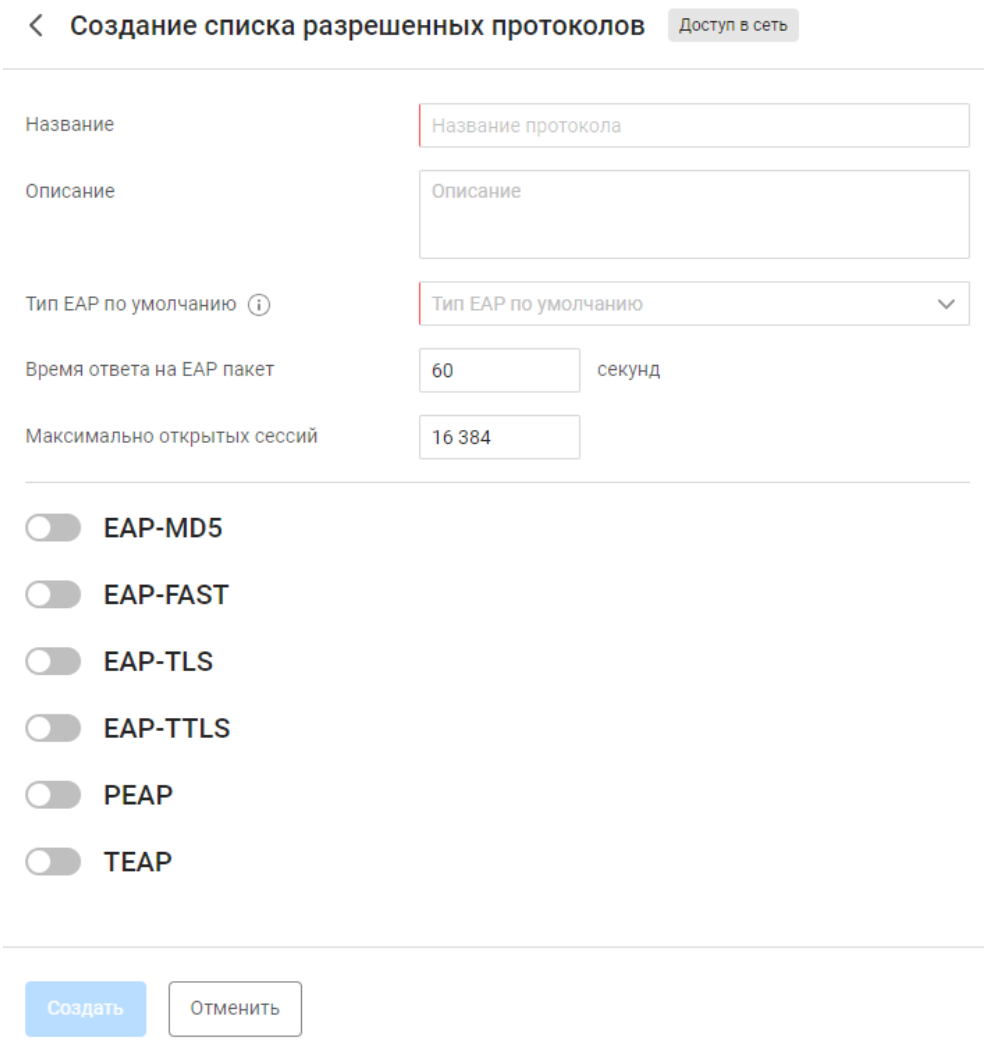



Рисунок 50 – Страница «Создание списка разрешенных протоколов «Доступ в сеть»

Таблица 22 – Состав и описание полей страницы создания списка разрешенных протоколов «Доступ в сеть»

| Поле | Описание |
|---|---|
| Поле «Название» | Текстовое поле для ввода названия списка разрешенных протоколов «Доступ в сеть».<br>Параметры ввода текста: от 1 до 50 символов.<br>Допустимые символы: буквы латинского алфавита, цифры, «_», «–» |
| Поле «Описание» | Текстовое поле для ввода описания списка разрешенных протоколов «Доступ в сеть».<br>Параметры ввода текста: от 1 до 250 любых символов |
| Поле «Тип EAP по умолчанию» | Раскрывающийся список типов EAP:<br>— «FAST»;<br>— «MD5»;<br>— «PEAP»;<br>— «TEAP»; |

| Поле | Описание |
|---|---|
| | — «TLS»;<br>— «TTLS» |
| Поле «Время ответа на EAP пакет» | Поле для ввода времени хранения данных аутентификатора между запросами и ответами на EAP-пакеты (в секундах). По истечении заданного интервала времени данные удаляются.<br>Допустимые значения: от 1 до 16384.<br>Значение по умолчанию: 60 |
| Поле «Максимально открытых сессий» | Поле для ввода максимального допустимого количества сеансов, отслеживаемых модулем «Efros ACS».<br>Допустимые значения: от 1 до 16384<br>Значение по умолчанию: 16384 |
| Переключатель «EAP-MD5» | Предназначен для включения/выключения использования расширяемого протокола EAP-MD5 |
| Группа полей для настройки протокола «EAP-FAST» | |
| Переключатель «EAP-FAST» | Предназначен для включения/выключения использования расширяемого протокола EAP-FAST.<br>При включении появляются дополнительные поля |
| Поле «Настройки TLS» | Поле со списком для выбора используемой конфигурации TLS. Список содержит наименования конфигураций в соответствии со списком вкладки «Настройки TLS» подраздела «Доступ в сеть» |
| Поле «Метод по умолчанию» | Раскрывающийся список методов EAP по умолчанию, при получении запроса на аутентификацию от АСО.<br>Не редактируемое поле.<br>Значение по умолчанию: «EAP-MSCHAPv2» |
| Поле «Идентификатор сервера» | Поля для ввода имени сервера, который отправляет клиенту учетные данные.<br>Значение по умолчанию: «Efros Defence Operation» |
| Поле «Срок действия PAC» | Поля для ввода срока действия ключа шифрования PAC |
| Поле «EAP-MSCHAPv2» | Переключатель использования метода «EAP-MSCHAPv2». Не редактируемое поле.<br>Значение по умолчанию: «Активен» |
| Группа полей для настройки протокола «EAP-TLS» | |
| Переключатель «EAP-TLS» | Предназначен для включения/выключения использования расширяемого протокола аутентификации и безопасности транспортного уровня EAP-TLS.<br>При включении появляется дополнительное поле |
| Поле «Настройки TLS» | Поле со списком для выбора используемой конфигурации TLS. Список содержит наименования конфигураций в соответствии со списком вкладки «Настройки TLS» подраздела «Разрешенные протоколы» |
| Группа полей для настройки протокола «EAP-TTLS» | |

| Поле | Описание |
|---|---|
| Переключатель «EAP-TTLS» | Предназначен для включения/выключения использования расширяемого протокола EAP-TTLS.<br>При включении появляются дополнительные поля |
| Поле «Настройки TLS» | Поле со списком для выбора используемой конфигурации TLS. Список содержит наименования конфигураций в соответствии со списком вкладки «Настройки TLS» подраздела «Доступ в сеть» |
| Поле «Метод по умолчанию» | Раскрывающийся список методов EAP по умолчанию, при получении запроса на аутентификацию от АСО |
| Группы полей «EAP-MSCHAPv2», «EAP-TLS», «EAP-GTC», «EAP-MD5» | Переключатели «EAP-MSCHAPv2», «EAP-TLS», «EAP-GTC» и «EAP-MD5» для включения/выключения использования методов EAP.<br>При включении переключателя «EAP-TLS» появляется дополнительное поле «Настройки TLS» |
| Поле «EAP-TNC» | Переключатель «EAP-TNC» для включения/выключения проверки подключаемого устройства на соответствие требованиям политики безопасности |
| Группа полей для настройки протокола «PEAP» | |
| Переключатель «PEAP» | Предназначен для включения/выключения использования расширяемого протокола PEAP.<br>При включении появляются дополнительные поля |
| Поле «Настройки TLS» | Поле со списком для выбора используемой конфигурации TLS. Список содержит наименования конфигураций в соответствии со списком вкладки «Настройки TLS» подраздела «Доступ в сеть» |
| Поле «Метод по умолчанию» | Раскрывающийся список методов EAP по умолчанию, при получении запроса на аутентификацию от АСО |
| Группы полей «EAP-MSCHAPv2», «EAP-TLS», «EAP-GTC» | Переключатели «EAP-MSCHAPv2», «EAP-TLS» и «EAP-GTC» для включения/выключения использования методов EAP.<br>При включении переключателя «EAP-TLS» появляется дополнительное поле «Настройки TLS» |
| Поле «EAP-TNC» | Переключатель «EAP-TNC» для включения/выключения проверки подключаемого устройства на соответствие требованиям политики безопасности |
| Группа полей для настройки протокола «TEAP» | |
| Переключатель «TEAP» | Предназначен для включения/выключения использования расширяемого протокола TEAP.<br>При включении появляются дополнительные поля |
| Поле «Настройки TLS» | Поле со списком для выбора используемой конфигурации TLS. Список содержит наименования конфигураций в соответствии со списком вкладки «Настройки TLS» подраздела «Доступ в сеть» |
| Поле «Метод по умолчанию» | Раскрывающийся список методов EAP по умолчанию, при получении запроса на аутентификацию от АСО.<br>Значение по умолчанию: «EAP-MSCHAPv2» |

| Поле | Описание |
|---|---|
| Поле «Идентификатор сервера» | Поля для ввода имени сервера, который отправляет клиенту учетные данные.<br>Значение по умолчанию: «Efros Defence Operation» |
| Поле «Срок действия PAC» | Поля для ввода срока действия ключа шифрования PAC |
| Поле «EAP-MSCHAPv2» | Переключатель использования метода «EAP-MSCHAPv2» |
| Поле «EAP-TLS» | Переключатель использования метода «EAP-TLS» |
| Элементы управления | |
| Создать | При нажатии кнопки выполняется переход на страницу с сохранением внесенных данных |
| Отменить | При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных |

### 3.9.2 Вкладка «Доступ на оборудование»

При установке комплекса по умолчанию добавлен один список разрешенных протоколов «Default_Device_Admin». Пользователь не имеет возможности вносить изменения или удалить список протоколов.

Данная вкладка содержит список разрешенных протоколов для проверки доступа на оборудование (рис. 51).

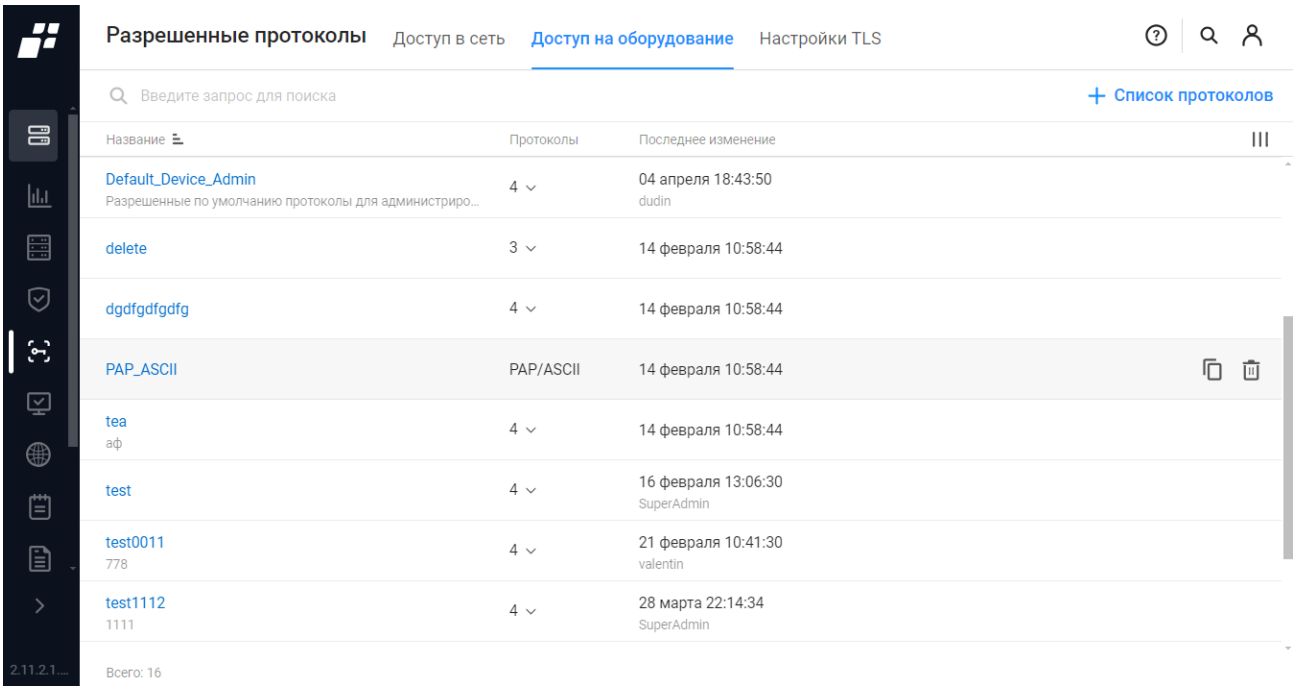



Рисунок 51 – Вкладка «Список разрешенных протоколов «Доступ на оборудование»

Для каждой записи списка отображаются данные:

- название – является ссылкой, при нажатии откроется страница редактирования протоколов;
- количество протоколов – является раскрывающимся списком протоколов;
- дата, время и логин пользователя, внесшего последние изменения.

Над списком располагаются:

- поле поиска ( Введите запрос для поиска );
- кнопка «Список протоколов» ( + Список протоколов );
- кнопка «Колонки» ( ).

Кнопки, появляющиеся в правой части экрана в строке списка протоколов:

- кнопка «Создать копию» ( );
- кнопка «Удалить» ( ).

### 3.9.2.1 Создание списка разрешенных протоколов «Доступ на оборудование»

Для создания нового списка разрешенных протоколов необходимо:

1) Нажать на вкладке «Доступ на оборудование» кнопку «Список протоколов» ( + Список протоколов ).
2) Откроется страница «Создание списка разрешенных протоколов «Доступ на оборудование» (рис. 52). Заполнить поля страницы необходимыми параметрами. Состав и описание полей страницы приведены в таблице 23.

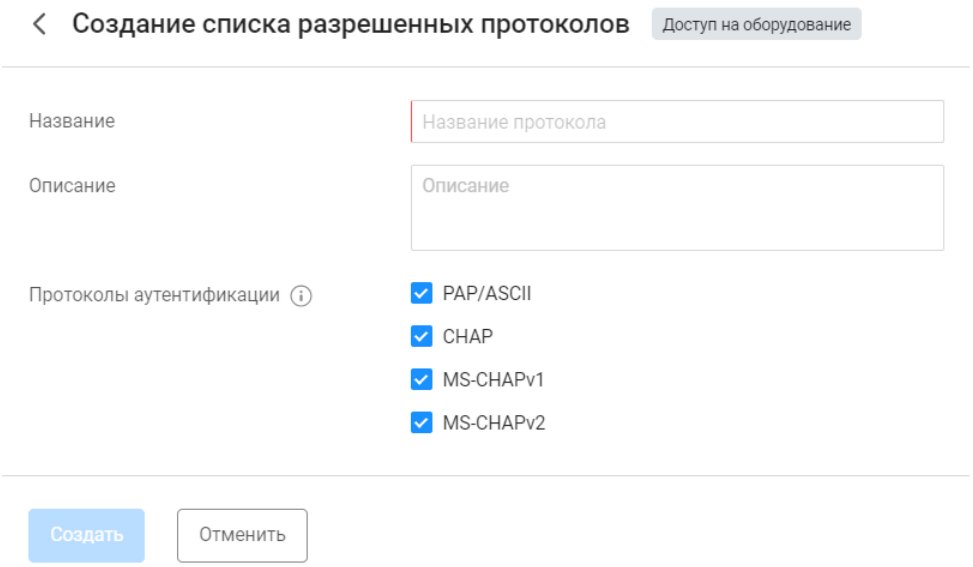



Рисунок 52 – Страница «Создание списка разрешенных протоколов «Доступ на оборудование»

Таблица 23 – Состав и описание полей страницы создания списка разрешенных протоколов

| Поле | Описание |
|---|---|
| Поле «Название» | Текстовое поле для ввода названия списка разрешенных протоколов.<br>Параметры ввода текста: от 1 до 50 символов.<br>Допустимые символы: буквы латинского алфавита, цифры, «_», «–» |
| Поле «Описание» | Текстовое поле для ввода описания списка разрешенных протоколов.<br>Параметры ввода текста: от 1 до 250 любых символов |
| Поле «Протоколы аутентификации» | Поле выбора протоколов аутентификации. Для выбора необходимо проставить флаг для требуемого параметра |
| Элементы управления | |
| Создать | При нажатии кнопки выполняется переход на страницу с протоколами с сохранением внесенных данных |
| Отменить | При нажатии кнопки выполняется переход на страницу списка без сохранения внесенных данных |

### 3.9.3 Настройки TLS

При установке комплекса по умолчанию доступна одна конфигурация с названием tls-common. Пользователь имеет возможность создавать новые конфигурации, вносить изменения в имеющиеся и удалять конфигурации. Для удаления доступны только те конфигурации, которые не привязаны ни к одному из протоколов.

Для выполнения настройки конфигураций TLS пользователю необходимо выбрать подраздел «Разрешенные протоколы» и вкладку «Настройки TLS» (рис. 53).

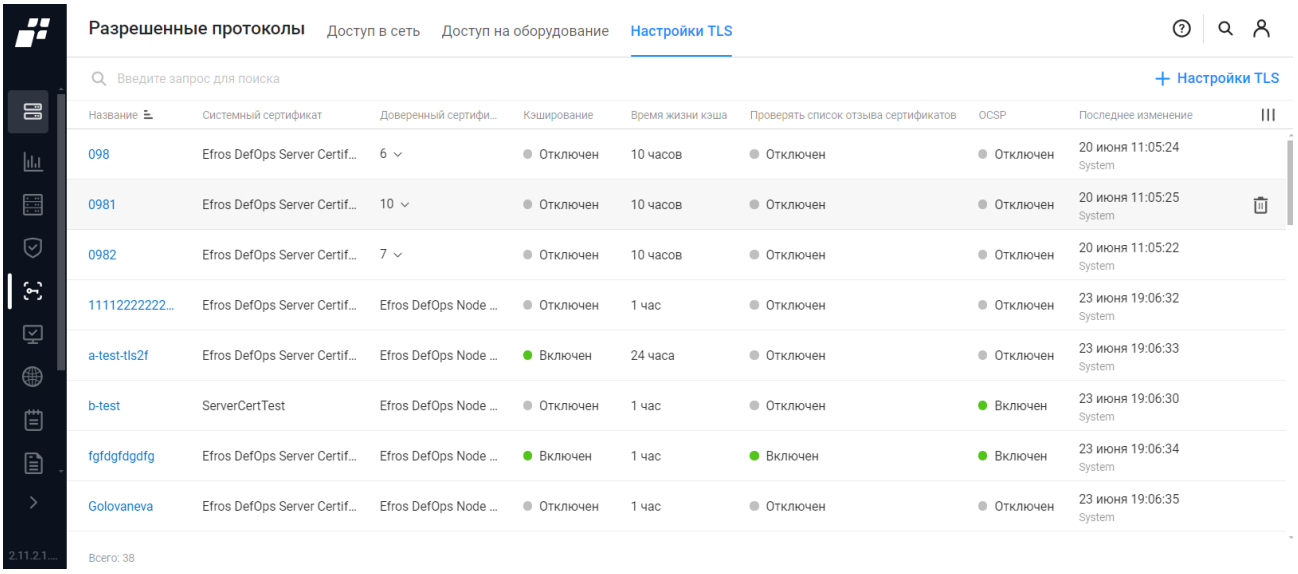



Рисунок 53 – Страница вкладки «Настройки TLS»

На странице список настроек реализован в виде таблицы. Для каждой записи списка отображаются следующие данные:

- название настройки;
- имя системного сертификата, используемого при аутентификации устройств в сети;
- имя доверенного сертификата, связанного с выбранным серверным сертификатом;
- кэширование;
- время жизни кэша;
- проверка списка отзывов сертификата;
- OCSP;
- дата, время и логин пользователя, внесшего последние изменения.

Над таблицей списка настроек располагаются:

- поле поиска ( Введите запрос для поиска );
- кнопка «Настройки TLS» ( + Добавить );
- кнопка «Колонки» ( ).

При наведении курсора на строку с настройкой, в правой части строки появляется кнопка «Удалить» ( ) для удаления настройки.

### 3.9.3.1 Создание настройки TLS

Для создания новой настройки TLS пользователю необходимо нажать кнопку «Добавить». Откроется страница создания настройки TLS (рис. 54). Заполнить поля

необходимыми параметрами и нажать кнопку «Создать». Состав и описание полей страницы приведены в таблице 24.

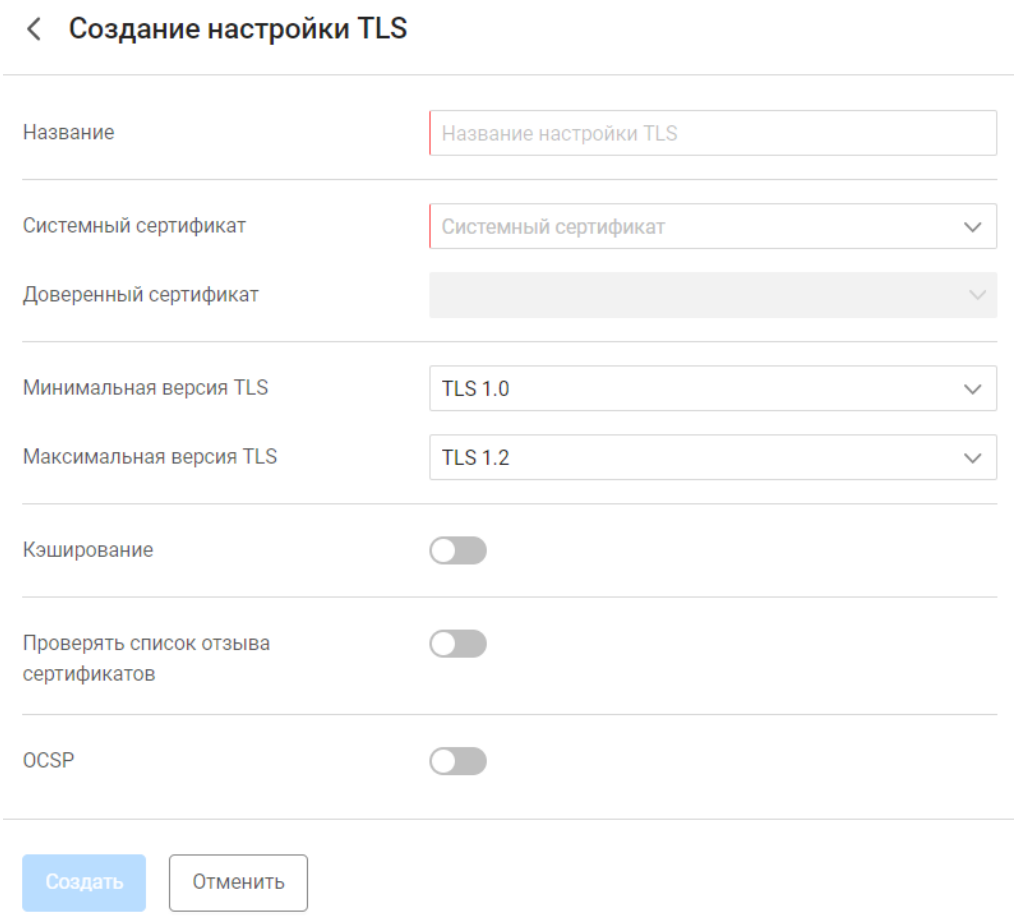



Рисунок 54 – Страница «Создание настройки TLS»

Таблица 24 – Состав и описание полей страницы создания настройки TLS

| Поле | Описание |
|---|---|
| Поле «Название» | Поле для ввода названия конфигурации.<br>Параметры ввода текста: от 1 до 50 символов.<br>Допустимые символы: буквы латинского алфавита, цифры, «_», «–» |
| Поле «Системный сертификат» | Поле со списком для выбора серверного сертификата, используемого при аутентификации устройств в сети.<br>Содержит список серверных сертификатов, для которых однозначно определен корневой сертификат.<br><br>Предварительно можно создать новый системный сертификат в разделе «Администрирование» → «Сертификаты» → вкладка «Системные» |
| Поле «Доверенный сертификат» | Поле заполняется автоматически после выбора серверного сертификата. Содержит название корневого сертификата, |

| Поле | Описание |
|---|---|
| | связанного с выбранным серверным сертификатом.<br>Изменить выбор доверенных сертификатов в раскрывающемся списке.<br><br>Предварительно можно создать новые доверенные сертификаты в разделе «Администрирование» → «Сертификаты» → вкладка «Доверенные» |
| Поле «Минимальная версия TLS» | Раскрывающийся список версий TLS |
| Поле «Максимальная версия TLS» | Раскрывающийся список версий TLS |
| Поле «Кэширование» | Переключатель:<br>— «Активен» ( ) – при восстановлении сеанса из кэша копируются атрибуты сеанса: ID сессии и имя пользователя;<br>— «Неактивен» ( ) – при восстановлении сеанса атрибуты из кэша не копируются.<br><br>При активации переключателя появляется дополнительное поле «Время жизни кэша» |
| Поле «Время жизни кэша» | Поле для ввода времени хранения атрибутов сессии: ID сессии и имя пользователя (в часах).<br>Допустимые значения: от 1 до 100.<br>Значение по умолчанию – 1.<br>Поле отображается и доступно для редактирования только если включен переключатель «Кэширование» (см. выше) |
| Поле «Проверять список отзыва сертификатов» | Переключатель:<br>— «Активен» ( ) – клиентские сертификаты проверяются в модуле «Efros NAC» на их наличие в списке отозванных сертификатов (CRL);<br>— «Неактивен» ( ) – проверка не выполняется |
| Поле «OCSP» | Переключатель:<br>— «Активен» ( ) – клиентские сертификаты проверяются в модуле «Efros NAC» с использованием протокола OCSP;<br>— «Активен» ( ) – проверка не выполняется.<br><br>При активации переключателя появляются дополнительные поля |
| Элементы управления | |
| Создать | При нажатии кнопки выполняется сохранение внесенных данных |
| Отменить | При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных |

## 3.10 Разрешенные MAC-адреса

С помощью подраздела «Разрешенные MAC-адреса» можно вести список MAC-адресов, по которым могут аутентифицироваться устройства (конечные точки).

На странице перечень разрешенных MAC-адресов реализован в виде списка (рис. 55).

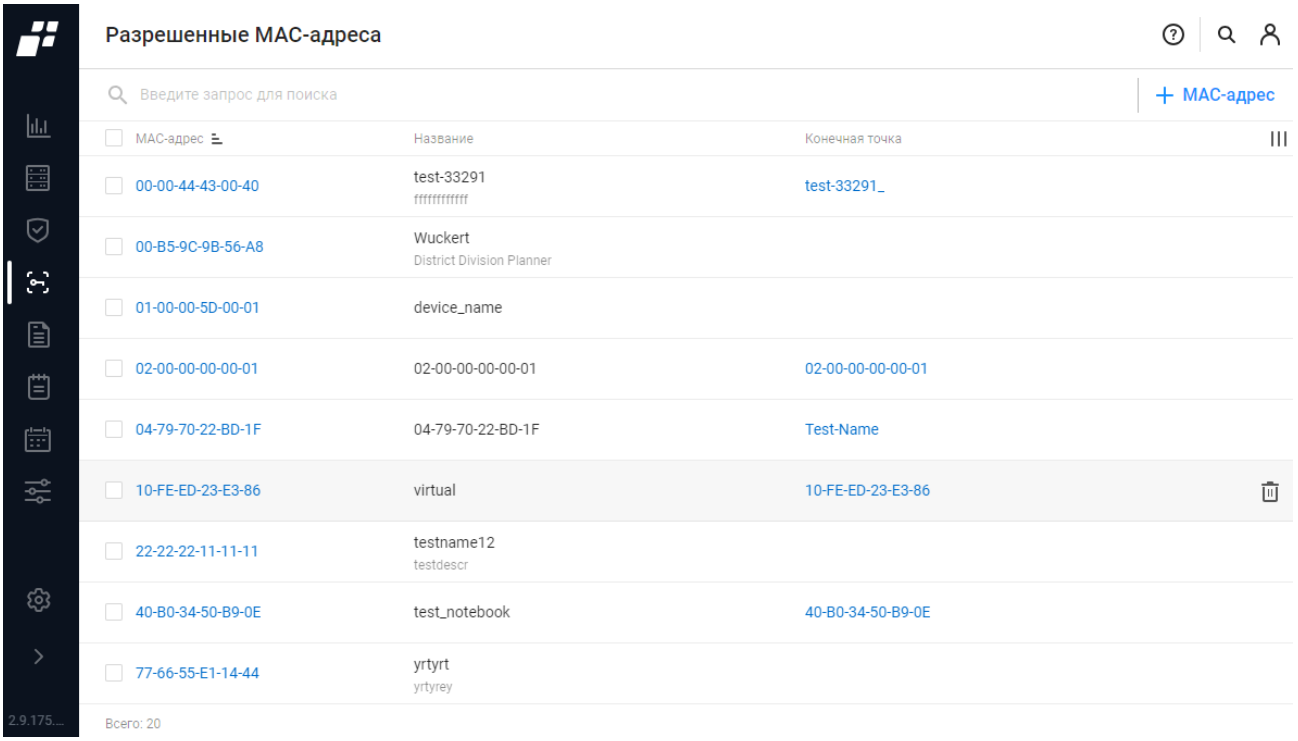



Рисунок 55 – Страница «Разрешенные MAC-адреса»

Для каждой записи списка отображаются данные:

- поле для флага;
- MAC-адрес – является ссылкой, при нажатии откроется страница редактирования разрешенного MAC-адреса конечной точки;
- название – содержит название и описание MAC-адрес конечной точки;
- конечная точка – название конечной точки в разделе «Объекты сети» → «Конечные точки». Является ссылкой, при нажатии откроется страница свойств конечной точки.

Над списком располагаются:

- поле поиска ( Введите запрос для поиска );
- кнопка «MAC-адрес» ( + MAC-адрес ).

При установке флага в строке с необходимым MAC-адресом над списком появляется кнопка «Удалить» ( ), которая позволяет удалить выбранный MAC-адрес.

Аналогичная кнопка появляется в правой части экрана в строке с MAC-адресом.

Более подробно о рекомендуемой последовательности действий для настройки доступа в сеть устройств по MAC-адресам написано в приложении В.

### 3.10.1 Создание разрешенного MAC-адреса

Для создания разрешенного MAC-адреса пользователю ПК «Efros DO» необходимо:

1) Нажать кнопку «MAC-адрес» ( + MAC-адрес ).
2) Откроется страница «Создание разрешенного MAC-адреса» (рис. 56). Заполнить поля необходимыми параметрами. Состав и описание полей страницы приведены в таблице 25.

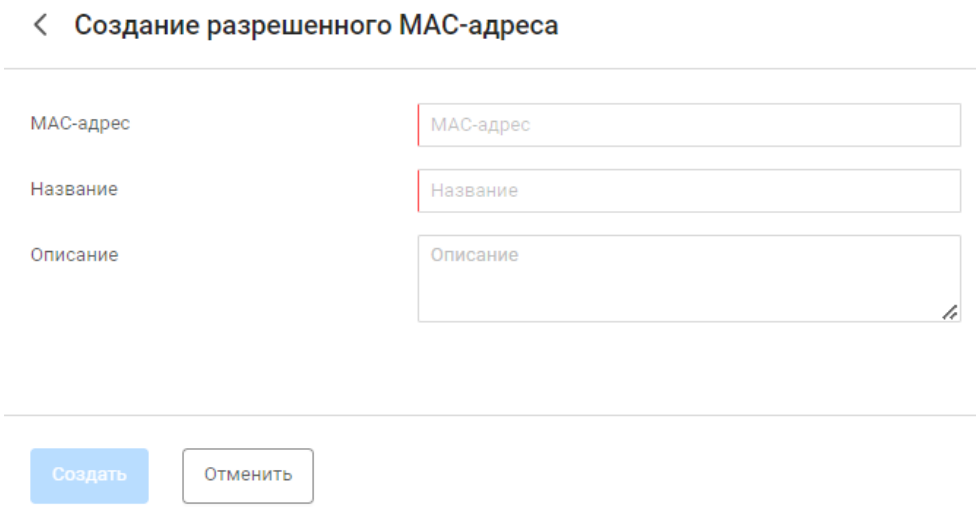



Рисунок 56 – Страница «Создание разрешенного MAC-адреса»

Таблица 25 – Состав и описание полей страницы создания разрешенного MAC-адреса

| Поле | Описание |
|---|---|
| Поле «MAC-адрес» | Поле для ввода MAC-адреса |
| Поле «Название» | Текстовое поле для ввода названия MAC-адреса.<br>Параметры ввода текста: от 1 до 50 символов.<br>Допустимые символы: буквы латинского алфавита, цифры, «_», «–» |
| Поле «Описание» | Текстовое поле для ввода описания MAC-адреса.<br>Параметры ввода текста: от 1 до 250 любых символов |
| Элементы управления | |
| Создать | При нажатии кнопки выполняется переход на страницу с MAC-адресами с сохранением внесенных данных |
| Отменить | При нажатии кнопки выполняется переход на страницу списка без сохранения внесенных данных |

## 3.11 Словари

Для обеспечения взаимодействия аутентификатора (коммутатора или точки доступа) с ПК «Efros DO» используются двоичные данные. В комплексе данные представлены в текстовой форме в виде словарей (рис. 57).

Страница состоит из следующих вкладок:

- «Системные» – словари, загруженные при установке комплекса. Вкладка активна по умолчанию;
- «Пользовательские» – словари, настроенные пользователем комплекса для типа оборудования, которое комплекс еще не поддерживает.

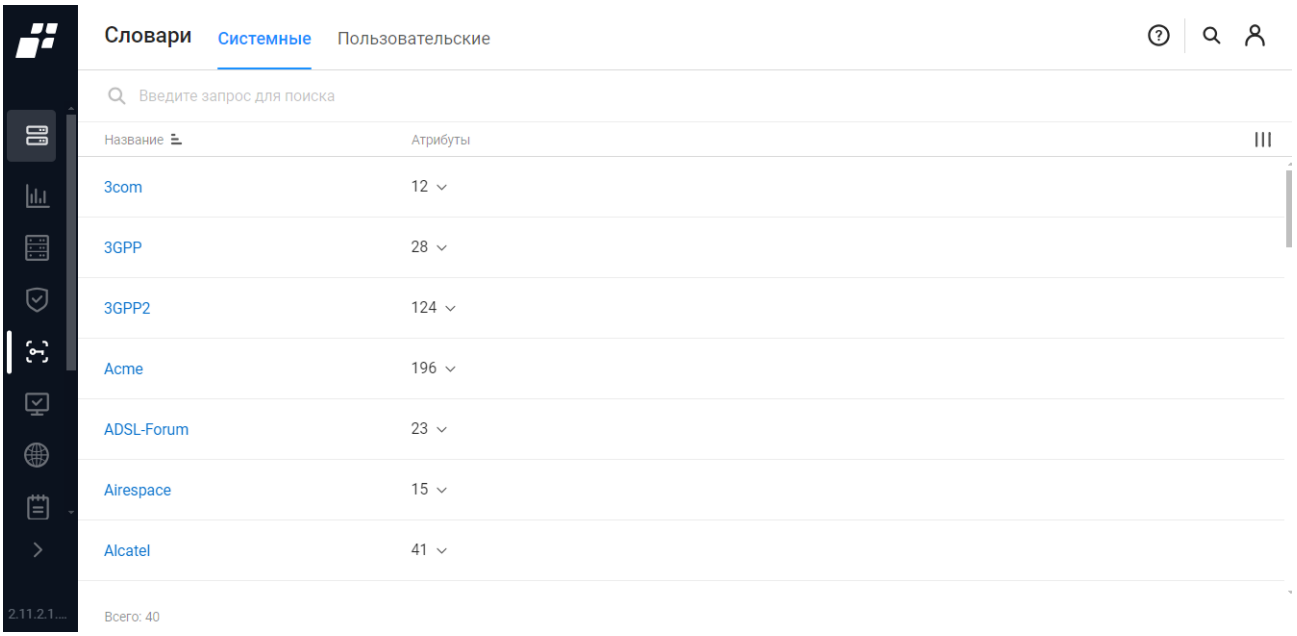



Рисунок 57 – Подраздел «Словари»

Словари содержат перечень атрибутов, тип данных и возможные значения, поддерживаемые протоколом, и применяются для создания и проверки данных пакетов, которыми обмениваются сетевое оборудование и сервер аутентификации.

Различные атрибуты и/или их значения используются в комплексе для настройки:

- профилей оборудования;
- профилей авторизации;
- политик доступа, а именно в основных условиях, правилах аутентификации и авторизации.

В ПК «Efros DO» используются следующие типы словарей:

1) Системные словари – это предустановленные словари, необходимые для обеспечения работоспособности протоколов RADIUS и TACACS+:
   a) Словари, используемые для RADIUS:
      - Gazinformservice – вспомогательный словарь. Содержит перечень

атрибутов, которые можно использовать для настройки правил доступа (описание приведено выборочно для наиболее используемых параметров, полный перечень атрибутов и допустимых значений приведен в подразделе «Словари»):

- GisAuthType – тип протокола аутентификации (CHAP, MS-CHAP, PAP);
- GisDomainName – название домена;
- GisEapAuthType – тип аутентификации EAP (GTC, MD5, MSCHAPv2, TLS);
- GisEapType – тип EAP (MD5, PEAP, TLS, TTLS);
- GisLdapName – название LDAP;
- GisNetworkDeviceName – имя аутентификатора;
- GisNetworkDeviceProfileName – профиль аутентификатора;
- GisRadiusFlowType – условия сценариев доступа, заданные в профиле оборудования (DeviceAdministration, RemoteAccessVPN, Wired802_1X, WiredMab, WiredWebAuth, Wireless802_1X, WirelessMab, WirelessWebAuth);
- GisRadiusPolicyAuthRuleName – название сработавшего правила аутентификации;
- GisRadiusPolicyAuthzRuleName – название сработавшего правила авторизации;
- GisRadiusPolicyName – название сработавшей политики.

б) FreeRadius;

— Radius – поддержка базовой функциональности протокола RADIUS, определенного в стандарте RFC 2865. В случае, если производитель оборудования не поддерживает атрибуты и значения, указанные в стандарте, может быть нарушена работоспособность протокола. Также, данный словарь содержит некоторые дополнительные атрибуты, необходимые для работы комплекса. Описание приведено выборочно для наиболее используемых параметров, полный перечень атрибутов и допустимых значений приведен в подразделе «Словари»:

- Called-station-id – обычно содержит адрес моста или точки доступа;
- Calling-station-id – MAC-адрес устройства, запрашивающего аутентификацию;
- NAS-Identifier – "DA-vWLC";
- NAS-IP-Address – IP-адрес сервера NAS, который запрашивает аутентификацию клиента;
- Nas-port – номер порта сервера NAS, который аутентифицируется клиентом;
- NAS-Port-Type – тип физического порта NAS, где аутентифицируется клиент. Атрибут может использоваться вместо или в добавление к атрибуту NAS-Port. Например, если

пользователь осуществил удаленный доступ (Telnet) в NAS, для того чтобы аутентифицировать себя как внешнего пользователя, запрос Access-Request может включать атрибут NAS-Port-Type = Virtual в качестве подсказки серверу RADIUS, что пользователь не является физическим портом;

- User-name – имя пользователя, для которого выполняется аутентификация. В случае, если аутентификация выполняется для устройства – в данном атрибуте может передаваться hostname устройства;
- Service-Type – тип услуг, которые запросил или получит клиент:
  - *Administrative – пользователю предоставляется доступ к административному интерфейсу NAS, с которого могут выполняться привилегированные команды;*
  - *Authenticate Only – запрашивается только аутентификация, не нужно возвращать никакой авторизационной информации Access-Accept.*

— словари, название которых соответствует названию производителя сетевого оборудования – многие производители могут использовать собственные атрибуты для реализации необходимой функциональности. В случае, если необходимый словарь отсутствует, можно добавить пользовательский словарь с необходимыми атрибутами и значениями либо обратиться в службу технической поддержки.

в) Словари, используемые для TACACS+:

— Calix;
— Internal;
— RFC8907 – используется для передачи значений, заданных в профиле авторизации доступа на оборудование с типом настроек «Shell;
— TACACS.

2) Пользовательские словари. Словари, созданные пользователем в комплексе.

3) Псевдословари – словари с динамически формирующимися значениями атрибутов:

а) Словари, используемые для TACACS+:

— AdDomainGroups – доменная группа. Используется при формировании условий правил авторизации для проверки наличия клиента в выбранной группе. Группы для проверки должны быть предварительно выбраны на странице соединения Active Directory в разделе «Настройки/Источники данных/Active Directory»;
— DHCP – параметры от источника профилирования DHCP;
— EndPointGroups – группа конечных точек;

- EndPoints – конечная точка. Атрибуты словаря:
  - BaseProfile – название примененного профиля;
  - MAC – MAC-адрес конечной точки;
  - VendorName – название производителя оборудования, определенного по MAC-адресу;
  - Tag – метка конечной точки.
- NetUserGroups – группа сетевых пользователей;
- NetUsers – сетевой пользователь.

б) Словари, используемые для RADIUS:
- EDO;
- Device – сетевое оборудование;
- NetUserGroups – группы сетевых пользователей;
- NetUsers – сетевой пользователь.

в) Словари, используемые для профилирования:
- CDP;
- DHCP;
- EdoAgent;
- LLDP;
- RADIUS;
- SNMP;
- UserAgent.

### 3.11.1 Вкладка «Системные»

При установке комплекса системные словари автоматически загружаются и отображаются на данной вкладке. Атрибуты системного словаря доступны только для просмотра и чтения.

Атрибут системного словаря отображается с описательным именем атрибута, внутренним именем, понятным для домена, и допустимыми значениями.

На странице список системных словарей реализован в виде таблицы. Для каждой записи списка отображаются следующие данные:

название – является ссылкой, при переходе по которой открывается окно с описанием словарей выбранного производителя;

атрибуты – раскрывающийся список атрибутов, зависящий от производителя.

Над списком с системными словарями располагаются:

- поле поиска (  );
- кнопка «Колонки» (  ).

### 3.11.2 Вкладка «Пользовательские»

Пользовательские словари – это словари, созданные пользователем комплекса для нового типа оборудования, производитель которого не добавлен в базу данных комплекса.

На странице список пользовательских словарей реализован в виде таблицы (рис. 58).

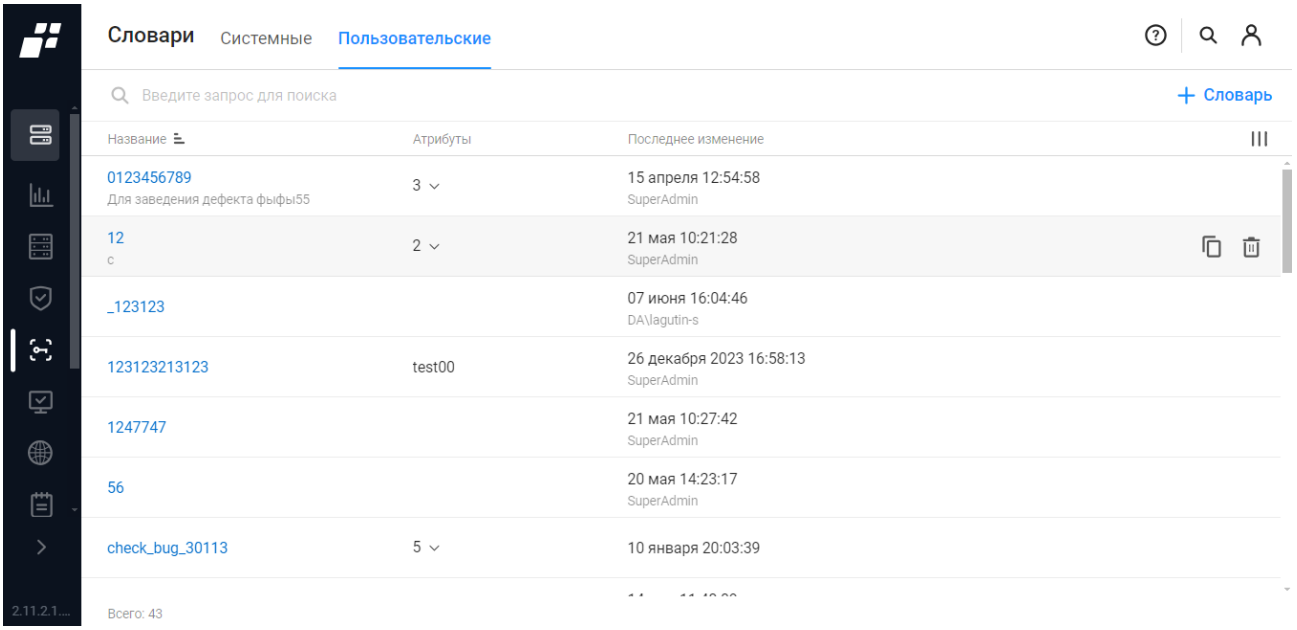



Рисунок 58 – Вкладка «Пользовательские»

Для каждой записи списка отображаются следующие данные:

- название – является ссылкой, при переходе по которой открывается окно редактирования выбранного пользовательского словаря;
- атрибуты – числовое значение, обозначающее количество атрибутов в данном словаре;
- последнее изменение – дата последнего изменения словаря.

Над списком с пользовательскими словарями располагаются:

- поле поиска ( Введите запрос для поиска );
- кнопка «Словарь» ( + Словарь );
- кнопка «Колонки» ( ).

Кнопки, появляющиеся в правой части экрана в строке с выбранным пользовательским словарем:

- кнопка «Создать копию» ( );
- кнопка «Удалить» ( ).

Аналогичные кнопки появляются в правой части экрана в строке пользовательского словаря.

### 3.11.3 Создание пользовательского словаря

Для создания пользовательского словаря необходимо выполнить следующее:

1) Нажать над списком кнопку «Словарь» ( + Словарь ).
2) Откроется страница создания нового словаря (рис. 59). Состав и описание полей страницы приведены в таблице 26.

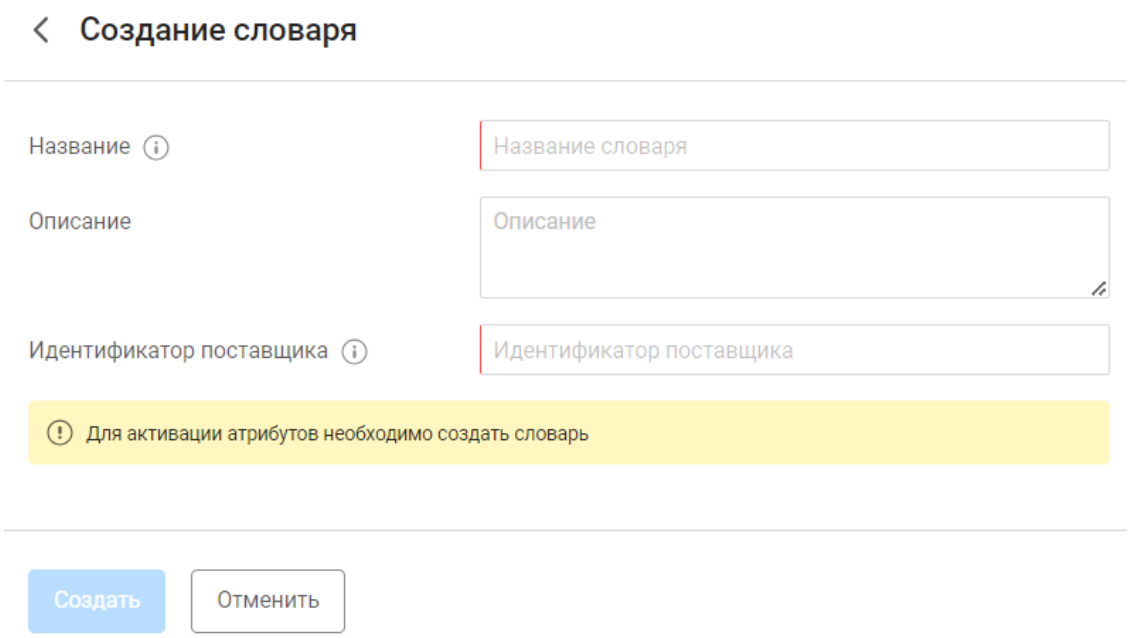



Рисунок 59 – Страница создания нового пользовательского словаря

Таблица 26 – Состав и описание полей окна создания нового пользовательского словаря

| Поле | Описание |
|---|---|
| Поле «Название» | Текстовое поле для ввода названия словаря.<br>Не более 250 символов. Допустимые символы: латинские буквы, цифры и символы "_", "-" |
| Поле «Описание» | Текстовое поле для ввода описания словаря |
| Поле «Идентификатор поставщика» | Номер, создаваемый пользователем комплекса.<br>Требования, которым должно соответствовать содержание поля: цифры от 0 до 9. Максимальное значение: 16777215, минимальное: 1 |
| Элементы управления | |
| Создать | При нажатии кнопки выполняется переход на страницу списка словарей с сохранением внесенных данных |
| Отменить | При нажатии кнопки выполняется переход на страницу списка без сохранения внесенных данных |

3) Заполнить поля страницы необходимыми параметрами.
4) Нажать кнопку «Создать». Произойдет автоматический переход на страницу добавления атрибутов в созданный словарь (рис. 60). Атрибуты можно добавить двумя способами:
   — по нажатию кнопки «Добавить атрибут» ( Создать атрибут ) (см. рис. 60) в центре страницы;
   — по нажатию кнопки «Атрибут» ( + Атрибут ).

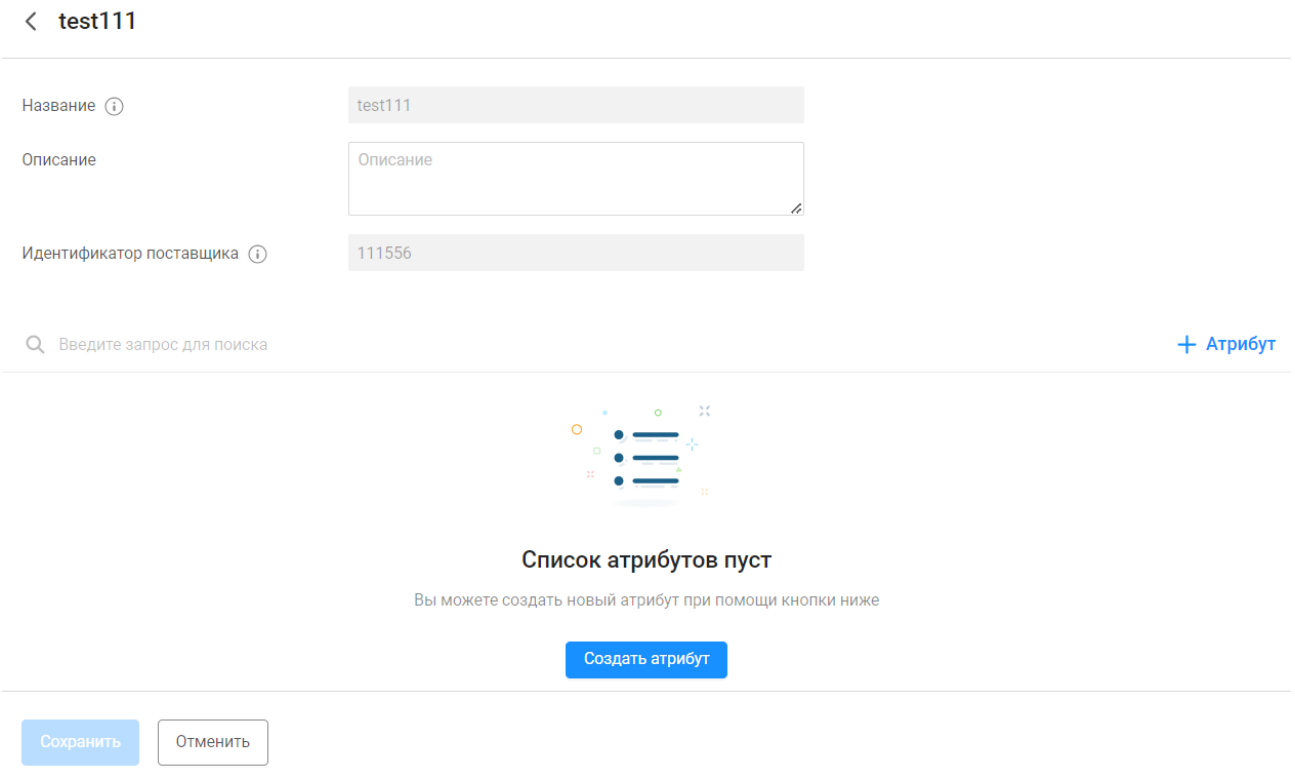



Рисунок 60 – Страница добавления атрибутов в созданный словарь

5) Откроется страница «Создание атрибута» (рис. 61). Состав и описание полей страницы приведены в таблице 27.

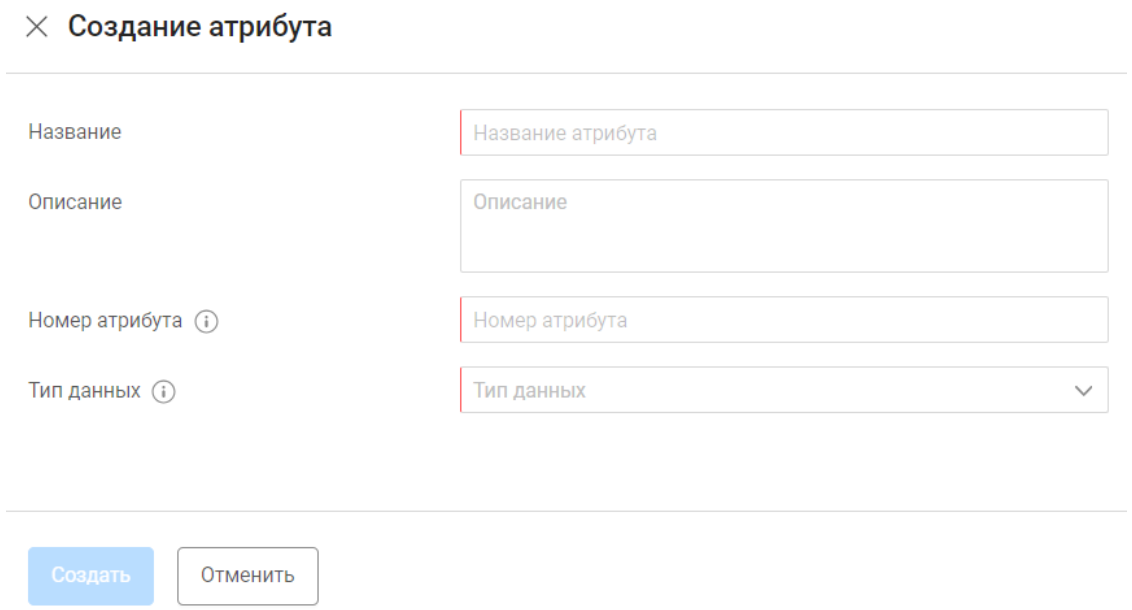



Рисунок 61 – Страница «Создание атрибута»

Таблица 27 – Состав и описание полей страницы создания нового атрибута

| Поле | Описание |
|---|---|
| Поле «Название» | Название атрибута |
| Поле «Описание» | Краткое описание атрибута |
| Поле «Номер атрибута» | Уникальный номер в рамках словаря |
| Поле «Тип данных» | Поле с раскрывающимся списком |
| Поле «Допустимые значения» | Список допустимых значений атрибутов словаря RADIUS, их описание и возможные принимаемые значения приведены в документе «RFC 2865 Remote Authentication Dial In User Service (RADIUS)».<br>Для сохранения добавленного значения необходимо нажать кнопку «✓». Для очистки полей – кнопку «✕». Кнопки «🗑» и «⧉» позволяют удалить или копировать атрибут |
| Элементы управления | |
| Создать | При нажатии кнопки выполняется переход на страницу со списком атрибутов созданного словаря с сохранением внесенных данных |
| Отменить | При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных |

## 3.12 Гостевые порталы

Подраздел «Гостевые порталы» предназначен для идентификации и контроля доступа внешних пользователей, осуществляющих подключение к публичной беспроводной сети. «Гостевой портал» представляет собой веб-страницу, на которую перенаправляются гостевые пользователи для прохождения процедуры аутентификации при попытке получения доступа к сети.

На странице ПК «Efros DO» перечень гостевых порталов реализован в виде списка (рис. 62).

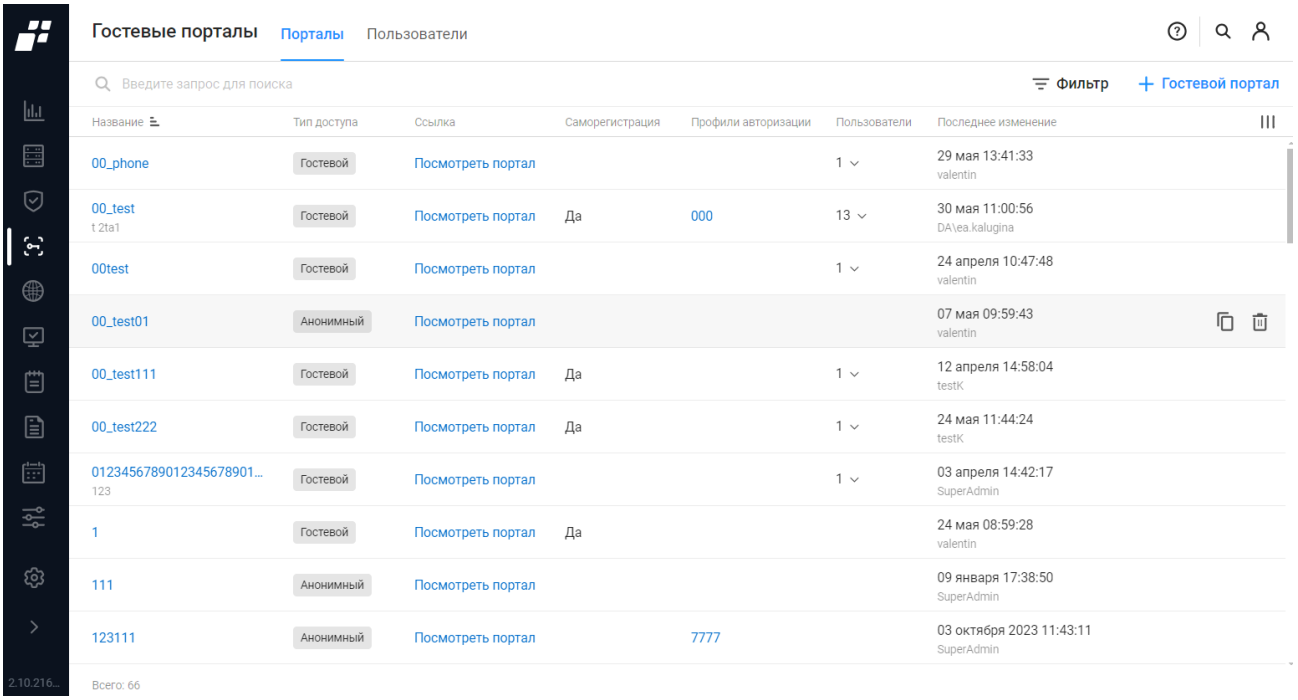



Рисунок 62 – Подраздел «Гостевой портал»

Страница состоит из вкладок:

- «Порталы»;
- «Пользователи».

Более подробно о рекомендуемой последовательности настройки доступа в сеть с использованием гостевого портала написано в приложении Г.

### 3.12.1 Вкладка «Порталы»

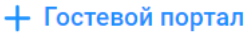
На странице вкладки «Порталы» список созданных гостевых порталов реализован в виде таблицы (см. рис. 62). Для каждой записи таблицы отображаются данные:

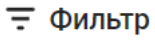
- название – является ссылкой, при переходе по которой открывается окно редактирования настроек гостевого портала;
- тип доступа – гостевой или анонимный;
- ссылка на страницу гостевого портала;
- саморегистрация – наличие или отсутствие;

— профили авторизации – раскрывающийся список профилей, которые являются ссылками;
— пользователи гостевого портала;
— дата изменения гостевого портала.

Над таблицей располагаются:

— поле поиска ( 

 );
— кнопка «Гостевой портал» ( 

 );
— кнопка «Фильтр» ( 

 );
— кнопка «Колонки» (  ).

Кнопки, появляющиеся в правой части экрана в строке списка гостевых порталов:

— кнопка «Создать копию» (  );
— кнопка «Удалить» (  ).

### 3.12.1.1 Создание гостевого портала

Добавление нового гостевого портала выполняется пользователем вручную. Предварительно должна быть уже настроена точка доступа (контроллер доступа). Для создания гостевого портала пользователю необходимо выполнить следующие шаги:

1) Нажать кнопку «Гостевой портал» ( 

 ).
2) Откроется страница создания гостевого портала. При выборе типа доступа «Гостевой» или «Анонимный» выводится различный состав полей для заполнения (рис. 63, 64). Состав и описание полей страницы приведены в таблице 28.
3) Заполнить поля страницы соответствующими данными.

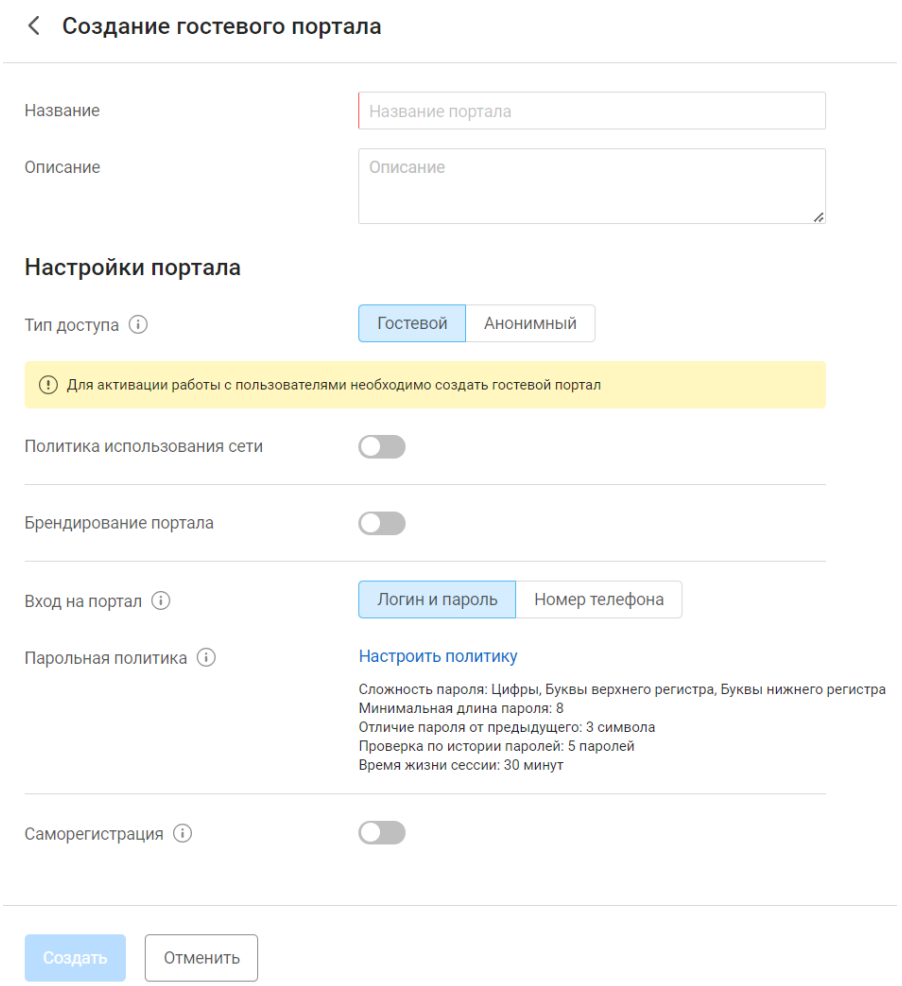



Рисунок 63 – Страница создания гостевого портала. Тип доступа «Гостевой»

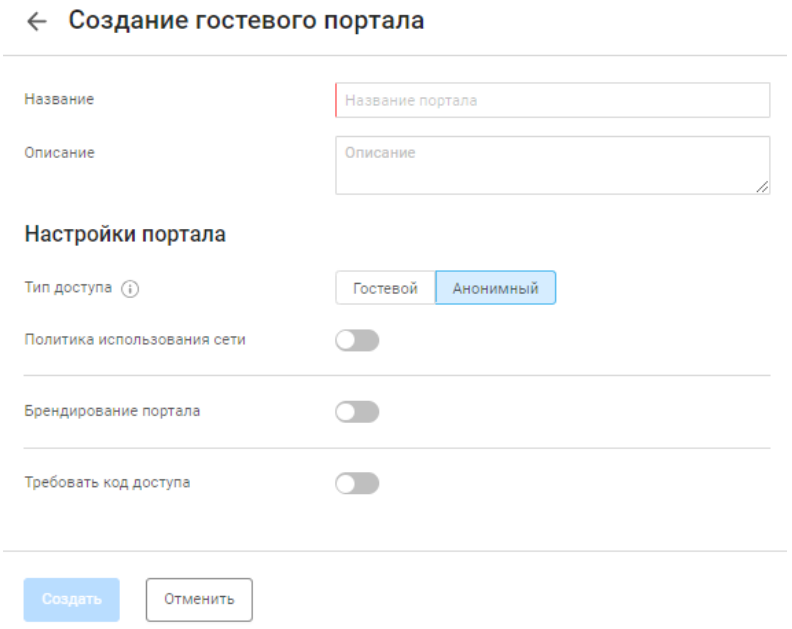



Рисунок 64 – Страница создания гостевого портала. Тип доступа «Анонимный»

Таблица 28 – Состав и описание полей страницы создания гостевого портала

| Поле | Описание |
|---|---|
| Поле «Название» | Текстовое поле для ввода названия гостевого портала.<br>Параметры ввода текста: от 1 до 50 символов.<br>Дополнительные символы: буквы латинского алфавита, цифры, «_», «–» |
| Поле «Описание» | Текстовое поле для ввода описания пользователя.<br>Параметры ввода текста: от 1 до 250 любых символов |
| Группа полей «Настройки портала» | |
| Поле «Тип доступа» | Переключатель:<br>— «Гостевой»;<br>— «Анонимный».<br><br>Тип доступа невозможно изменить после создания гостевого портала |
| Поле «Политика использования сети» | Переключатель:<br>— «Активен» ( ) – политика использования (лицензионное соглашение) активирована. На веб-странице входа на гостевой портал появляется надпись «Продолжая, вы подтверждаете согласие с политикой использования сети»;<br>— «Неактивен» ( ) – политика использования (лицензионное соглашение) не активирована.<br><br>При активации переключателя появляется дополнительное поле «Текст политики» |
| Поле «Текст политики» | Содержит кнопку «Добавить», при нажатии на которую открывается окно для добавления текста политики использования сети.<br>На веб-странице входа на гостевой портал появится ссылка, которая содержит введенный текст политики |
| Поле «Брендирование портала» | Переключатель:<br>— «Активен» ( ) – позволяет настроить внешний вид портала. При активации появляются дополнительные поля;<br>— «Неактивен» ( ) – отключает дополнительные поля для настройки внешнего вида гостевого портала |
| Поле «Логотип» | Позволяет загрузить логотип портала.<br>Рекомендуемое разрешение: 200x160px.<br>Поддерживаемые форматы: png, svg, jpeg.<br>Максимальный размер: 5 МБ |
| Поле «Задний фон» | Позволяет загрузить задний фон портала в виде картинки.<br>Рекомендуемый размер 1920x1080px.<br>Поддерживаемые форматы: png, jpeg.<br>Максимальный размер: 5 МБ |
| Поле «Корпоративный | Цветовая шкала для выбора корпоративного цвета портала (цвет |

| Поле | Описание |
|---|---|
| цвет» | кнопок подключения и цвет знаков успешного соединения) |
| Блок полей для типа доступа «Гостевой» | |
| Поле «Вход на портал» | Переключатель:<br>— «Логин и пароль» – вход на гостевой портал для пользователя осуществляется по вводу логина и пароля. При выборе появляется дополнительное поле «Парольная политика»;<br>— «Номер телефона» – вход на гостевой портал для пользователя осуществляется по номеру телефона и ввода кода проверки. При выборе появляется блок полей «Подтверждение учетных данных», в котором нужно выбрать требуемый «SMS-провайдер»<br><br>Значение невозможно изменить после создания гостевого портала |
| Поле «Парольная политика» | Содержит ссылку для перехода в окно «Парольная политика».<br>Перечень настраиваемых параметров:<br>— сложность пароля: настроенные параметры применяются при создании учетной записи гостевого пользователя администратором на вкладке «Пользователи» либо пользователем самостоятельно через портал;<br>— время жизни сессии: период после открытия веб-страницы входа на гостевой портал до успешного подключения к сети. По истечении времени пользователю необходимо повторно подключиться к гостевому порталу.<br><br>Парольная политика доступна при выборе варианта входа на портал «Логин и пароль».<br><br>Парольная политика влияет только на пользователей текущего гостевого портала |
| Поле «Саморегистрация» | Переключатель:<br>— «Активен» ( ) – возможность для пользователей самостоятельно создавать учетные записи на веб-странице входа на гостевой портал;<br>— «Неактивен» ( ).<br><br>При активации переключателя появляются дополнительные поля |
| Поле «Поля для заполнения» | Выбранные поля будут отображаться при создании учетной записи пользователем и обязательны для заполнения:<br>— «ФИО»;<br>— «Компания»;<br>— «E-mail» – при выборе появляется блок полей |

| Поле | Описание |
|---|---|
| | «Подтверждение учетных данных», в котором можно выбрать подтверждение e-mail;<br>— «Телефон» – при выборе появляется блок полей «Подтверждение учетных данных», в котором можно выбрать подтверждение номера телефона;<br>— «Комментарий (необязательное)» |
| Поле «Удалять при неактивности» | Переключатель:<br>— «Активен» ( ) – удаление учетной записи, созданной гостевым пользователем самостоятельно, при неактивности больше указанного периода;<br>— «Неактивен» ( ).<br><br>При активации переключателя появляется дополнительное поле «Период неактивности» |
| Поле «Период неактивности» | Поле для ввода количества дней периода неактивности, после которого произойдет удаление учетной записи, созданной гостевым пользователем самостоятельно |
| Поле «Требовать код при регистрации» | Переключатель:<br>— «Активен» ( ) – при создании учетной записи пользователем необходимо дополнительно ввести код, заданный в поле «Код доступа»;<br>— «Неактивен» ( ).<br><br>Переключатель «Требовать код при регистрации» доступен при выборе варианта входа на портал «Логин и пароль».<br>При активации переключателя появляется дополнительное поле «Код доступа» |
| Поле «Код доступа» | Поле для ввода кода доступа, запрашиваемый при создании учетной записи. При необходимости код можно сгенерировать, нажав на кнопку «Сгенерировать код» |
| Поле «Статус при саморегистрации» | Переключатель:<br>— «Активный» – пользователь портала получает доступ к ресурсам сразу после регистрации;<br>— «Заблокированный» – изменение статуса производится пользователем комплекса |
| Блок полей «Подтверждение учетных данных», выводится при выборе поля для заполнения «Телефон» или вход на портал по номеру телефона | |
| Поле «Номер телефона» | Переключатель:<br>— «Не подтверждать»;<br>— «Подтверждать» – при входе на гостевой портал требуется подтвердить учетные данные вводом кода, который придет по номеру телефона. |

| Поле | Описание |
|---|---|
| | При выборе значения «Подтверждать» появляется дополнительное поле «SMS-провайдер» |
| Поле «SMS-провайдер» | Раскрывающийся список для выбора SMS-провайдера.<br>Предварительно необходимо произвести настройку внешней системы «SMS-провайдеры» в разделе «Настройки» |
| Блок полей «Подтверждение учетных данных», выводится при выборе поля для заполнения «E-mail» | |
| Поле «E-mail» | Переключатель:<br>— «Не подтверждать»;<br>— «Exchange» – при входе на гостевой портал требуется подтвердить учетные данные вводом кода, который придет по Microsoft Exchange на указанный e-mail;<br>— «SMTP» – при входе на гостевой портал требуется подтвердить учетные данные вводом кода, который придет по SMTP на указанный e-mail.<br>Предварительно необходимо произвести настройку серверов отправки «Почтовые серверы» в разделе «Настройки» |
| Блок полей для типа доступа «Анонимный» | |
| Поле «Требовать код доступа» | Переключатель:<br>— «Активен» ( ) – код для подключения к сети, вводимый на веб-странице входа на гостевой портал.;<br>— «Неактивен» ( ).<br>При активации переключателя появляется поле «Код доступа» |
| Поле «Код доступа» | Поле для ввода кода доступа, запрашиваемый при входе на гостевой портал. При необходимости код можно сгенерировать, нажав на кнопку «Сгенерировать код» |
| Элементы управления | |
| Создать | При нажатии кнопки выполняется переход на страницу списка гостевых порталов с сохранением внесенных данных |
| Отменить | При нажатии кнопки выполняется переход на страницу списка без сохранения внесенных данных |

После создания гостевого портала автоматически создается метка с названием гостевого портала: (GuestPortal) <название портала>.

Метка гостевого портала будет автоматически присвоена устройству гостевого пользователя (конечной точке, с которой выполняется подключение к сети) успешно прошедшего аутентификацию на гостевом портале.

Метки гостевого портала у конечных точек очищаются ежедневно в 00:00 (часов:минут). Это необходимо для повторного прохождения гостевыми пользователями процедуры аутентификации для получения доступа к сети.

При удалении гостевого портала соответствующие метки у конечных точек автоматически удаляются.

Для просмотра созданного гостевого портала необходимо нажать на ссылку «Посмотреть портал».

### 3.12.2 Вкладка «Пользователи»

На странице вкладки «Пользователи» список пользователей гостевых порталов реализован в виде таблицы (рис. 65).

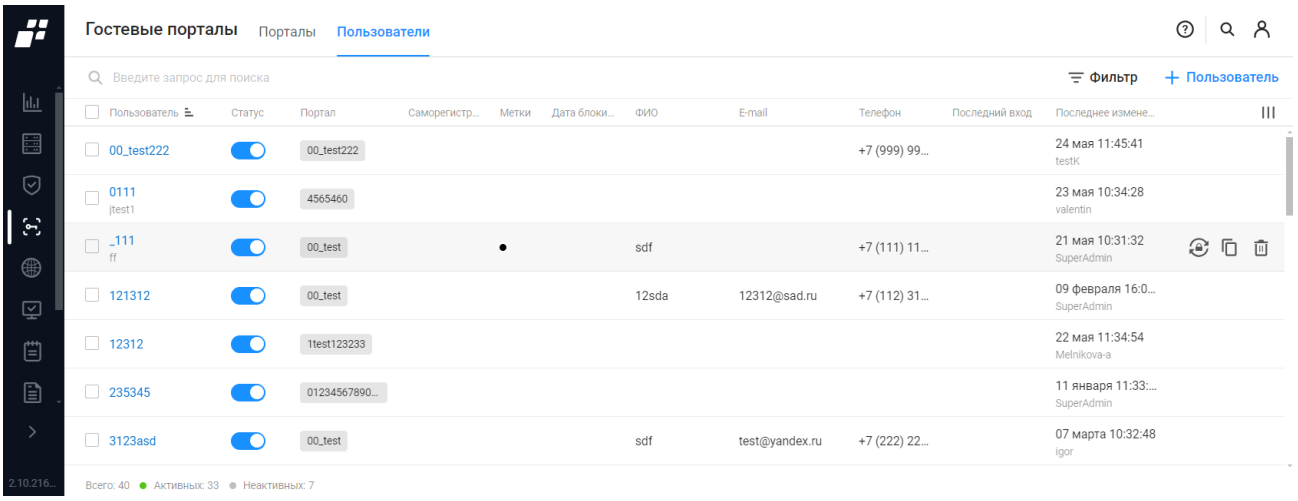


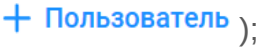
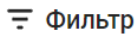

Рисунок 65 – Вкладка «Пользователи»

Для каждой записи таблицы отображаются данные:

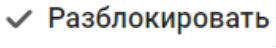
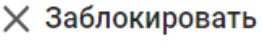
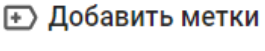
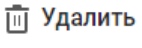
- пользователь – является ссылкой, при переходе по которой открывается окно для редактирования данных пользователя;
- статус (активен/неактивен)
- портал – название портала, к которому у пользователя есть доступ;
- саморегистрация. Значение «Да» в случае, если регистрация осуществлялась пользователем самостоятельно. Если пользователь создавался в комплексе, значение остается пустым;
- метки с названием гостевого портала;
- дата блокировки учетной записи пользователя;
- Ф.И.О. пользователя;
- E-mail пользователя;
- телефон пользователя;
- дата последнего входа;

— дата последнего изменения пользователем ПК «Efros DO»;
— компания, где работает пользователь;
— комментарий.

Над таблицей располагаются:

— поле поиска (  );
— кнопка «Пользователь» (  );
— кнопка «Фильтр» (  );
— кнопка «Колонки» (  ) для изменения отображения колонок на странице.

При установке флага в строке с необходимым гостевым порталом над списком появляются следующие кнопки:

— кнопка «Разблокировать» (  );
— кнопка «Заблокировать» (  );
— кнопка «Добавить метки» (  );
— кнопка «Удалить» (  ).

При выборе строки с необходимым пользователем в правом углу строки появляются следующие кнопки:

— кнопка «Изменить пароль» (  ) – для пользователя гостевого портала с вариантом входа на портал «Логин и пароль»;
— кнопка «Создать копию» (  );
— кнопка «Удалить» (  ).

### 3.12.2.1 Создание пользователя гостевого портала

Для создания пользователя необходимо выполнить следующие действия:

1) Нажать на странице «Пользователи» кнопку «Пользователь» (  ).
2) Откроется страница «Создание пользователя портала» (рис. 66). Заполнить поля необходимыми параметрами. Состав и описание полей страницы приведены в таблице 29.

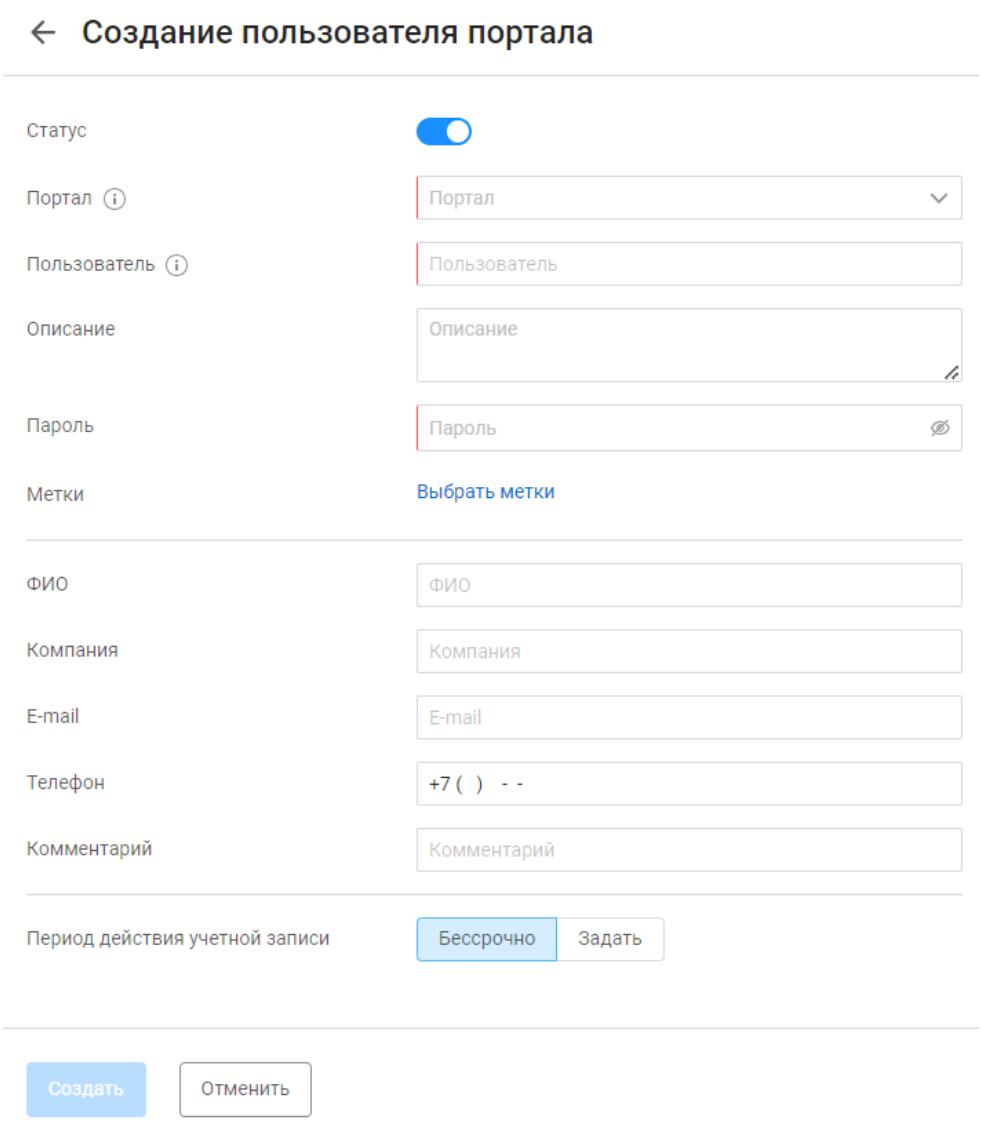



Рисунок 66 – Страница «Создание пользователя портала»

Таблица 29 – Состав и описание полей страницы создания пользователей портала

| Поле | Описание |
|---|---|
| Поле «Статус» | Переключатель:<br>— «Активен» ( ) – пользователю разрешен доступ к порталу;<br>— «Неактивен» ( ) – пользователю запрещен доступ к порталу |
| Поле «Портал» | Раскрывающийся список доступных порталов |
| Поле «Пользователь» | Текстовое поле для ввода логина пользователя.<br>Параметры ввода текста: от 1 до 32 символов.<br>Дополнительные символы: буквы латинского алфавита, цифры, «_», «–» |

| Поле | Описание |
|---|---|
| Поле «Описание» | Текстовое поле для ввода описания пользователя.<br>Параметры ввода текста: от 1 до 250 любых символов |
| Поле «Пароль» | Текстовое поле для ввода пароля пользователя.<br>Поле доступно при выборе варианта входа на портал «Логин и пароль» |
| Поле «Метки» | Ссылка для выбора меток |
| Поле «ФИО» | Текстовое поле для ввода фамилии, имени и отчества пользователя.<br>Параметры ввода текста: от 1 до 250 любых символов |
| Поле «Компания» | Текстовое поле для ввода названия компании, где работает пользователь.<br>Параметры ввода текста: от 1 до 250 любых символов |
| Поле «E-mail» | В поле указывается почтовый адрес пользователя для привязки к почте аккаунта пользователя |
| Поле «Телефон» | Текстовое поле для ввода номера телефона пользователя.<br>Параметры ввода текста: от 1 до 50 символов.<br>Допустимые символы: цифры и символы «-», «+», «()» |
| Поле «Комментарий» | Текстовое поле для ввода комментария.<br>Параметры ввода текста: от 1 до 250 любых символов |
| Поле «Период действия учетной записи» | Переключатель:<br>— «Бессрочно» – учетная запись пользователя действует на гостевом портале без ограничений;<br>— «Задать» – учетная запись пользователя действует на гостевом портале определенный период времени.<br><br>При выборе «Задать» появляется поле «Дата блокировки» |
| Элементы управления | |
| Создать | При нажатии на кнопку окно создания пользователя закрывается, пользователь отображается в списке |
| Отменить | При нажатии на кнопку окно создания пользователя закрывается без сохранения данных |

# 4 Раздел «Агенты»

Раздел «Агенты» доступен пользователю для работы при наличии лицензии на функциональный модуль «Efros NAC».

Агент «Efros Defence Operations» (агент ПК «Efros DO» или агент) совместно с ПК «Efros DO» позволяет управлять доступом пользователей к корпоративным ресурсам при проводном и беспроводном подключении с учетом состояния защищенности рабочих мест и соответствия принятым в организации требованиям по информационной безопасности.

Раздел «Агенты» предоставляет следующие возможности:

- просмотр и настройка агентов, установленных на устройствах (конечных точках) и подключенные к комплексу;
- просмотр параметров устройства полученные при инвентаризации данных устройства;
- настройка политики безопасности;
- настройка политики контроля целостности до загрузки ОС;
- просмотр результатов проверки устройств на соответствие требованиям настроенных политик;
- настройка расписаний для установки и обновления требуемых компонентов.

Для выполнения проверки устройства на соответствие требованиям политики безопасности на этапе подключения к корпоративным ресурсам требуется использовать суппликант ПК «Efros DO» (суппликант).

Подробное описание локальной и удаленной установки агента ПК «Efros DO» и суппликанта ПК «Efros DO» на устройство приведено в документе «Руководство администратора».

Сценарии работы с агентом ПК «Efros DO» и суппликантом ПК «Efros DO» приведены в документе «Руководство пользователя. Часть 5. Агент «Efros Defence Operations».

## 4.1 Агенты

Агент ПК «Efros DO» выполняет сбор сведений об устройстве. На основе полученных данных определяется статус соответствия требованиям политики безопасности. Формирование списка агентов производится автоматически (рис. 67).

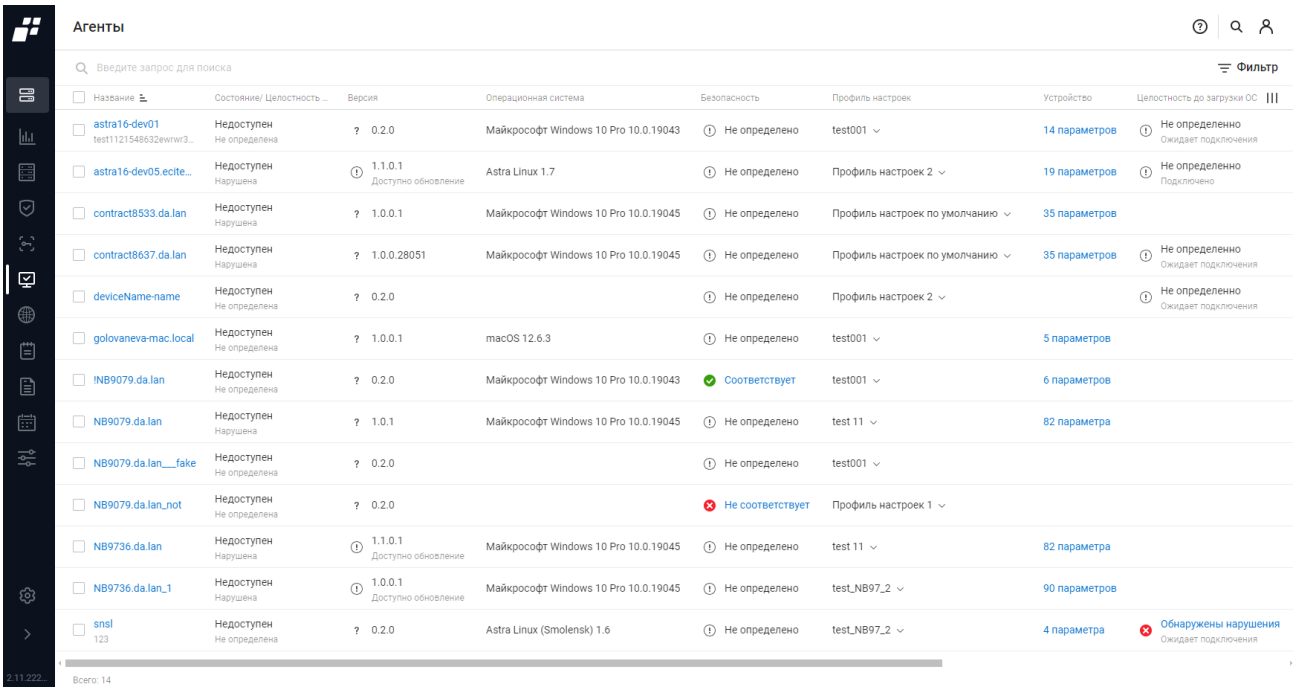



Рисунок 67 – Подраздел «Агенты»

Список агентов реализован в виде таблицы. Для каждой записи списка отображаются данные:

- название и описание агента. Является ссылкой, при переходе по которой открывается окно для просмотра и редактирования;
- состояние (активнен/ недоступен) и целостность агента (подтверждена/ нарушена/ не определена)
- версия агента и состояние версии (актуальная версия/ доступно обновление/ нет данных);
- операционная система, на которой установлен агент;
- безопасность – статус соответствия подключенного устройства требованиям политики безопасности (соответствует/ не соответствует/ не определено). Значения «Соответствуют» и «Не соответствуют» являются ссылкой, при переходе по которой открывается окно просмотра результата проверки подключенного устройства (см. п. 4.1.2);
- профиль настроек, который применяются к агенту. При нажатии на профиль в выпадающем окне выводятся настройки, заданные в выбранном профиле настроек;
- устройство. Является ссылкой, при переходе по которой открывается окно просмотра списка параметров устройства полученные при инвентаризации данных устройства;
- целостность до загрузки ОС – статус соответствия подключенного устройства требованиям политики контроля целостности до загрузки ОС (нарушения отсутствуют/ обнаружены нарушения/ не определено). Значение «Обнаружены нарушения» является ссылкой, при переходе по которой открывается окно

просмотра списка нарушений обнаруженные при проверке подключенного устройства (см. п. 4.1.3). Также для модуля контроля целостности отображается состояние подключения (подключено/ ожидает подключения/ ошибка подключения);
- политика контроля целостности, который применяется к устройству. При нажатии на политику в выпадающем окне выводятся количество объектов для ОС, заданные в выбранной политике;
- тип подключения к сети с устройства, на котором установлен агент, пользователь и дата выполнения последнего подключения;
- последнее изменение – дата внесения последних изменений для агента и имя пользователя ПК «Efros DO», вносившего последние изменения.

Над списком агентов располагаются:

- кнопка «Поиск» ( Введите запрос для поиска );
- кнопка «Фильтр» ( Фильтр );
- кнопка «Колонки» ( ).

При установке флага в строке с необходимым агентом над списком появляются следующие кнопки:

- кнопка «Профиль настроек» ( Профиль настроек );
- кнопка «Контроль целостности» ( Контроль целостности );
- кнопка «Обновить версию» ( Обновить версию );
- кнопка «Удалить» ( ).

Кнопка «Удалить» ( ) также появляется в правой части экрана при наведении курсора на строку списка.

### 4.1.1 Просмотр и редактирование настроек агента

Для просмотра и редактирования настроек агента пользователю необходимо:

1) На странице (см. рис. 67) нажать на название необходимого агента.
2) Откроется страница редактирования (рис. 68). На вкладке «Настройки» необходимо заполнить поля требуемыми параметрами и нажать кнопку «Сохранить». Состав и описание полей страницы приведены в таблице 30.
3) На вкладке «Дополнительно» выбранного агента доступен просмотр параметров устройства, полученные при инвентаризации данных устройства (рис. 69).

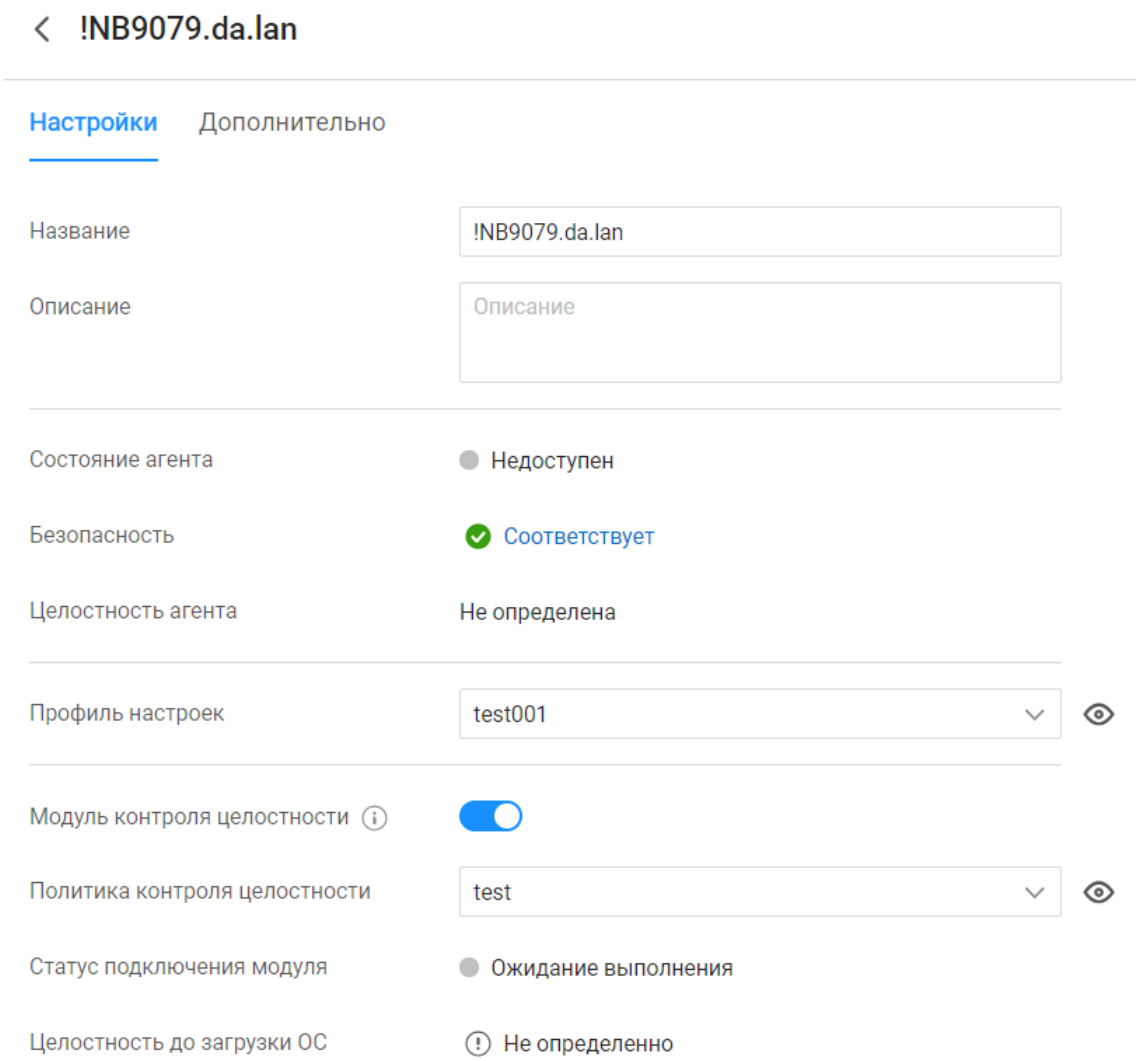



Рисунок 68 – Вкладка «Настройки» выбранного агента

Таблица 30 – Состав и описание полей окна редактирования агента

| Поле | Описание |
|---|---|
| Поле «Название» | Текстовое поле для ввода названия агента.<br>Параметры ввода текста: от 1 до 50 символов.<br>Допустимые символы: латинские буквы, цифры и символы «_», «-».<br>По умолчанию: содержит имя устройства, на котором установлен агент |
| Поле «Описание» | Текстовое поле для ввода описания агента.<br>Параметры ввода текста: от 1 до 250 любых символов |
| Поле «Состояние агента» | Статус доступности агента. Возможные значения:<br>— «Активен» – зеленый индикатор;<br>— «Недоступен» – серый индикатор.<br><br>Статус обновляется по результатам проверки активности |

| Поле | Описание |
|---|---|
| | подключенного агента |
| Поле «Безопасность» | Статус соответствия подключенного устройства требованиям политики безопасности. Возможные значения:<br>— «Соответствует»;<br>— «Не соответствует»;<br>— «Не определено».<br><br>Значения «Соответствуют» и «Не соответствуют» являются ссылкой, при переходе по которой открывается окно просмотра результата проверки подключенного устройства (см. п. 4.1.2) |
| Поле «Целостность агента» | Проверка целостности агента по контрольным суммам основных компонентов агента. Возможные значения:<br>— «Подтверждена»;<br>— «Нарушена»;<br>— «Не определена».<br><br>Периодичность проверки целостности компонентов агента можно настроить в подразделе «Профили настроек» |
| Поле «Профиль настроек» | Поле для выбора профиля настроек из раскрывающегося списка.<br>Поле содержит список созданных профилей.<br><br>Предварительно необходимо произвести настройку профиля в подразделе «Профили настроек» |
| Поле «Модуль контроля целостности» | Переключатель:<br>— «Активен» (  ) – применение политики контроля целостности объектов до загрузки операционной системы;<br>— «Неактивен» (  ) – политика контроля целостности не применяется.<br><br>При активации переключателя появляется дополнительное поле «Политика контроля целостности».<br><br>Для корректного выполнения проверки после изменения политики необходимо перезагрузить устройство с агентом |
| Поле «Политика контроля целостности» | Поле для выбора политики контроля целостности объектов до загрузки операционной системы из раскрывающегося списка.<br>Поле содержит список созданных политик.<br><br>Предварительно необходимо произвести настройку политик в подразделе «Наборы политик» |
| Поле «Статус подключения модуля» | Статус активации модуля контроля целостности до загрузки ОС. Возможные значения:<br>— «Ожидание выполнения» – отправлена команда подключения |

| Поле | Описание |
|---|---|
| | к модулю контроля целостности;<br>— «Подключен» – команда выполнена, модуль контроля целостности успешно подключен;<br>— «Ошибка подключения» – команда выполнена, при попытке подключения к модулю контроля целостности возникла ошибка.<br><br>Поле появляется после выбора политики контроля целостности |
| Поле «Целостность до загрузки ОС» | Статус проверки контроля целостности объектов до загрузки ОС. Возможные значения:<br>— «Нарушения отсутствуют» – модуль контроля целостности подключен, в ходе проверки целостности объектов ОС нарушений не обнаружены;<br>— «Обнаружены нарушения» – модуль контроля целостности подключен, в ходе проверки целостности объектов ОС обнаружены нарушения;<br>— «Не определено» – нет подключения к модулю контроля целостности или с момента последнего подключения к устройству были изменения в политике контроля целостности.<br><br>Поле появляется после выбора политики контроля целостности |
| Элементы управления | |
| Сохранить | При нажатии на кнопку окно редактирования агента закрывается с сохранением изменений |
| Отменить | При нажатии на кнопку окно создания заявки закрывается без сохранения данных |

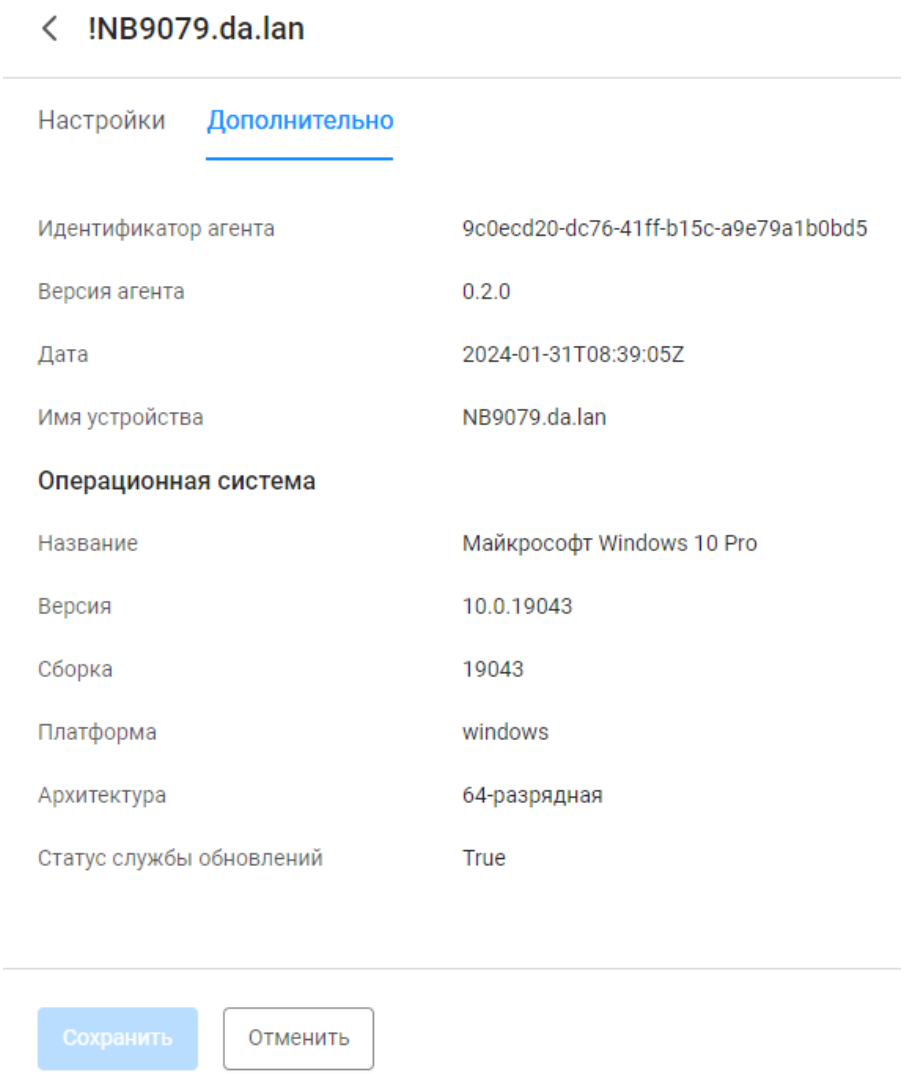



Рисунок 69 – Вкладка «Дополнительно» выбранного агента

### 4.1.2 Проверка требований политики безопасности

Результат проверки подключенного устройства на соответствие заданным требованиям политики безопасности приведен в колонке «Безопасность» подраздела «Агенты» (см. рис. 67) или на станице выбранного агента (см. рис. 68). Значения «Соответствуют» и «Не соответствуют» являются ссылкой, при переходе по которой открывается окно просмотра результата проверки подключенного устройства (рис. 70-71).

Проверка требований политики безопасности производится при наличии подключения агента ПК «Efros DO» к комплексу и предварительно настроенной политики безопасности.

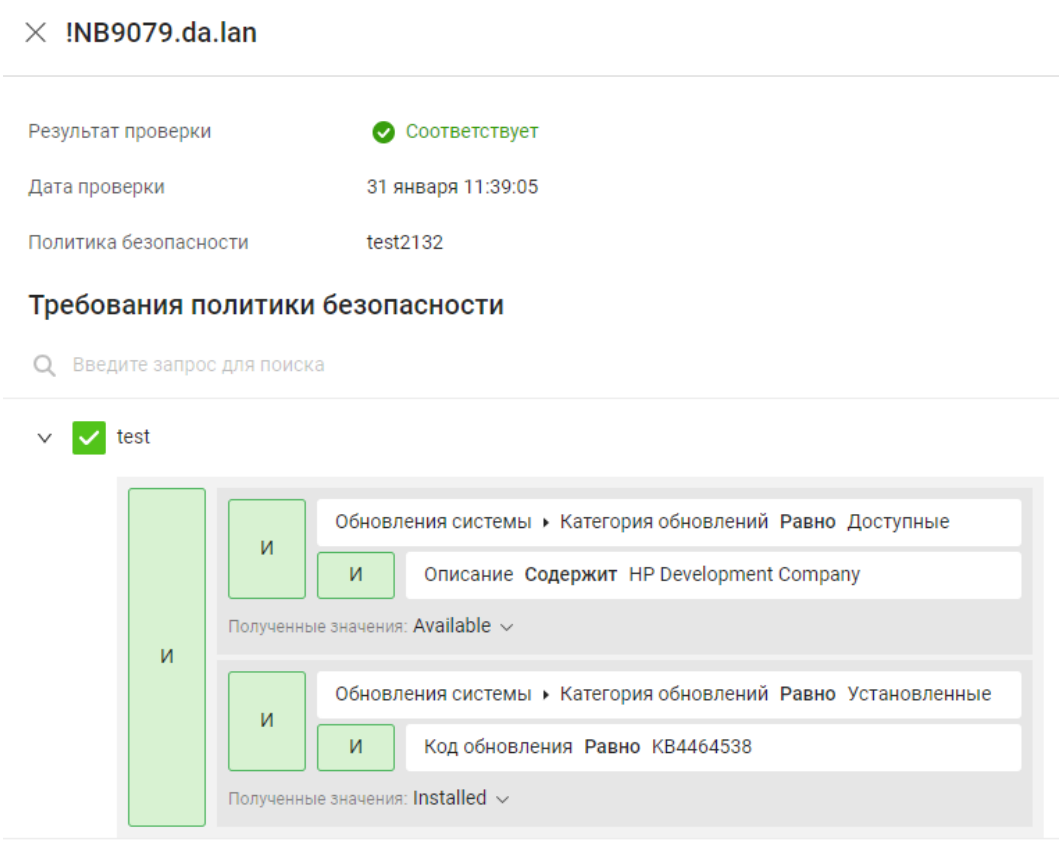



Рисунок 70 – Окно результата проверки «Соответствует»

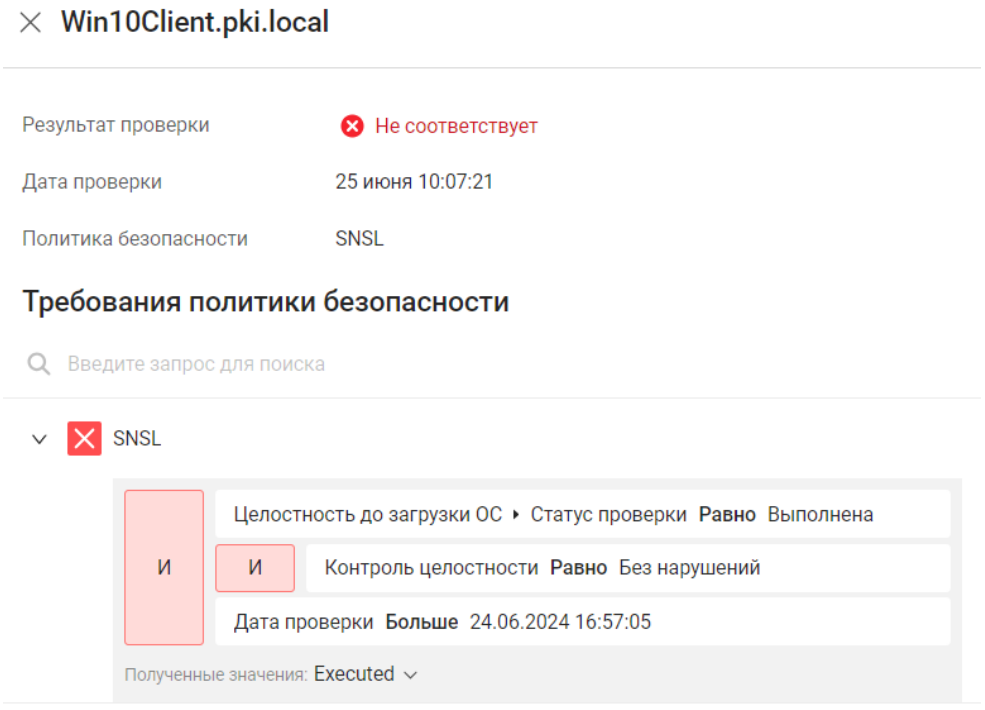



Рисунок 71 – Окно результата проверки «Не соответствует»

Для агента в заголовке указано наименование и приведены следующие данные:

- результат проверки: «Соответствует», «Не соответствует»;
- дата и время проверки;
- наименование политики безопасности.

Область «Требования политики безопасности» содержит поле поиска по названию требования и список проверок с раскрывающимися строками блоков условий. Блоки условий состоят из наименования, описания требований политики безопасности и объединены логическими операторами «И», «ИЛИ».

В зависимости от результата проверки требований, для блока условий применены следующие цветовые обозначения:

- зеленый – проверка пройдена успешно;
- красный – проверка не пройдена;
- серый – проверка не производилась.

Количество полученных значений, сформированных в ходе проверки условий блока, приводится под блоком условия. Для просмотра значений необходимо нажать на кнопку «Полученные значения».

### 4.1.3 Проверка требований политики контроля целостности

Результат проверки подключенного устройства на соответствие заданным требованиям политики контроля целостности объектов до загрузки операционной системы приведен в колонке «Целостность до загрузки ОС» подраздела «Агенты» (см. рис. 67) или на станице выбранного агента (см. рис. 68). Значение «Обнаружены нарушения» является ссылкой, при переходе по которой открывается окно просмотра списка нарушений обнаруженные при проверке подключенного устройства (рис. 72).

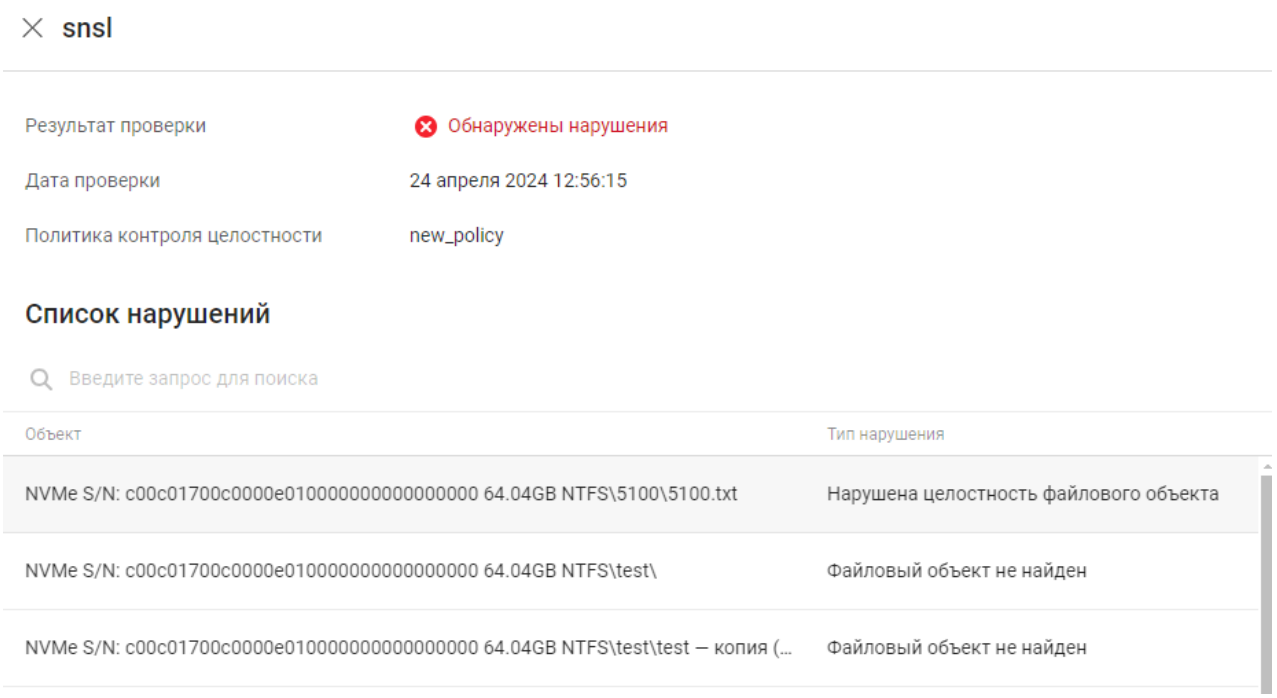



Рисунок 72 – Окно просмотра списка нарушений

Для устройства, у которого обнаружены нарушения до загрузки ОС, приведены следующие данные:

- результат проверки: «Обнаружены нарушения»;
- дата и время проверки;
- наименование политики контроля целостности.

Список нарушений реализован в виде таблицы. Для каждой записи списка отображаются данные:

- объект – путь к проверяемому объекту;
- тип нарушения.

## 4.2 Наборы политик

Подраздел «Наборы политик» в разделе «Агенты» позволяет управлять политиками безопасности и политикам контроля целостности до загрузки ОС, которым должно соответствовать устройство, чтобы считаться надежным и безопасным для получения доступа к сетевым ресурсам организации (рис. 73).

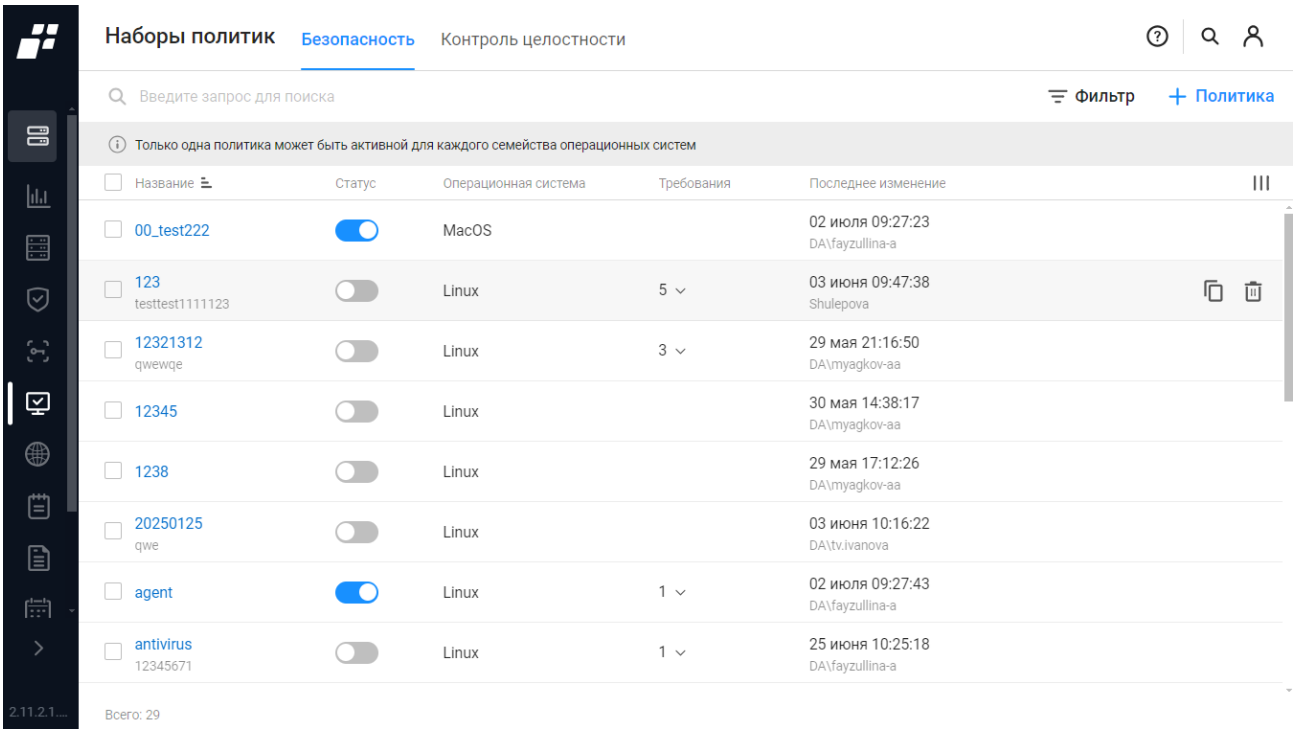



Рисунок 73 – Подраздел «Наборы политик», вкладка «Безопасность»

Страница содержит вкладки:

- «Безопасность»;
- «Контроль целостности».

### 4.2.1 Вкладка «Безопасность»

Вкладка «Безопасность» содержит список политик, которыми управляет пользователь комплекса. Данный список позволяет настраивать параметры проверки политики безопасности.

На странице список политик реализован в виде таблицы (см. рис. 73).

Только одна политика безопасности может быть активной для каждого семейства операционных систем.

Для успешного срабатывания политики безопасности при работе с суппликантом необходимо убедиться, что включен протокол EAP-TNC – переключатель установлен в положение «Активен» ( ) в разделе «Контроль доступа» → «Разрешенные протоколы» → вкладка «Доступ в сеть».

Для каждой записи списка отображаются следующие данные:

- поле для флага;
- название и описание политики безопасности. Является ссылкой, при переходе по которой открывается окно для редактирования;
- статус (активен/неактивен);

— операционная система;
— требования для выполнения политики;
— последнее изменение – дата внесения последних изменений и пользователя.

Над списком располагаются:

— поле поиска ( Введите запрос для поиска );
— кнопка «Политика» ( + Политика );
— кнопка «Фильтр» ( Фильтр );
— кнопка «Колонки» ( ).

При установке флага в строке с необходимым набором политики над списком появляются следующие кнопки:

— кнопка «Создать копию» ( );
— кнопка «Удалить» ( ).

Аналогичные кнопки появляются в правой части экрана в строке с выбранным набором политик.

#### 4.2.1.1 Создание новой политики безопасности

Для добавления в список новой политики безопасности необходимо:

1) Нажать на странице кнопку «Политика» ( + Политика ).
2) Откроется страница «Создание политики (Безопасность)», приведенная на рис. 74. Состав и описание полей вкладки приведены в таблице 31.

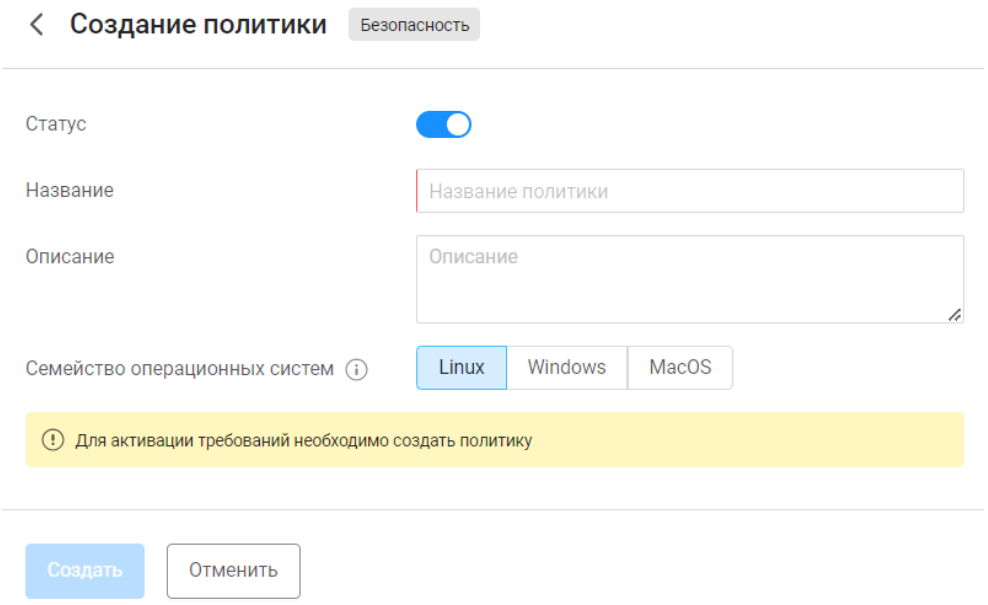



Рисунок 74 – Страница «Создание политики (Безопасность)»

Таблица 31 – Состав и описание полей страницы «Создание политики (Безопасность)»

| Поле | Описание |
|---|---|
| Поле «Статус» | Переключатель:<br>— «Активен»;<br>— «Неактивен» |
| Поле «Название» | Текстовое поле для ввода названия политики.<br>Параметры ввода текста: от 1 до 50 символов.<br>Допустимые символы: буквы латинского алфавита, цифры, «_», «–» |
| Поле «Описание» | Текстовое поле для ввода описания политики.<br>Параметры ввода текста: от 1 до 250 любых символов |
| Поле «Семейство операционных систем» | Переключатель:<br>— «Linux»;<br>— «Windows»;<br>— «MacOS» |
| Элементы управления | |
| Создать | При нажатии кнопки выполняется переход на страницу списка политик с сохранением внесенных данных |
| Отменить | При нажатии кнопки выполняется переход на страницу списка без сохранения внесенных данных |

3) Заполнить поля страницы соответствующими данными добавляемой политики.
4) После создания нажать на название-ссылку созданной политики. Перейти на вкладку «Требования» (рис. 75).

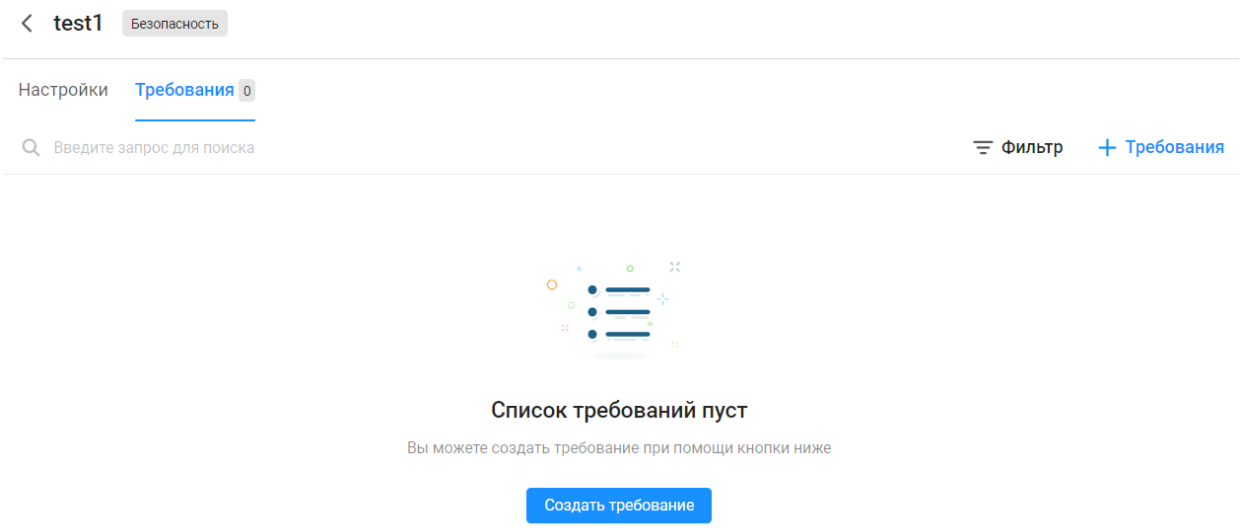



Рисунок 75 – Вкладка «Требования»

5) Нажать на кнопку «Требование» ( + Требование ).
6) Откроется страница создания требования (рис. 76). Состав и описание полей страницы приведены в таблице 32.

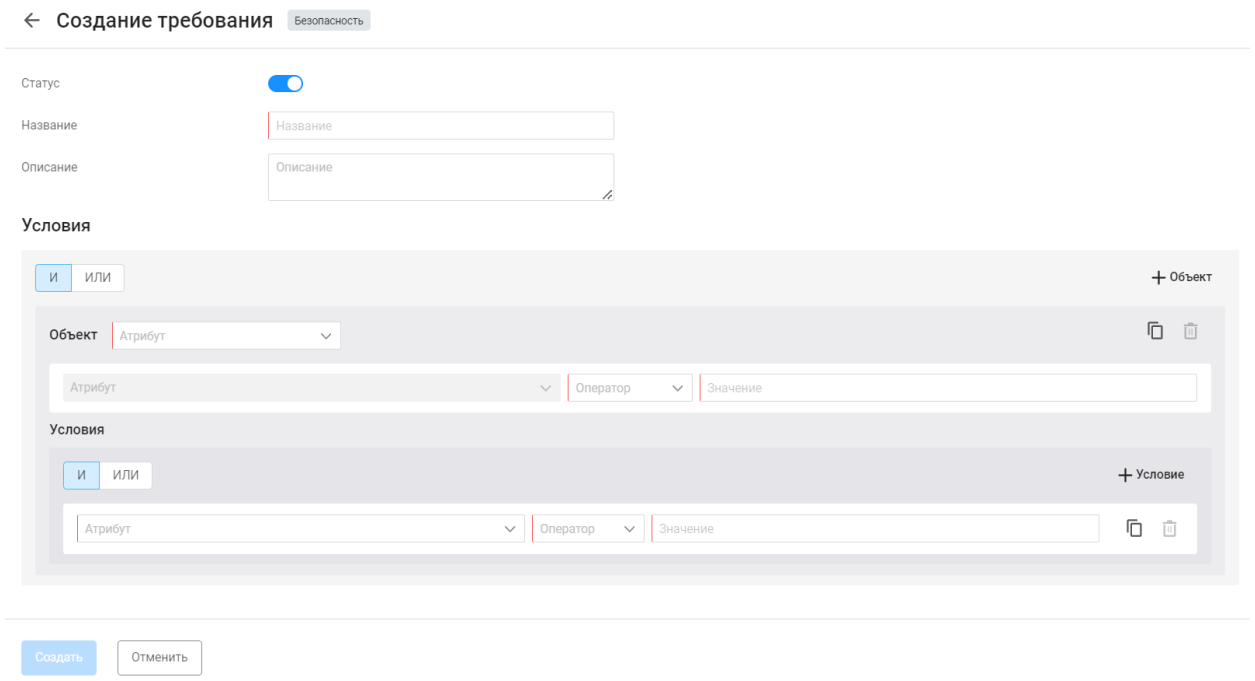



Рисунок 76 – Страница создания требования (Безопасность)

Таблица 32 – Состав и описание полей страницы создания требования (Безопасность)

| Поле | Описание |
|---|---|
| Поле «Статус» | Переключатель:<br>— «Активен»;<br>— «Неактивен» |
| Поле «Название» | Текстовое поле для ввода названия требования политики.<br>Параметры ввода текста: от 1 до 50 символов.<br>Допустимые символы: буквы латинского алфавита, цифры, «_», «–» |
| Поле «Описание» | Текстовое поле для ввода описания требования политики.<br>Параметры ввода текста: от 1 до 250 любых символов |
| Условия срабатывания политики | |
| Формирование условия происходит на основе выбора атрибута, оператора и значения для объекта и для условия | |
| Поле «Объект» | Раскрывающийся список атрибутов для ОС Linux:<br>— USB устройства;<br>— антивирусные приложения;<br>— операционная система;<br>— пакеты;<br>— процессы;<br>— сетевые интерфейсы; |

| Поле | Описание |
|---|---|
| | — файлы;<br>— целостность до загрузки ОС.<br><br>Раскрывающийся список атрибутов для ОС Windows:<br>— USB устройства;<br>— антивирусные приложения;<br>— обновления системы;<br>— операционная система;<br>— параметры реестра;<br>— программы;<br>— процессы;<br>— разделы реестра;<br>— сетевые интерфейсы;<br>— службы;<br>— файлы;<br>— целостность до загрузки ОС.<br><br>Раскрывающийся список атрибутов для ОС MacOS:<br>— USB устройства;<br>— антивирусные приложения;<br>— операционная система;<br>— пакеты;<br>— процессы;<br>— сетевые интерфейсы;<br>— файлы |
| Поле «Условие» | Раскрывающийся список условий, различный для разных атрибутов ОС.<br>Перечень условий для атрибутов ОС Linux:<br>— «USB-устройства»: модель, производитель, состояние;<br>— «Антивирусные приложения»: версия, дата обновления антивирусных баз, состояние, состояние защиты;<br>— «Операционная система»: архитектура, версия, дата установки, название, платформа, сборка;<br>— «Пакеты»: архитектура, версия, издатель, состояние;<br>— «Процессы»: имя пользователя, команда, путь, состояние;<br>— «Сетевые интерфейсы»: общее количество, производитель, состояние, тип;<br>— «Файлы»: дата изменения, дата создания, права, размер (в байтах), существование;<br>— «Целостность до загрузки ОС»: контроль целостности.<br><br>Перечень условий для атрибутов ОС Windows:<br>— «USB-устройства»: модель, производитель, состояние; |

| Поле | Описание |
|---|---|
| | — «Антивирусные приложения»: версия, состояние, состояние защиты, статус обновления AV баз;<br>— «Обновление системы»: дата установки, описание, статус;<br>— «Операционная система»: архитектура, версия, дата установки, название, платформа, сборка, сервис обновлений;<br>— «Параметры реестра»: значение (строка), значение (числовое), существование;<br>— «Программы»: версия, дата установки, издатель, источник установки, расположение, состояние;<br>— «Процессы»: имя пользователя, команда, путь, состояние;<br>— «Разделы реестра»: содержимое, существование;<br>— «Сетевые интерфейсы»: общее количество, производитель, служебное имя, состояние, тип;<br>— «Службы»: исполняемый файл, описание, отображаемое имя, состояние, тип запуска;<br>— «Файлы»: версия, дата изменения, дата создания, размер (в байтах), существование;<br>— «Целостность до загрузки ОС»: контроль целостности.<br><br>Перечень условий для атрибутов ОС MacOS:<br>— «USB-устройства»: модель, производитель, состояние;<br>— «Антивирусные приложения»: версия, дата обновления антивирусных баз, состояние, состояние защиты;<br>— «Операционная система»: архитектура, версия, дата установки, название, платформа, сборка;<br>— «Пакеты»: архитектура, версия, издатель, состояние;<br>— «Процессы»: имя пользователя, команда, путь, состояние;<br>— «Сетевые интерфейсы»: общее количество, производитель, состояние, тип;<br>— «Файлы»: дата изменения, дата создания, права, размер (в байтах), существование |
| Элементы управления | |
| Создать | При нажатии кнопки выполняется переход на страницу списка политик с сохранением внесенных данных |
| Отменить | При нажатии кнопки выполняется переход на страницу списка без сохранения внесенных данных |

7) Заполнить блок условий для объекта – выбрать объект, задать оператора и значение.
8) Заполнить список дополнительных условий для проверки объекта: указать атрибут задать оператора и значение.

### 4.2.2 Вкладка «Контроль целостности»

Вкладка «Контроль целостности» содержит список политик, которыми управляет пользователь комплекса. Данный список позволяет настраивать параметры проверки политики контроля целостности до загрузки ОС.

На странице список политик реализован в виде таблицы (рис. 77).

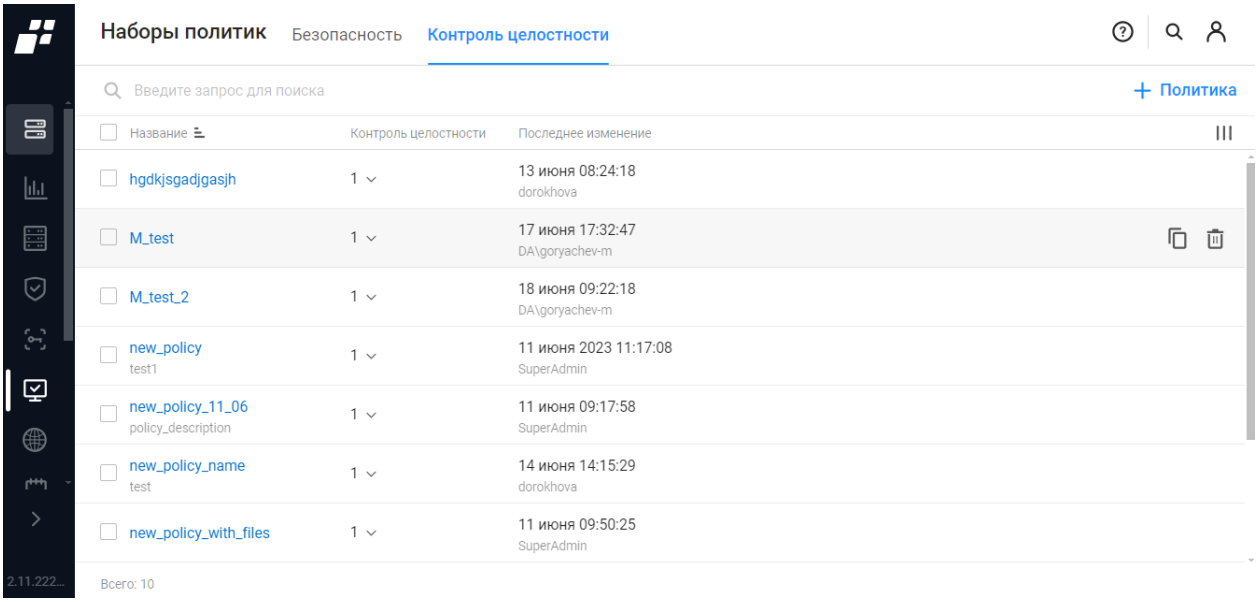



Рисунок 77 – Вкладка «Контроль целостности»

Для каждой записи списка отображаются следующие данные:

- поле для флага;
- название и описание политики контроля целостности до загрузки ОС. Является ссылкой, при переходе по которой открывается окно для редактирования;
- контроль целостности, который применяются к устройству. При нажатии на значение в выпадающем окне выводятся тип контроля целостности и количество проверяемых объектов на выбранных ОС;
- последнее изменение – дата внесения последних изменений и пользователя.

Над списком располагаются:

- поле поиска ( Введите запрос для поиска );
- кнопка «Политика» ( + Политика );
- кнопка «Колонки» ( ).

При установке флага в строке с необходимым набором политики над списком появляется кнопка «Удалить» ( ).

В строке с выбранной политикой в правой части экрана появляются следующие кнопки:

- кнопка «Создать копию» ( );

— кнопка «Удалить» ( ).

#### 4.2.2.1 Создание новой политики контроля целостности

Для добавления в список новой политики контроля целостности до загрузки ОС необходимо:

1) Нажать на странице кнопку «Политика» ( + Политика ).
2) Откроется страница «Создание политики (Контроль целостности)», приведенная на рис. 78. Необходимо заполнить поля требуемыми параметрами и нажать кнопку «Создать». Состав и описание полей страницы приведены в таблице 33.

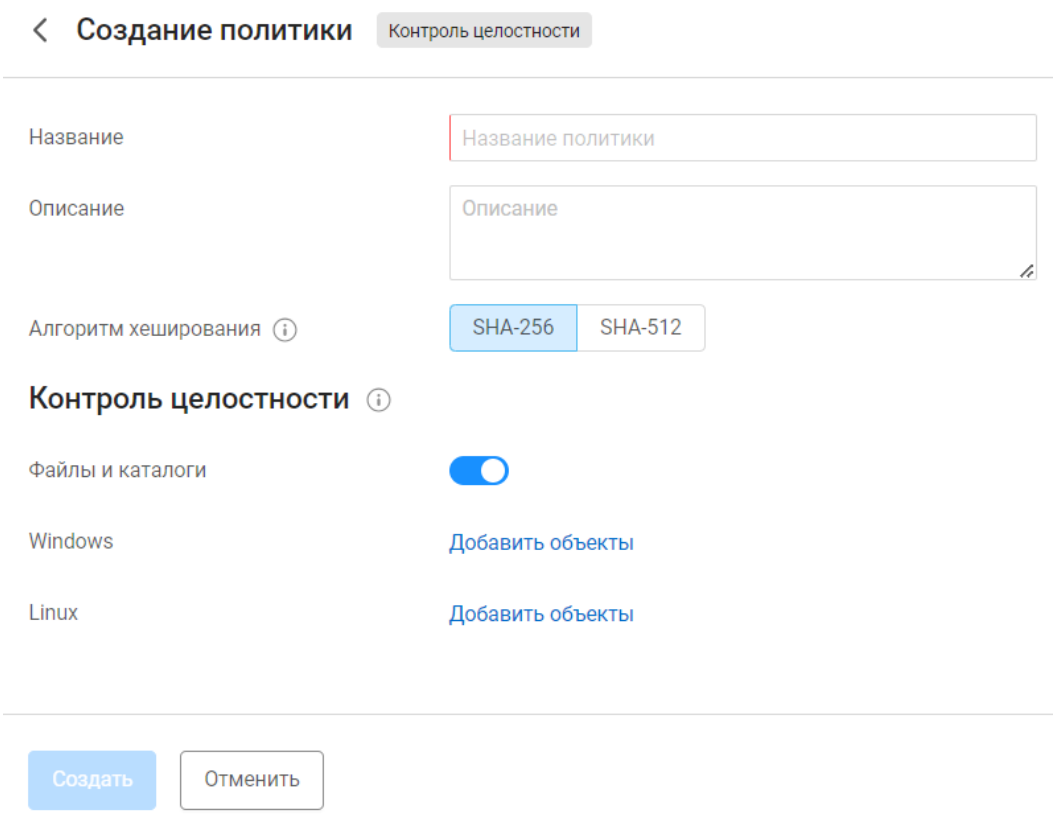



Рисунок 78 – Страница «Создание политики (Контроль целостности)»

Таблица 33 – Состав и описание полей страницы «Создание политики (Контроль целостности)»

| Поле | Описание |
|---|---|
| Поле «Название» | Текстовое поле для ввода названия политики.<br>Параметры ввода текста: от 1 до 50 символов.<br>Допустимые символы: буквы латинского алфавита, цифры, «_», «–» |
| Поле «Описание» | Текстовое поле для ввода описания политики.<br>Параметры ввода текста: от 1 до 250 любых символов |

| Поле | Описание |
|---|---|
| Поле «Алгоритм хеширования» | Переключатель выбора алгоритма расчета контрольных сумм объектов, поставленных на контроль целостности:<br>— «SHA-256»;<br>— «SHA-512» |
| Группа полей «Контроль целостности» | |
| Поле «Файлы и каталоги» | Переключатель:<br>— «Активен» ( ) – включение проверки файлов и каталогов устройства до загрузки ОС;<br>— «Неактивен» ( ) – не включать проверку.<br>При активации переключателя появляются дополнительные поля |
| Поле «Windows» | Содержит ссылку для перехода на страницу «Файлы и каталоги Windows», в которой кнопкой «Объект» ( + Объект ) можно добавить требуемые объекты ОС |
| Поле «Linux» | Содержит ссылку для перехода на страницу «Файлы и каталоги Linux», в которой кнопкой «Объект» ( + Объект ) можно добавить требуемые объекты ОС |
| Элементы управления | |
| Создать | При нажатии кнопки выполняется переход на страницу списка политик с сохранением внесенных данных |
| Отменить | При нажатии кнопки выполняется переход на страницу списка без сохранения внесенных данных |

Для применения созданных/обновленных политик контроля целостности необходимо перезагрузить конечное устройство.

## 4.3 Профили настроек

Подраздел «Профили настроек агентов» (рис. 79) предназначен для формирования профилей настроек агентов. В дальнейшем созданные профили применяются при редактировании параметров подключенных агентов ПК «Efros DO».

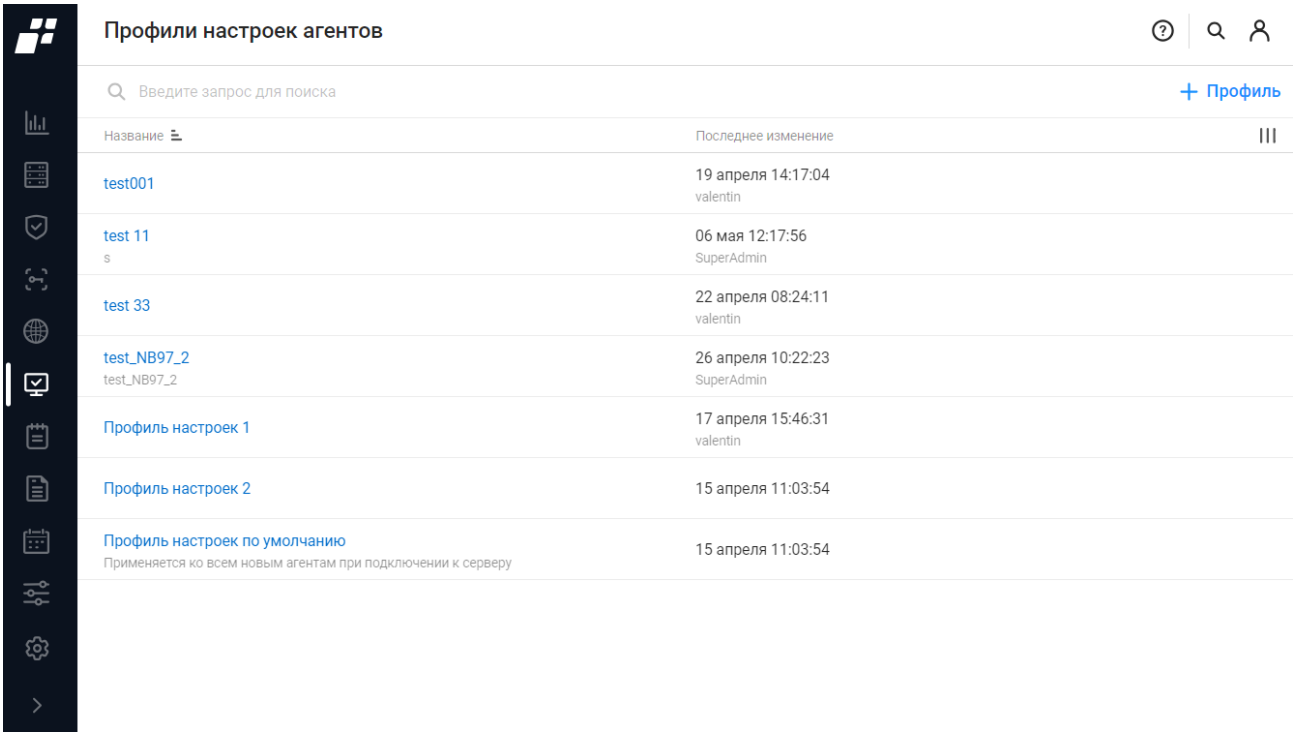



Рисунок 79 – Подраздел «Профили настроек агентов»

Список профилей реализован в виде таблицы. Для каждой записи списка отображаются данные:

- название и описание профиля настройки агента. Является ссылкой, при переходе по которой открывается окно редактирования;
- последнее изменение – дата внесения последних изменений и имя пользователя ПК «Efros DO», вносившего последние изменения.

Над списком агентов располагаются:

- кнопка «Поиск» ( Введите запрос для поиска );
- кнопка «Профиль» ( + Профиль );
- кнопка «Колонки» ( ).

При наведении курсора на строку списка в правой части экрана появляется кнопка «Удалить» ( ).
Запись «Профиль настроек по умолчанию» располагается в конце списка, является предустановленной и недоступна для удаления.

### 4.3.1 Создание профиля настроек агента

Для создания нового профиля настроек агентов пользователю ПК «Efros DO» необходимо:

1) Нажать кнопку «Профиль» ( + Профиль ).
2) Откроется страница «Создание профиля» (рис. 80). Необходимо заполнить

поля требуемыми параметрами и нажать кнопку «Создать». Состав и описание полей страницы приведены в таблице 34.

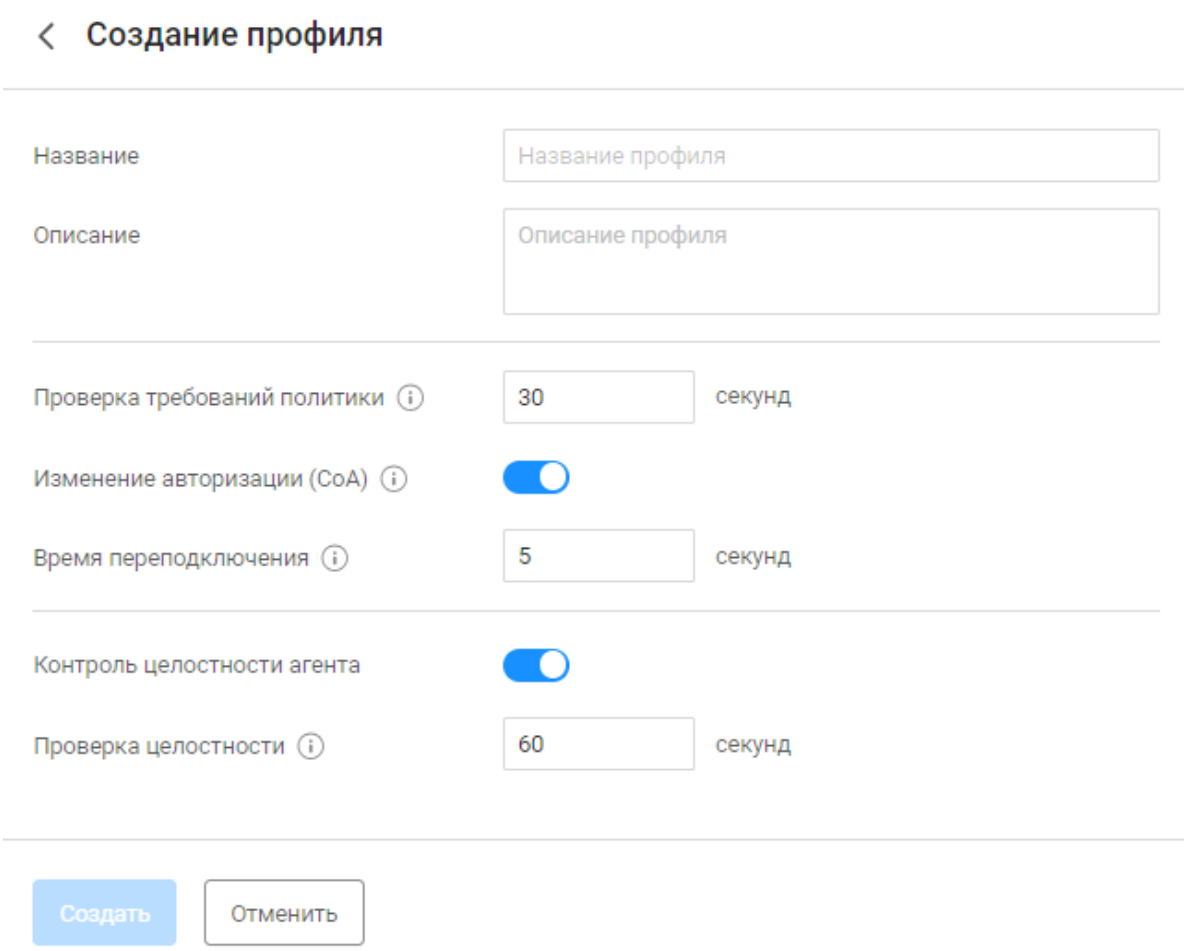



Рисунок 80 – Страница «Создание профиля»

Таблица 34 – Состав и описание полей страницы «Создание профиля»

| Поле | Описание |
|---|---|
| Поле «Название» | Текстовое поле для ввода названия профиля настроек агентов.<br>Параметры ввода текста: от 1 до 50 символов.<br>Допустимые символы: буквы латинского алфавита, цифры, «_», «–» |
| Поле «Описание» | Текстовое поле для ввода описания профиля настроек агентов.<br>Параметры ввода текста: от 1 до 250 любых символов |
| Поле «Проверка требований политики» | Числовое поле для ввода значения периода времени проверки требований политики безопасности, предъявляемых к устройству (секунд).<br>Значение по умолчанию: 30 секунд |

| Поле | Описание |
|---|---|
| Поле «Изменение авторизации (CoA)» | Переключатель:<br>— «Активен» (  ) – при включении выполняется отправка запроса на оборудование на изменение параметров сессии (Change of Authorization) при изменении статуса соответствия подключенного к сети устройства требованиям политики безопасности;<br>— «Неактивен» (  ) – отправка запроса на оборудование на изменение параметров сессии не выполняется.<br><br>При активации переключателя появляется дополнительное поле «Время переподключения»<br><br>Параметры запроса настраиваются в профиле оборудования в блоке «Change of Authorization» |
| Поле «Время переподключения» | Числовое поле для ввода значения допустимого периода времени ожидания возобновления связи с агентом после изменения авторизации (CoA).<br>По истечению времени состояние агента будет изменено на «Недоступен».<br>Значение по умолчанию: 5 секунд |
| Поле «Контроль целостности агента» | Переключатель:<br>— «Активен» (  ) – при включении выполняется проверка целостности агента осуществляется по контрольным суммам основных компонентов агента;<br>— «Неактивен» (  ) – проверка целостности агента не выполняется.<br><br>При активации переключателя появляется дополнительное поле «Проверка целостности» |
| Поле «Проверка целостности» | Числовое поле для ввода значения периода времени проверки целостности компонентов агента.<br>Значение по умолчанию: 5 секунд |
| Элементы управления | |
| Создать | При нажатии кнопки выполняется переход на страницу списка профилей с сохранением внесенных данных |
| Отменить | При нажатии кнопки выполняется переход на страницу списка без сохранения внесенных данных |

## 4.4 Установка и обновление

Подраздел «Установка и обновление» (рис. 81) предназначен для просмотр списка доступных для экспорта инсталляционных пакетов агента ПК «Efros DO».

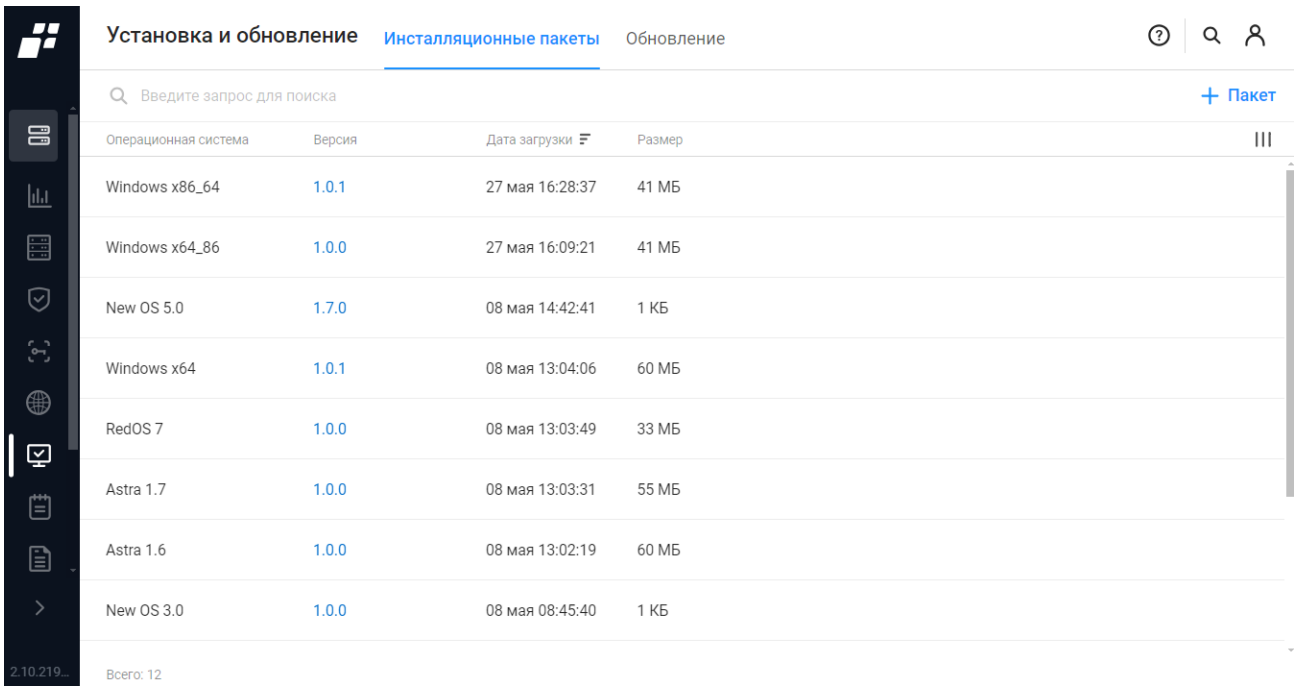



Рисунок 81 – Подраздел «Установка и обновление»

Страница состоит из вкладок:

- «Инсталляционные пакеты»;
- «Обновление».

### 4.4.1 Вкладка «Инсталляционные пакеты»

Данная вкладка содержит список операционных систем с актуальными инсталляционными паркетами. Список реализован в виде таблицы (см. рис. 81)

Инсталляционный пакет представляет собой архив формата .zip с набором файлов, необходимых для установки на устройство пользователя, и содержит:

- дистрибутив агента ПК «Efros DO»;
- дистрибутив суппликанта ПК «Efros DO» – предназначен для выполнения проверки устройства на соответствие требованиям политики безопасности на этапе подключения к корпоративной сети;
- дистрибутив модуля «Контроль целостности до загрузки ОС» – предназначен для проверки политики контроля целостности объектов до загрузки операционной системы;
- защищенный файл со следующими данными:
  - данные о версии пакета и операционной системе, для которой предназначен пакет;
  - список изменений версий агентов;

- эталонные контрольные суммы отдельных компонентов и всего инсталляционного пакета.

Для каждой записи списка отображаются данные:

— название операционной системы;
— версия агента. Является ссылкой, при переходе по которой открывается окно версий инсталляционных пакетов агента для выбранного ОС с возможностью экспорта;
— размер – размер архива инсталляционного пакета агента;
— дата загрузки – дата последней загрузки инсталляционного пакета агента.

Над списком агентов располагаются:

— кнопка «Поиск» ( 

 );
— кнопка «Пакет» ( 

 );
— кнопка «Колонки» (  ).

#### 4.4.1.1 Загрузка инсталляционного пакета

Загрузка инсталляционного пакета производится пользователями ПК «Efros DO» после получения актуальной версии.

Для загрузки инсталляционного пакета пользователю ПК «Efros DO» необходимо:

1) Нажать кнопку «Пакет» ( 

 ).
2) Откроется окно загрузки архива инсталляционного пакета. Необходимо выбрать и загрузить требуемый архив формата .zip.

При загрузке выбранного файла в комплексе выполняется:

— извлечение и валидация содержимого архива;
— извлечение данных о пакете из зашифрованного файла (список изменений версий агентов, версия, ОС, эталонные контрольные суммы);
— проверка загружаемой версии:
  - на уникальность: версия инсталляционного пакета для операционной системы ранее не загружалась;
  - на совместимость с ПК «Efros DO»: версия инсталляционного пакета совместима с текущей версией комплекса;
  - загружаемая версия новее, чем последняя доступная загруженная версия для операционной системы.

#### 4.4.1.2 Экспорт инсталляционного пакета

Экспорт инсталляционного пакета производится для удаленной установки и/или обновления агента, суппликанта и модуля доверенной загрузки на конечном устройстве.

Для экспорта инсталляционного пакета на требуемое ОС пользователю

необходимо:

1) На странице подраздела «Установка и обновление» в строке с требуемым ОС нажать на кнопку версии (см. рис. 81).
2) Откроется окно версий инсталляционных пакетов агента для выбранного ОС (рис. 82). Рекомендуется выбрать последнюю версию и нажать кнопку «Экспорт» ( ).

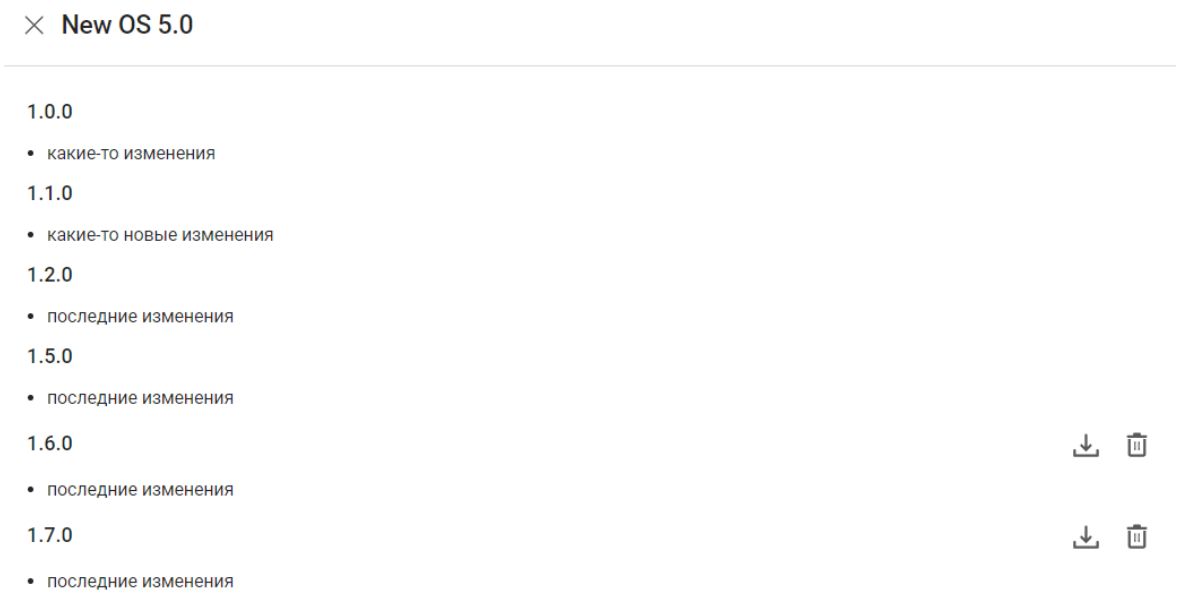



Рисунок 82 – Окно версий инсталляционных пакетов агента для выбранного ОС

Для удаления инсталляционного пакета определенной версии необходимо нажать кнопку «Удалить» ( ).

Удаленная установка инсталляционного пакета производится с помощью скрипта. Описание приведено в документе «Руководство администратора».

### 4.4.2 Вкладка «Обновление»

Данная вкладка содержит список расписаний для запуска обновления агентов, и модулей контроля целостности до загрузки ОС на конечных устройствах.

Список расписаний реализован в виде таблицы (рис. 83).

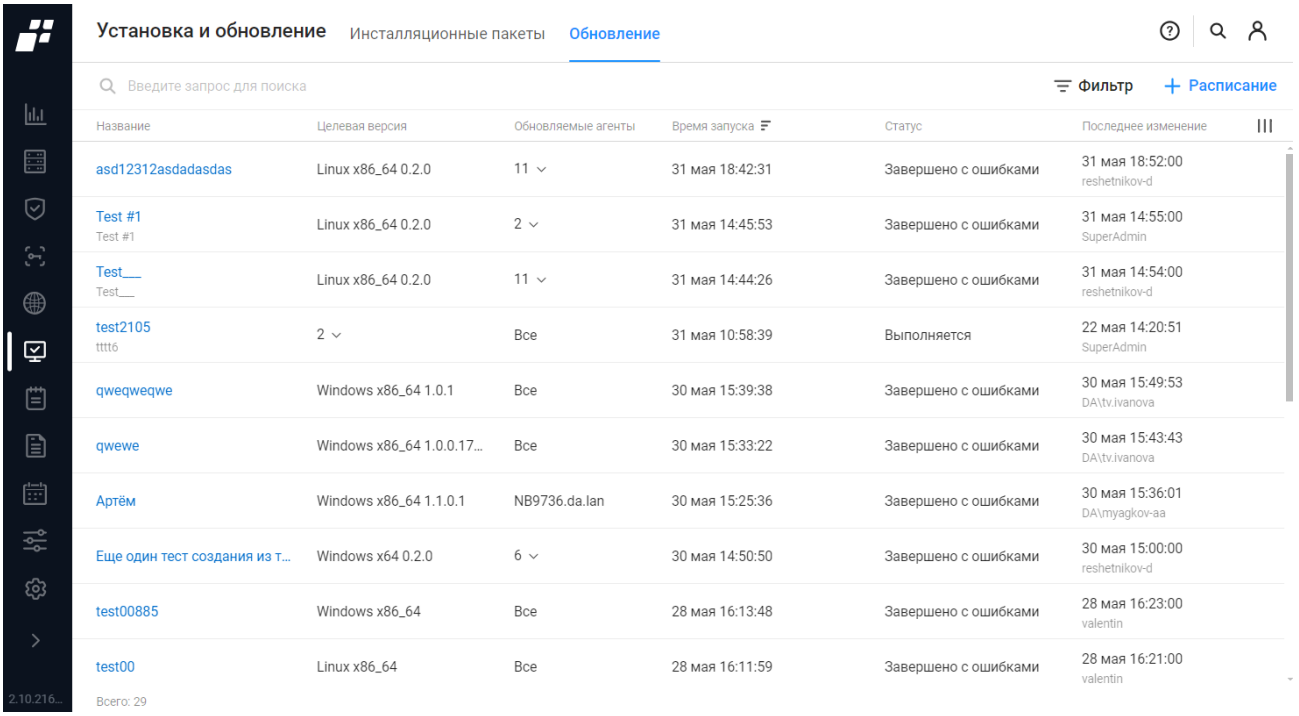



Рисунок 83 – Вкладка «Обновление»

Для каждой записи списка отображаются данные:

- название и описание расписания. Является ссылкой, при переходе по которой открывается окно редактирования расписания;
- целевая версия – ОС конечного устройства и версия агента, которая будет установлена;
- обновляемые агенты – список агентов для обновления;
- дата запуска – дата и время запуска, настроенные в расписании. Если в настройках расписания указано значение «Немедленно», то отображается дата и время сохранения задачи;
- статус. Возможные значения:
  - «Ожидание запуска» – статус нового расписания;
  - «Выполняется» – статус расписания при запуске;
  - «Ошибка запуска» – статус, если возникла ошибка и запуск задачи выполнить не удалось. Дополнительно логируется текст ошибки;
  - «Завершено» – статус, если обновление всех агентов или установка на все устройства выполнена успешно;
  - «Завершено с ошибками» – статус, если возникли ошибки при обновлении хотя бы одного агента или при установке хотя бы на одно устройство.
- последнее изменение – дата внесения последних изменений и имя пользователя ПК «Efros DO», вносившего последние изменения.

Над списком расписаний располагаются:

— кнопка «Поиск» ( Введите запрос для поиска );
— кнопка «Расписание» ( + Расписание );
— кнопка «Фильтр» ( Фильтр );
— кнопка «Колонки» ( ).

Кнопки, появляющиеся в правой части экрана в строке с выбранным расписанием:

— кнопка «Создать копию» ( );
— кнопка «Удалить» ( ).

#### 4.4.2.1 Создание расписания

Для создания расписания пользователю необходимо выполнить следующие действия:

1) Нажать на вкладке «Обновление» кнопку «Расписание» ( + Расписание ).
2) Откроется страница «Создание расписания» (рис. 84). Необходимо заполнить поля требуемыми параметрами и нажать кнопку «Сохранить». Состав и описание полей страницы приведены в таблице 35.

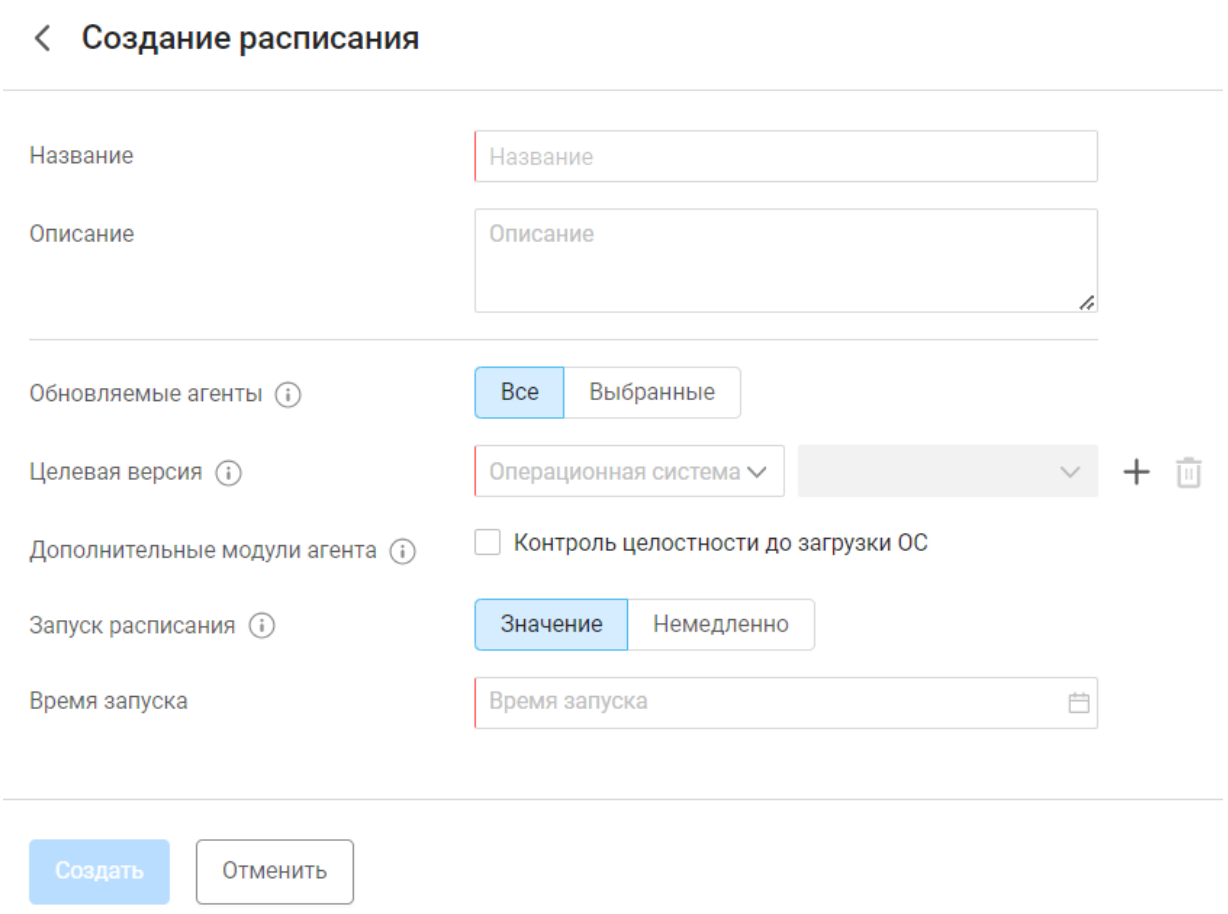



Рисунок 84 – Страница «Создание расписания»

Таблица 35 – Состав и описание полей страницы «Создание расписания»

| Поле | Описание |
|---|---|
| Поле «Название» | Текстовое поле для ввода названия расписания.<br>Параметры ввода текста: от 1 до 250 символов.<br>Допустимые символы: буквы латинского и кириллического алфавитов, цифры, знак «пробел», «_», «–» |
| Поле «Описание» | Текстовое поле для ввода описания группы устройств.<br>Параметры ввода текста: от 1 до 4000 любых символов |
| Поле «Обновляемые агенты» | Переключатель:<br>— «Все» – пользователю разрешен доступ к порталу;<br>— «Выбранные» – пользователю запрещен доступ к порталу.<br><br>При выборе значения «Выбранные» появится дополнительное поле «Агенты» |
| Поле «Агенты» | Значения является ссылка, нажатие на которую открывает окно выбора требуемых агентов |
| Поле «Целевая версия» | Раскрывающийся список для выбора ОС и раскрывающееся список для выбора версии обновляемого инсталляционного пакета.<br>Для обновления агентов и дополнительных модулей, на нескольких операционных системах необходимо добавить поле нажатием на кнопку « + ». Для удаления лишнего поля нажать на кнопку « 🗑 ».<br><br>Если версия агента и/или дополнительных модулей ниже целевой версии, то они будут обновлены до целевой версии.<br>Если версия агента выше целевой версии, то обновление выполняться не будет.<br>Если версия дополнительных модулей не соответствует версии агента, то они будут переустановлены |
| Поле «Дополнительные модули агента» | Предназначено для выбора дополнительного модуля «Контроль целостности до загрузки ОС», которые необходимо установить из инсталляционного пакета в случае его отсутствия на устройстве.<br><br>Если модуль уже установлен, то он будет обновлен автоматически при запуске задачи, выбирать его в настройках расписания не требуется |

| Поле | Описание |
|---|---|
| Поле «Запуск расписания» | Переключатель:<br>— «Значение» – задача будет запущена в указанное время;<br>— «Немедленно» – задача будет запущена сразу после сохранении расписания.<br><br>При выборе «Значение» появится дополнительное поле «Время запуска» |
| Поле «Время запуска» | Поле для ввода даты и времени запуска задачи по расписанию |
| Элементы управления | |
| Создать | При нажатии на кнопку окно создания расписания закрывается, расписание отображается в списке |
| Отменить | При нажатии на кнопку окно создания расписания закрывается без сохранения данных |

#### 4.4.2.2 Редактирование расписания

Для редактирования доступно расписание со статусом «Ожидает запуска».

Для редактирования расписания пользователю необходимо выполнить следующие действия:

1) Нажать на вкладке «Обновление» нажать на название созданного расписания.
2) Откроется страница редактирования расписания». Необходимо изменить заполнение полей требуемыми параметрами.
3) После нажать кнопку «Изменить».

Для запущенного расписания появляются 2 вкладки:

— «Настройки» – соответствуют полям при создании, но без возможности редактирования;
— «История обновления» (рис. 85).

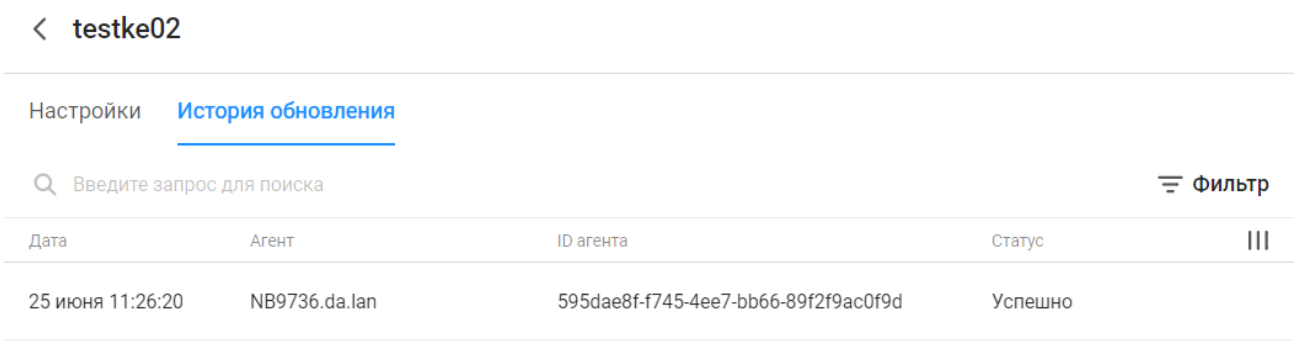



Рисунок 85 – Вкладка «История обновления»

Для каждой записи списка отображаются данные:

- дата и время обновления;
- наименование агента;
- ID агента;
- статус обновления. Возможные значения:
  - «Успешно»;
  - «Ожидание»;
  - «Ошибка».

Над списком расписаний располагаются:

- кнопка «Поиск» ( Введите запрос для поиска );
- кнопка «Фильтр» ( Фильтр );
- кнопка «Колонки» ( ).

# Приложение А

# Рекомендуемая последовательность действий для настройки типового сценария взаимодействия с использованием протокола RADIUS или TACACS+

## А.1 Использование протокола RADIUS

Краткая последовательность действий для настройки типового сценария взаимодействия с RADIUS представлена в таблице 36. Схематичные шаги показаны на рис. 86.

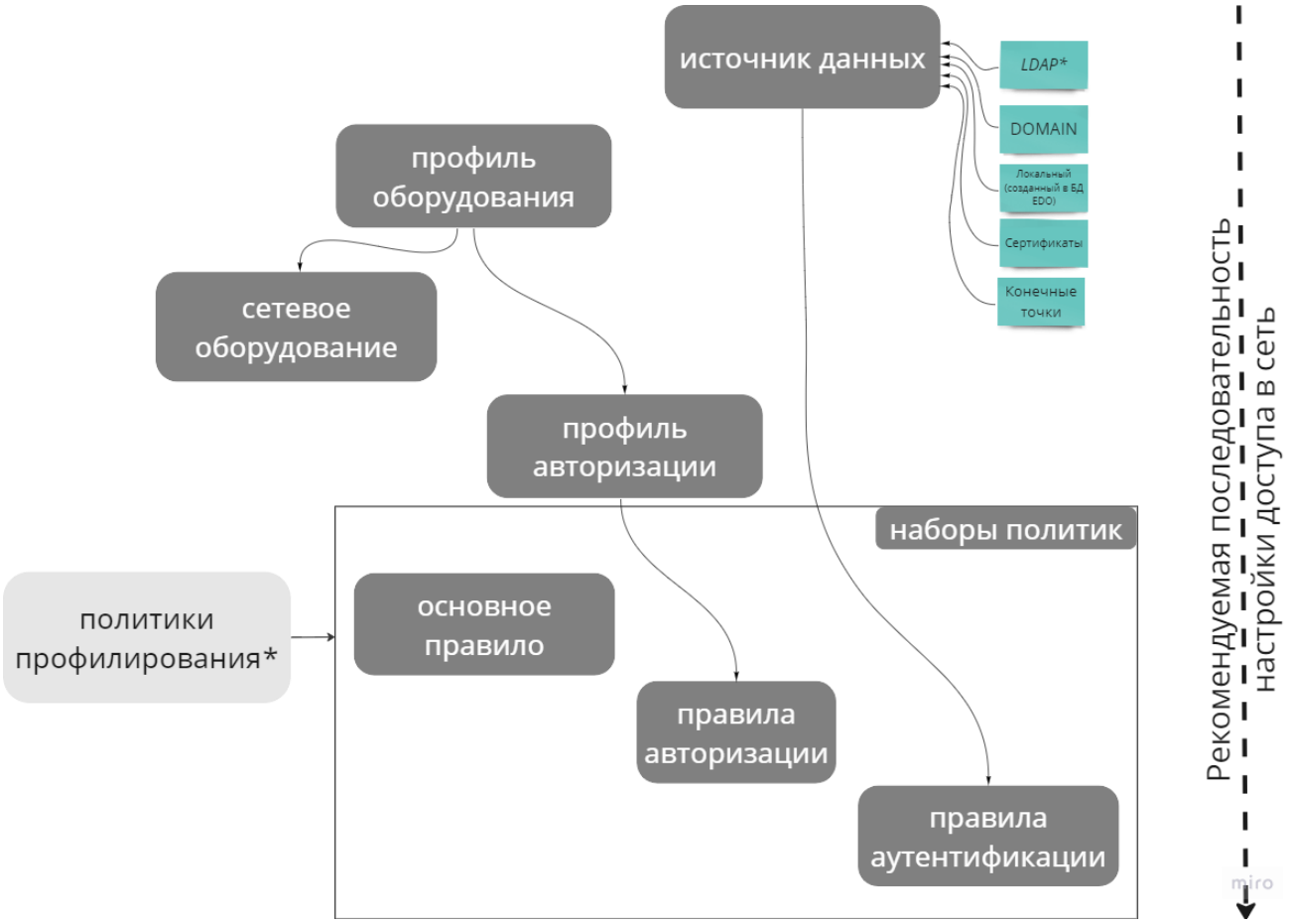



Рисунок 86 – Схема с кратким алгоритмом настройки типового сценария взаимодействия с протоколом RADIUS

Таблица 36 – Краткая последовательность действий для настройки типового сценария взаимодействия с RADIUS

| № п/п | Действие | Описано в разделе документа |
|---|---|---|
| 1 | Создать/добавить/подключить необходимые источники данных[4]: | |
| | • конечные точки; | - |
| | • локальные сетевые пользователи/группы; | 3.3.1.1 |
| | • LDAP; | - |
| | • домен; | - |
| | • сертификаты | - |
| 2 | Создать профиль сетевого оборудования | 3.5.1 |
| 3 | Создать профиль авторизации | 3.6 |
| 4 | Создать набор политик | 3.4.1.1 |
| 4.1 | Создать правила аутентификации | 3.4.1.2 |
| 4.2 | Создать правила авторизации | 3.4.1.3 |
| 5 | Создать сетевое оборудование | 3.2.1.1 |

Для настройки типового сценария взаимодействия с использованием протокола RADIUS пользователю комплекса необходимо сделать следующие шаги:

1) Определить источник данных, где будет сверяться пользователь и\или устройство, которому необходимо предоставить доступ в сеть:

— если в качестве источника выбраны конечные точки/группы конечных точек, то необходимо сделать следующее:

- перейти в раздел «Объекты сети», подраздел «Конечные точки», вкладка «Конечные точки» (рис. 87);
- нажать кнопку « + Конечная точка »;
- заполнить поля страницы создания конечной точки сети необходимыми параметрами (рис. 88) (более подробно о конечной точке сети написано в документе «Руководство пользователя. Часть 1. Администрирование»).

[4] Добавление сертификатов, настройка подключения к AD (LDAP) и создание конечной точки описано в документе «Руководство пользователя. Часть 1. Администрирование»

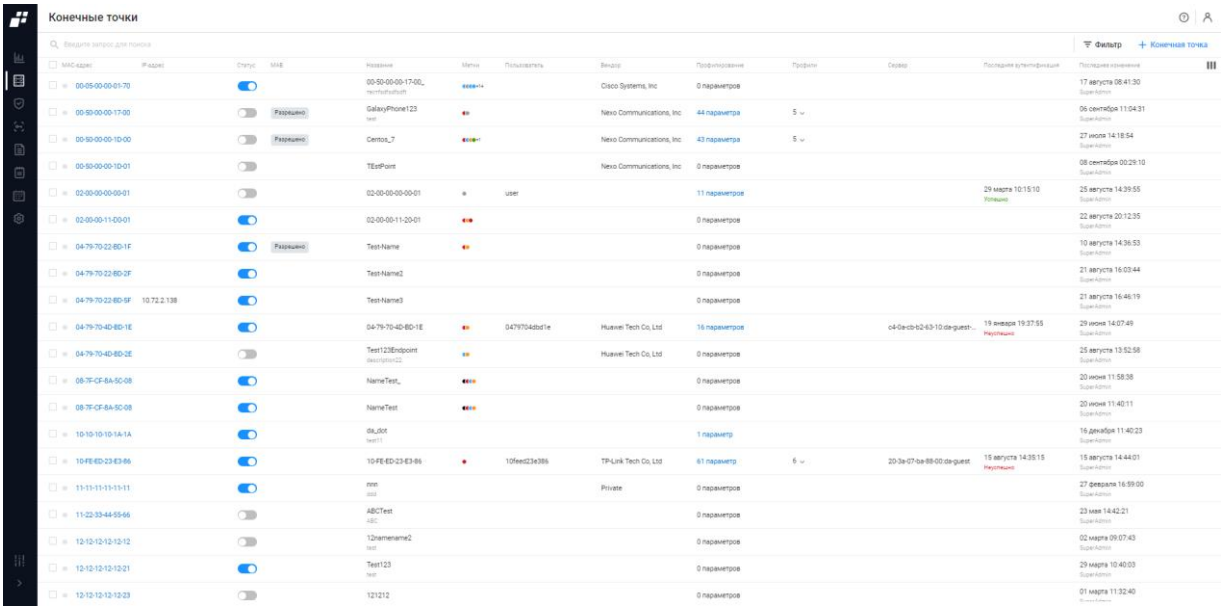



Рисунок 87 – Конечные точки как источник данных

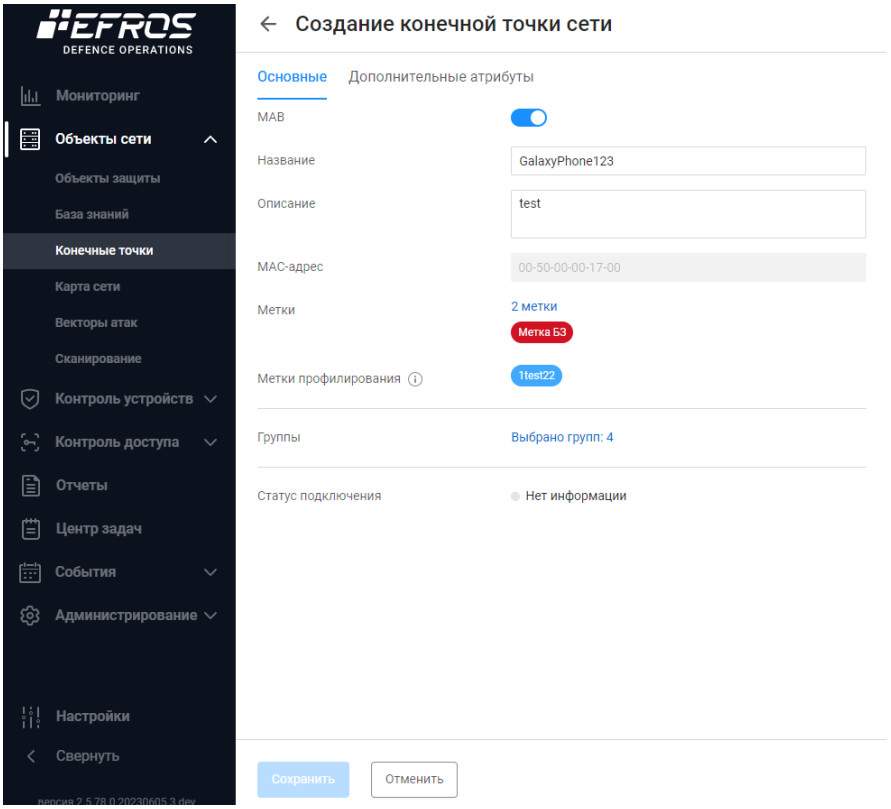



Рисунок 88 – Создание конечной точки

— если в качестве источника выбраны локальные пользователи, то необходимо сделать следующее:
  - перейти в раздел «Контроль доступа», подраздел «Сетевые пользователи», вкладка «Пользователи» (рис. 89);

- нажать кнопку « + Пользователь »;
- заполнить поля страницы (рис. 90) необходимыми параметрами и нажать кнопку «Создать» (более подробно о создании локального сетевого пользователя написано в п.п. 3.3.1.1).

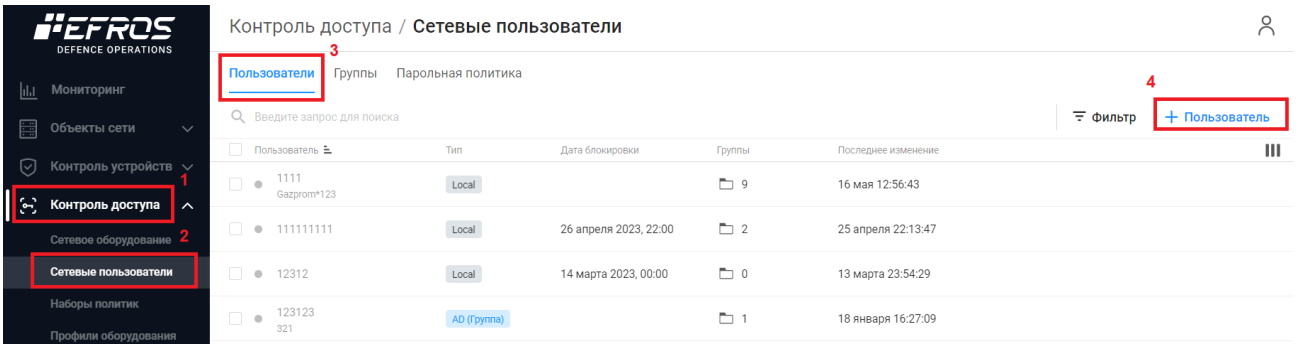



Рисунок 89 – Источник данных – локальный сетевой пользователь

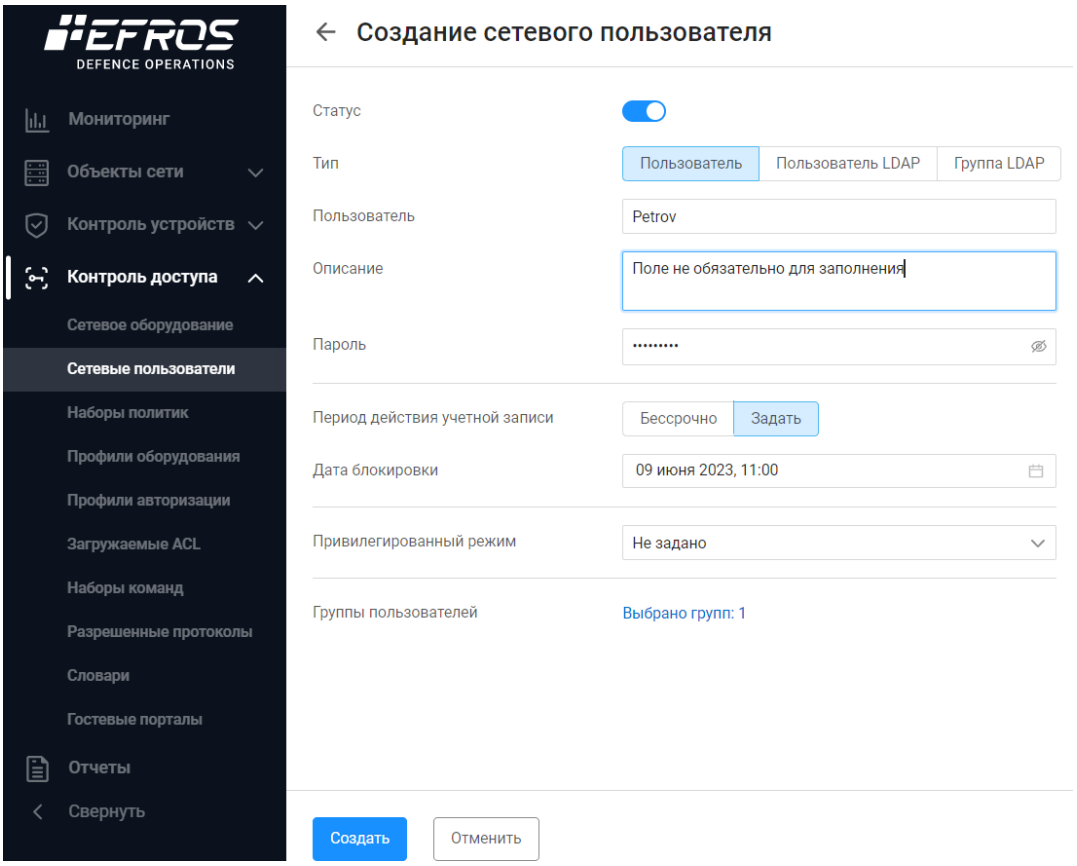



Рисунок 90 – Создание локального сетевого пользователя

— если в качестве источника выбран внешний источник данных – служба каталогов LDAP, то необходимо сделать следующее:

- перейти в раздел «Настройки», подраздел «Источники данных», вкладка «LDAP» (рис. 91);
- нажать кнопку « + Соединение »;

- заполнить поля страницы (рис. 92) соответствующими параметрами и нажать кнопку «Создать» (более подробно об LDAP соединении написано в документе «Руководство пользователя. Часть 1. Администрирование»);
- перейти в раздел «Контроль доступа», подраздел «Сетевые пользователи», вкладка «Пользователи» (рис. 93);
- создать сетевого пользователя LDAP (более подробно о создании пользователя LDAP написано в п.п. 3.3.1.1).

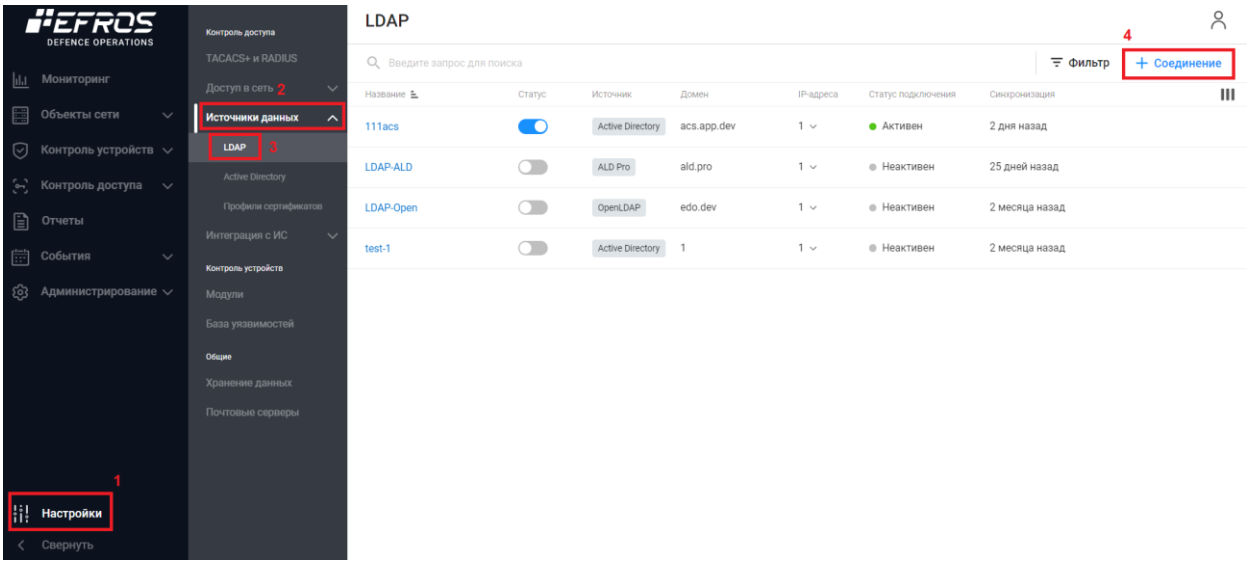



Рисунок 91 – Источник данных – служба каталогов LDAP

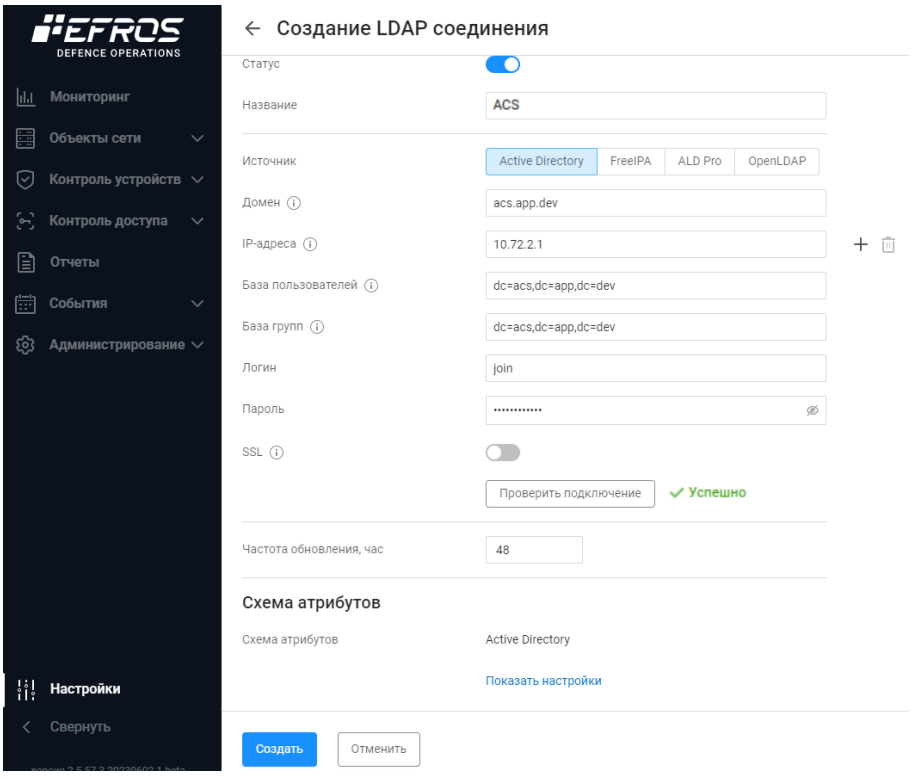



Рисунок 92 – Создание нового соединения

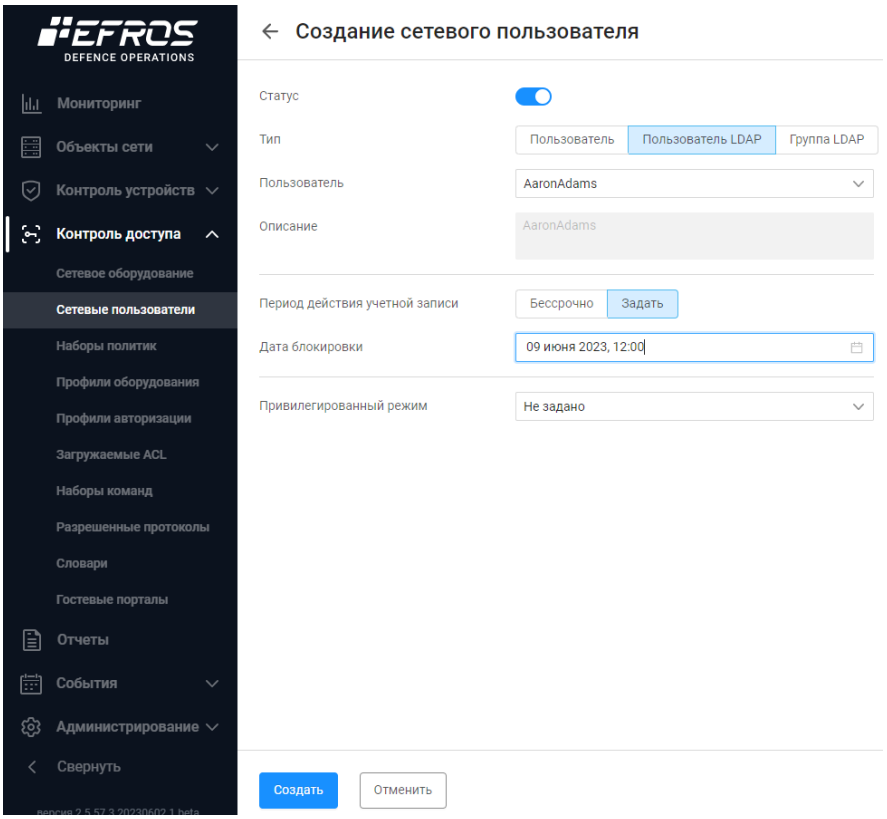



Рисунок 93 – Создание сетевого пользователя LDAP

— если в качестве источника выбран домен, то необходимо сделать следующее:

- перейти в раздел «Настройки», подраздел «Источники данных», вкладка «Active Directory» (рис. 94);
- нажать кнопку «+ Соединение»;
- заполнить поля страницы (рис. 95) необходимыми параметрами и нажать кнопку «Создать» (более подробно о создании нового соединения описано в документе «Руководство пользователя. Часть 1. Администрирование»).

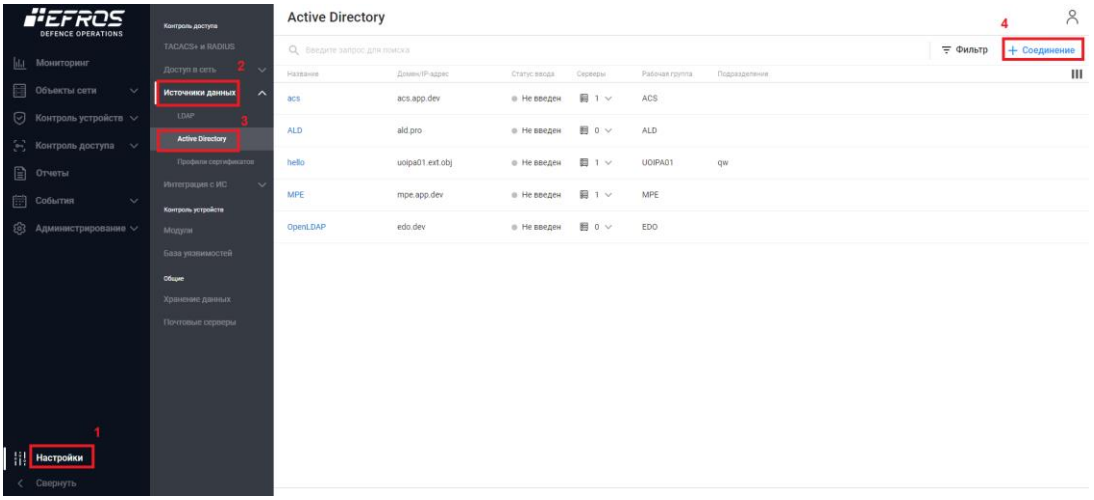



Рисунок 94 – Источник данных Active Directory

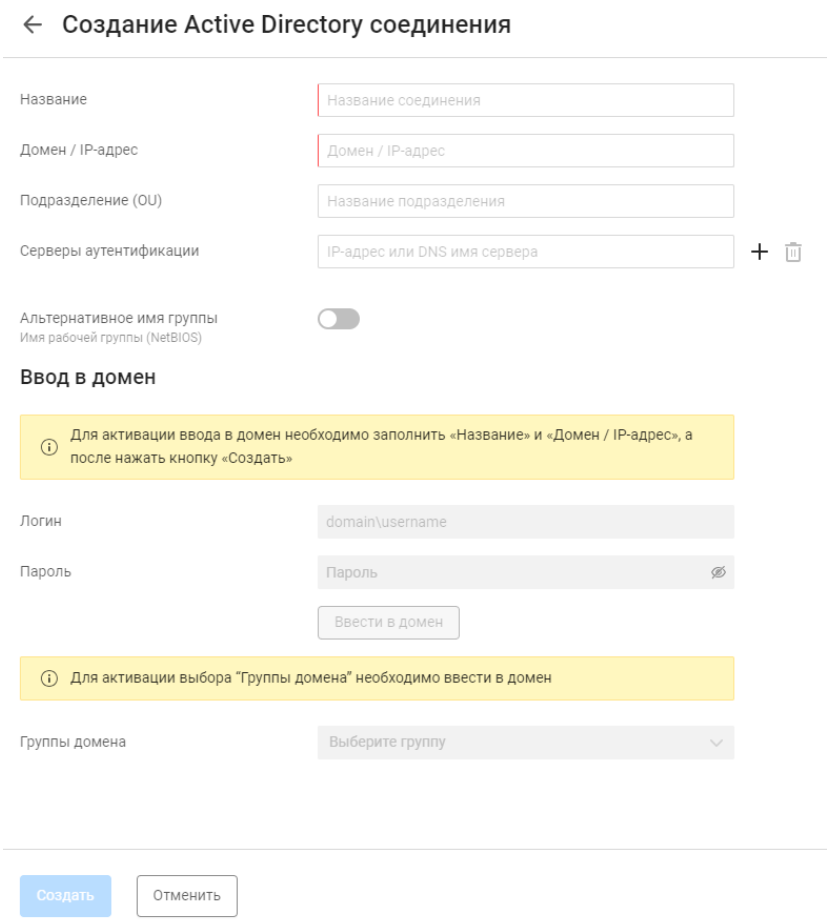



Рисунок 95 – Создание Active Directory соединения

— если в качестве источника выбраны сертификаты, то необходимо сделать следующее:
  - перейти в раздел «Администрирование», подраздел «Сертификаты»;
  - выбрать вкладку «Корневые»;
  - скачать корневой сертификат. При необходимости, если корневой сертификат выпущен сторонней организацией, добавить его в БД комплекса;
  - выбрать вкладку «Клиентские»;
  - выпустить и скачать клиентский сертификат;
  - установить корневой и клиентский сертификаты на устройство.

2) Создать профиль сетевого оборудования[5]:

— перейти в раздел «Контроль доступа», подраздел «Профили оборудования» (рис. 96);

— нажать кнопку «+ Профиль оборудования»;

[5] Профиль сетевого оборудования необходим для назначения общих правил аутентификации и авторизации на оборудовании для сетевых пользователей

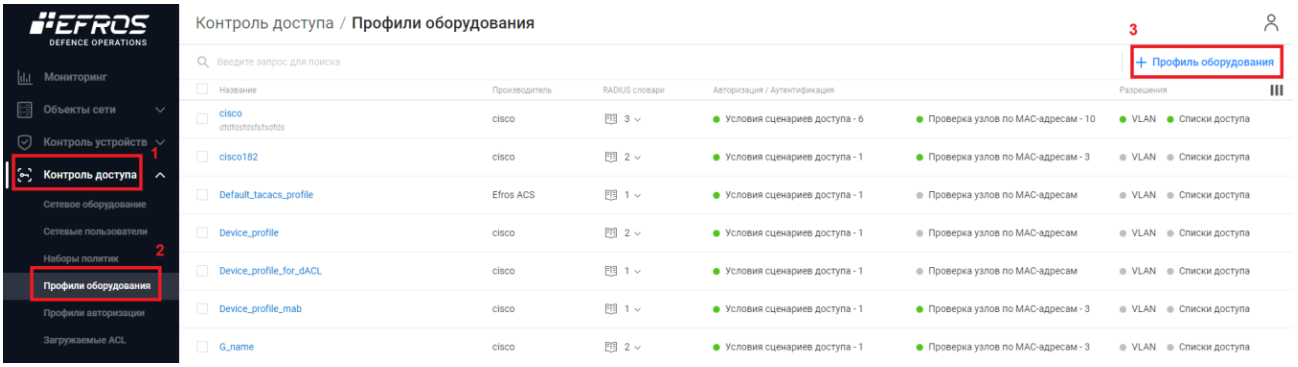



Рисунок 96 – Раздел «Контроль доступа», подраздел «Профили оборудования»

— заполнить поля страницы (рис. 97) необходимыми параметрами (более подробно о создании профиля написано в п. 3.5.1).

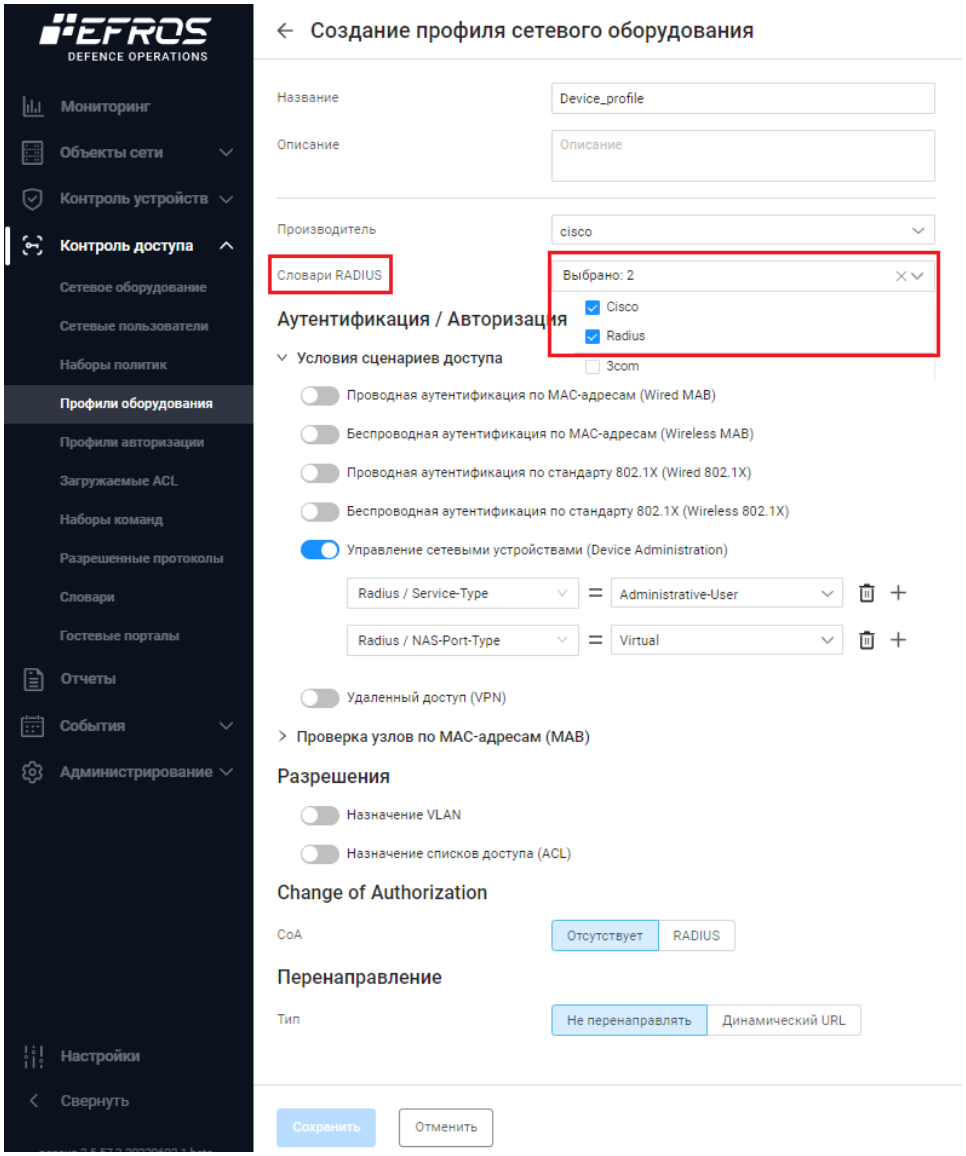



Рисунок 97 – Создание профиля сетевого оборудования

Для создания корректного профиля сетевого оборудования необходимо выбрать соответствующий словарь RADIUS. От этого зависит набор атрибутов для настройки сценариев доступа.

Часто используемые условия сценариев доступа приведены во встроенном профиле оборудования default_device_profile. Пользователь может создать копию на основе данного профиля и внести требуемы изменения.

Рекомендуется активировать следующие словари:

— RADIUS;
— Gazinformservice;
— Словарь, соответствующий названию производителя оборудования.

3) Создать профиль авторизации «Доступ в сеть» (для оборудования, запрашивающего доступ в сеть, либо к оборудованию с использованием протокола RADIUS):

— выбрать на странице «Профиль авторизации» вкладку «Доступ в сеть» (рис. 98);
— нажать кнопку «+ Профиль»;

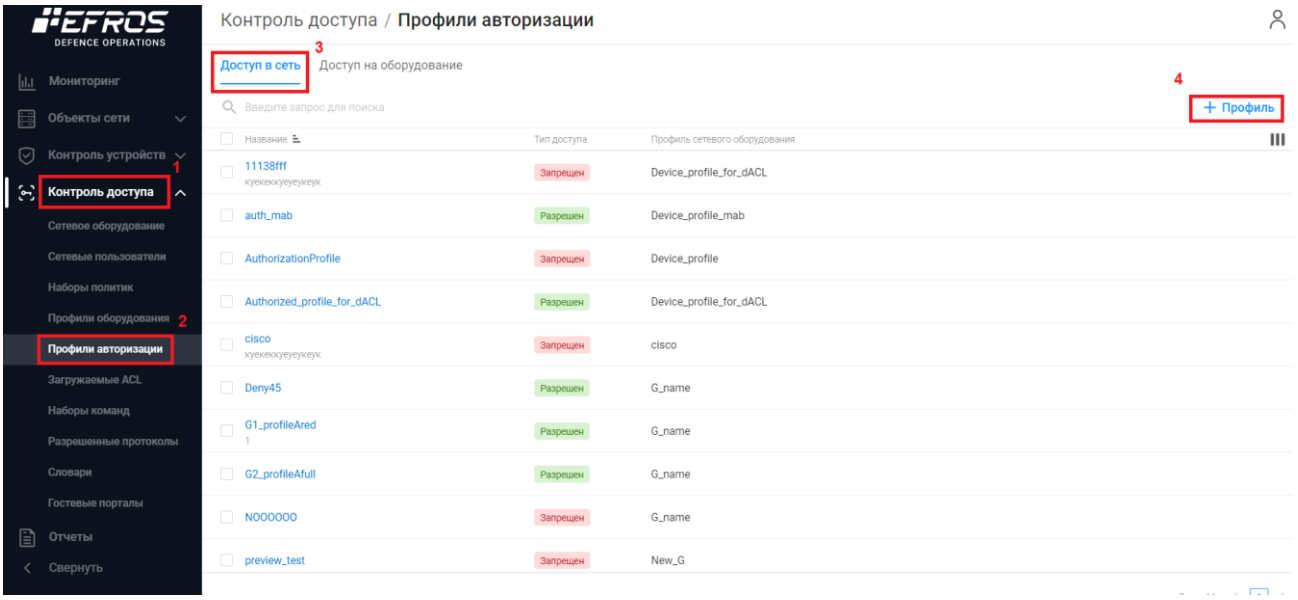



Рисунок 98 – Создание профиля авторизации «Доступ в сеть»

— заполнить необходимые поля на странице создания профиля авторизации (более подробно о создании профиля авторизации доступа в сеть написано в п. 3.6.1) (рис. 99).

Количество и тип полей в группе полей «Основные настройки» зависят от выбранного профиля сетевого оборудования.

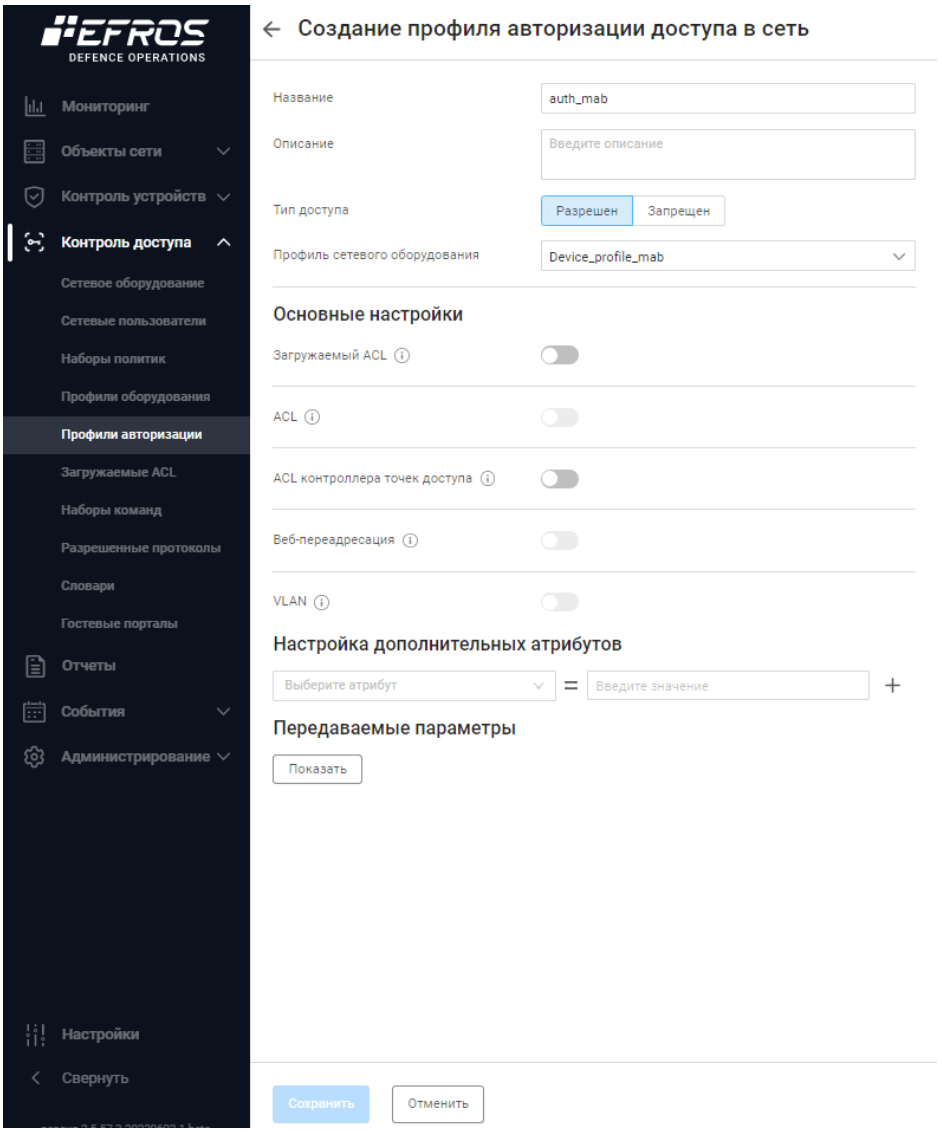



Рисунок 99 – Создание профиля авторизации доступа в сеть

4) Создать требуемый набор политик доступа (более подробно о наборе политик написано в подразделе 3.4). Для этого необходимо:

— перейти в раздел «Контроль доступа», подраздел «Наборы политик»;

— выбрать вкладку «Доступ в сеть», которая позволяет создать набор политик доступа в сеть для сетевого оборудования.

— на вкладке «Доступ в сеть» нажать кнопку « + Политика » (рис. 100);

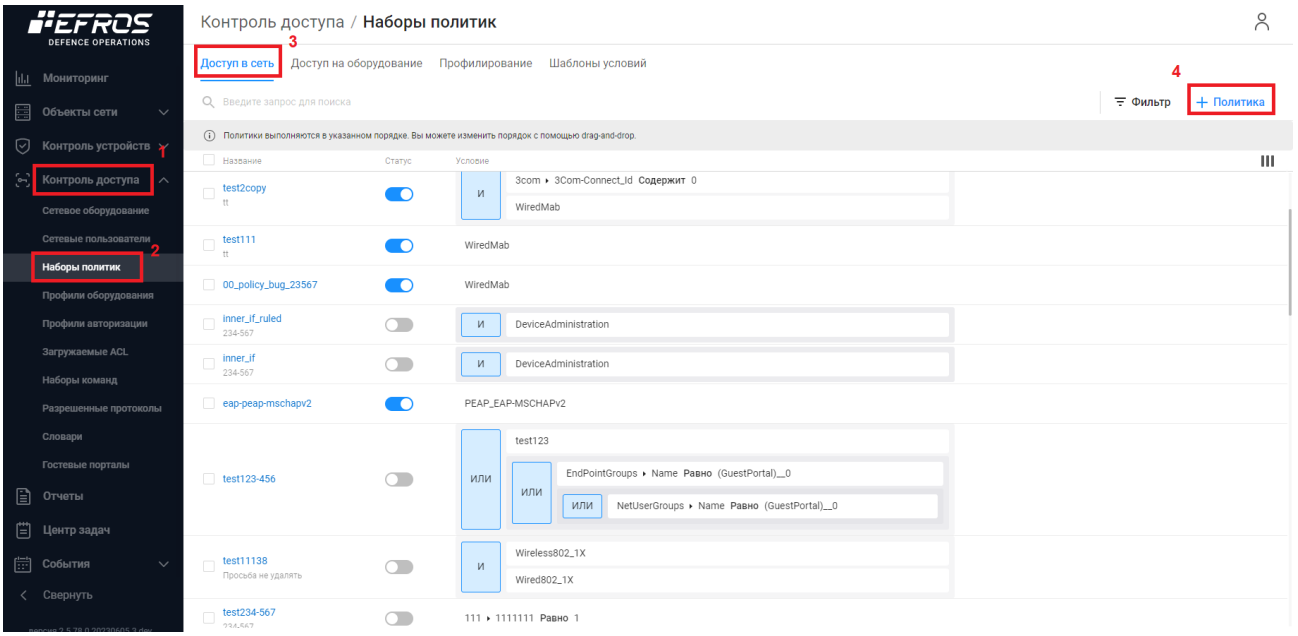



Рисунок 100 – Создание набора политик «Доступ в сеть»

— на вкладке «Настройки» создать условия срабатывания политики[6] или выбрать условие из шаблона условий (рис. 101);

Вкладка «Шаблоны условий» позволяет создавать шаблоны условий в виде отдельных полей, которые можно хранить в списке шаблонов условий, а затем повторно использовать для других условий или политик. Такие шаблоны будут считаться пользовательскими.

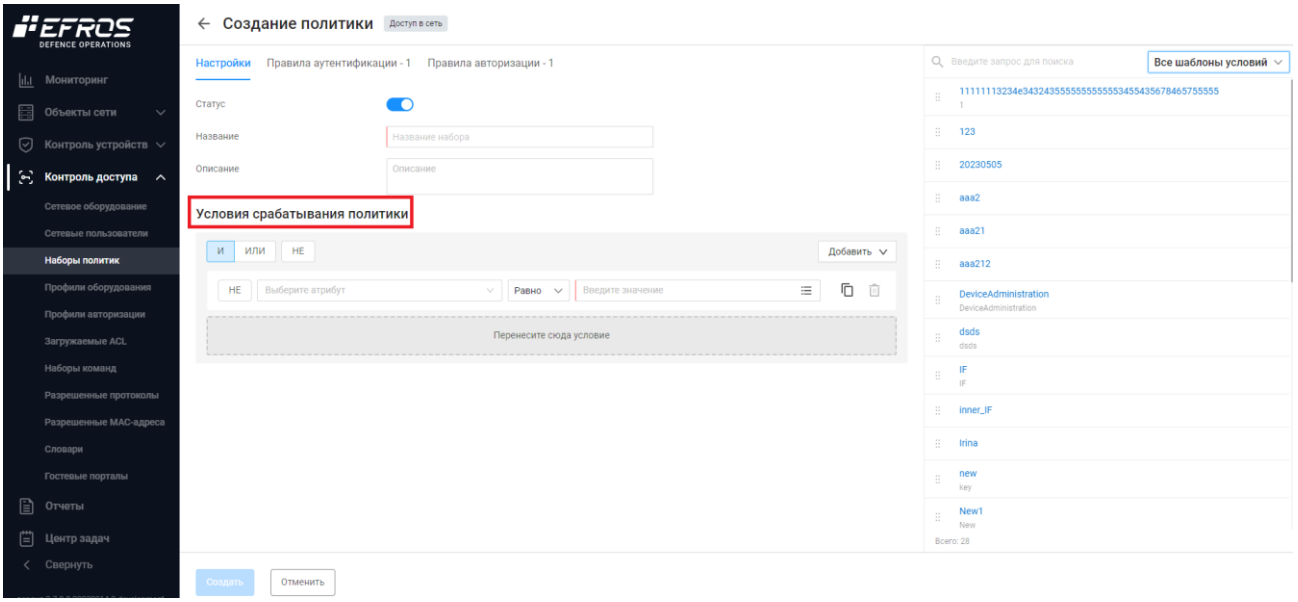



Рисунок 101 – Создание условия срабатывания политики

[6] Это условия, которым в первую очередь должно соответствовать устройство при попытке получения доступа в сеть

— на вкладке «Правила аутентификации» определить, каким образом и где происходит аутентификация устройства (рис. 102). Для этого необходимо в первую очередь настроить правило «Default» (правило "по умолчанию", которое будет выполнено, если не сработает ни одно созданное дополнительно правило. Рекомендуется выставить параметры для запрета доступа на оборудование):
  - выбрать источник данных. Для правила по умолчанию рекомендуется выбрать «DenyAccess»;
  - выбрать действие при ошибке аутентификации. Для правила по умолчанию рекомендуется выбрать «Отклонить»;
  - выбрать действие, если пользователь не найден. Для правила по умолчанию рекомендуется выбрать «Отклонить».

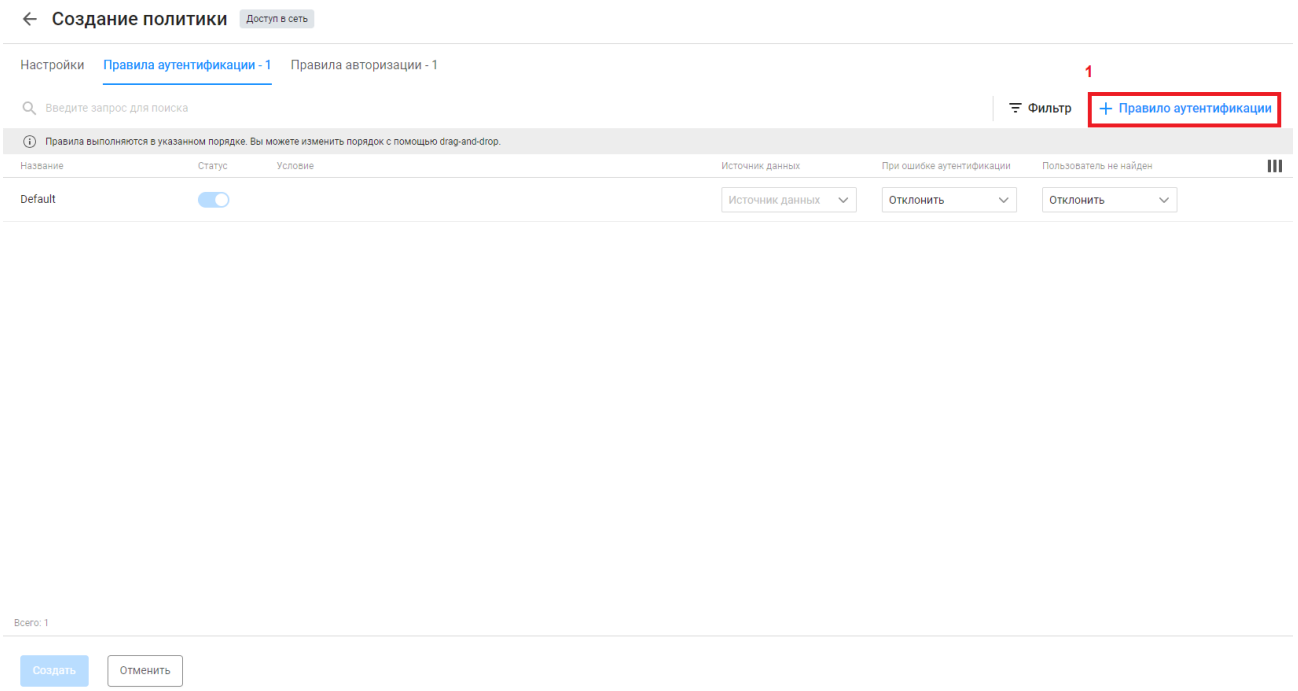



Рисунок 102 – Создание политики «Доступ в сеть». Правило аутентификации

— нажать кнопку « + Правило аутентификации » (см. рис. 102). Заполнить поля необходимыми данными (рис. 103):
  - выбрать статус;
  - указать название политики;
  - указать источник данных (об источниках данных написано в шаге 1);
  - указать действие при ошибке аутентификации;
  - указать действие, если пользователь не будет найден;
  - создать условие для срабатывания правила или выбрать условие из предлагаемых шаблонов:
    - *выбрать атрибут из раскрывающегося списка;*
    - *выбрать значение атрибута;*

– *выбрать логическую операцию из раскрывающегося списка. Допускается использовать регулярные выражения.*

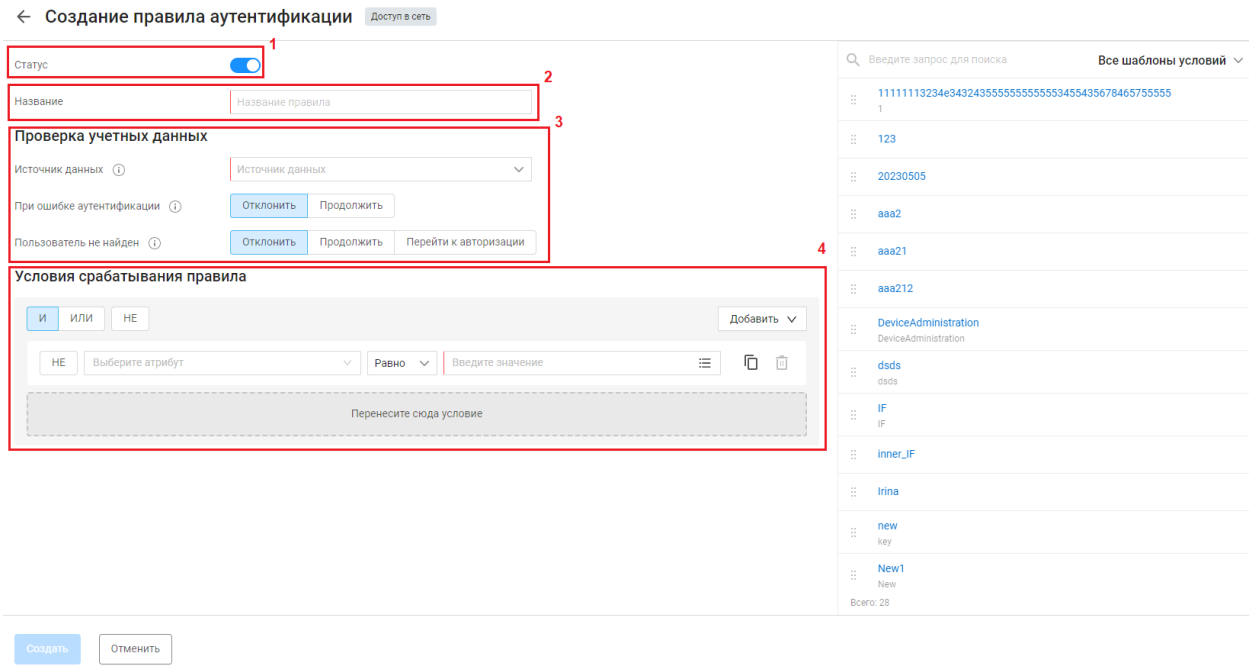



Рисунок 103 – Создание правила аутентификации

— перейти на вкладку «Правила авторизации» (рис. 104). На вкладке «Правила авторизации» нужно определить, каким образом происходит авторизация пользователя на устройстве. Для этого необходимо в первую очередь настроить правило «Default» (правило "по умолчанию", которое будет выполнено, если не сработает ни одно созданное дополнительно правило. Рекомендуется выставить параметры для запрета доступа на оборудование) – выбрать созданный ранее профиль авторизации.

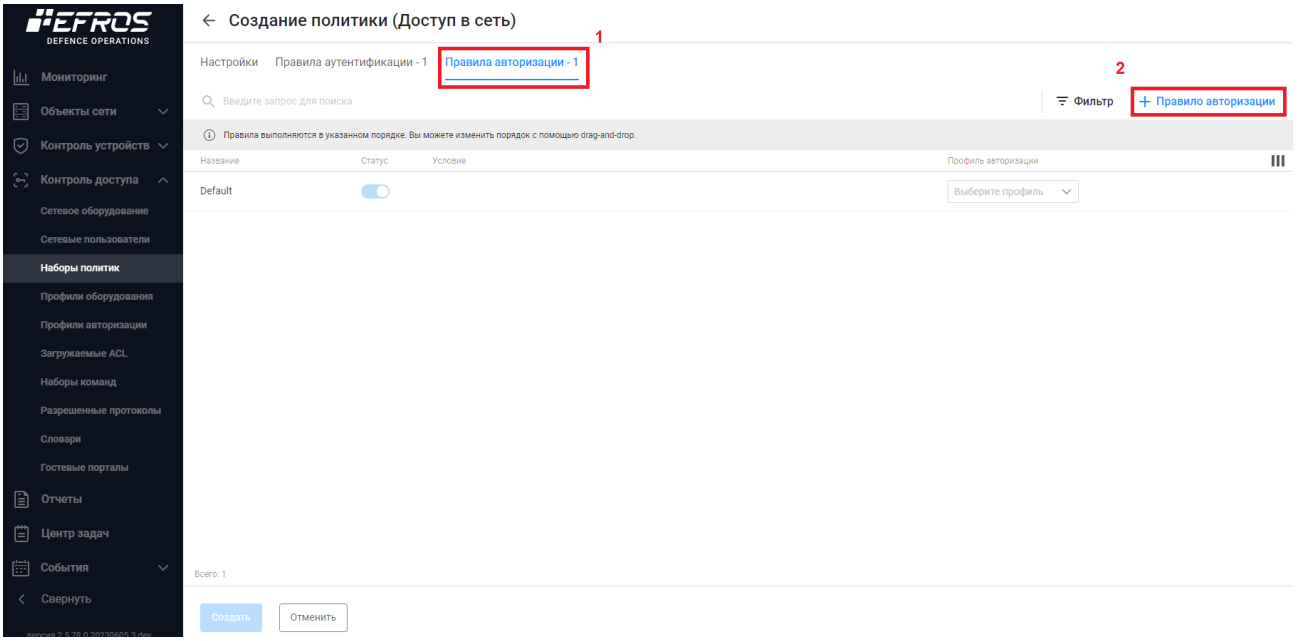



Рисунок 104 – Создание политики «Доступ в сеть». Правило авторизации

— на вкладке нажать кнопку «+ Правило авторизации» (см. рис. 104). Заполнить поля необходимыми данными (рис. 105):
  - выбрать профиль авторизации, который будет применен при срабатывании заданного условия (использовать профиль, созданный в шаге 3);
  - создать условие для срабатывания правила или выбрать условие из предлагаемых шаблонов:
    - *выбрать атрибут из раскрывающегося списка;*
    - *выбрать значение атрибута;*
    - *выбрать логическую операцию из раскрывающегося списка. Допускается использовать регулярные выражения.*
— нажать кнопку «Сохранить».

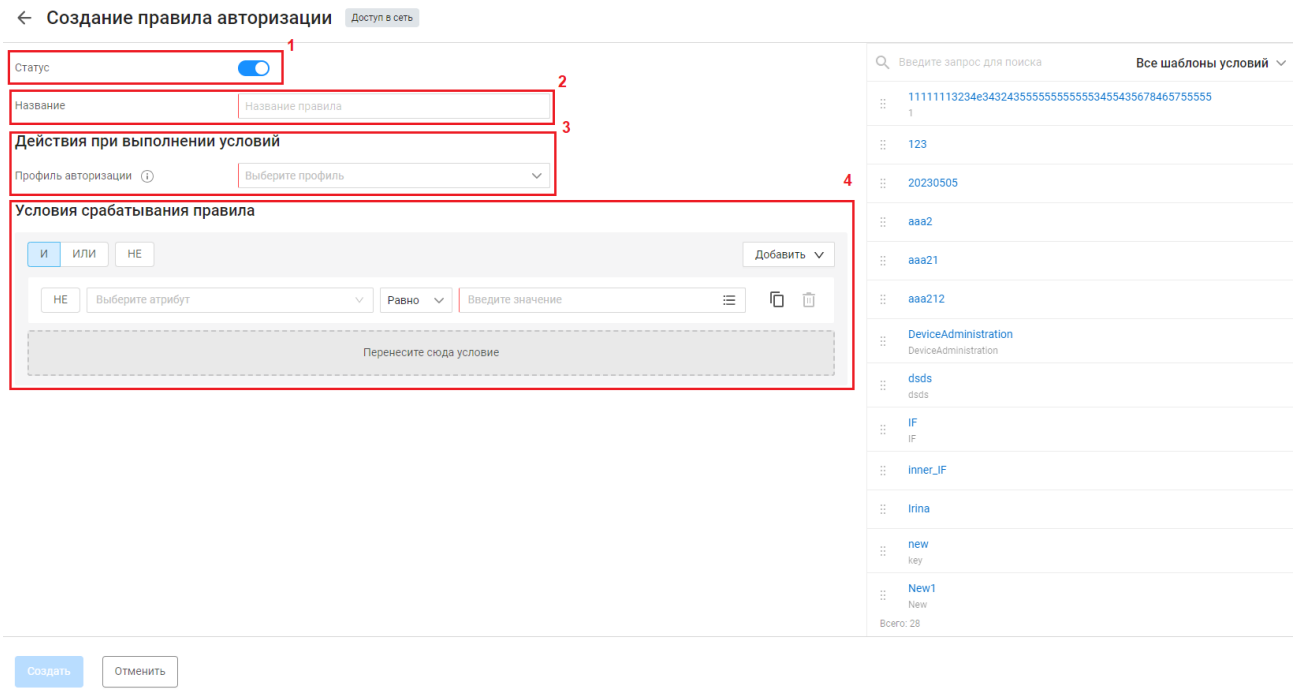



Рисунок 105 – Создание правила авторизации

5) Перейти в раздел «Контроль доступа», подраздел «Сетевое оборудование». Создать сетевое оборудование. Для этого необходимо:

— на вкладке «Устройства» нажать кнопку «+ Устройство» (рис. 106);
— заполнить поля необходимыми данными (указать профиль сетевого оборудования, созданный в шаге 2) (рис. 107);
— указать RADIUS Shared key.

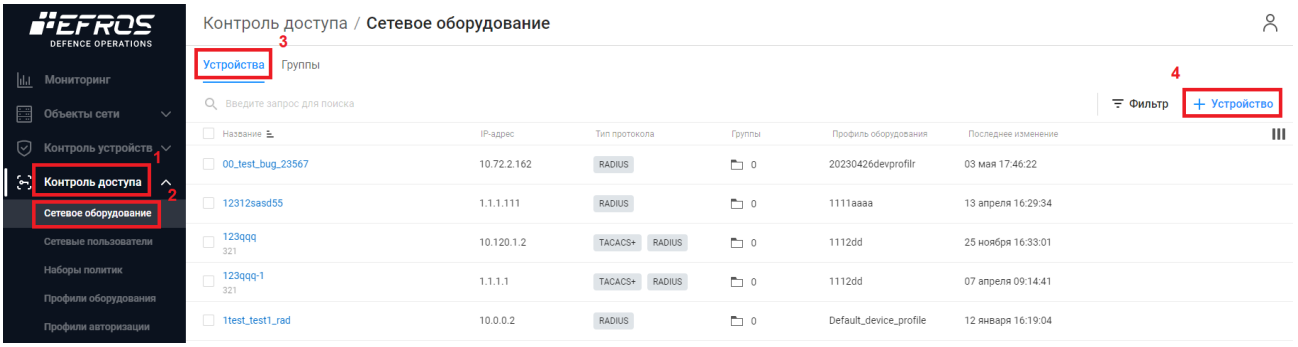



Рисунок 106 – Создание устройства

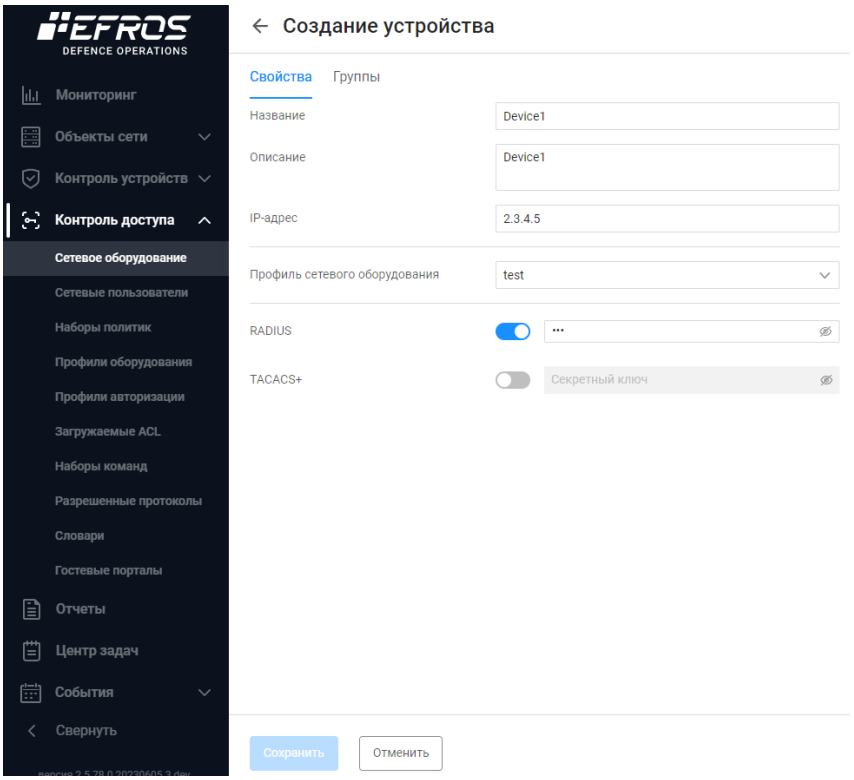



Рисунок 107 – Создание устройства

## A.2 Использование протокола TACACS+

Краткая последовательность действий для настройки типового сценария взаимодействия с TACACS+ представлена в таблице 37. Схематичные шаги показаны на рис. 108.

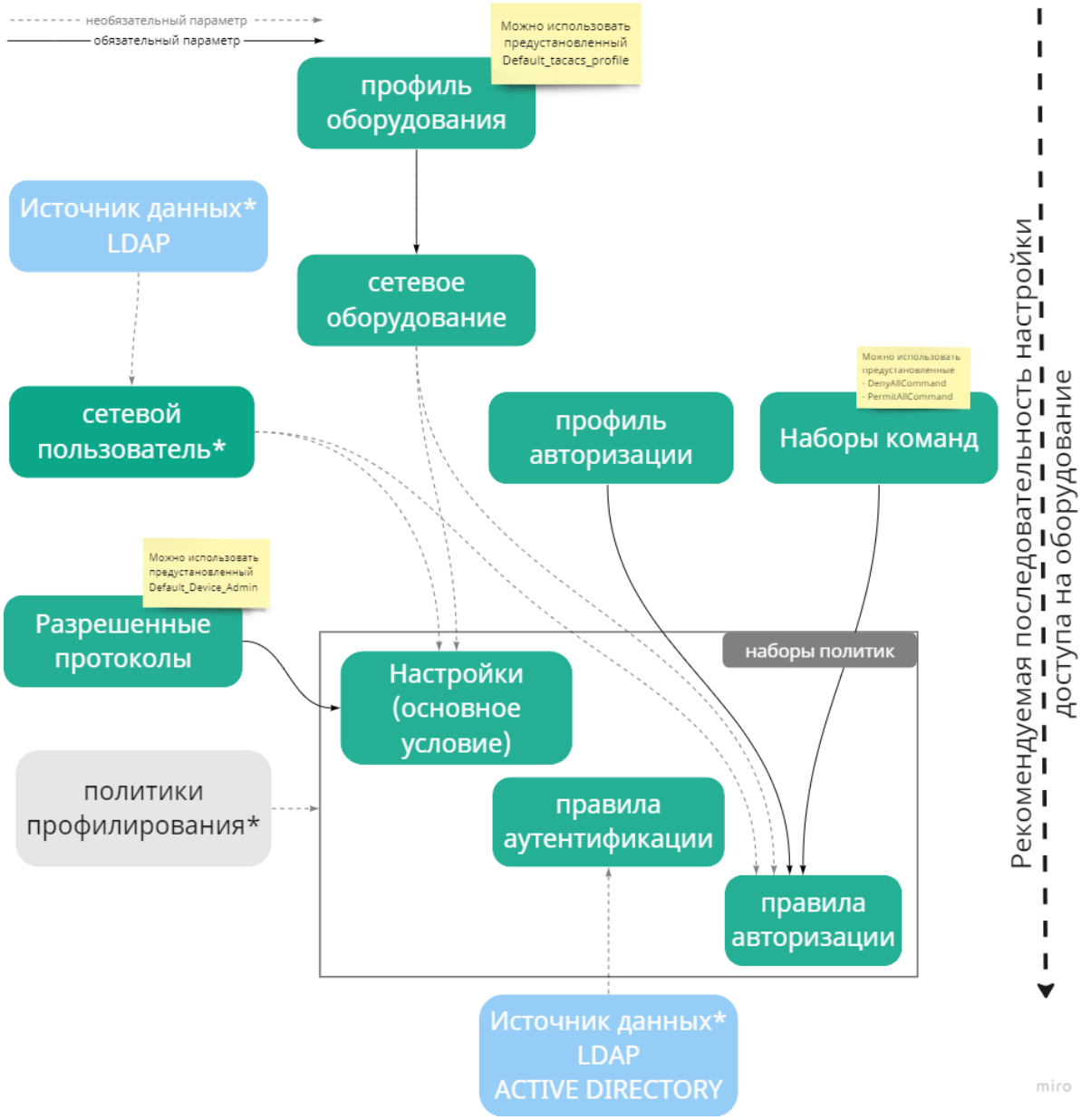



Рисунок 108 – Схема с кратким алгоритмом настройки типового сценария взаимодействия с протоколом TACACS+

Таблица 37 – Краткая последовательность действий для настройки типового сценария взаимодействия с TACACS+

| № п/п | Действие | Описано в разделе документа |
|---|---|---|
| 1 | Создать/добавить/подключить необходимые источники данных[7]:<br>• конечные точки;<br>• локальные сетевые пользователи/группы;<br>• LDAP;<br>• домен;<br>• сертификаты | — |
| 2 | Создать набор команд | 3.8 |
| 3 | Создать список разрешенных протоколов | 3.9 |
| 4 | Создать профиль оборудования | 3.5 |
| 5 | Создать сетевое оборудование | 3.2 |
| 6 | Создать профиль авторизации | 3.6 |
| 7 | Создать набор политик | 3.4 |
| 7.1 | Создать правила аутентификации | 3.4.2.2 |
| 7.2 | Создать правила авторизации | 3.4.2.3 |

Для настройки типового сценария взаимодействия с использованием протокола TACACS+ пользователю комплекса необходимо выполнить следующие шаги:

1) Предварительно настроить сетевое оборудование для взаимодействия с сервером ПК «Efros DO» с использованием механизмов AAA по протоколу TACACS+.
2) Определить источник данных, где будет сверяться пользователь, которому необходимо предоставить доступ на оборудование. Более подробно см. пункт 1) «Использование протокола RADIUS».
3) Создать список разрешенных протоколов для аутентификации:

— перейти в раздел «Контроль доступа», подраздел «Разрешенные протоколы» (рис. 109);

[7] Добавление сертификатов, настройка подключения к AD (LDAP) и создание конечной точки описано в документе «Руководство пользователя. Часть 1. Администрирование»

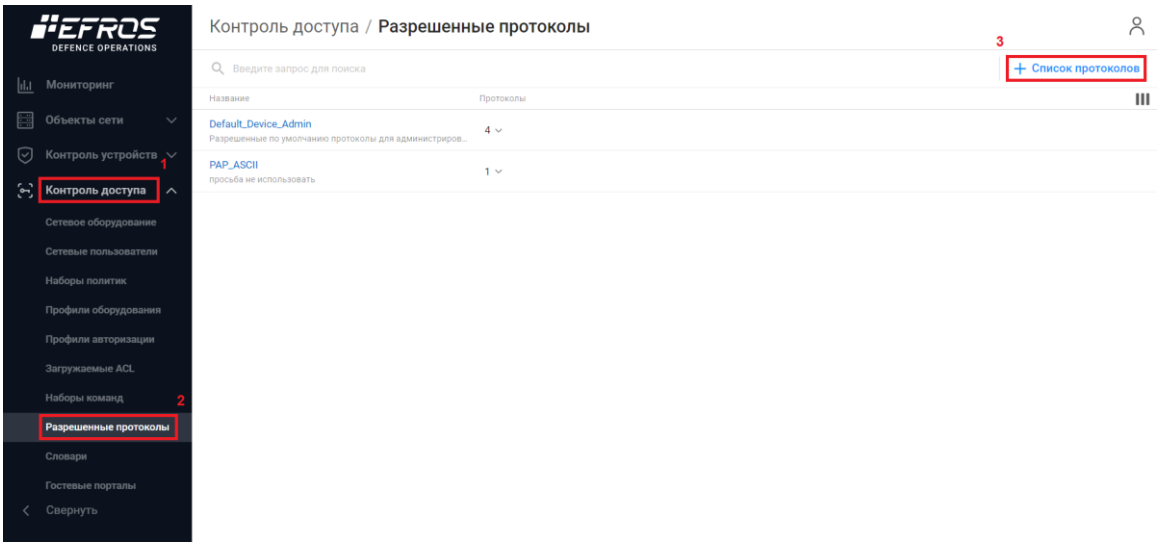



Рисунок 109 – Разрешенные протоколы

— на странице нажать кнопку « + Список протоколов »;
— заполнить поля страницы необходимыми параметрами (рис. 110) (более подробно о создании списка протоколов написано в п. 3.9).

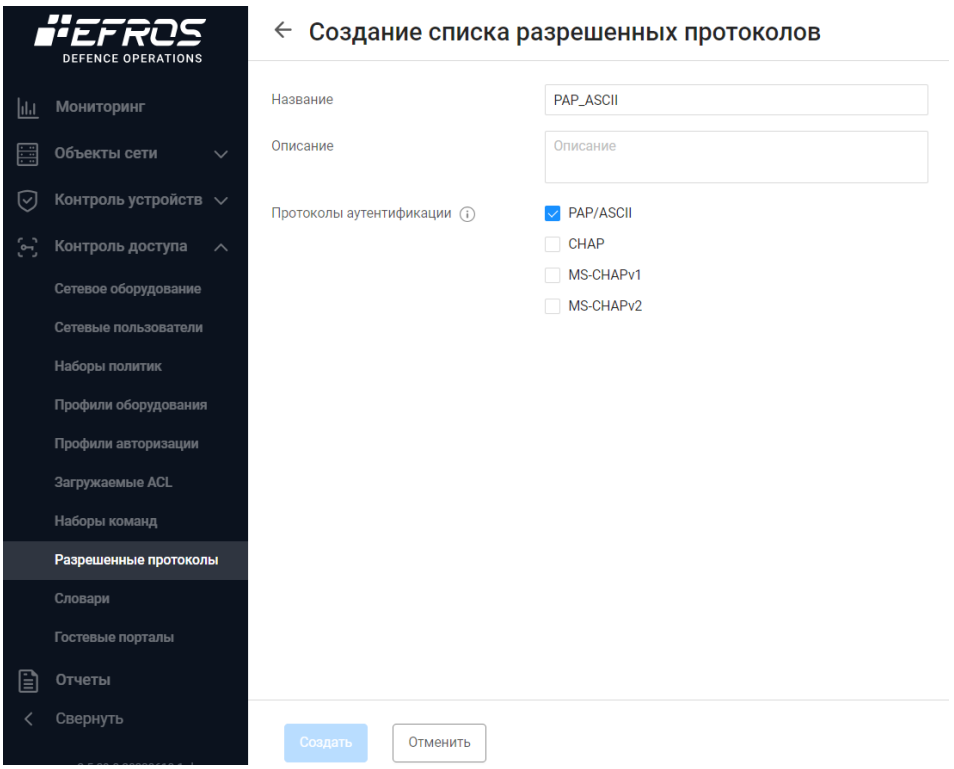



Рисунок 110 – Создание списка разрешенных протоколов

4) Создать набор команд:

— перейти в раздел «Контроль доступа», подраздел «Разрешенные протоколы» (рис. 111);

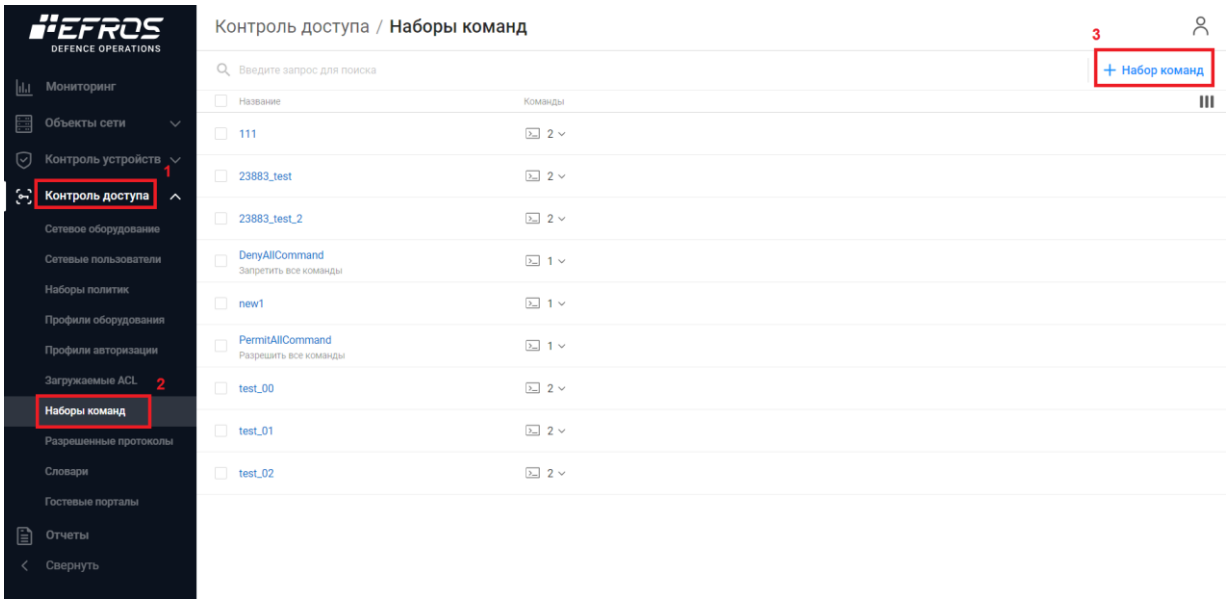



Рисунок 111 – Набор команд

— на странице нажать кнопку « + Набор команд »;
— заполнить поля страницы необходимыми параметрами (рис. 112) (более подробно о наборе команд написано в п. 3.8).

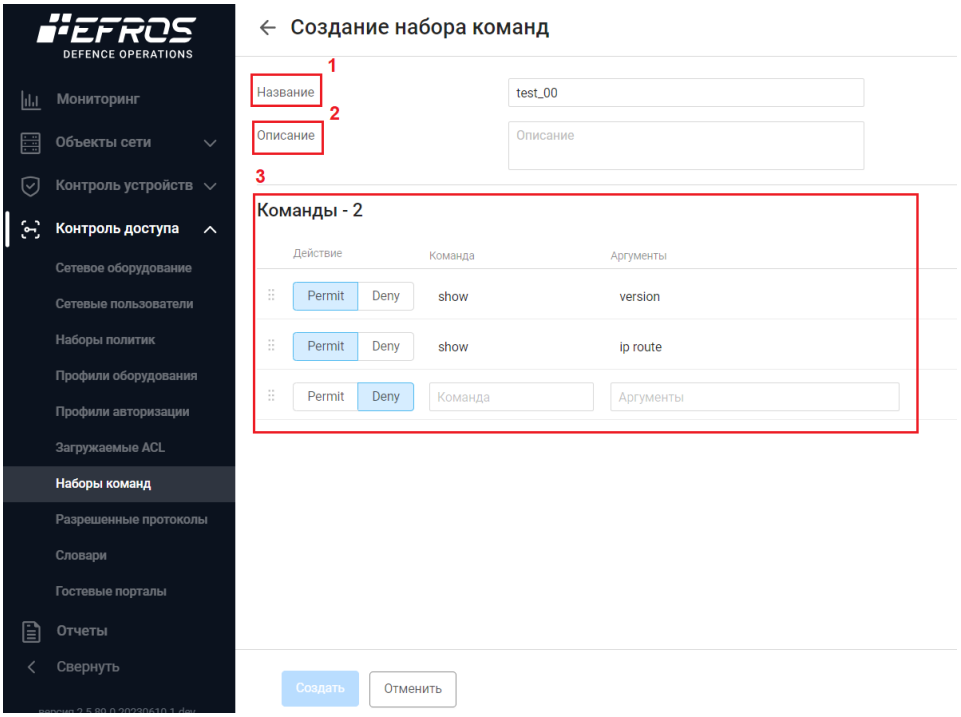



Рисунок 112 – Создане набора команд

5) Создать профиль сетевого оборудования. Профиль оборудования необходим для назначения общих правил аутентификации и авторизации на оборудовании для сетевых пользователей:

— перейти в раздел «Контроль доступа», подраздел «Профили оборудования»;

— нажать кнопку « + Профиль оборудования » (рис. 113);

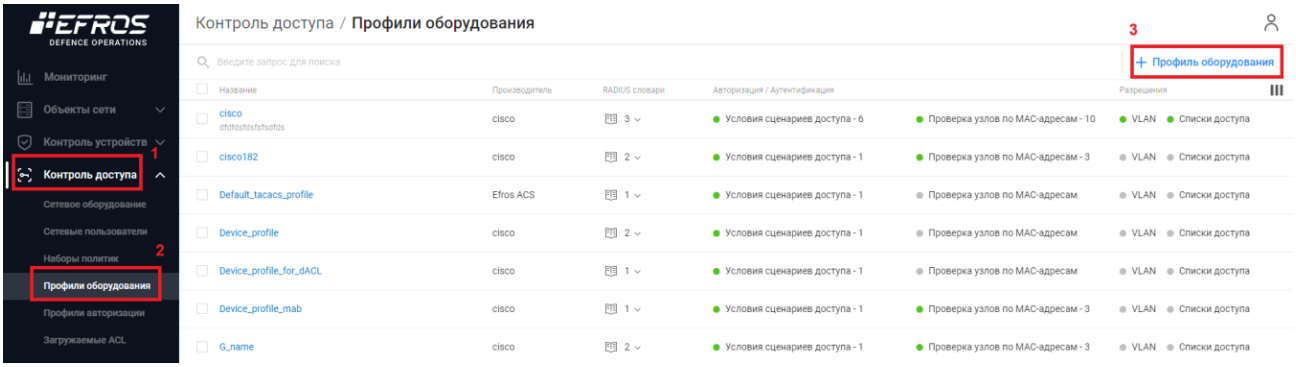



Рисунок 113 – Создание сетевого профиля оборудования

— заполнить поля страницы создания профиля сетевого оборудования необходимыми параметрами (рис. 114) (более подробно о профиле оборудования написано в п. 3.5.1).

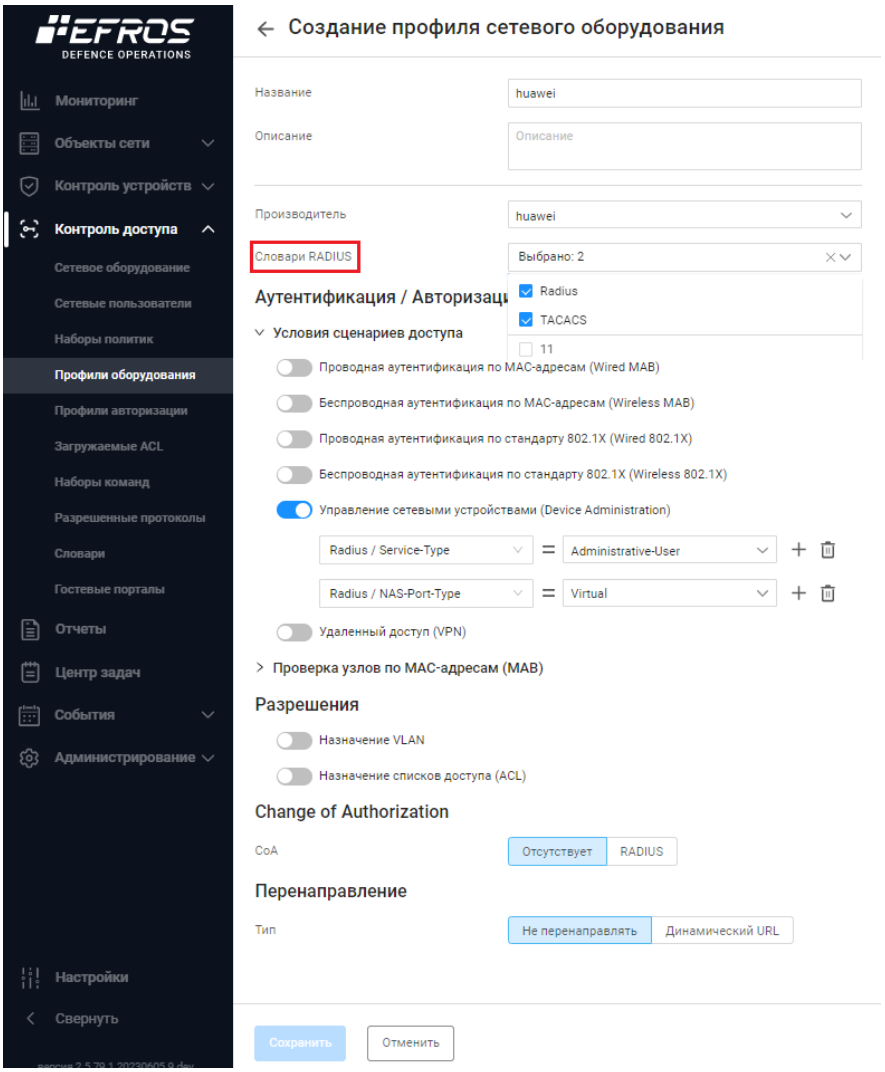



Рисунок 114 – Создание сетевого профиля оборудования

Словари RADIUS не влияют на настройку сценария доступа по протоколу TACACS+. Пользователь может выбрать любой.

6) Перейти в раздел «Контроль доступа», подраздел «Сетевое оборудование». Создать сетевое оборудование. Для этого необходимо:

— на вкладке «Устройства» нажать кнопку « + Устройство » (рис. 115);
— заполнить поля необходимыми данными, указать профиль сетевого оборудования, созданный на шаге 5 (рис. 116);
— указать TACACS+ Shared key.

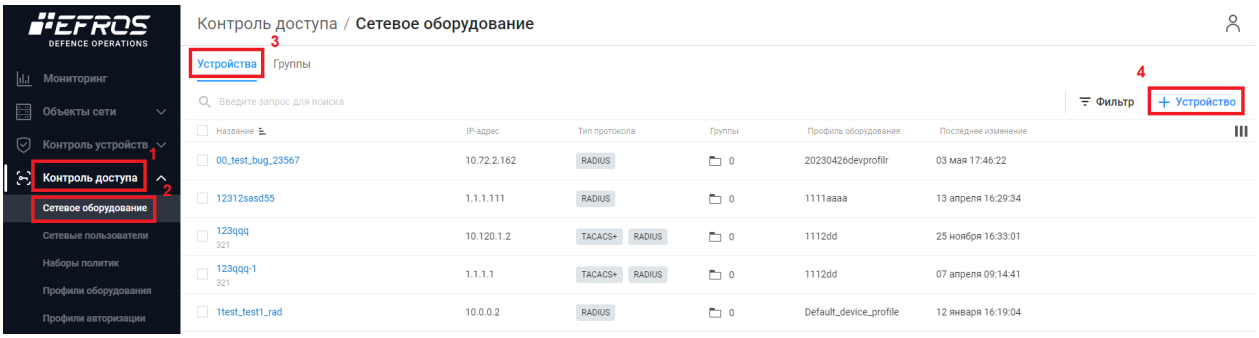



Рисунок 115 – Создание устройства

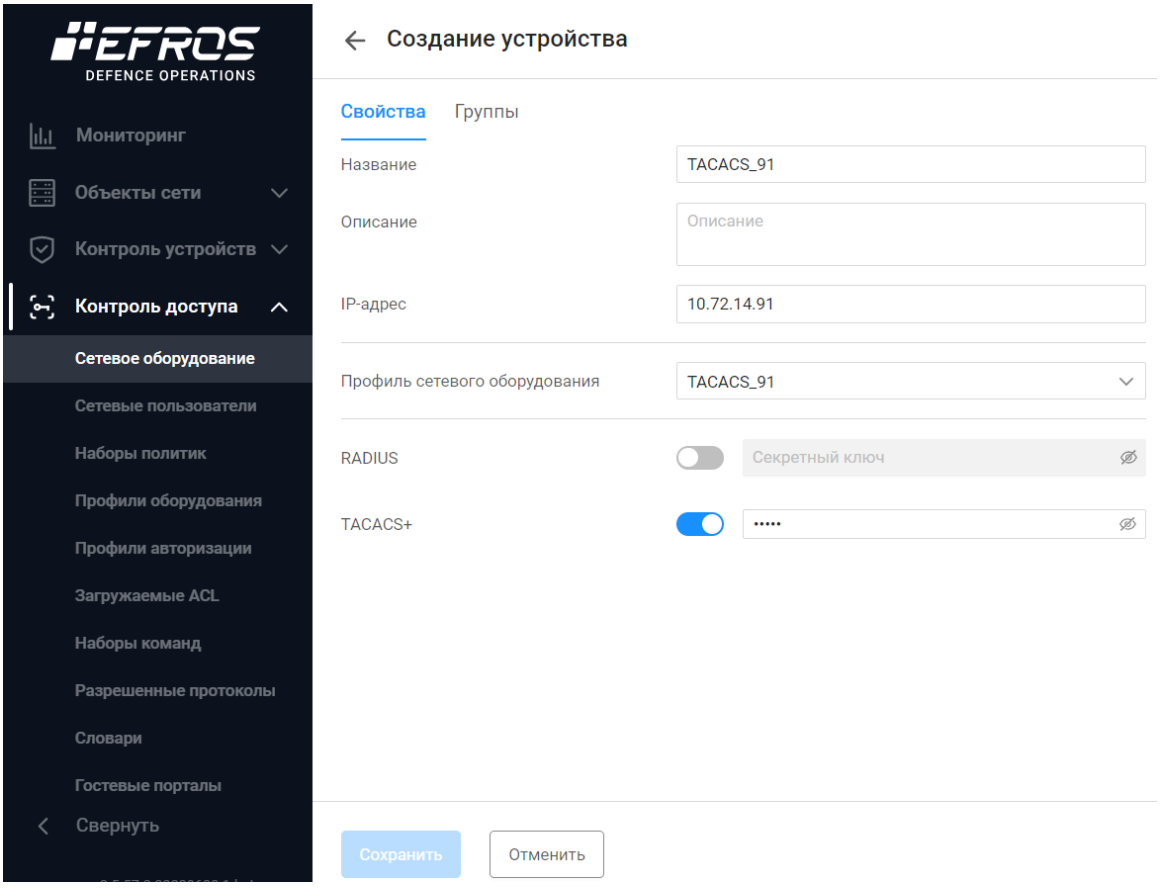



Рисунок 116 – Создание устройства

7) Создать сетевого пользователя.

— перейти в раздел «Контроль доступа», подраздел «Сетевые пользователи», вкладка «Пользователи»;

— нажать кнопку «+ Пользователь» (рис. 117);

— заполнить поля страницы необходимыми параметрами и нажать кнопку «Создать» (более подробно о сетевом пользователе написано в п.п. 3.3.1.1). Примеры создания сетевого пользователя представлены на рис. 118 – рис. 120.

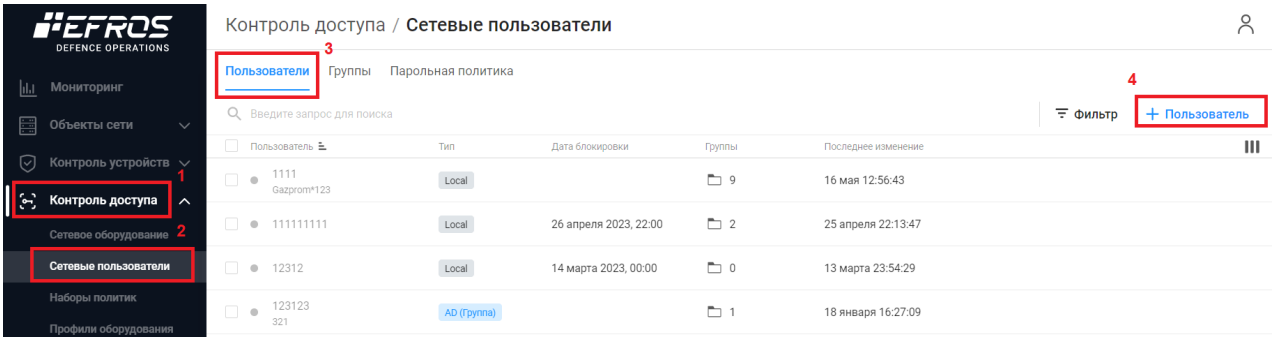



Рисунок 117 – Создание сетевого пользователя

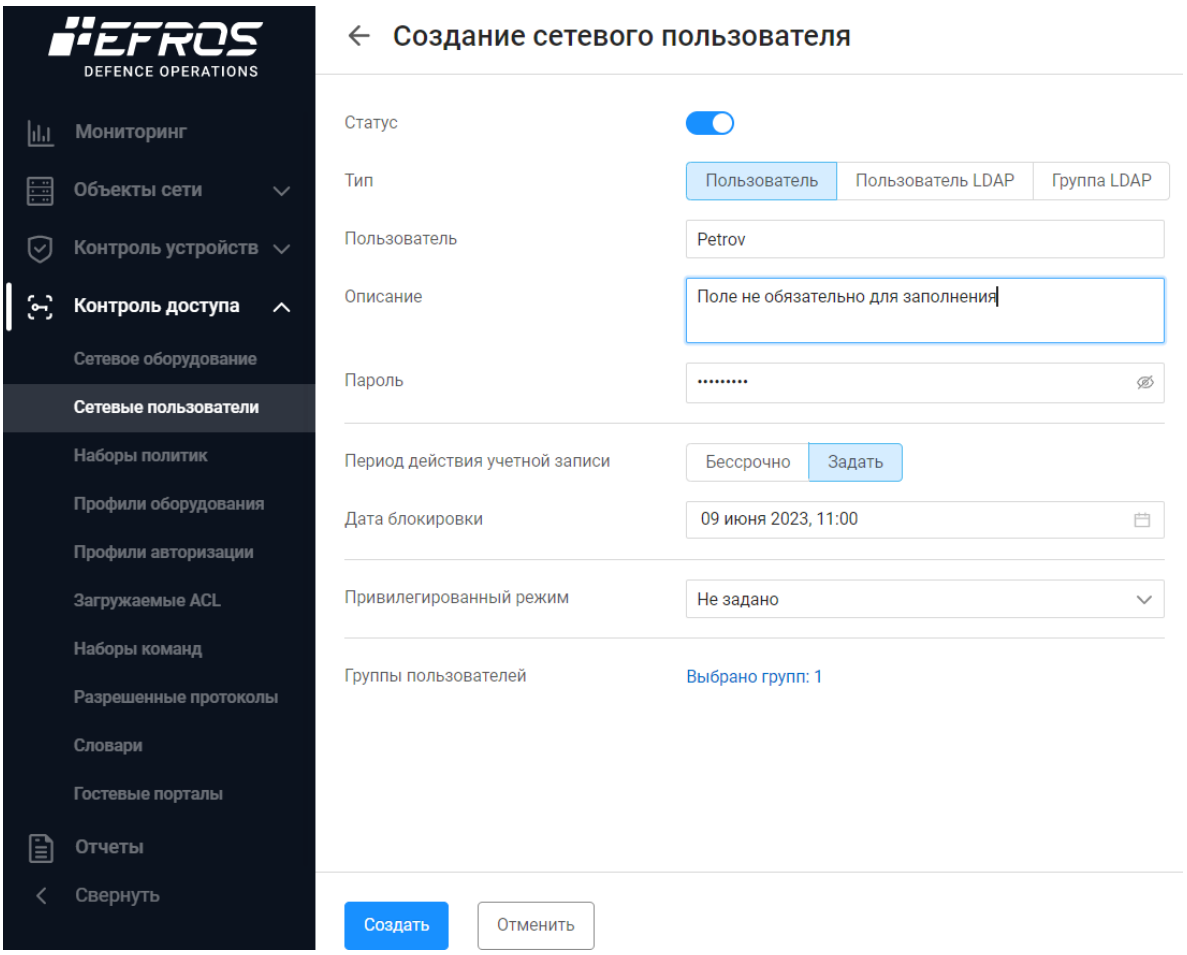



Рисунок 118 – Создание локального сетевого пользователя

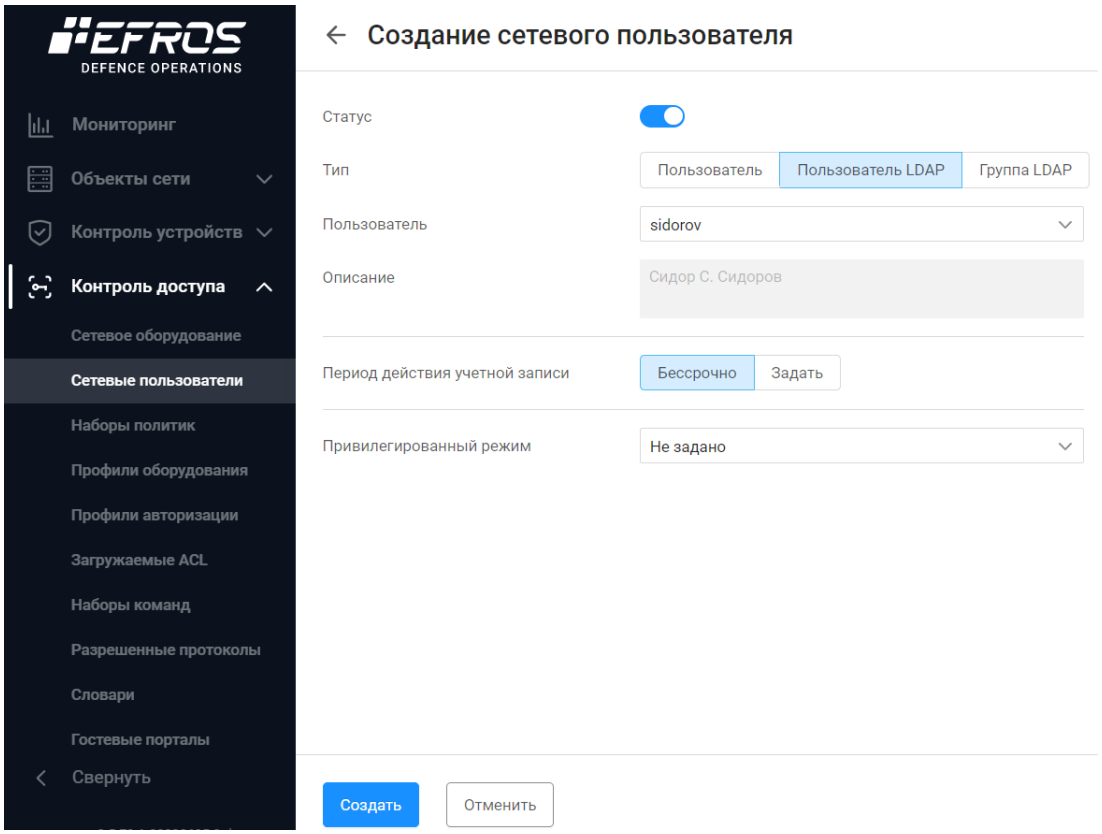



Рисунок 119 – Создание пользователя LDAP

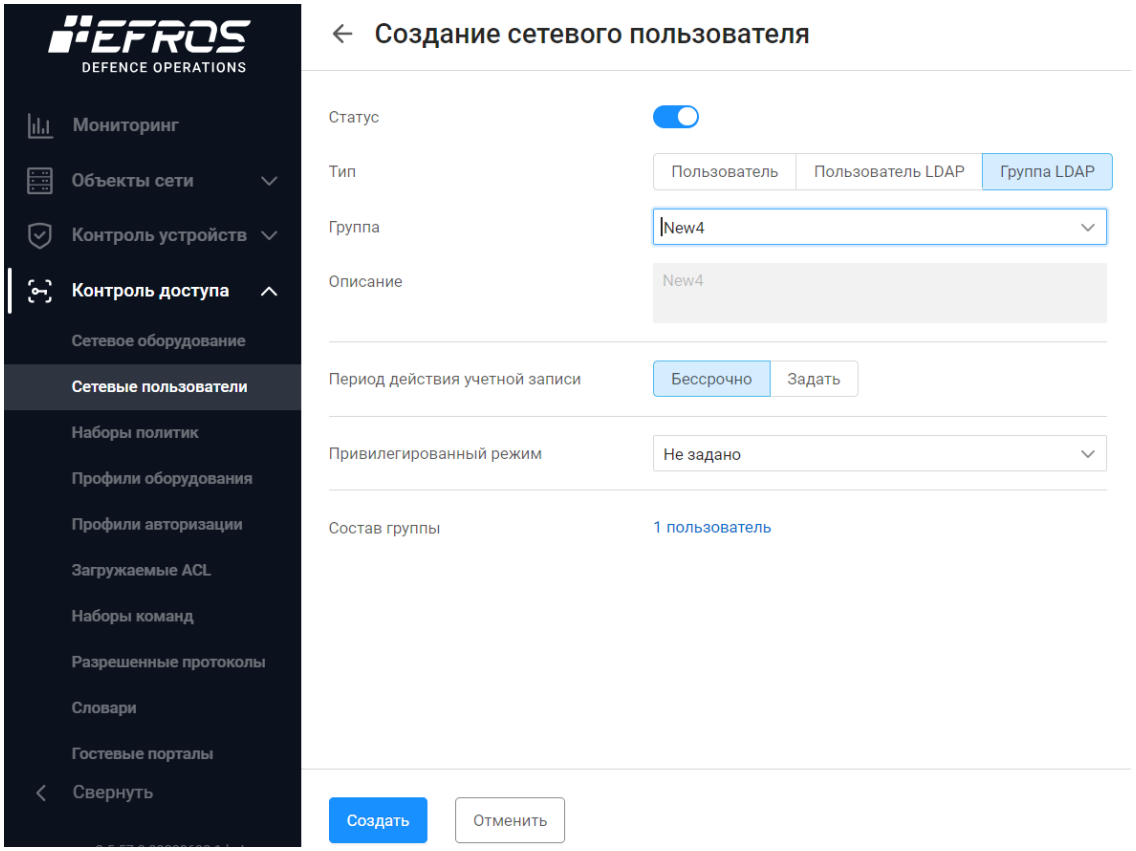



Рисунок 120 – Создание группы LDAP

8) Создать профили авторизации «Доступ на оборудование» (для предоставления доступа к оборудованию с использованием протокола TACACS+). Для создания профиля авторизации необходимо выполнить следующее:

— выбрать на странице «Профиль авторизации» вкладку «Доступ в сеть»;

— нажать кнопку «+ Профиль» (рис. 121);

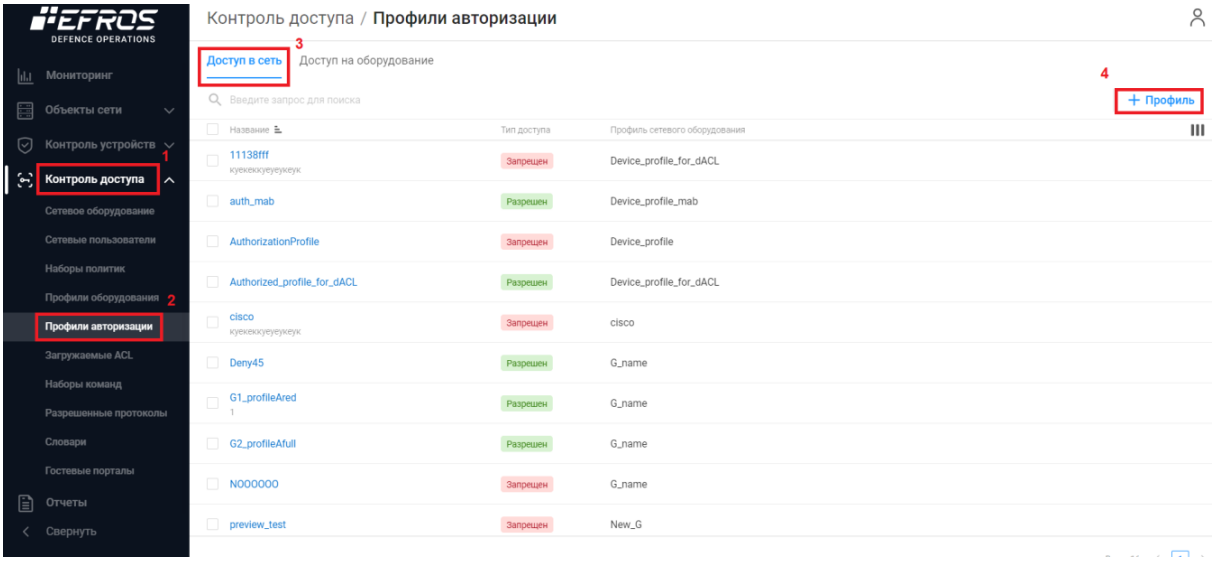



Рисунок 121 – Создание профиля авторизации «Доступ на оборудование»

— заполнить необходимые поля на странице создания профиля авторизации (более подробно о профилях авторизации доступа на оборудование написано в п. 3.6.2) (рис. 122).

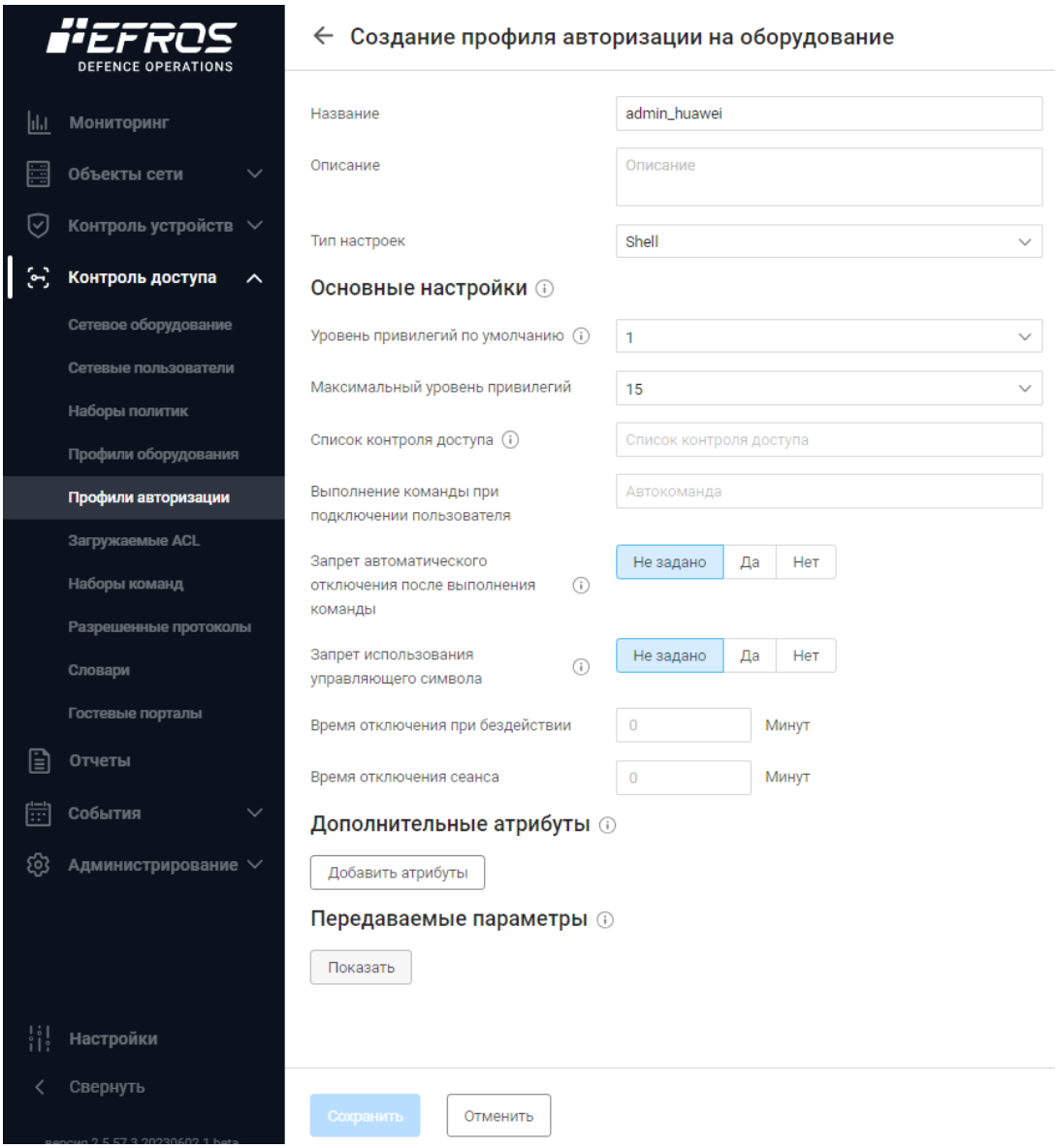



Рисунок 122 – Создание профиля авторизации доступа в сеть

9) Создать требуемый набор политик доступа (более подробно о создании набора политик написано в подразделе 3.1). Для этого необходимо:

— перейти в раздел «Контроль доступа», подраздел «Наборы политик»;
— выбрать вкладку «Доступ на оборудование», которая позволяет создать набор политик доступа на оборудование для сетевого пользователя.

Вкладка «Шаблоны условий» позволяет создавать шаблоны условий в виде отдельных полей, которые можно сохранить в списке шаблонов условий, а затем повторно использовать для других условий или политик. Такие шаблоны будут считаться пользовательскими.

— нажать кнопку « + Политика » (рис. 123);

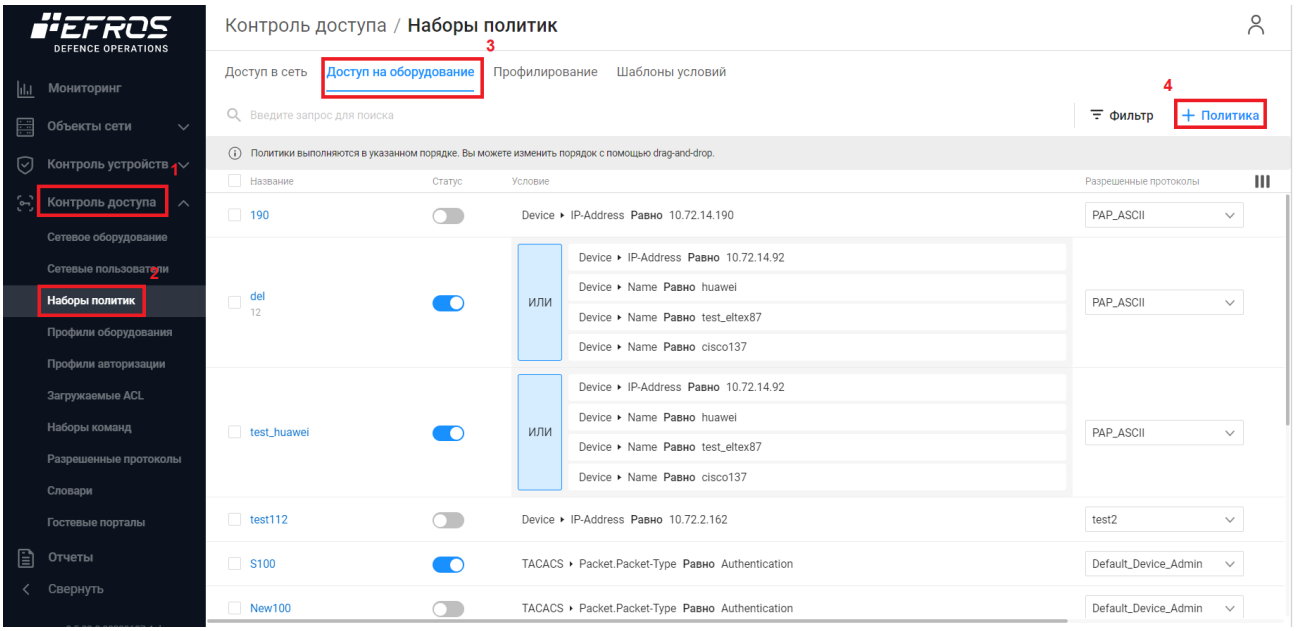



Рисунок 123 – Создание набора политик «Доступ на оборудование»

— указать название/описание политики, выбрать статус, выбрать список разрешенных протоколов (из созданных выше или выбрать стандартный Default_Device_Admin), создать условия срабатывания политики[8] или выбрать условие из шаблона условий (рис. 124);

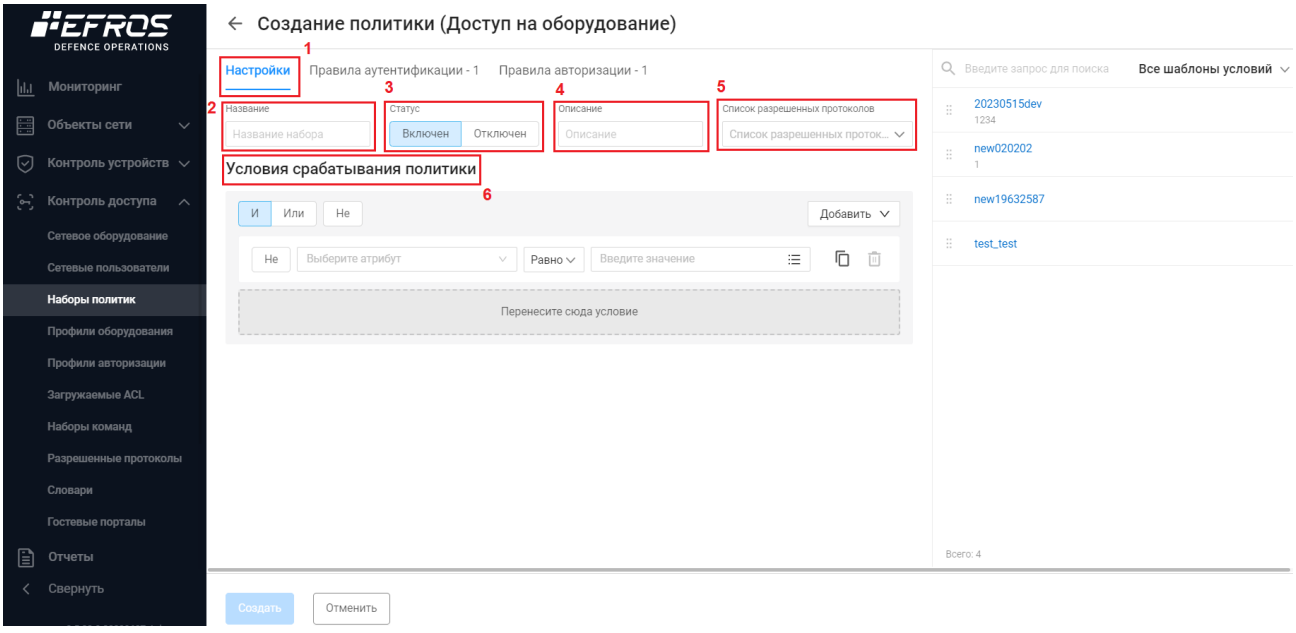



Рисунок 124 – Создание условия срабатывания политики

— на вкладке «Правила аутентификации» нужно определить, каким образом и где происходит аутентификация устройства (рис. 125). Для этого необходимо в

[8] Это условия, которым в первую очередь должен соответствовать пользователь при попытке получения доступа на оборудование

первую очередь настроить правило «Default» (правило "по умолчанию", которое будет выполнено, если не сработает ни одно созданное дополнительно правило. Рекомендуется выставить параметры для запрета доступа на оборудования):

- выбрать источник данных. Для правила по умолчанию рекомендуется выбрать «DenyAccess»;
- выбрать действие при ошибке аутентификации. Для правила по умолчанию рекомендуется выбрать «Отклонить».

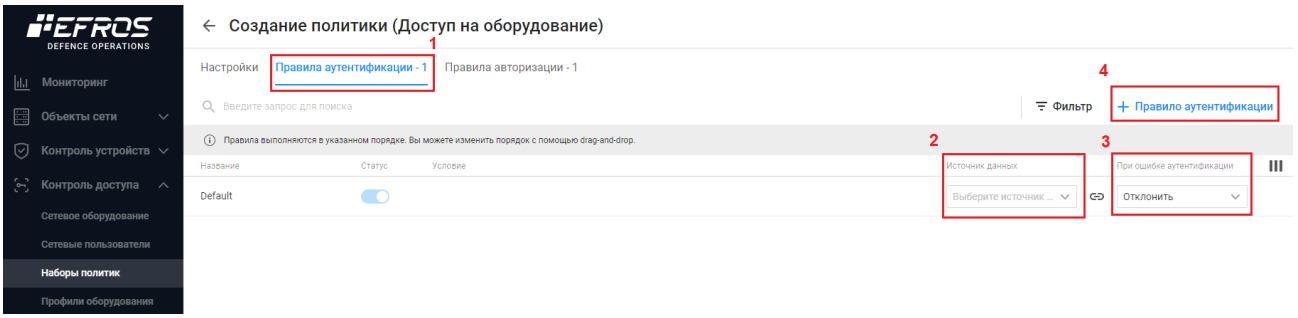



Рисунок 125 – Создание правила аутентификации

— нажать кнопку « + Правило аутентификации »;
— заполнить поля необходимыми данными (рис. 126):

- указать название правила;
- выбрать статус «Активен»;
- указать источник данных из предлагаемых значений (об источниках данных написано в шаге 1);
- указать действие, которое будет выполняться в случае, если аутентификация не пройдена;
- создать условие для срабатывания правила или выбрать условие из предлагаемых шаблонов:
  - *выбрать атрибут из раскрывающегося списка;*
  - *выбрать значение атрибута;*
  - *выбрать логическую операцию из раскрывающегося списка. Допускается использовать регулярные выражения.*

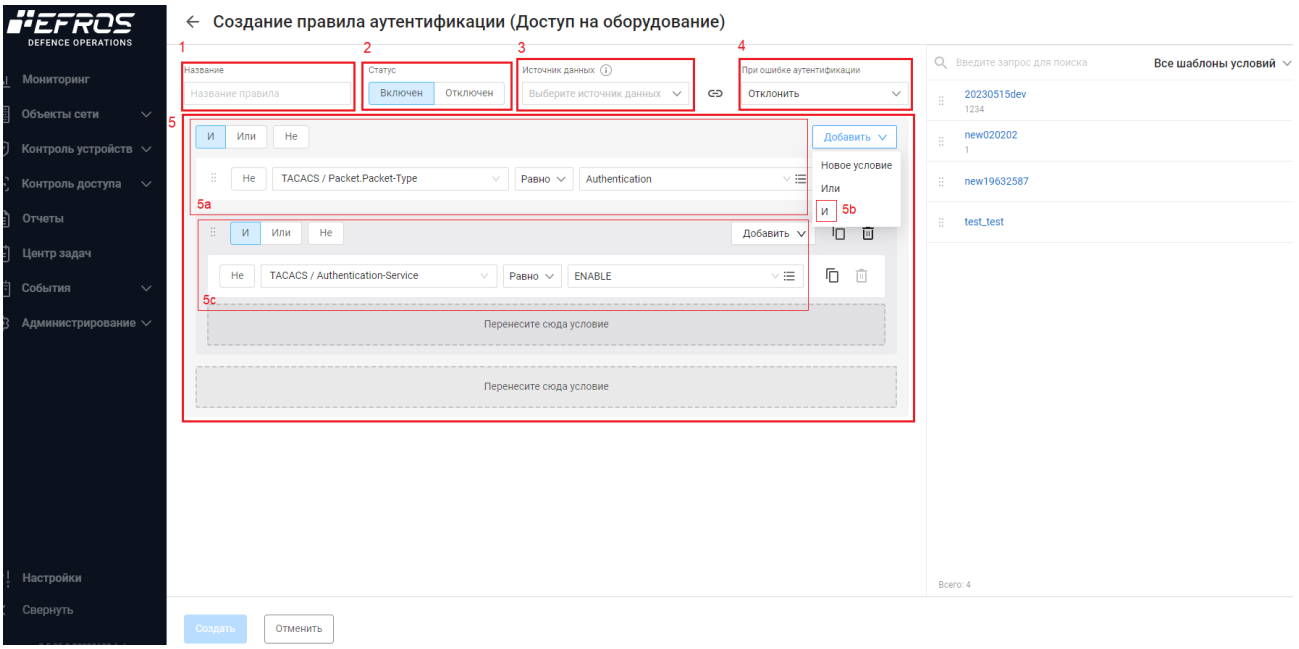



Рисунок 126 – Создание правила аутентификации

— перейти на вкладку «Правила авторизации» (рис. 127). На вкладке «Правила авторизации» нужно определить, каким образом происходит авторизация пользователя на устройстве. Для этого необходимо в первую очередь настроить правило «Default» (правило "по умолчанию", которое будет выполнено, если не сработает ни одно созданное дополнительно правило. Рекомендуется выставить параметры для запрета доступа на оборудования):

- выбрать созданный ранее набор команд;
- выбрать созданный ранее профиль авторизации.

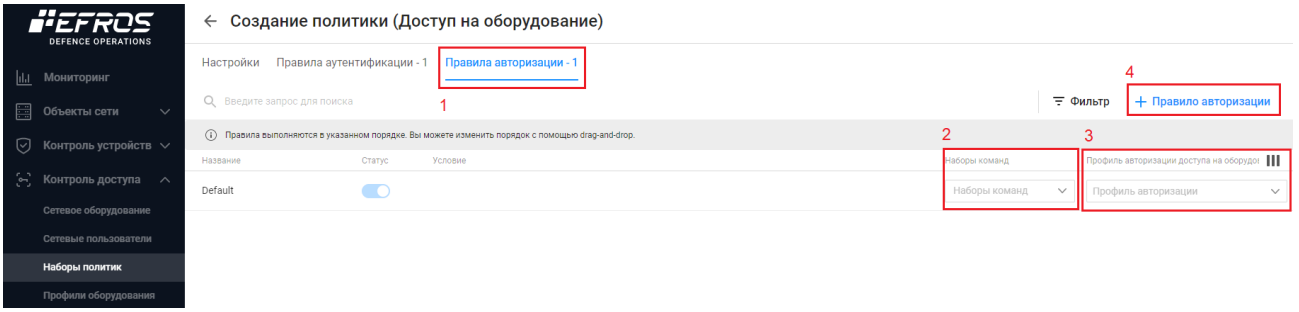



Рисунок 127 – Создание правила авторизации

— на вкладке нажать кнопку « + Правило авторизации »;
— заполнить поля необходимыми данными (рис. 128):

- указать название правила;
- выбрать статус «Активен»;
- выбрать набор команд, созданный ранее;
- выбрать профиль авторизации, созданный ранее;

- создать условие для срабатывания правила или выбрать условие из предлагаемых шаблонов:
  - *выбрать атрибут из раскрывающегося списка;*
  - *выбрать значение атрибута;*
  - *выбрать логическую операцию из раскрывающегося списка.*

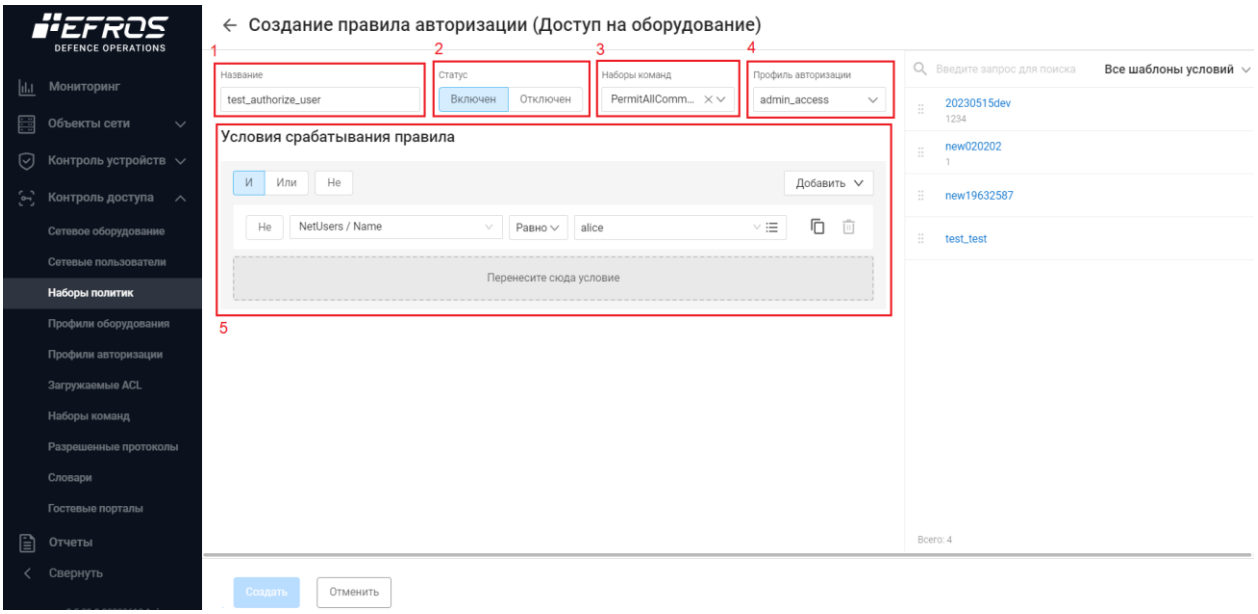



Рисунок 128 – Создание правила авторизации

10) Нажать кнопку «Создать».

Если создано несколько политик доступа, при запросе подключения проверка по условиям срабатывания будет осуществляется по списку политик в указанном порядке (сверху вниз).

# Приложение Б
# Рекомендуемая последовательность действий для настройки доступа в сеть с использованием профилирования

Поддерживаемые в ПК «Efros DO» источники профилирования:

- CDP;
- DHCP;
- Edo-Agent;
- LLDP;
- RADIUS;
- SNMP;
- UserAgent.

При получении или обновлении параметров профилирования от источников профилирования конечной точки, осуществляется проверка на соответствие полученных данных условиям политик, заданным в политиках профилирования («Наборы политик» → вкладка «Профилирование»). В случае совпадения с условиями одной или нескольких политик – конечной точке назначается один или несколько профилей, которые соответствуют названию сработавших активных политик.

Если в политике профилирования выбрать метки при назначении профиля, то они автоматически будут добавлены к конечной точке при срабатывании политики.

## Б.1 Источник профилирования RADIUS

Профилирование с использованием протокола RADIUS заключается в определении производителя (вендора) устройства по его MAC-адресу при создании конечной точки (при запросе доступа подключения к сети).

Для определения вендора по данным атрибутов протокола RADIUS политики профилирования не используются.

База производителей предустановлена в ПК «Efros DO», возможность её редактирования отсутствует.

Для использования информации о производителе оборудования конечной точки в условиях политики доступа в сеть, а также входящих в ее состав правилах аутентификации и авторизации, необходимо выбрать значение атрибута словаря EndPoints/VendorName.

Для использования информации о назначенной метке конечной точки в условиях политики доступа в сеть необходимо выбрать значение атрибута словаря EndPoints/Tag.

Для создания набора политик доступа в сеть с использованием назначаемого профиля конечной точке пользователю комплекса необходимо сделать следующие шаги:

1) Настроить конечную точку на стороне заказчика и инициировать запрос доступа в сеть;
2) Использовать предустановленную политику профилирования или сформировать политику вручную:

— перейти в подраздел «Наборы политик», вкладка «Профилирование»;
— нажать кнопку «Политика». Откроется страница создания политики профилирования (рис. 129).

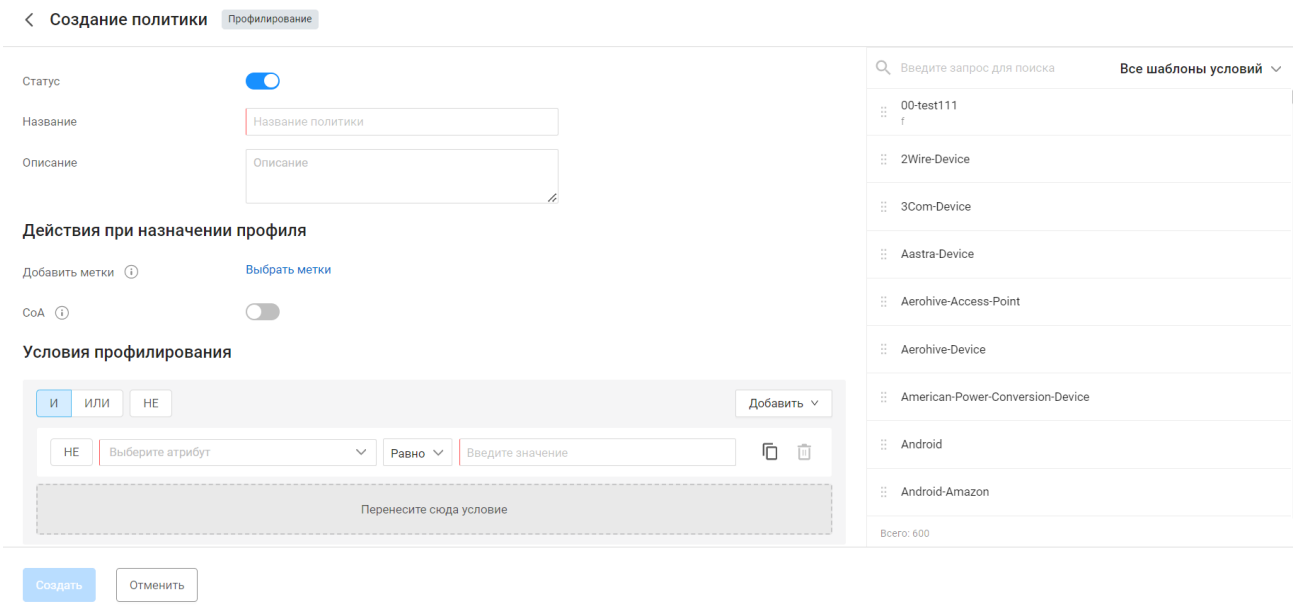



Рисунок 129 – Создание политики профилирования

— заполнить поля страницы необходимыми параметрами. Особенности заполнения полей описаны ниже:

- поле «Статус»: активен;
- поле «Название»: любое;
- поле «Описание»: любое;
- поле «Добавить метки»: при необходимости назначить метки для возможности использования их в политике доступа в сеть (условия, правила аутентификации и авторизации);
- поле «CoA»: Повторная аутентификация при назначении профиля конечной точке в результате срабатывания политики профилирования.

Действие не выполняется, если на сетевом оборудовании, взаимодействующем с сервером ПК «Efros DO», отсутствует настройка «Change of Authorization», если для сетевого оборудования не заданы настройки в профиле оборудования и если оборудование не поддерживает «CoA»;

- создать условия профилирования (или выбрать условие из шаблонов):
  - *выбрать условие «И\ИЛИ или НЕ»;*
  - *выбрать атрибут: например, «Radius/UserName»;*
  - *назначить значение этому атрибуту;*
  - *назначить логический оператор.*

Как только конечная точка появится в сети, комплекс, согласно созданным политикам профилирования, автоматически присвоит конечной точке определенный профиль. В случае создания/изменения политик профилирования, будет осуществлена проверка для всех существующих конечных точек на соответсвие политикам.

3) Создать требуемую политику доступа в сеть. Данная политика будет применяться именно к конечной точке/группе конечных точек, которым присвоен профиль, соответствующий политикам профилирования.

Для использования в условиях политики и правилах аутентификации набора политик доступа в сеть информации о назначенных конечной точке:

метке – необходимо выбрать значение атрибута словаря EndPoints/Tag;
профиле – необходимо выбрать значение атрибута словаря EndPoints/BaseProfile.

## Б.2 Источник профилирования DHCP

ПК «Efros DO» использует атрибуты, передаваемые конечной точкой на сервер DHCP при запросе доступа в сеть для получения IP-адреса. Профилирование по источнику DHCP позволяет определить такие параметры, как: MAC-адрес конечной точки, hostname, вендор, ОС, модель устройства и др.

Для того, чтобы комплекс получал информацию от источника DHCP, необходимо настроить перенаправление копии DHCP-трафика на сетевом оборудовании, которое пересылает DHCP-запросы от конечных точек на сервер DHCP.

Для настройки ретрансляции DHCP-трафика на коммутаторах производителя Cisco используется команда «ip helper-address», после которой необходимо указать адрес сервера ПК «Efros DO».

Для создания набора политик доступа в сеть с использованием источника профилирования DHCP пользователю комплекса необходимо сделать следующие шаги:

1) Настроить перенаправление копии DHCP-трафика на сетевом оборудовании, которое пересылает DHCP-запросы от конечных точек на сервер DHCP.
2) Настроить конечную точку на стороне заказчика и инициировать запрос доступа в сеть.
3) Использовать предустановленную политику профилирования или сформировать политику вручную, для чего:

— перейти в подраздел «Наборы политик», вкладка «Профилирование»;
— нажать кнопку «Политика». Откроется окно создания политики профилирования (см. рис. 129).
— заполнить поля страницы необходимыми параметрами. Особенности заполнения полей описаны ниже:

- поле «Статус»: активен;
- поле «Название»: любое;
- поле «Описание»: любое;
- поле «Добавить метки»: при необходимости назначить метки для логического группирования конечных точек по общему признаку;
- поле «CoA»: Повторная аутентификация при назначении профиля конечной точке в результате срабатывания политики профилирования. Действие не выполняется, если на сетевом оборудовании, взаимодействующем с сервером аутентификации, отсутствует настройка Change of Authorization;
- создать условия профилирования (или выбрать условие из шаблонов) (рис. 130):
  - *выбрать условие «И\ИЛИ или НЕ»;*
  - *выбрать атрибут: например, «ParameterRequestListString»;*
  - *назначить значение этому атрибуту;*
  - *назначить логический оператор.*

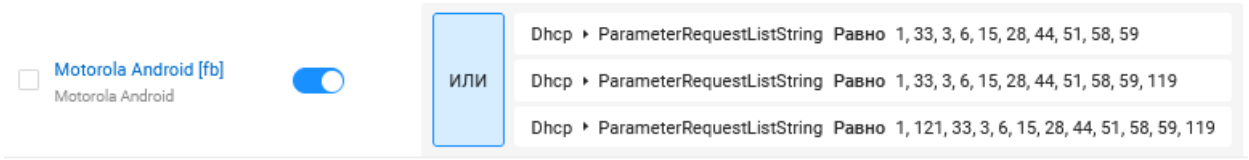



Рисунок 130 – Пример условий политики профилирования с атрибутом ParameterRequestListString

Основные атрибуты, которые рекомендуется использовать при формировании политик профилирования с использованием данных от источника DHCP:

— «Clientmac» – содержит MAC-адрес устройства. Значение данного атрибута используется для определения производителя оборудования;
— «Hostname» – содержит hostname устройства;
— «VendorClassIdentifier» – опция 60 из пакета DHCP. В данной опции содержится информация об аппаратной конфигурации или другой идентификационной

информации о конечной точке;

— «ParameterRequestListString» – опция 55 из пакета DHCP. Строка, передаваемая в данной опции, состоит из набора чисел. По последовательности чисел в этой строке определяются различные параметры оборудования – установленная ОС, модель оборудования, класс устройства и пр.

Как только конечная точка получает доступ в сеть, комплекс, согласно созданным правилам профилирования, автоматически присваивает конечной точке соответствующий профиль. Также профиль будет назначен уже существующим конечным точкам, которые соответствуют созданным политикам профилирования.

4) Создать требуемый набор политик. Данный набор политик будет применяться именно к конечной точке/группе конечных точек, которым присвоен профиль, соответствующий политикам профилирования.

## Б.3 Источник профилирования User-Agent

HTTP User-Agent – заголовок запроса, содержащий информацию, которая позволяет идентифицировать ОС и браузер, используемые на конечной точке.

Получение информации от источника профилирования «User-Agent» осуществляется при использовании сценария гостевого доступа при открытии пользователем браузера для аутентификации на гостевом портале (более подробно о гостевом портале написано в подразделе 3.12 и приложении Г).

Для создания набора политик доступа в сеть с использованием источника профилирования «User-Agent» пользователю комплекса необходимо сделать следующие шаги:

1) Создать и настроить гостевой портал.
2) Использовать предустановленную политику профилирования или сформировать политику вручную:

— перейти в подраздел «Наборы политик», вкладка «Профилирование»;

— нажать кнопку «Политика». Откроется окно создания политики профилирования (см. рис. 129).

— заполнить поля страницы необходимыми параметрами. Особенности заполнения полей описаны ниже:

- поле «Статус»: активен;
- поле «Название»: любое;
- поле «Описание»: любое;
- поле «Добавить метки»: при необходимости назначить метки для логического группирования конечных точек по общему признаку;
- поле «CoA»: Повторная аутентификация при назначении профиля конечной точке в результате срабатывания политики профилирования.

Действие не выполняется, если на сетевом оборудовании, взаимодействующем с сервером аутентификации, отсутствует настройка Change of Authorization;

- создать условия профилирования (или выбрать условие из шаблонов) (рис. 131):
  - *выбрать условие «И\ИЛИ или НЕ»;*
  - *выбрать атрибут: например, «UserAgent/userAgent»;*
  - *назначить значение этому атрибуту;*
  - *назначить логический оператор.*


Рисунок 131 – Пример условий политики профилирования с атрибутом «User-Agent»

Как только пользователь откроет страницу гостевого портала в браузере для подключения к сети, комплекс, согласно созданным политикам, автоматически присвоит конечной точке определенный профиль. Также профиль будет назначен уже существующим конечным точкам, которые соответствуют созданным политикам профилирования.

Профилирование по источнику «User-Agent» позволяет определить ОС конечной точки, которая подключается, и браузер, в котором открыт гостевой портал.

3) Создать требуемый набор политик.

## Б.4 Пример присвоения метки профилирования при подключении конечной точкой к сети

Для присвоения метки профилирования при подключении к конечной точки к сети необходимо сделать следующие шаги:

1) Создать конечную точку в ПК «Efros DO» (рис. 132).

(«Объекты сети» → «Конечные точки»).

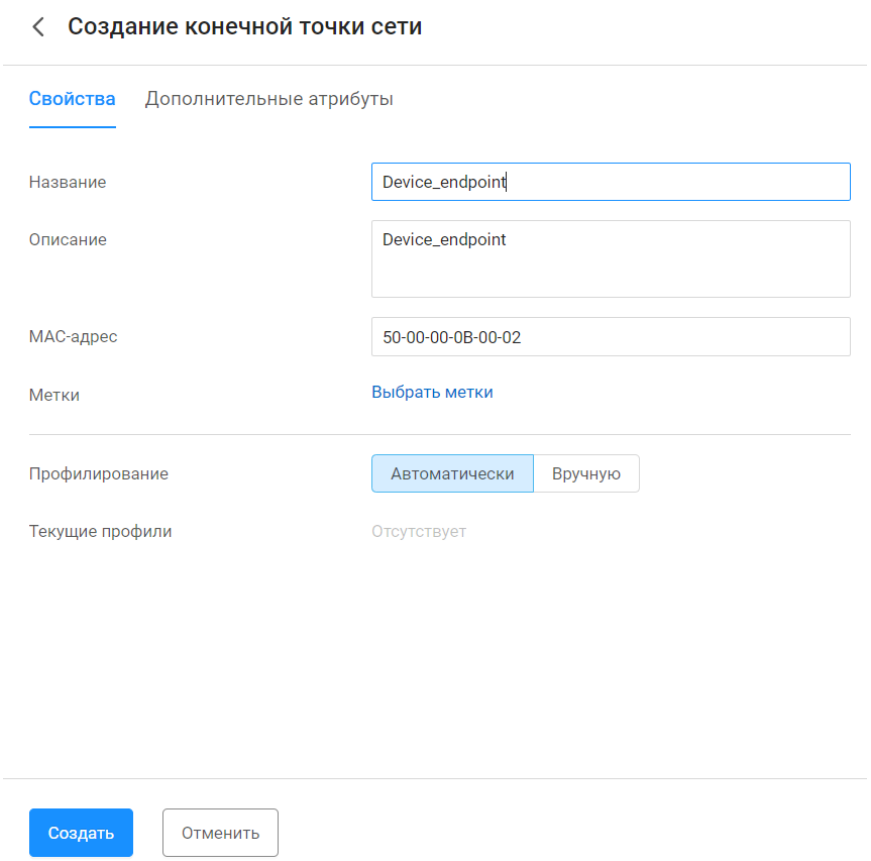



Рисунок 132 – Создание конечной точки

2) Добавить конечную точку в список разрешенных MAC адресов (рис. 133). («Контроль доступа» → «Разрешенные MAC- адреса»).

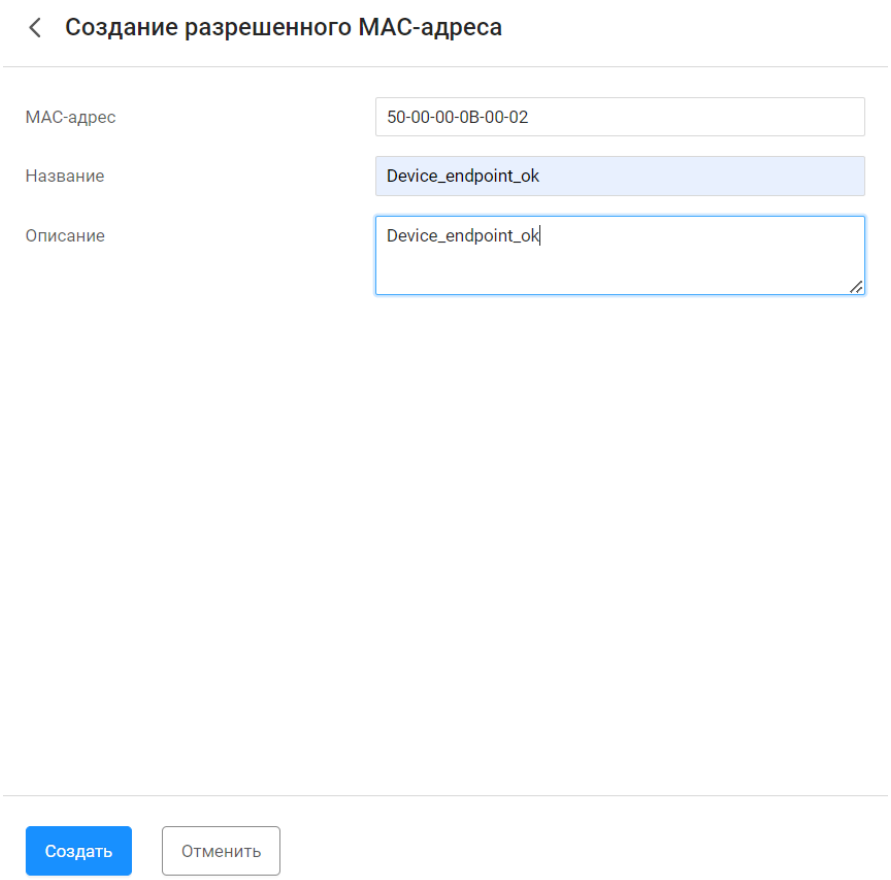



Рисунок 133 – Добавление конечной точки в список

3) Создать профиль сетевого оборудования (рис. 134). («Контроль доступа» → «Профили оборудования»).

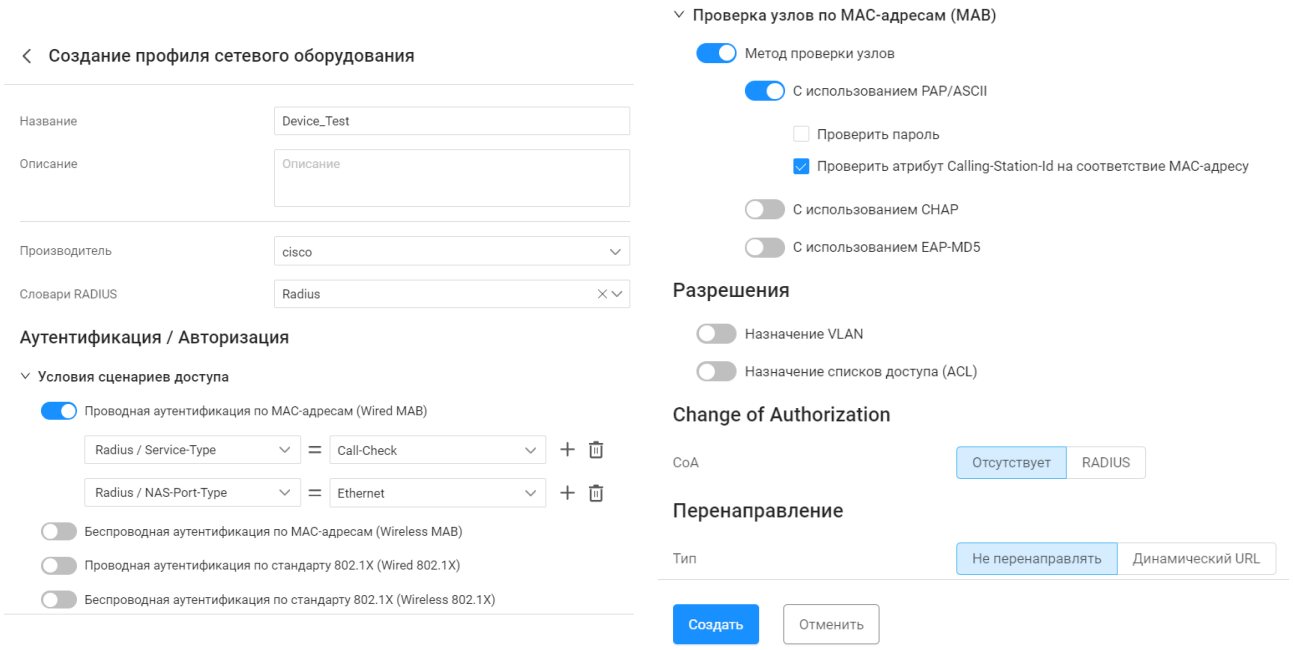



Рисунок 134 – Создание профиля сетевого оборудования

4) Создать сетевое оборудование (рис. 135).
(«Контроль доступа» → «Сетевое оборудование»).

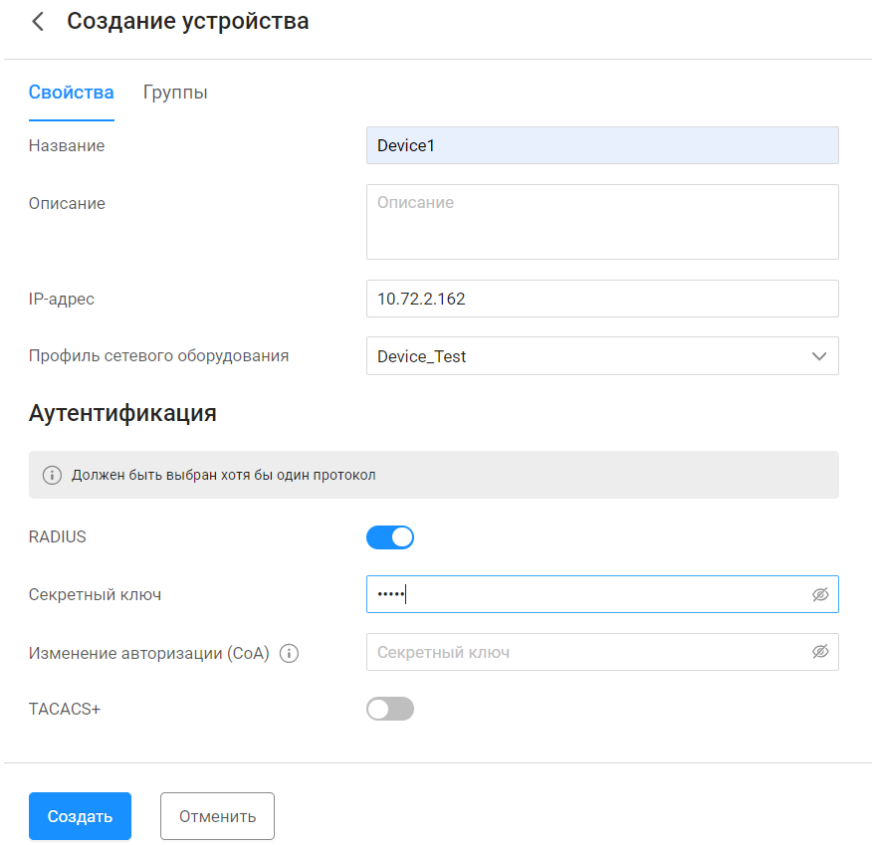



Рисунок 135 – Создание сетевого оборудования

5) Создать профиль авторизации (рис. 136).
(«Контроль доступа» → «Профили авторизации» → вкладка «Доступ в сеть»).

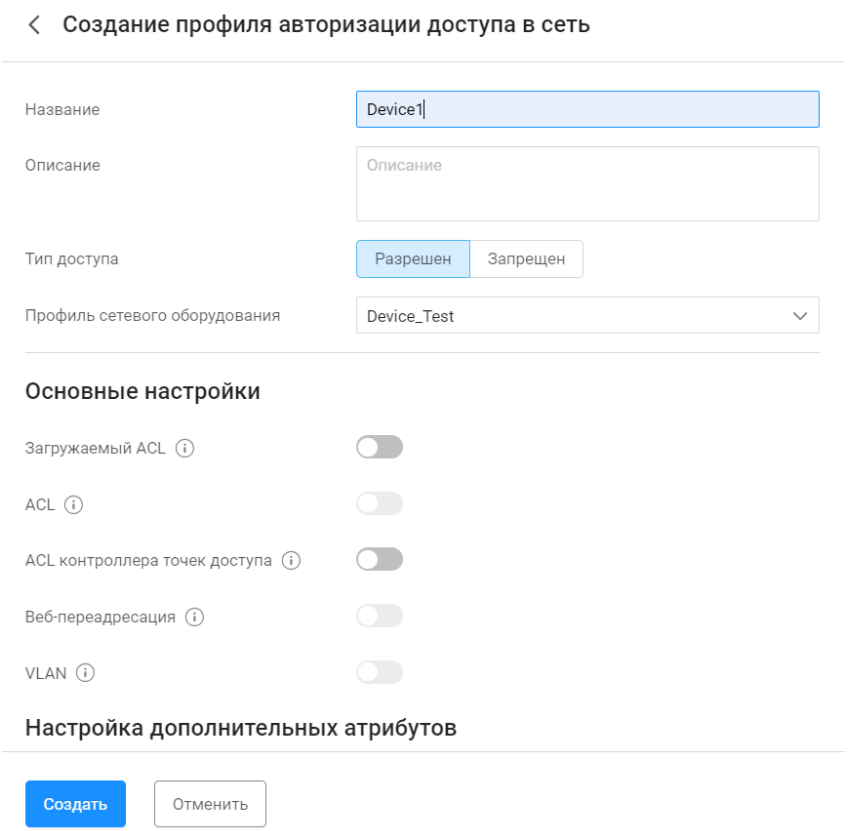



Рисунок 136 – Создание профиля авторизации

6) Создать набор политик («Контроль доступа» → «Наборы политик» → вкладка «Доступ в сеть»).

Вкладка «Настройки» (рис. 137).

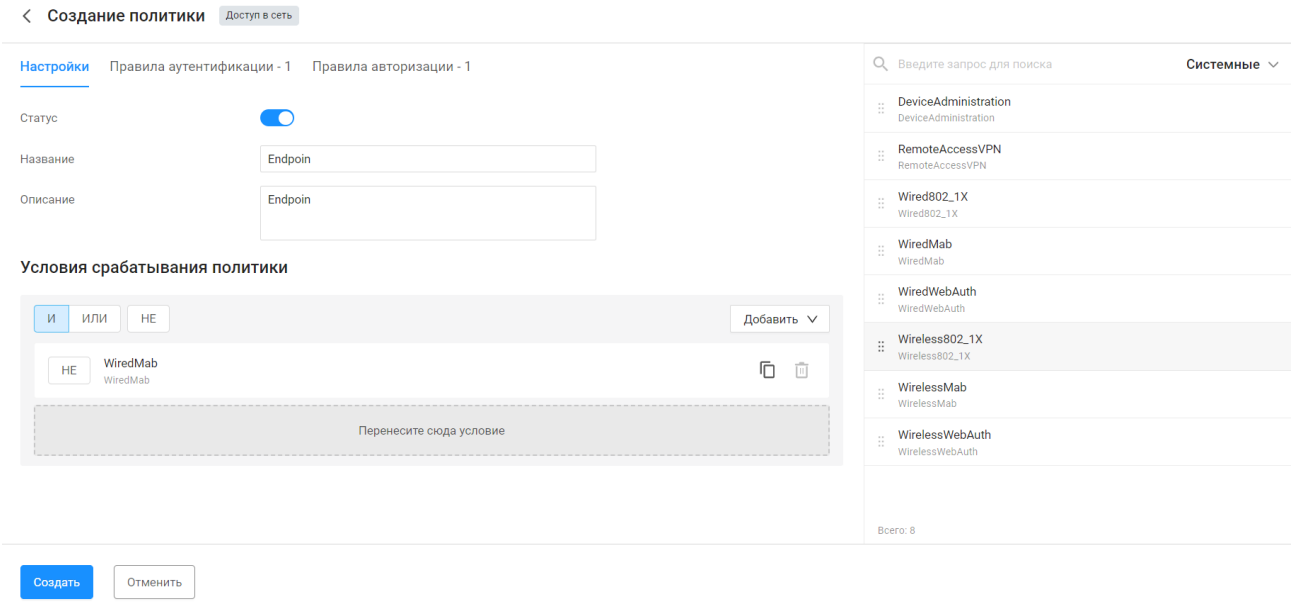



Рисунок 137 – Вкладка «Настройки»

Вкладка «Правила аутентификации» (рис. 138)

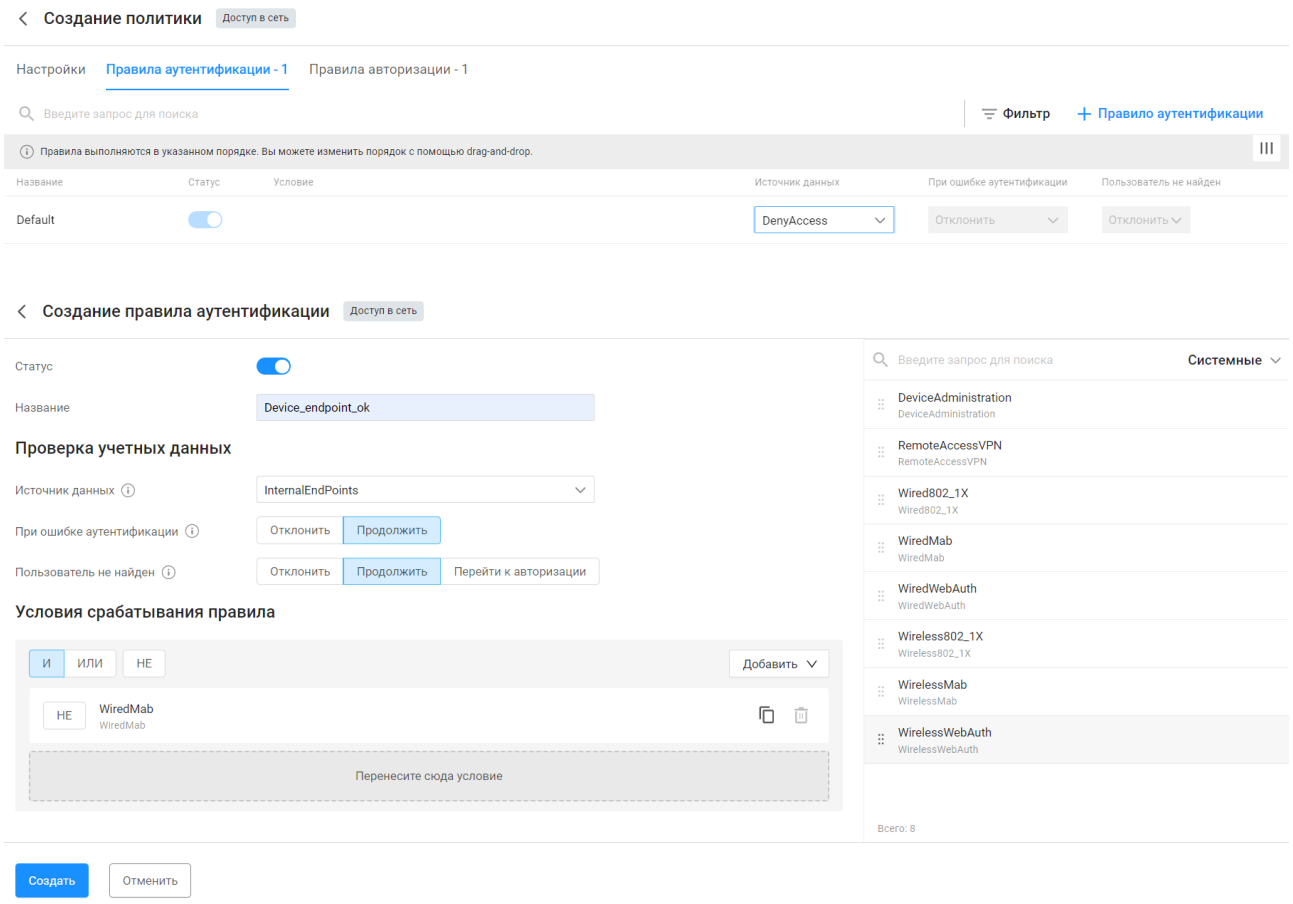



Рисунок 138 – Вкладка «Правила аутентификации»

Вкладка «Правила авторизации» (рис. 139).

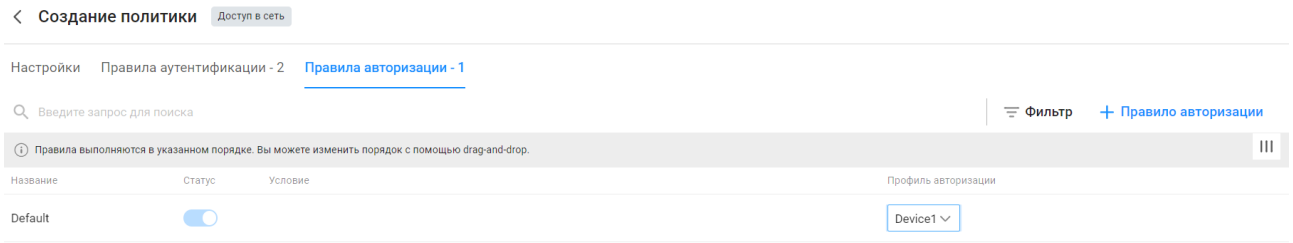



Рисунок 139 – Вкладка «Правила авторизации»

7) Настроить конечную точку для доступа в сеть.
8) Убедиться в успешной аутентификации устройства (рис. 140).

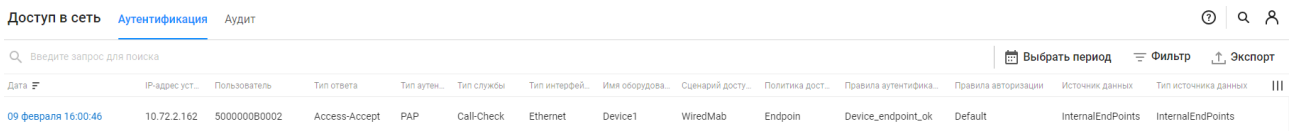



Рисунок 140 – Событие об аутентификации устройства

9) Создать набор политик профилирования (рис. 141).

(«Контроль доступа» → «Наборы политик» → вкладка «Профилирование»).

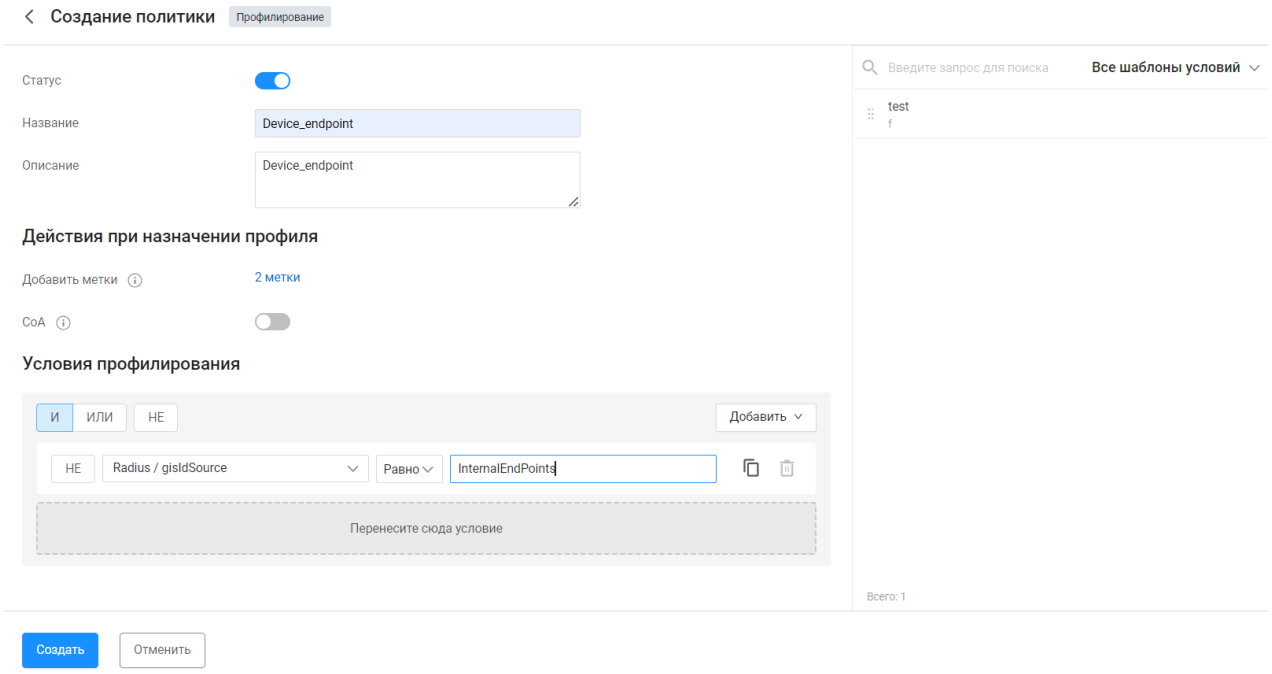



Рисунок 141 – Создание политики профилирования

10) При подключении конечной точки ей будут присвоены соответствующие метки в поле «Метка» (рис. 142).

(«Объекты сети» → «Конечные точки»).

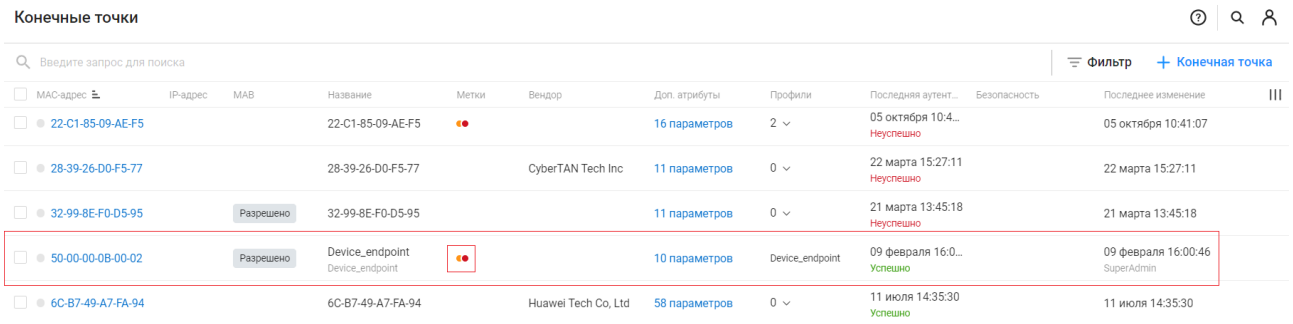



Рисунок 142 – Присвоение метки конечной точке

# Приложение В

## Рекомендуемая последовательность действий для настройки доступа в сеть устройств по MAC-адресам

Последовательность действий для настройки доступа в сеть устройств по MAC-адресам:

1) Настроить точку доступа и контроллер точек доступа.
2) Добавить разрешенные MAC-адреса.
3) Создать профиль сетевого оборудования для контроллера точек доступа.
4) Создать сетевое оборудование – контроллер точек доступа.
5) Создать профиль авторизации.
6) Создать политику доступа в сеть.
7) Настроить правила аутентификации.
8) Настроить правила авторизации.

В инструкции приведен пример заполнения минимально необходимых полей для настройки беспроводного доступа в сеть устройств по MAC-адресам.

Настройка беспроводного доступа в сеть устройств по MAC-адресам:

1) Настроить точку доступа и контроллер точек доступа (см. подраздел приложения Г.2).
2) Добавить разрешенные MAC-адреса:

— перейти в раздел «Контроль доступа», подраздел «Разрешенные MAC-адреса»;
— нажать кнопку «+ MAC-адрес» (рис. 143);
— заполнить поля страницы необходимыми параметрами (рис. 144).

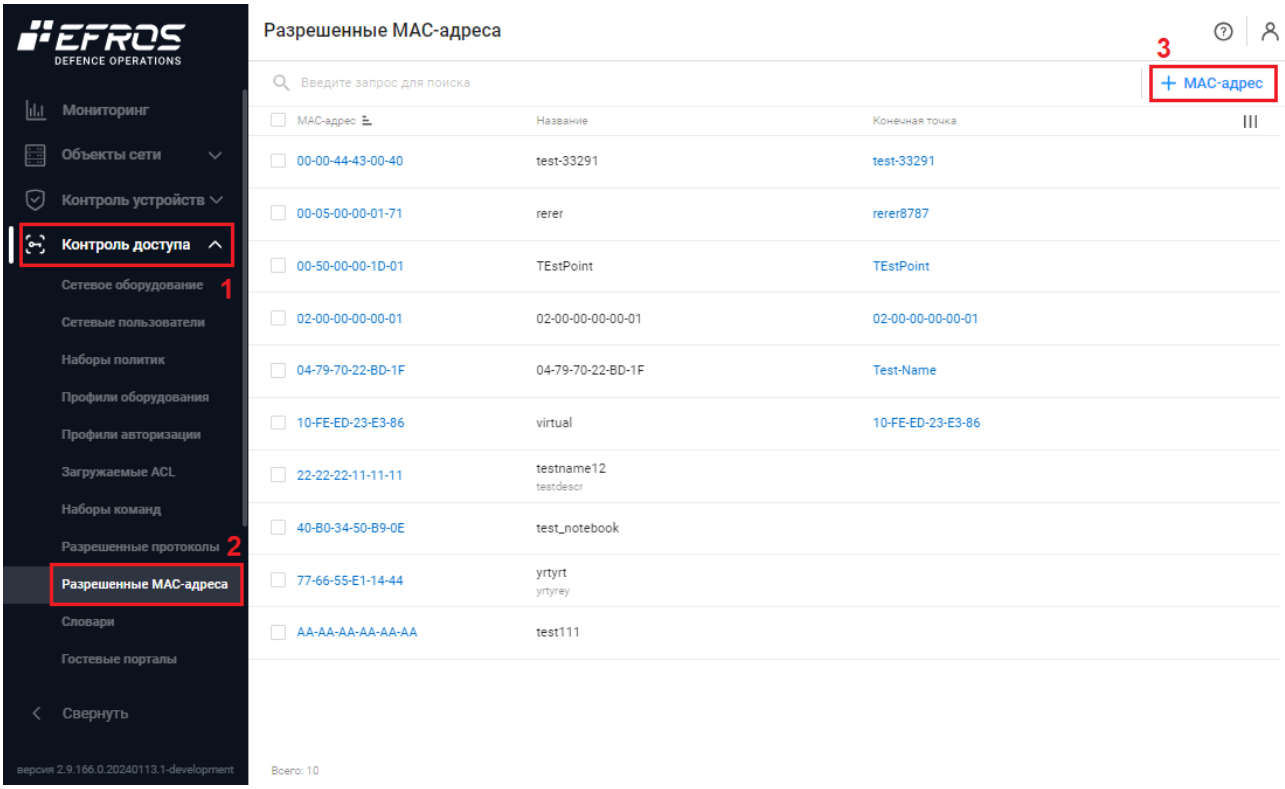



Рисунок 143 – Подраздел «Разрешенные MAC-адреса»

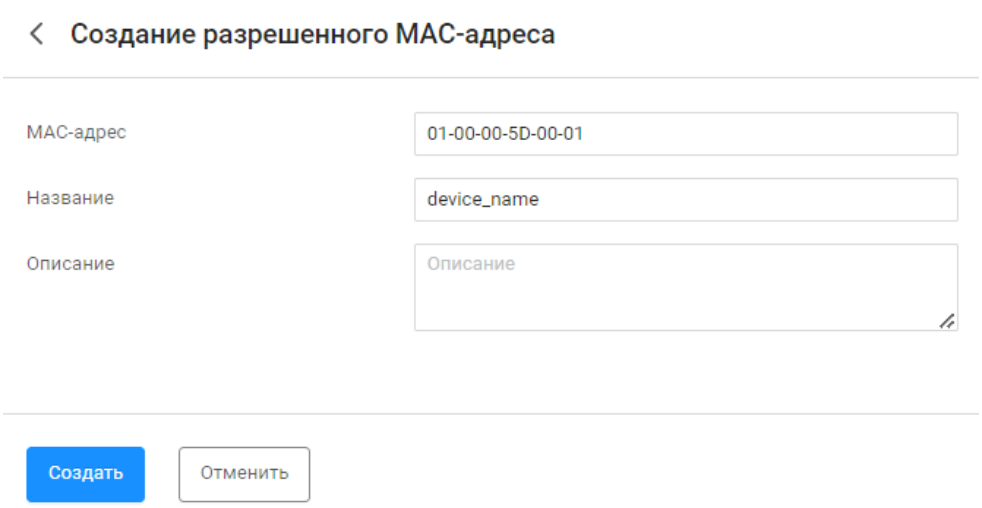



Рисунок 144 – Создание разрешенного MAC-адреса

Особенности заполнения полей описаны ниже:

- поле «MAC-адрес»: MAC-адрес устройства;
- поле «Название»: любое;
- поле «Описание»: любое.

3) Создать профиль сетевого оборудования для контроллера точек доступа:

- перейти в раздел «Контроль доступа», подраздел «Профили оборудования»;

— нажать кнопку « + Профиль оборудования » (рис. 145);
— заполнить поля страницы необходимыми параметрами (рис. 146).

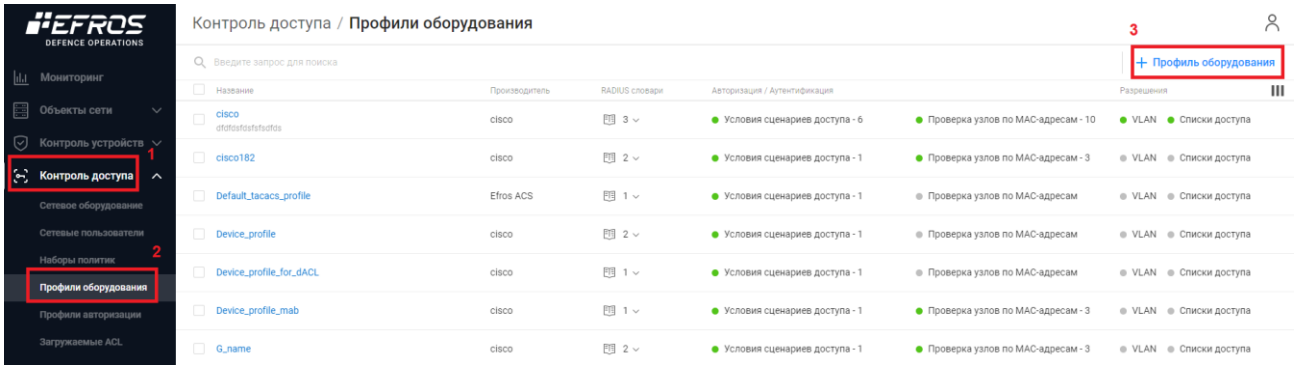



Рисунок 145 – Подраздел «Профили оборудования»

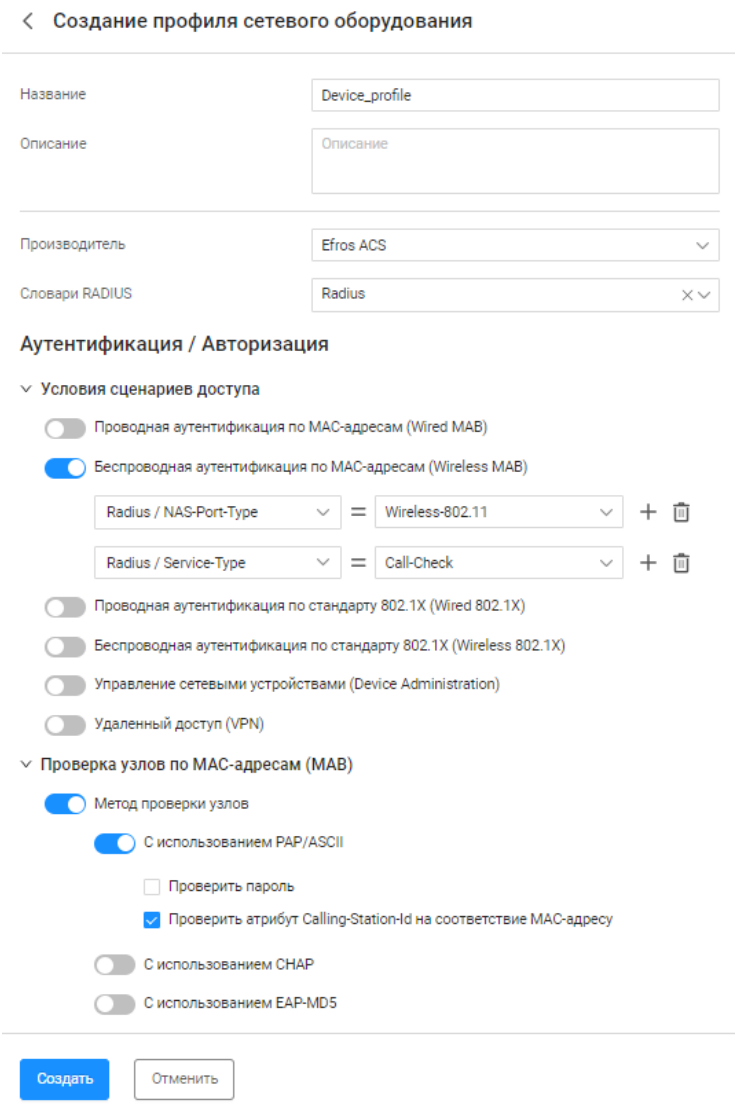



Рисунок 146 – Создание профиля сетевого оборудования

Особенности заполнения полей описаны ниже:

- поле «Название»: любое;
- поле «Производитель»: выбрать производителя из списка (если проиизводитель отсутствует, можно использовать предустановленный «Efros ACS»);
- поле «Словари RADIUS»: Radius;
- блок полей «Аутентификация/авторизация»:
    1. Блок полей «Условия сценариев доступа»:
        - беспроводная аутентификация по MAC-адресам (Wireless MAB), перевести переключатель в положение «Активно»:
            1. *Radius / NAS-Port-Type = Wireless-802.11*
            2. *Radius / Service-Type = Call-Check*
    2. Блок полей «Проверка узлов по MAC-адресам (MAB)», перевести переключатель в положение «Активно»:
        - перевести переключатель Метод проверки узлов» в положение «Активен» с использованием PAP/ASCII:
            1. *Проверять атрибут Calling-Station-Id на соответствие MAC-адресу.*

4) Создать сетевое оборудование – контроллер точек доступа:

- перейти в раздел «Контроль доступа», подраздел «Сетевое оборудование»;
- нажать кнопку « + Устройство » (рис. 147);
- заполнить поля страницы необходимыми параметрами (рис. 148).

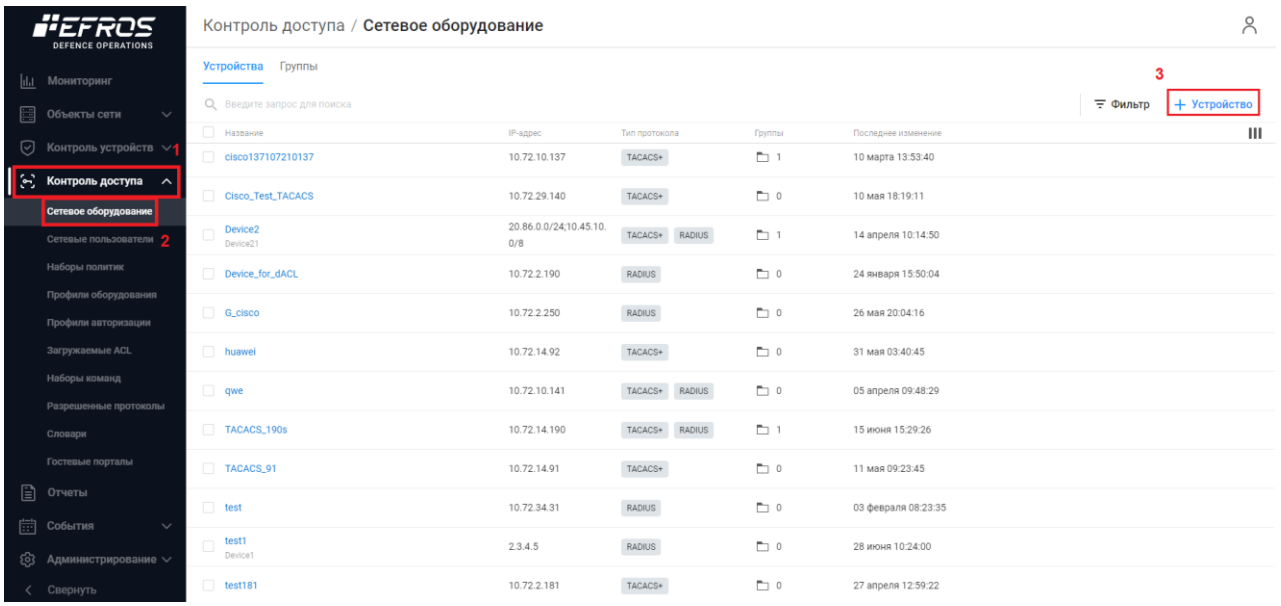



Рисунок 147 – Подраздел «Сетевое оборудование»

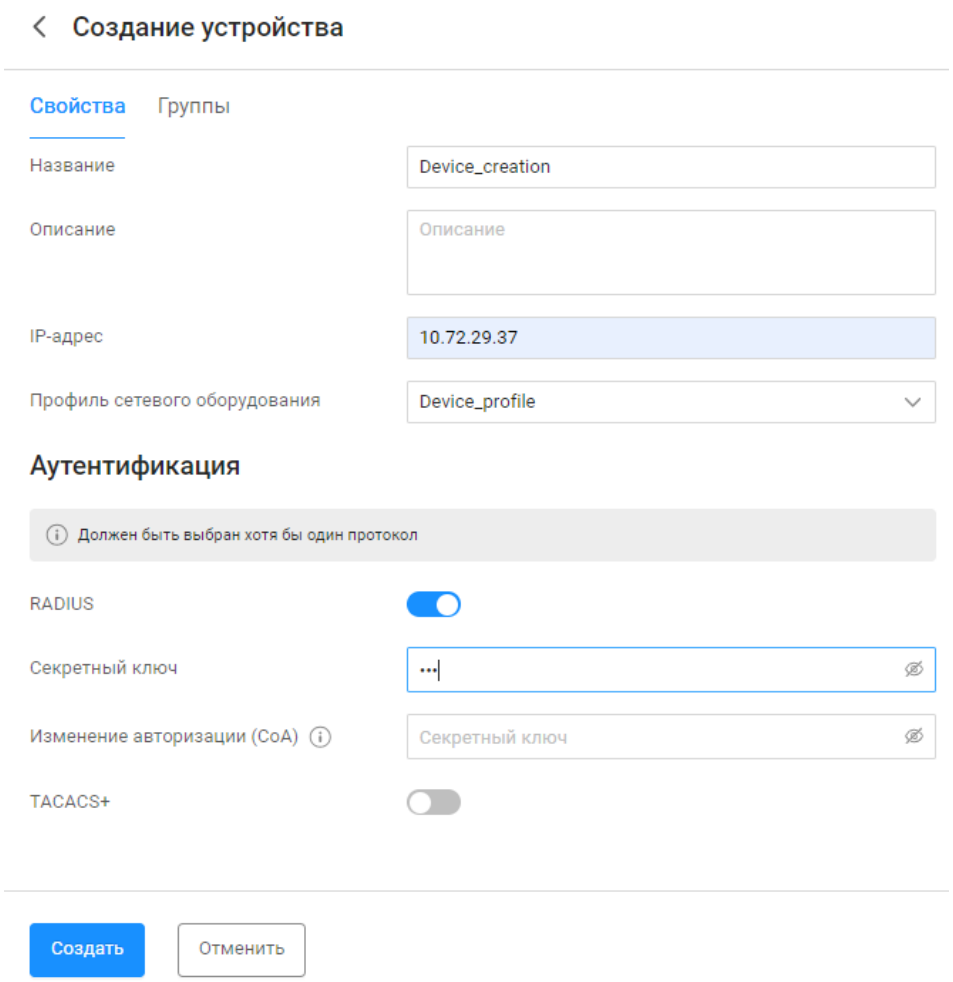



Рисунок 148 – Создание сетевого оборудования

Особенности заполнения полей описаны ниже:

- поле «Название»: любое;
- поле «IP-адрес»: IP-адрес контроллера точек доступа;
- поле «Профиль сетевого оборудования»: созданный в п. 3;
- поле «RADIUS»: перевести переключатель в положение «Активно» и ввести секретный ключ, указанный в настройках подключения контроллера точек доступа к серверу RADIUS.

5) Создать профиль авторизации:

- перейти в раздел «Контроль доступа», подраздел «Профили авторизации», вкладка «Доступ в сеть»;
- нажать кнопку «+ Профиль» (рис. 149);
- заполнить поля страницы необходимыми параметрами (рис. 150).

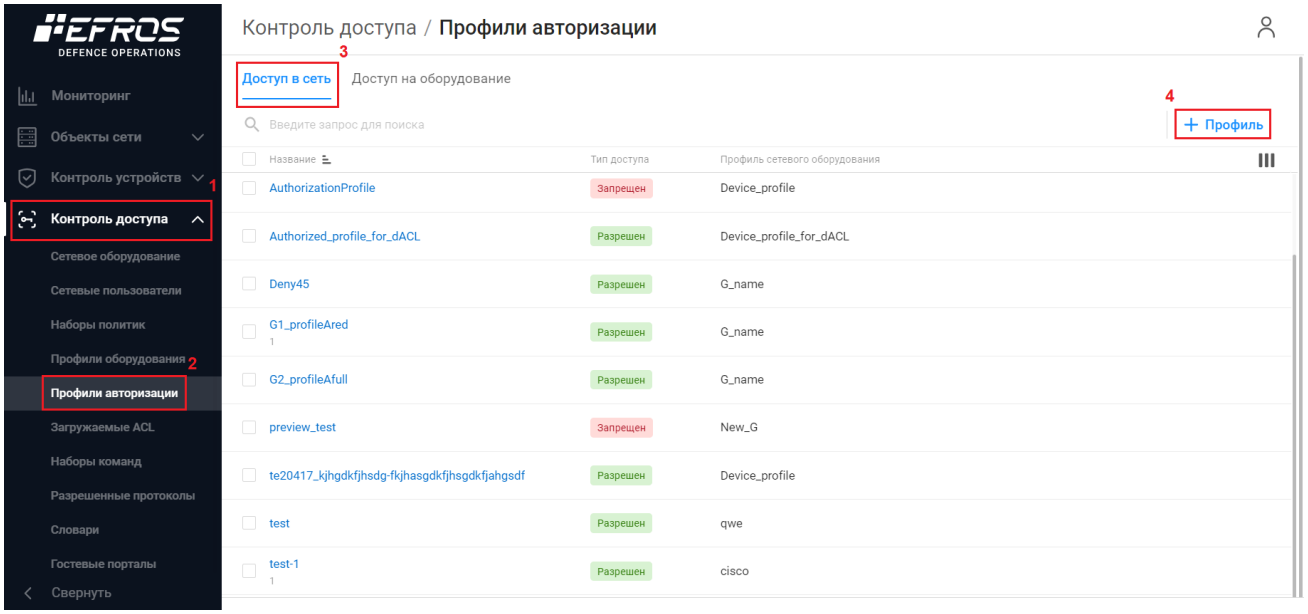



Рисунок 149 – Подраздел «Профили авторизации»

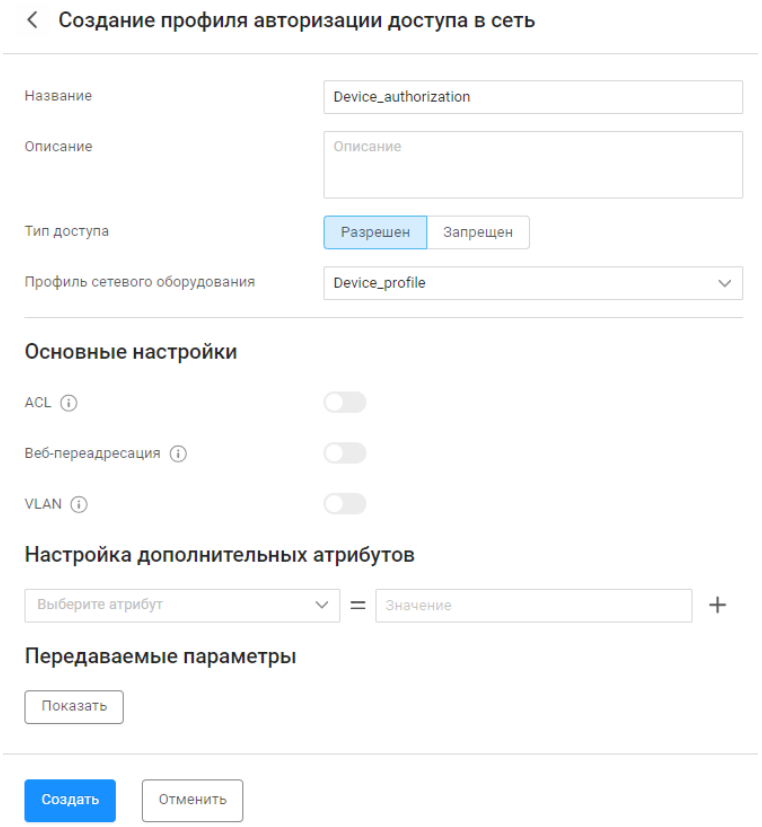



Рисунок 150 – Создание профиля авторизации доступа в сеть

Особенности заполнения полей описаны ниже:

- поле «Название»: любое;
- поле «Тип доступа»: разрешен;
- поле «Профиль сетевого оборудования»: созданный в п. 3.

Созданный профиль авторизации используется для разрешения доступа устройствам, соответствующим условиям сценария доступа профиля сетевого оборудования.

6) Создать политику доступа в сеть:

— перейти в раздел «Контроль доступа», подраздел «Наборы политик», вкладка «Доступ в сеть»;

— нажать кнопку « + Политика » (рис. 151);

— заполнить поля страницы необходимыми параметрами (рис. 152).

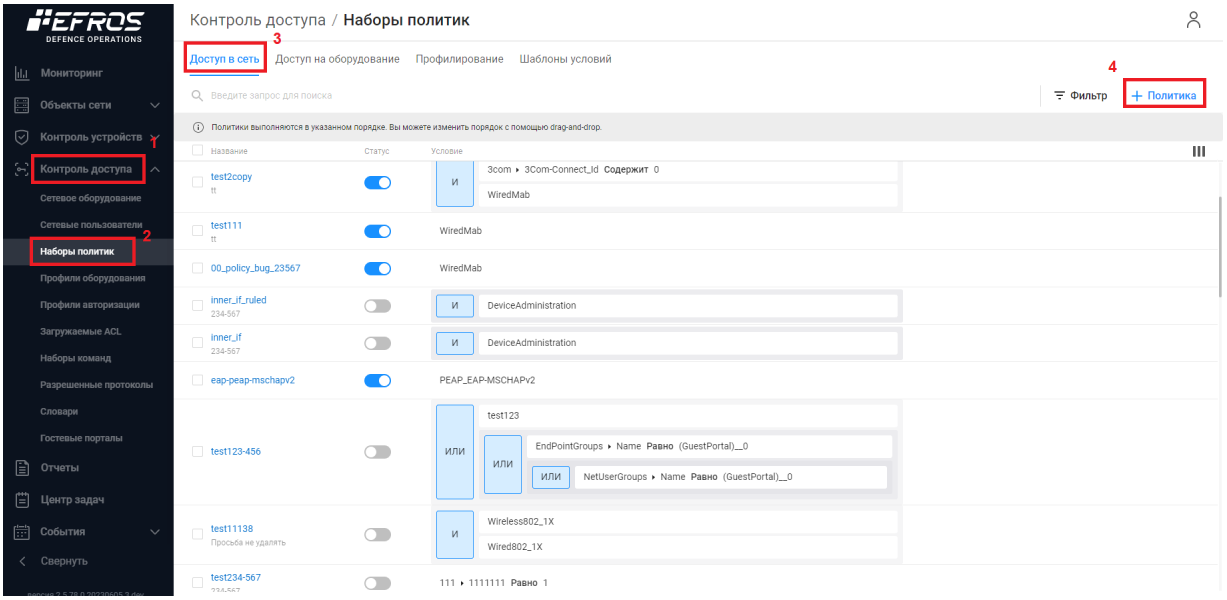



Рисунок 151 – Подраздел «Наборы политик»

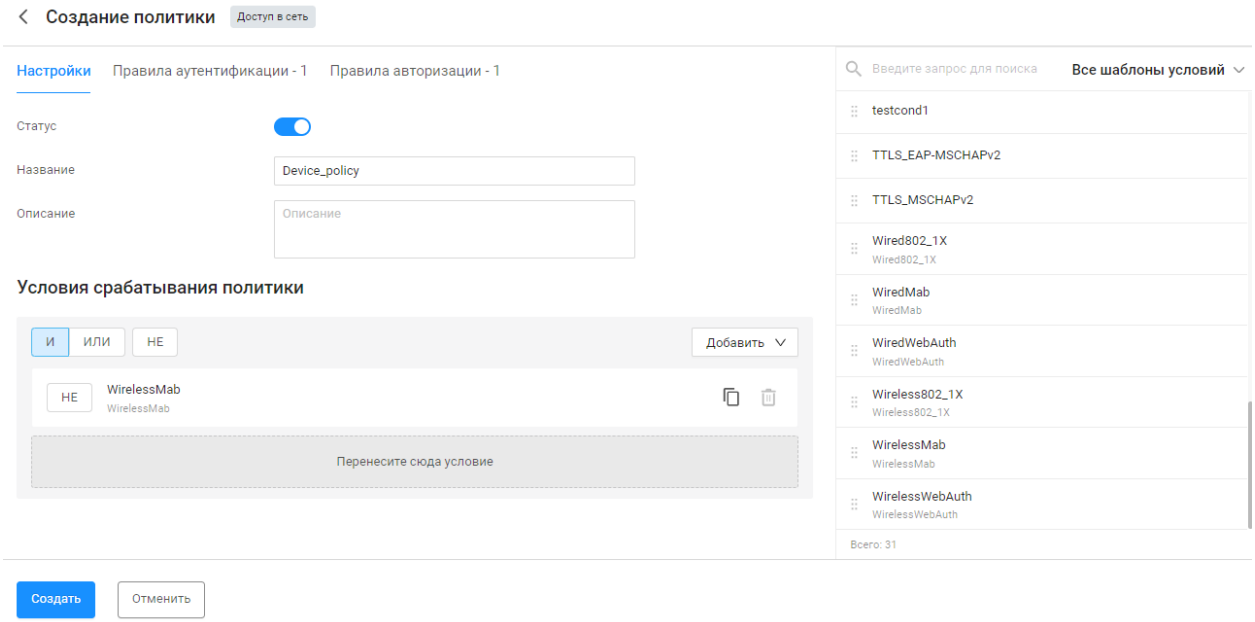



Рисунок 152 – Создание политики доступа в сеть

Особенности заполнения полей описаны ниже:

- поле «Статус»: активен;
- поле «Название»: любое;
- поле «Условия срабатывания политики»: Wireless MAB (из шаблонов условий).

Шаблон условий «Wireless MAB» – это набор условий для аутентификации устройств, подключенных к беспроводной сети по MAC-адресам.

В наборе правил «Условия срабатывания политики» используются атрибуты и значения, заданные в профиле оборудования. В зависимости от того, какое сетевое оборудование будет запрашивать доступ, для подключаемого устройства – могут быть использованы разные значения из профиля оборудования.

В данном случае в профиле сетевого оборудования применено условие «Беспроводная аутентификация по MAC-адресам (Wireless MAB)» (задано в блоках полей «Аутентификация / Авторизация» → «Условия сценариев доступа», см. п. 3).

7) Настроить правила аутентификации:

- на странице «Создание политики» перейти на вкладку «Правила аутентификации» (рис. 152);
- нажать кнопку «+ Правило аутентификации». Откроется окно «Создание правила аутентификации». Создаваемое правило аутентификации предназначено для проверки наличия MAC-адреса устройства, запрашивающего доступ в сеть, в списке разрешенных MAC-адресов;
- заполнить поля страницы необходимыми параметрами (рис. 153).

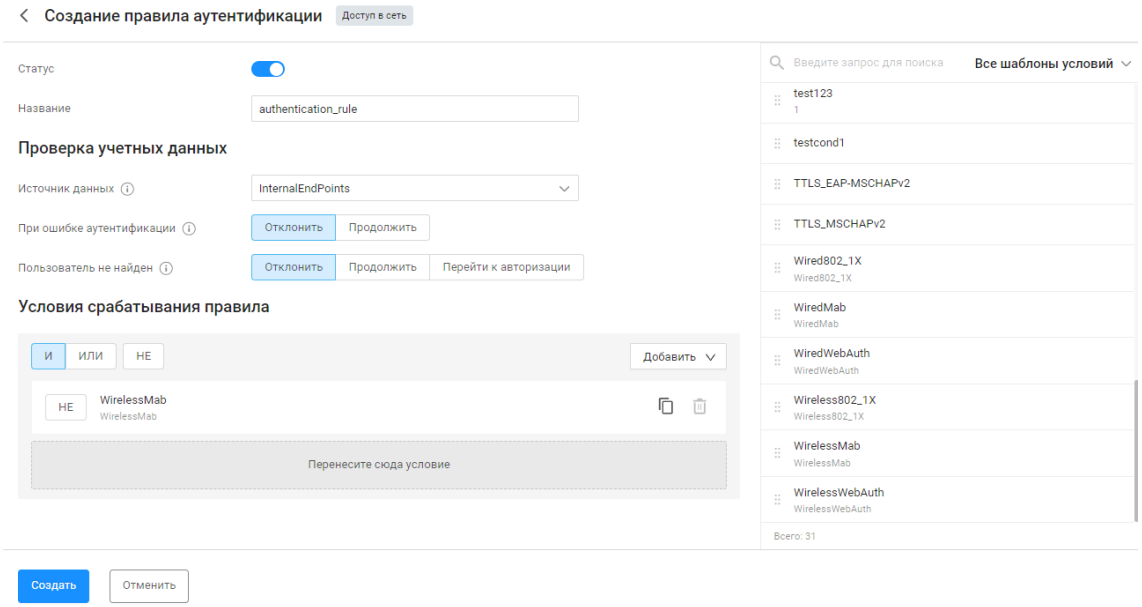



Рисунок 153 – Создание правила аутентификации

Особенности заполнения полей описаны ниже:

- поле «Статус»: активен;
- поле «Название»: любое;
- поле «Источник данных»: InternalEndPoints;
- поле «При ошибке аутентификации»: отклонить;
- поле «Пользователь не найден»: отклонить;
- поле «Условия срабатывания правила»: Wireless MAB (из шаблонов условий).

Для запрета доступа в сеть устройств, не соответствующих ранее созданным правилам аутентификации, необходимо в строке правила «Default» указать источник данных «DenyAccess» (рис. 154).

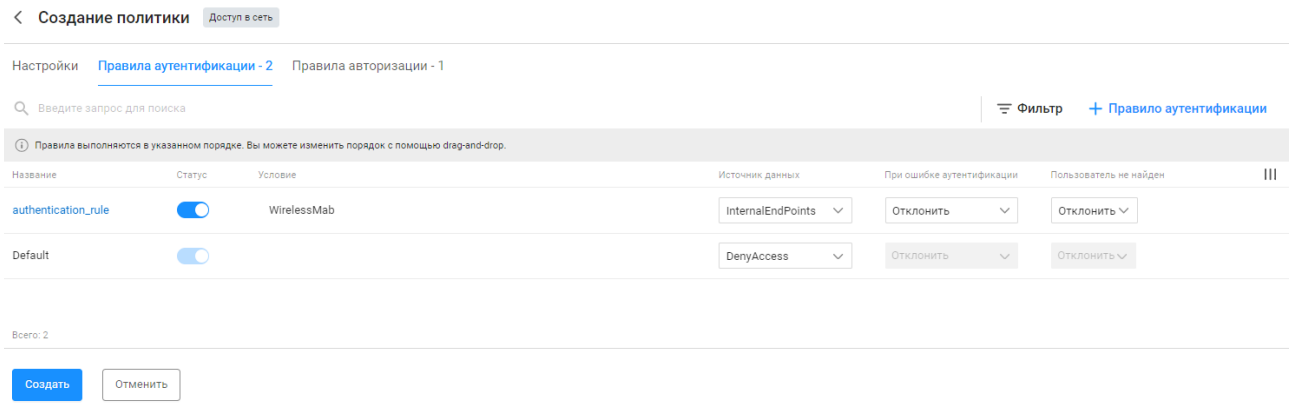



Рисунок 154 – Редактирование правила аутентификации «Default» для запрета доступа в сеть устройств, не соответствующим правилам аутентификации

8) Настроить правила авторизации:

- на странице «Создание политики» перейти на вкладку «Правила авторизации» (см. рис. 153);
- в строке правила «Default» указать профиль авторизации, созданный в п. 5 (рис. 155).

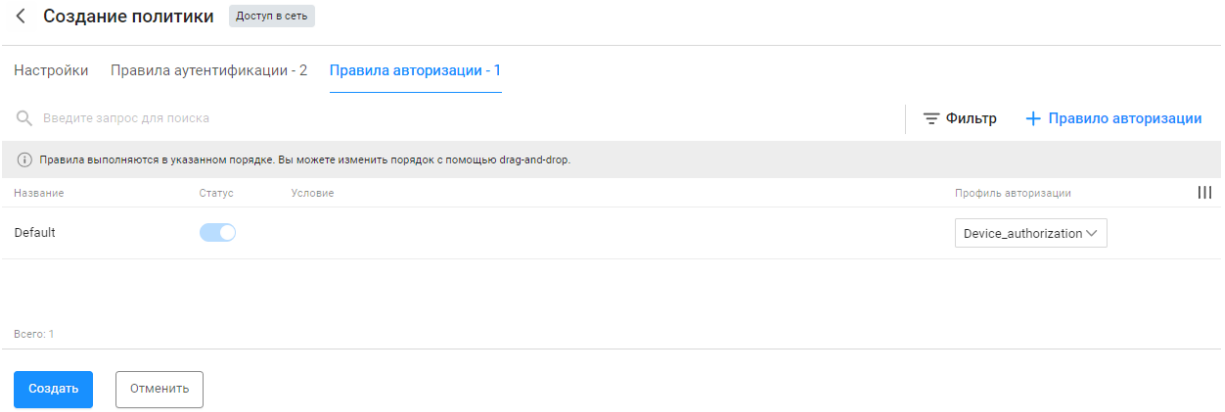



Рисунок 155 – Редактирование правила авторизации «Default»

# Приложение Г

## Рекомендуемая последовательность действий для настройки доступа в сеть с использованием гостевого портала

Последовательность действий для настройки доступа в сеть с использованием гостевого портала:

1) Настроить точку доступа и контроллер точек доступа.
2) Создать страницу гостевого портала. Если тип портала – гостевой, то необходимо создать учетные записи пользователей либо активировать параметр «саморегистрация» в настройках гостевого портала.
3) Создать профиль сетевого оборудования для контроллера точек доступа.
4) Создать сетевое оборудование – контроллер точек доступа.
5) Создать профиль авторизации для переадресации пользователя на гостевой портал.
6) Создать профиль авторизации, назначаемый после успешной авторизации пользователя.
7) Создать политику доступа в сеть.
8) Настроить правила аутентификации.
9) Настроить правила авторизации.

В инструкции приведен пример заполнения минимально необходимых полей для настройки беспроводного доступа в сеть с использованием гостевого портала.

На данный момент поддерживается работа с оборудованием Cisco.

Для корректной работы необходимо отключить рандомизацию MAC-адреса на устройстве (конечной точке), с которого выполняется подключение к сети.

Если контроллер точек доступа поддерживает механизм RADIUS Change of Authorization, а также для него в ПК «Efros DO» настроен CoA в профиле оборудования, то получение пользователем соответствующих прав доступа после аутентификации на гостевом портале происходит автоматически. В случае, если механизм CoA не поддерживается/не настроен, то пользователю необходимо отключиться от сети и совершить подключение заново.

На рис. 156 приведена очередность настройки гостевого портала администратором гостевого портала (пользователь ПК «Efros DO»), и процесс беспроводного доступа в сеть с использованием гостевого портала сетевым пользователем.

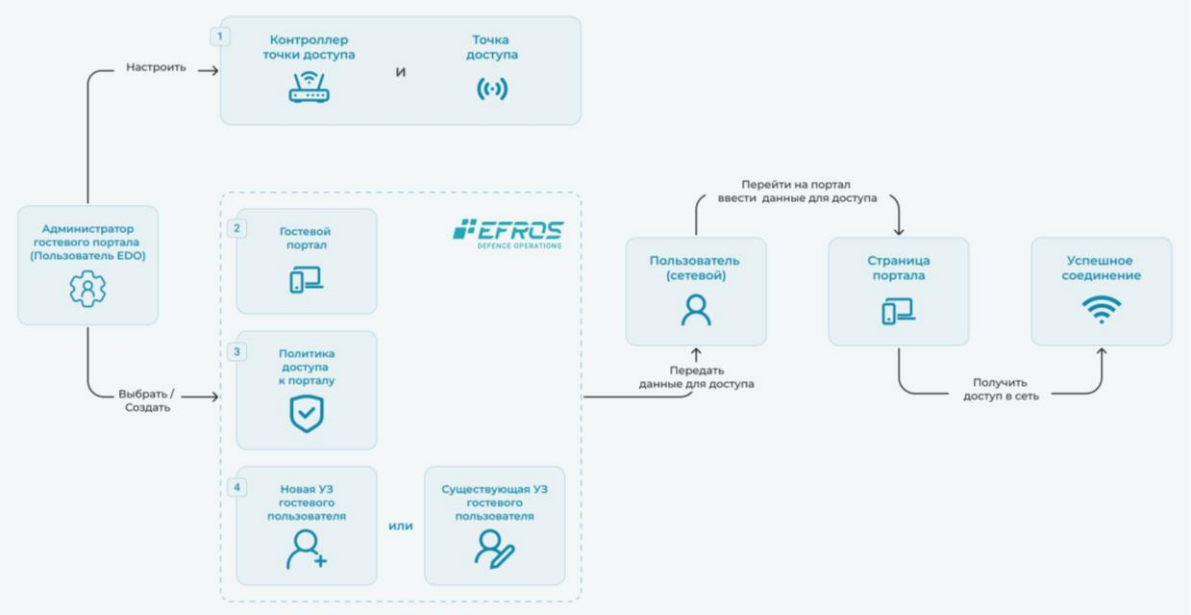



Рисунок 156 – Схема очередности настройки и беспроводного доступа в сеть с использованием гостевого портала

Схема предоставления пользователю беспроводного доступа в сеть с использованием настроенного гостевого портала приведена на рис. 157.

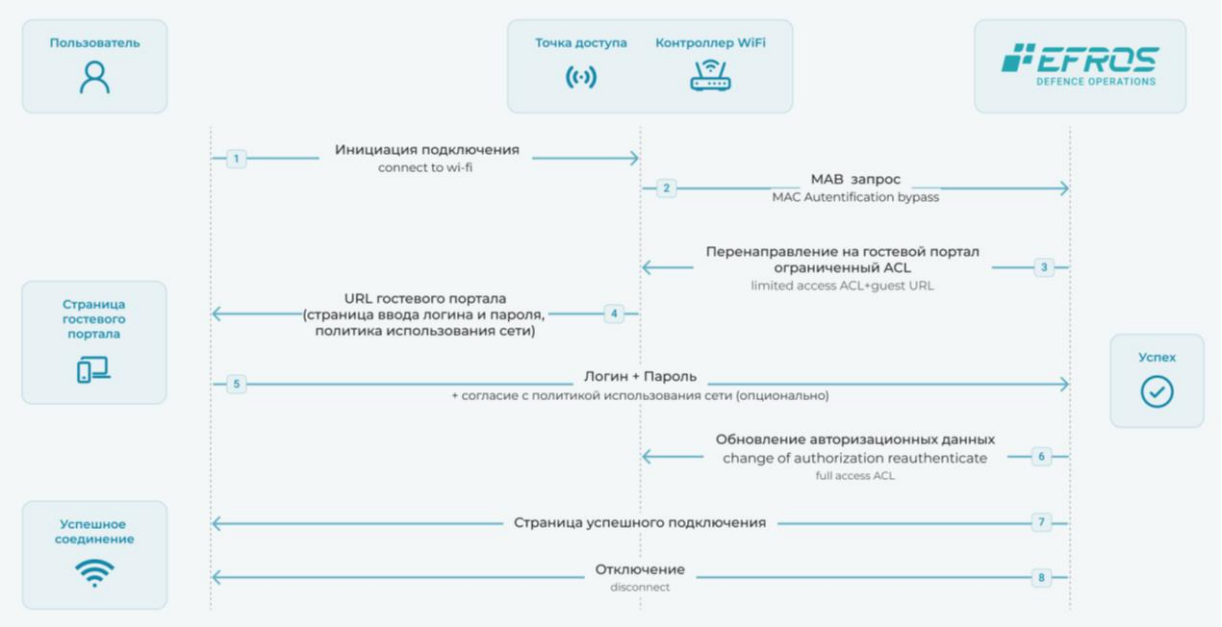



Рисунок 157 – Схема беспроводного доступа в сеть с использованием настроенного гостевого портала

## Г.1 Настройка беспроводного доступа в сеть с использованием гостевого портала

Последовательность действий для настройки беспроводного доступа в сеть с использованием гостевого портала:

1) Настроить точку доступа и контроллер точек доступа (см. подраздел приложения Г.2).
2) Создать страницу гостевого портала:

— перейти в раздел «Контроль доступа», подраздел «Гостевые порталы»;

— нажать кнопку « + Гостевой портал » (рис. 158);

— заполнить поля страницы необходимыми параметрами (рис. 159 - 160).

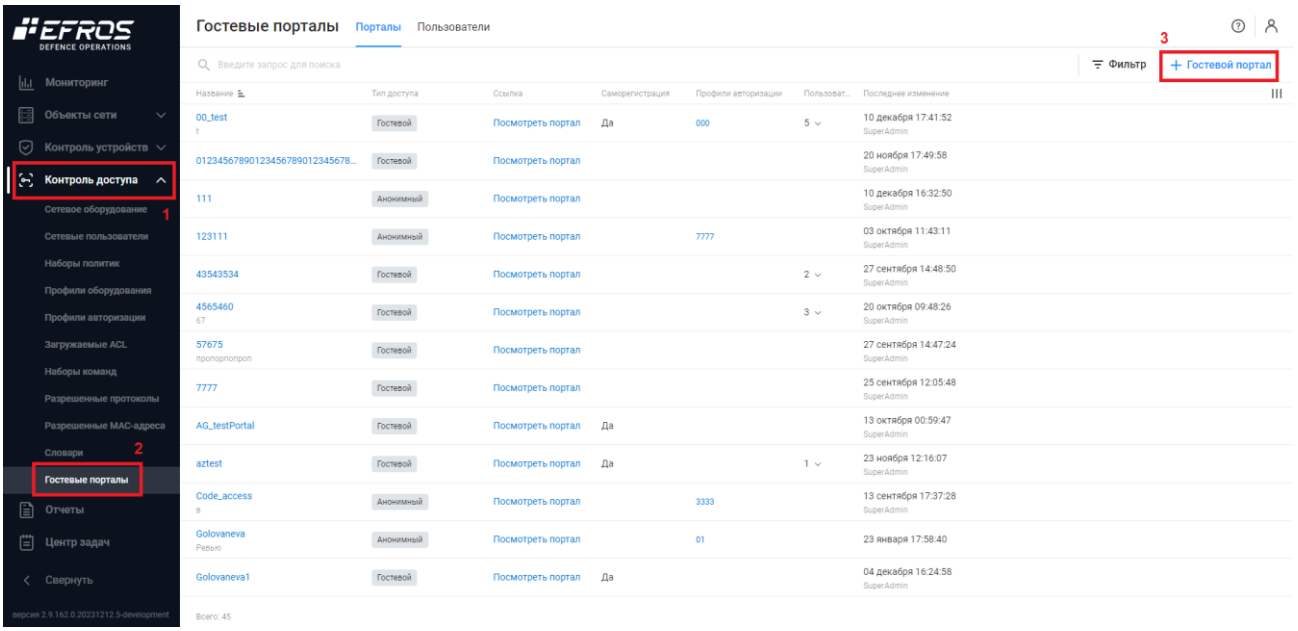



Рисунок 158 – Подраздел «Гостевые порталы»

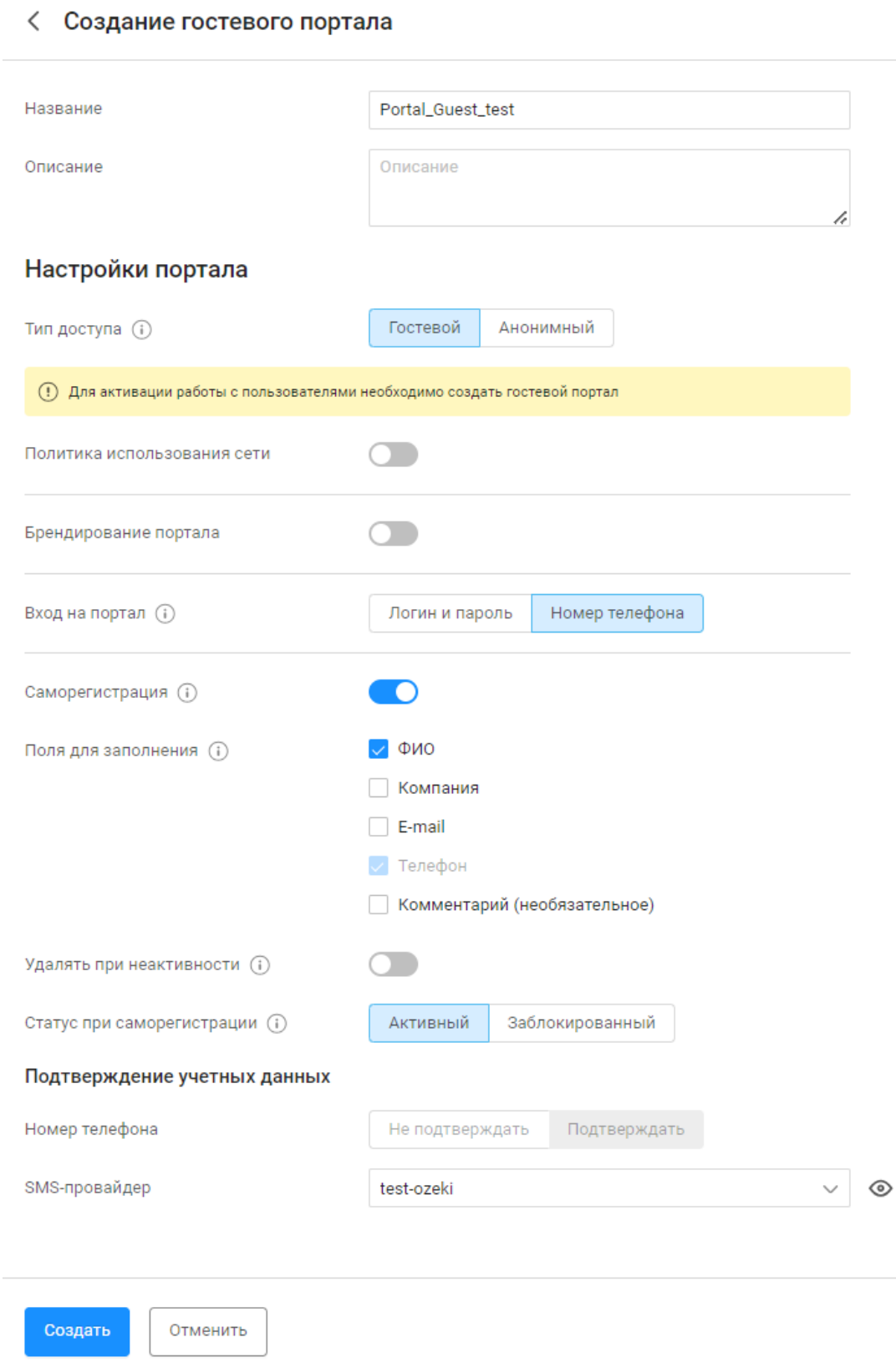



Рисунок 159 – Создание гостевого портала. Тип доступа «Гостевой»

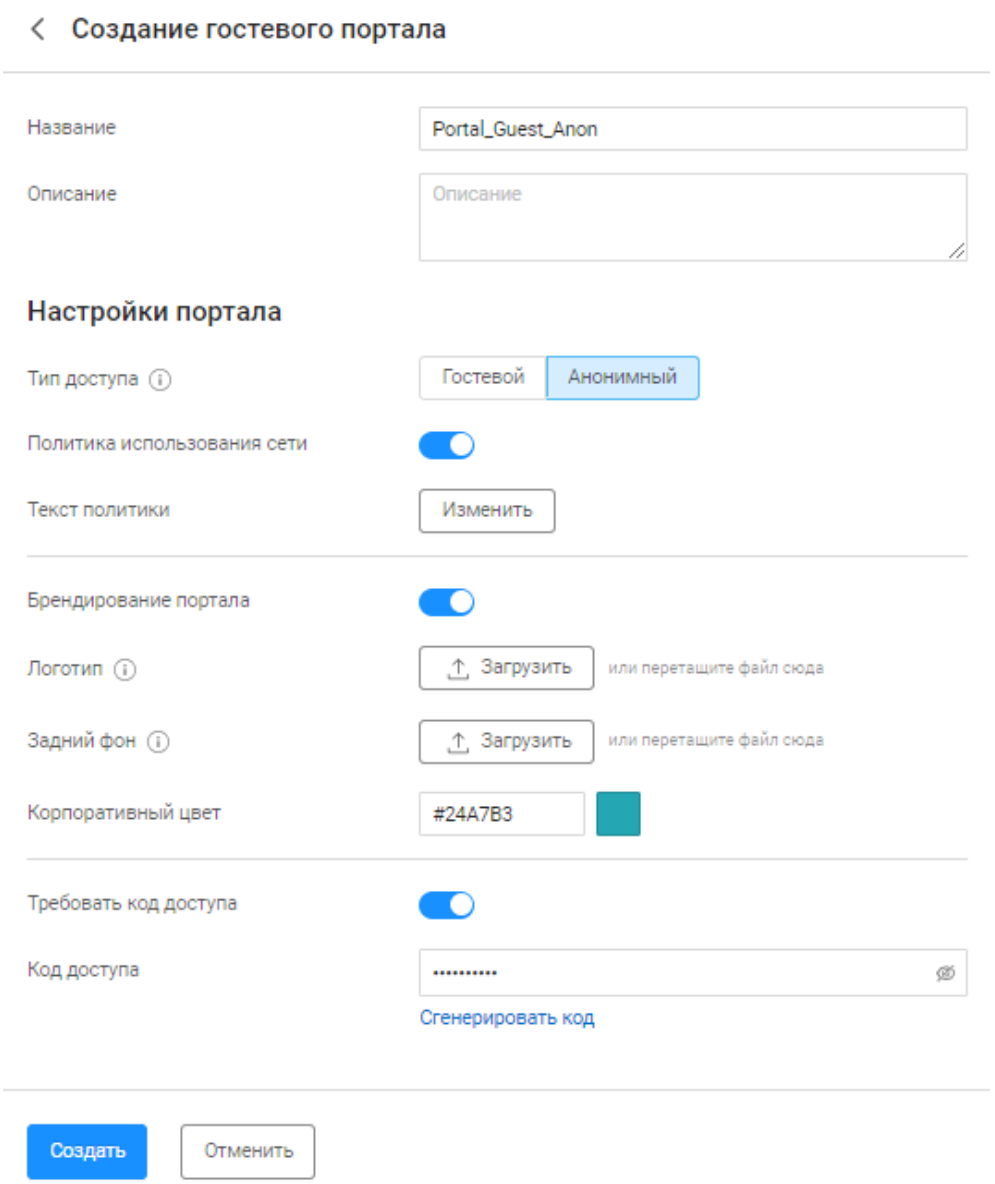


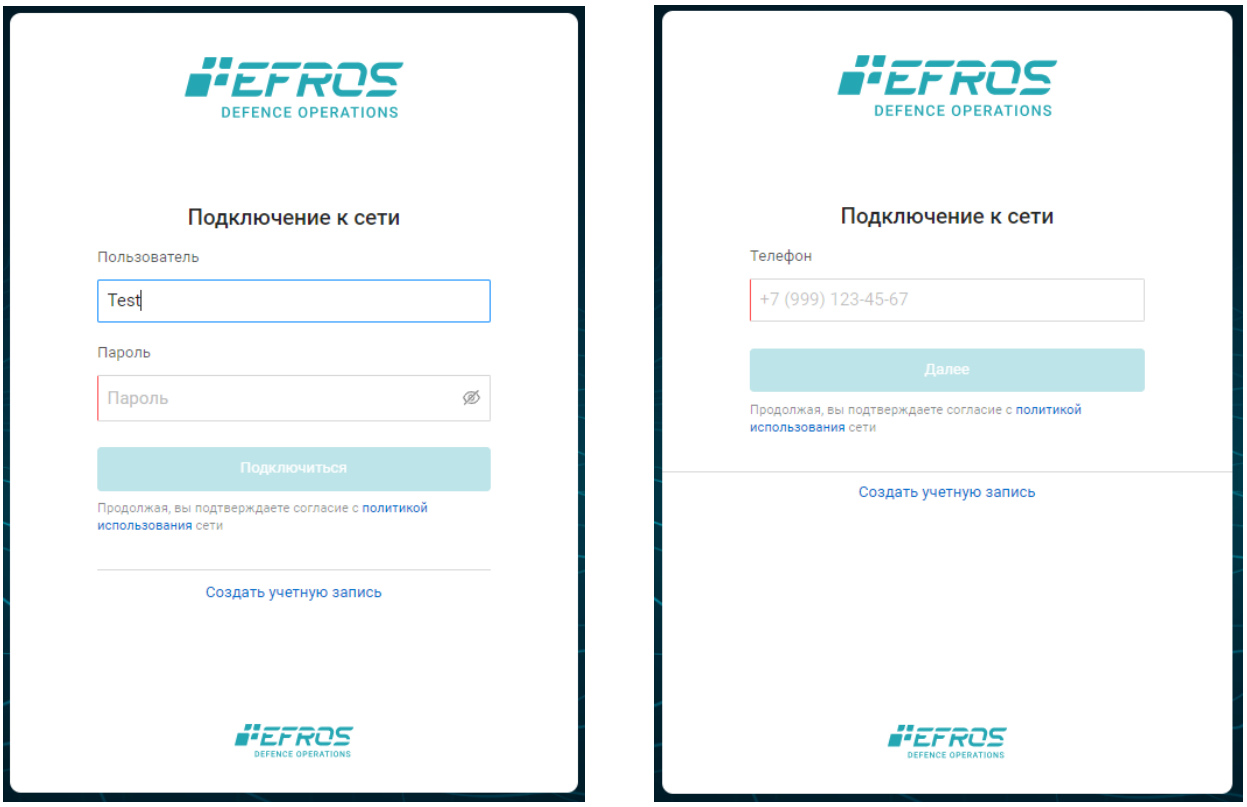

Рисунок 160 – Создание гостевого портала. Тип доступа «Анонимный»

Особенности заполнения общих полей описаны ниже:

— поле «Название»: любое;

— блок полей «Настройки портала»:

- тип доступа: «Гостевой» или «Анонимный»;
- переключатель «Политика использования сети». При включении данного параметра, на веб-странице входа на гостевой портал появляется поле подтверждения согласия с политикой использования сети в виде ссылки (рис. 161). При переходе по ссылке отображается текст, введенный в поле «Текст политики».




а) вариант входа «Логин и пароль» б) вариант входа «Номер телефона»

Рисунок 161 – Веб-страница входа на гостевой портал

— переключатель «Брендирование портала» позволяет загрузить логотип, выбрать задний фон и корпоративный цвет портала (цвет кнопок подключения и цвет знаков успешного соединения).

Особенности заполнения полей при выборе типа доступа «Гостевой»:

— поле «Вход на портал»:
  - логин и пароль: вход на гостевой портал для пользователя осуществляется по вводу логина и пароля (вид веб-страницы входа на гостевой портал приведен на рис. 161, а). При выборе появляется возможность настройки парольной политики в поле «Парольная политика»;
  - номер телефона: вход на гостевой портал для пользователя осуществляется по номеру телефона и ввода кода проверки (вид веб-страницы входа на гостевой портал приведен на рис. 161, б). При выборе появляется блок полей «Подтверждение учетных данных», в котором нужно выбрать требуемый «SMS-провайдер». Предварительно необходимо произвести настройку внешней системы «SMS-провайдеры» в разделе «Настройки».

— поле «Парольная политика». Настраивается при выборе входа на портал «Логин и пароль». Настройки парольной политики влияют только на пользователей текущего гостевого портала. Перечень настраиваемых параметров:

- сложность пароля: настроенные параметры применяются при создании учетной записи гостевого пользователя администратором на вкладке «Пользователи» либо пользователем самостоятельно через портал;
- время жизни сессии: период после открытия веб-страницы входа на гостевой портал до успешного подключения к сети. По истечении времени пользователю необходимо повторно подключиться к гостевому порталу.

— переключатель «Саморегистрация». При включении, у пользователей гостевого портала будет возможность самостоятельно создавать учетные записи на веб-странице входа на гостевой портал;
— блок полей «Подтверждение учетных данных» выводится при выборе поля для заполнения «Телефон»:
- поле «Номер телефона»: при выборе значения «Подтверждать» требуется заполнить поле «SMS-провайдеры». Для этого предварительно необходимо произвести настройку внешней системы «SMS-провайдеры» в разделе «Настройки».

Особенности заполнения полей при выборе типа доступа «Анонимный»:
— переключатель «Требовать код доступа». При включении, для анонимного пользователя будет произведен запрос кода для подключения к сети, который необходимо ввести на веб-странице входа на гостевой портал.

После создания гостевого портала автоматически создается метка с названием гостевого портала: (GuestPortal) <название портала>.

Метка гостевого портала будет автоматически присвоена устройству гостевого пользователя (конечной точке, с которой выполняется подключение к сети) успешно прошедшего аутентификацию на гостевом портале.

Метки гостевого портала у конечных точек очищаются ежедневно в 00:00 (часов:минут). Это необходимо для повторного прохождения гостевыми пользователями процедуры аутентификации для получения доступа к сети.

При удалении гостевого портала соответствующие метки у конечных точек автоматически удаляются.

3) Создать профиль сетевого оборудования для контроллера точек доступа:
— перейти в раздел «Контроль доступа», подраздел «Профили оборудования»;
— нажать кнопку «+ Профиль оборудования» (рис. 162);
— заполнить поля страницы необходимыми параметрами (рис. 163-165).

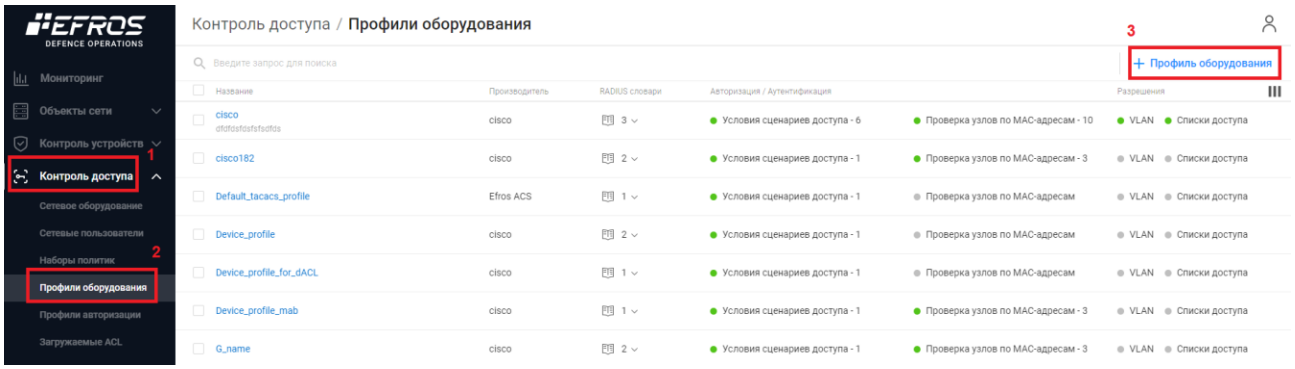



Рисунок 162 – Подраздел «Профили оборудования»

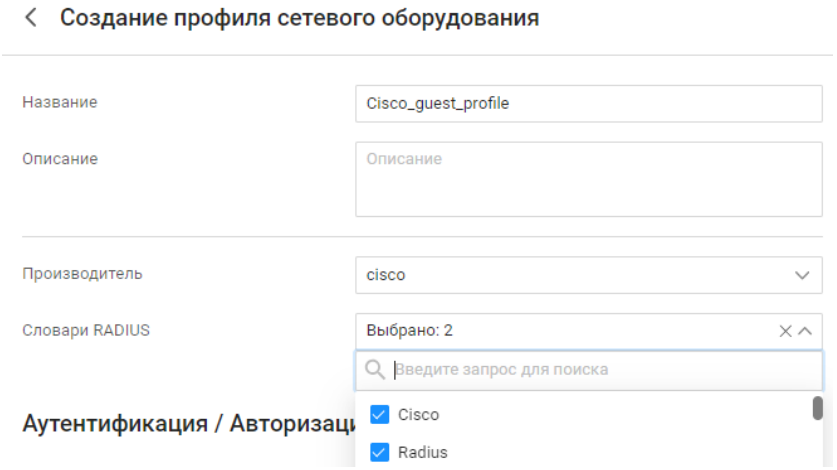



Рисунок 163 – Создание профиля сетевого оборудования

Особенности заполнения верхних полей описаны ниже:

- поле «Название»: любое;
- поле «Производитель»: Cisco;
- поле «Словари RADIUS»: Radius, Cisco.

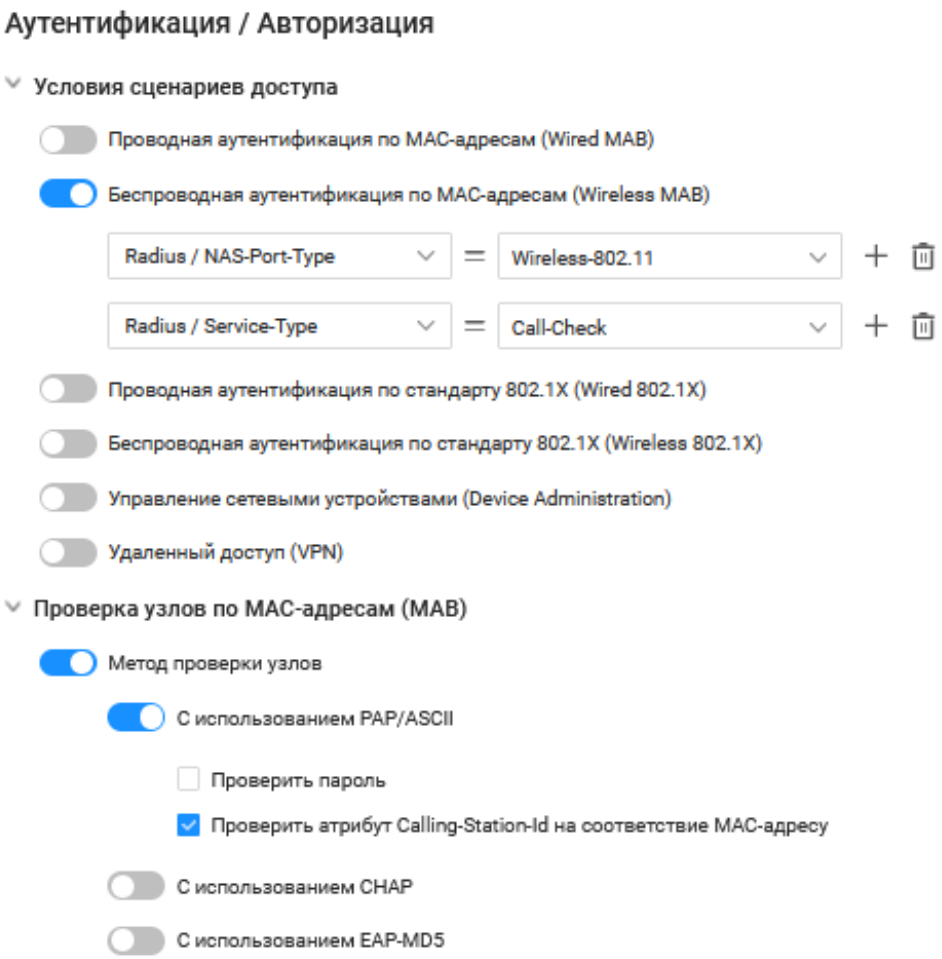



Рисунок 164 – Создание профиля сетевого оборудования. Блок полей «Аутентификация / авторизация»

Особенности заполнения блока полей «Аутентификация/авторизация» описаны ниже:

— блок полей «Аутентификация/авторизация»:

1. Блок полей «Условия сценариев доступа»

   - беспроводная аутентификация по MAC-адресам (Wireless MAB), перевести переключатель в положение «Активно»:
     1. *Radius / NAS-Port-Type = Wireless-802.11*
     2. *Radius / Service-Type = Call-Check*

2. Блок полей «Проверка узлов по MAC-адресам (MAB)», перевести переключатель в положение «Активно»:

   - перевести переключатель «Метод проверки узлов» в положение «Активен» с использованием PAP/ASCII:
     1. *Проверять атрибут Calling-Station-Id на соответствие MAC-адресу.*

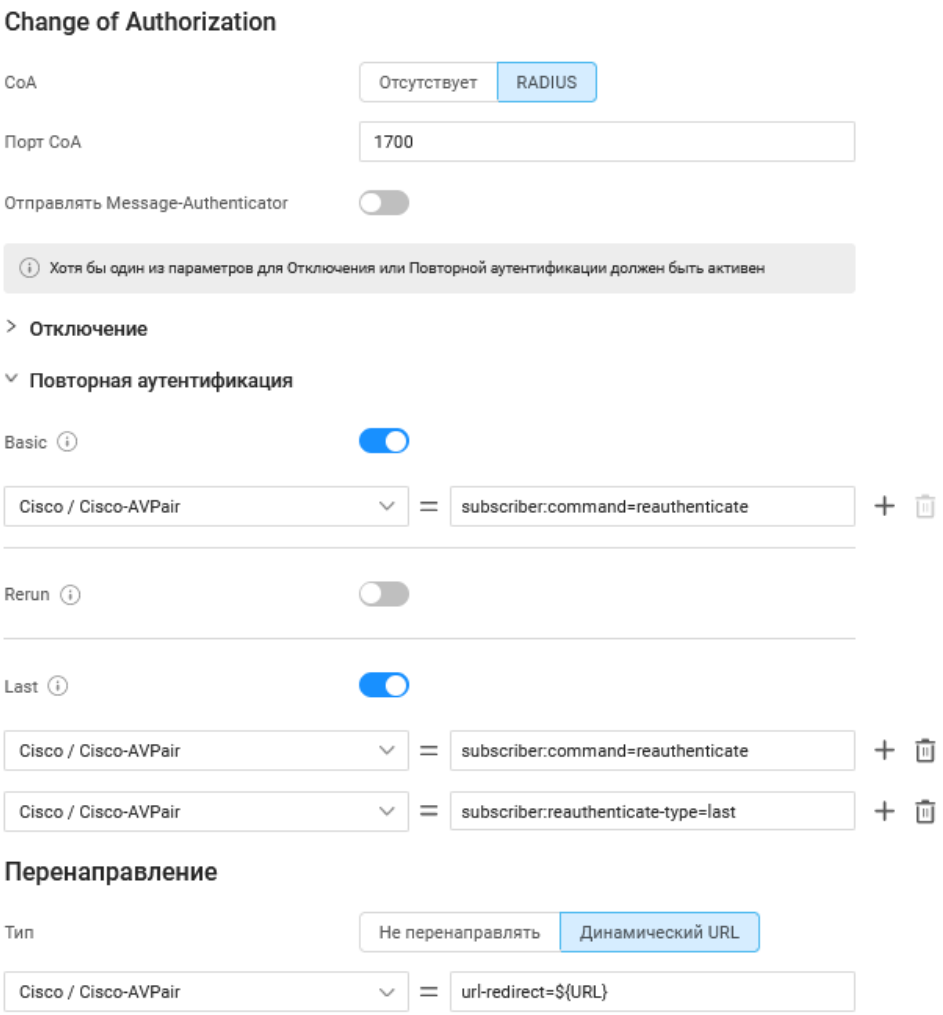



Рисунок 165 – Создание профиля сетевого оборудования. Блок полей «Change of Authorization»

Особенности заполнения блока полей «Change of Authorization» описаны ниже:

— блок полей «Change of Authorization»:
  - CoA: RADIUS;
  - Порт CoA: 1700.

— блок полей «Повторная аутентификация»:
  - Basic: Cisco / Cisco-AVPair = subscriber:command=reauthenticate;
  - Last:

    Cisco / Cisco-AVPair = subscriber:command=reauthenticate
    Cisco / Cisco-AVPair = subscriber:reauthenticate-type=last

— поле «Перенаправление»:
  - Тип: Динамический URL;
  - Атрибуты: Cisco / Cisco-AVPair = url-redirect=${URL}.

4) Создать сетевое оборудование – контроллер точек доступа:

— перейти в раздел «Контроль доступа», подраздел «Сетевое оборудование»;

— нажать кнопку « + Устройство » (рис. 166);
— заполнить поля страницы необходимыми параметрами (рис. 167).

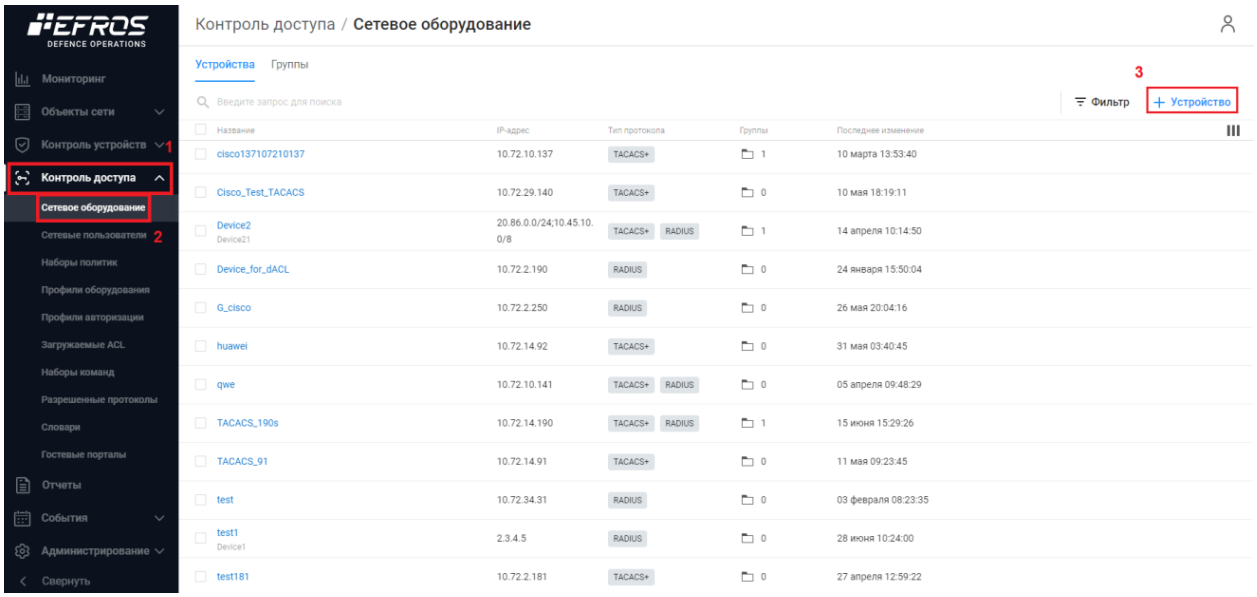



Рисунок 166 – Подраздел «Сетевое оборудование»

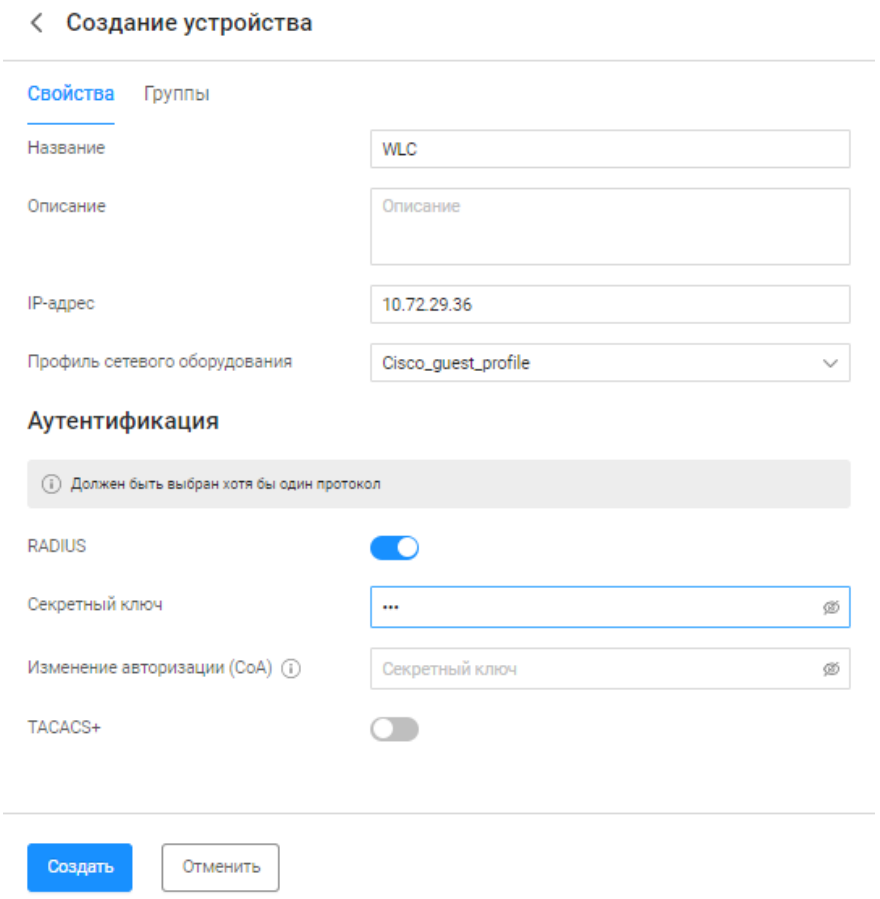



Рисунок 167 – Создание сетевого оборудования

Особенности заполнения полей описаны ниже:

- поле «Название»: любое;
- поле «IP-адрес»: IP-адрес контроллера точек доступа;
- поле «Профиль сетевого оборудования»: созданный в п. 3;
- поле «RADIUS»: перевести переключатель в положение «Активно» и ввести секретный ключ, указанный в настройках подключения контроллера точек доступа к серверу RADIUS.

5) Создать профиль авторизации для переадресации пользователя на гостевой портал:

- перейти в раздел «Контроль доступа», подраздел «Профили авторизации», вкладка «Доступ в сеть»;
- нажать кнопку «+ Профиль» (рис. 168);
- заполнить поля страницы необходимыми параметрами (рис. 169).

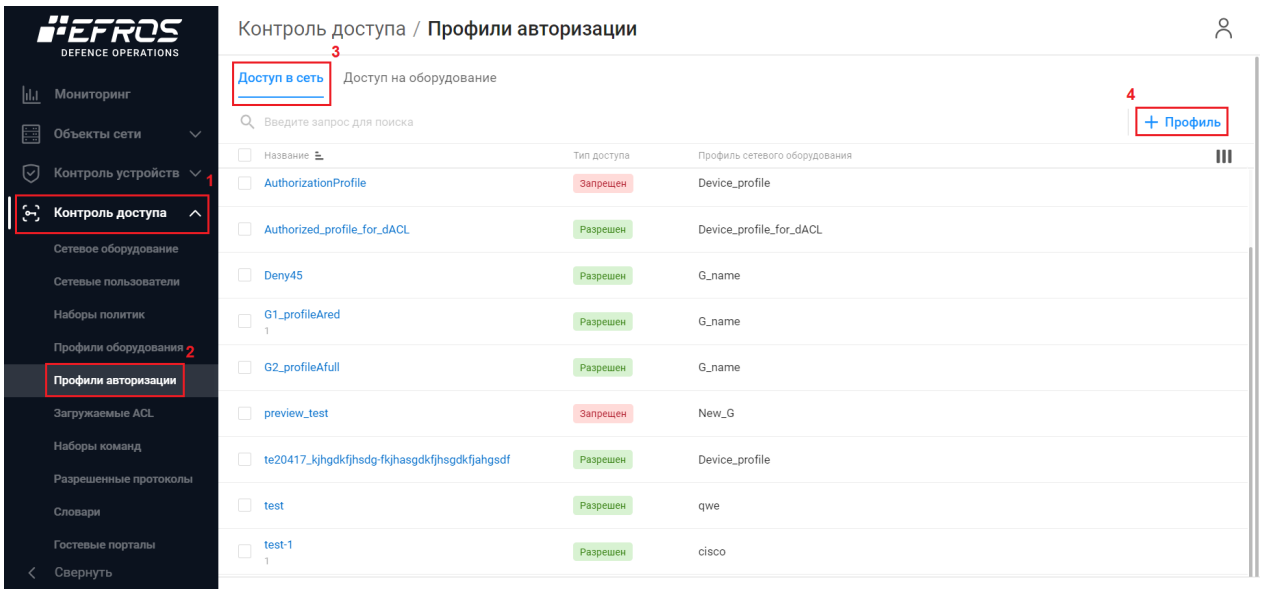



Рисунок 168 – Подраздел «Профили авторизации»

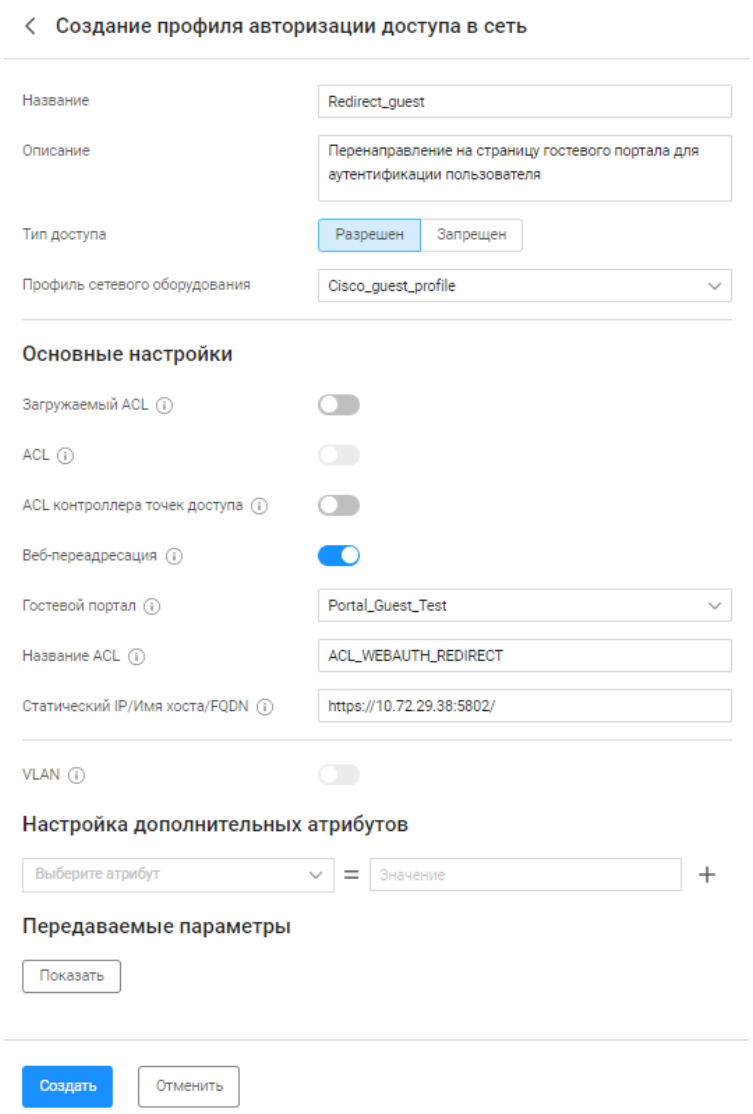



Рисунок 169 – Создание профиля авторизации доступа в сеть для переадресации пользователя на гостевой портал

Особенности заполнения полей описаны ниже:

- поле «Название»: любое;
- поле «Тип доступа»: разрешен;
- поле «Профиль сетевого оборудования»: созданный в п. 3;
- поле «Веб-переадресация», перевести переключатель в положение «Активно»:
  - поле «Гостевой портал» – название ранее созданного гостевого портала;
  - поле «Название ACL» – название ACL, предварительно созданного на контроллере точек доступа с ограниченными правами доступа (к серверу DHCP и серверу ПК «Efros DO» (порт 5802));
  - поле «Статический IP/Имя хоста/FQDN» – адрес сервера ПК «Efros DO», на котором создан указанный выше гостевой портал в формате https://{адрес сервера EDO}:5802.

Созданный профиль авторизации используется для перенаправления внешнего

пользователя (пользователя гостевого портала) на гостевой портал для ввода логина и пароля и для ознакомления с политикой использования сети (опционально).

Параметры, указанные в блоке «Веб-переадресация», используются для формирования url-адреса веб-страницы гостевого портала, на который будет перенаправлен внешний пользователь.

6) Создать профиль авторизации, назначаемый после успешной авторизации пользователя:

— перейти в раздел «Контроль доступа», подраздел «Профили авторизации», вкладка «Доступ в сеть»;
— нажать кнопку «+ Профиль» (рис. 168);
— заполнить поля страницы необходимыми параметрами (рис. 170).

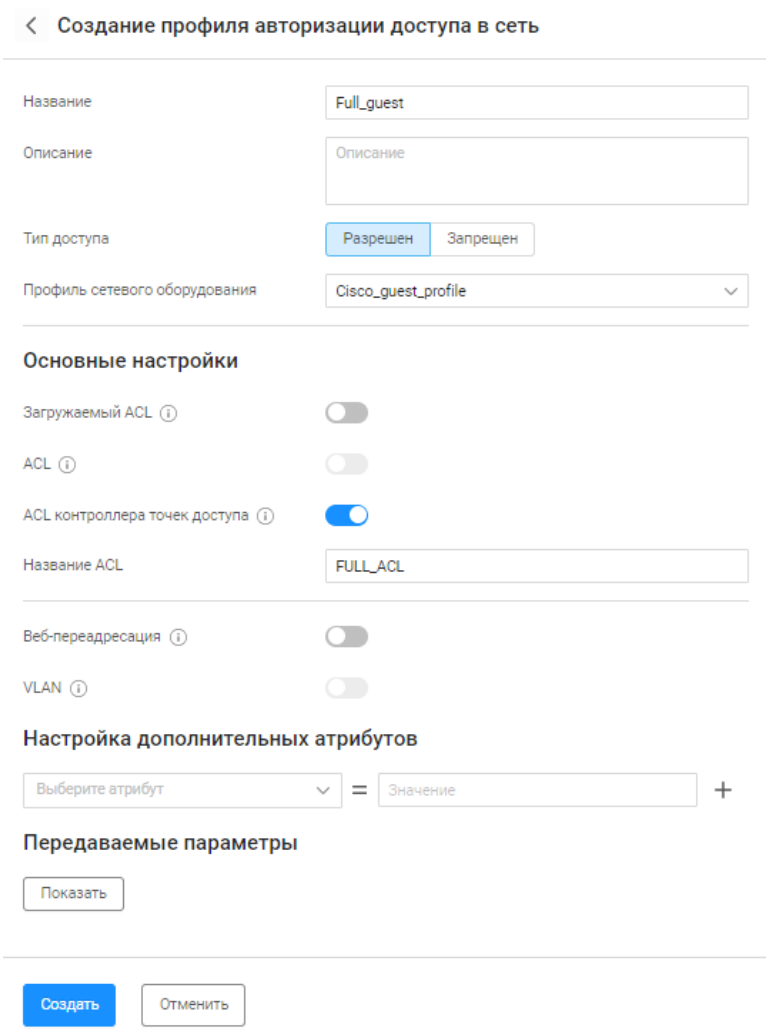



Рисунок 170 – Создание профиля авторизации доступа в сеть, назначаемый после успешной авторизации пользователя

Особенности заполнения полей описаны ниже:

— поле «Название»: любое;
— поле «Описание»: любое;
— поле «Тип доступа»: разрешен;
— поле «Профиль сетевого оборудования»: созданный в п. 3;
— блок полей «Основные настройки»:
  - поле «ACL контроллера точек доступа», перевести переключатель в положение «Активно»;
  - поле «Название ACL»: название ACL созданного на контроллере точек доступа (с правами доступа, которые получит пользователь после успешной аутентификации).

7) Создать политику доступа в сеть:

— перейти в раздел «Контроль доступа», подраздел «Наборы политик», вкладка «Доступ в сеть»;
— нажать кнопку « + Политика » (рис. 171);
— заполнить поля страницы необходимыми параметрами (рис. 172).

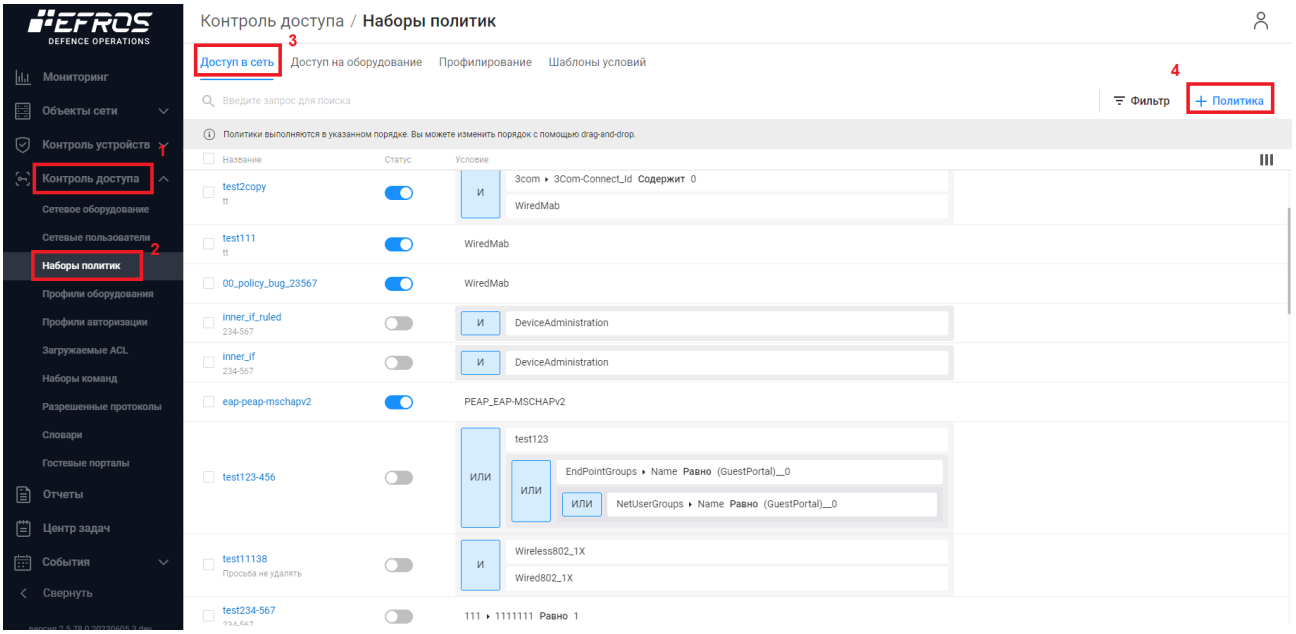



Рисунок 171 – подраздел «Наборы политик»

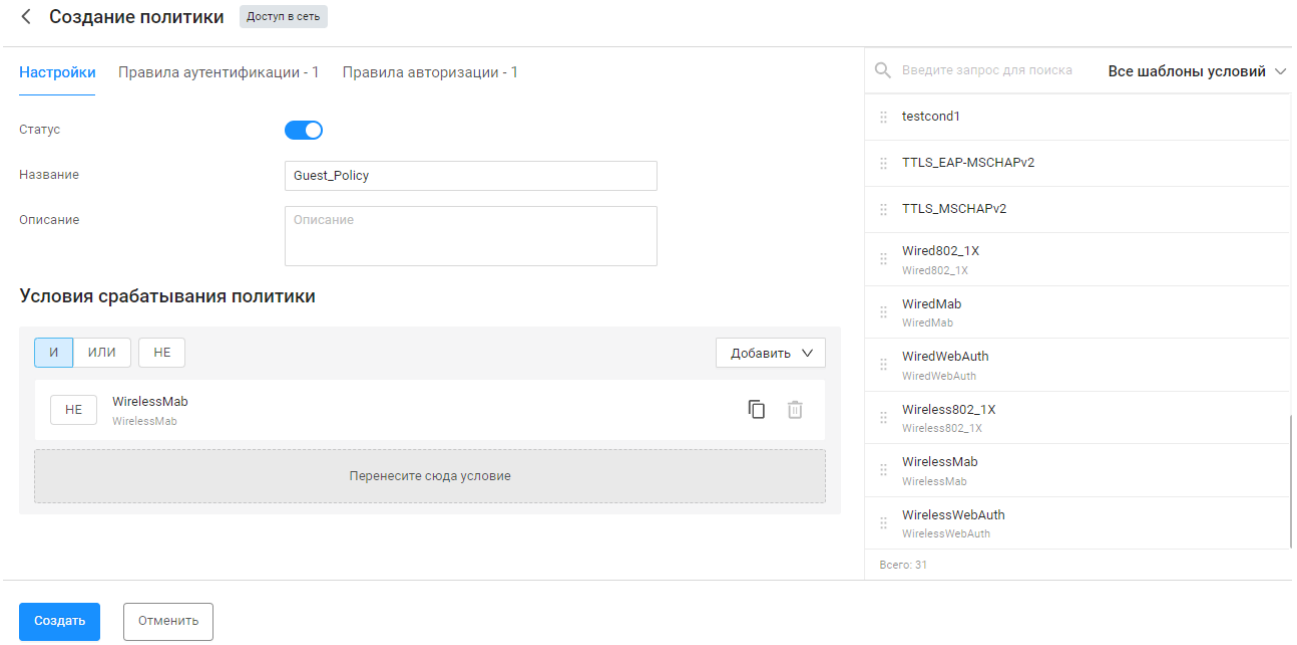



Рисунок 172 – Создание основного правила политики

Особенности заполнения полей описаны ниже:

— поле «Статус»: активен;
— поле «Название»: любое;
— поле «Основное правило»: Wireless MAB (из шаблонов условий).

Шаблон условий «Wireless MAB» – это набор условий для аутентификации устройств, подключенных к беспроводной сети по MAC-адресам.

В наборе правил «Условия срабатывания политики» используются атрибуты и значения, заданные в профиле оборудования. В зависимости от того, какое сетевое оборудование будет запрашивать доступ, для подключаемого устройства – могут быть использованы разные значения из профиля оборудования.
В данном случае в профиле сетевого оборудования применено условие «Беспроводная аутентификация по MAC-адресам (Wireless MAB)» (задано в блоках полей «Аутентификация / Авторизация» → «Условия сценариев доступа», см. п. 3).

8) Настроить правила аутентификации:

— на странице «Создание политики» перейти на вкладку «Правила аутентификации» (рис. 172);
— нажать кнопку «+ Правило аутентификации». Создаваемое правило аутентификации предназначено для разрешения пользователям переходить к авторизации;
— заполнить поля страницы необходимыми параметрами (рис. 173).

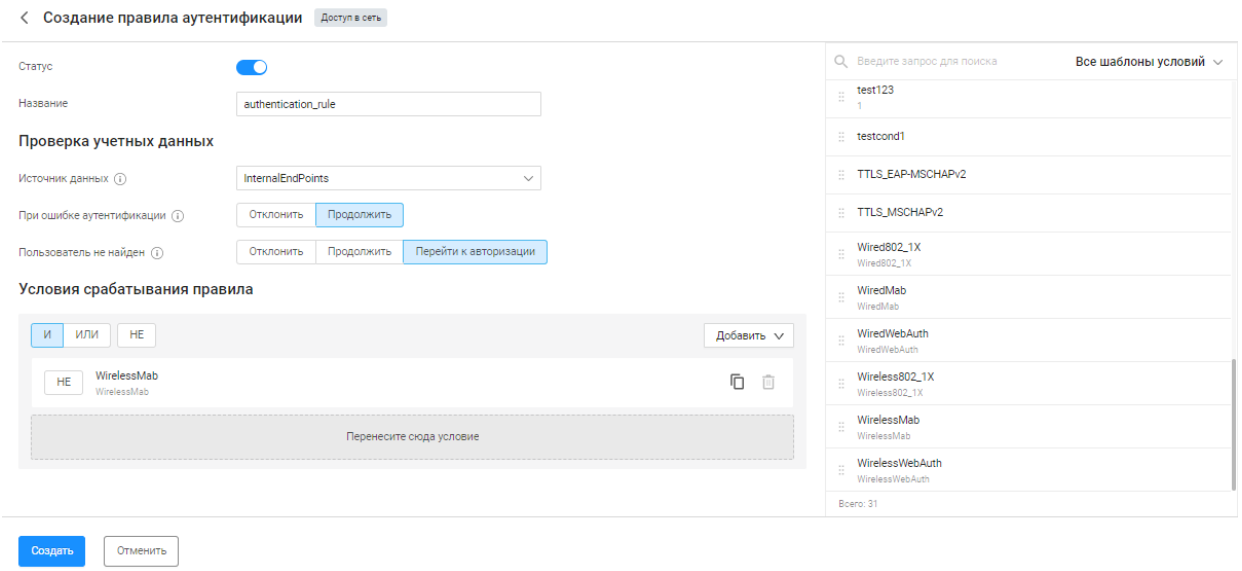



Рисунок 173 – Создание правила аутентификации

Особенности заполнения полей (рис. 173) описаны ниже:

- поле «Статус»: активен;
- поле «Название»: любое;
- поле «Источник данных»: InternalEndPoints;
- поле «При ошибке аутентификации»: продолжить;
- поле «Пользователь не найден»: перейти к авторизации;
- поле «Условия срабатывания правила»: Wireless MAB (из шаблонов условий).

Для запрета доступа в сеть пользователей, не соответствующих ранее созданным правилам аутентификации, необходимо в строке правила «Default» указать источник данных «DenyAccess» (рис. 174).

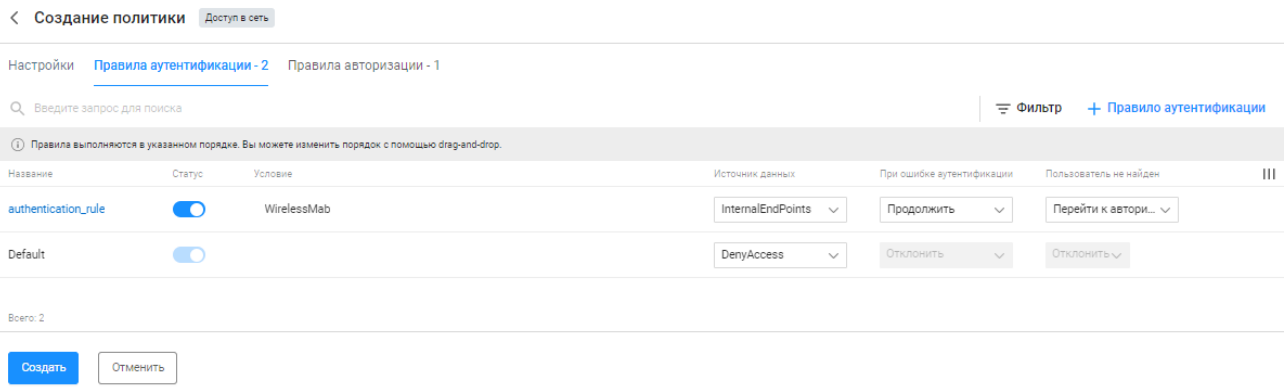



Рисунок 174 – Редактирование правила аутентификации «Default» для запрета доступа в сеть пользователей, не соответствующих правилам аутентификации

9) Настроить правила авторизации:

- на странице «Создание политики» перейти на вкладку «Правила аутентификации» (см. рис. 172);

— нажать кнопку «+ Правило авторизации». Создаваемое правило авторизации предназначено для предоставления доступа в сеть пользователям, прошедшим аутентификацию на гостевом портале;
— заполнить поля страницы необходимыми параметрами (рис. 175).

Необходимо соблюдать порядок условий. Выше по списку должно находиться правило авторизации, осуществляющее проверку на наличие у конечной точки метки гостевого портала, присваиваемой конечной точке автоматически в случае успешной аутентификации пользователя на гостевом портале.

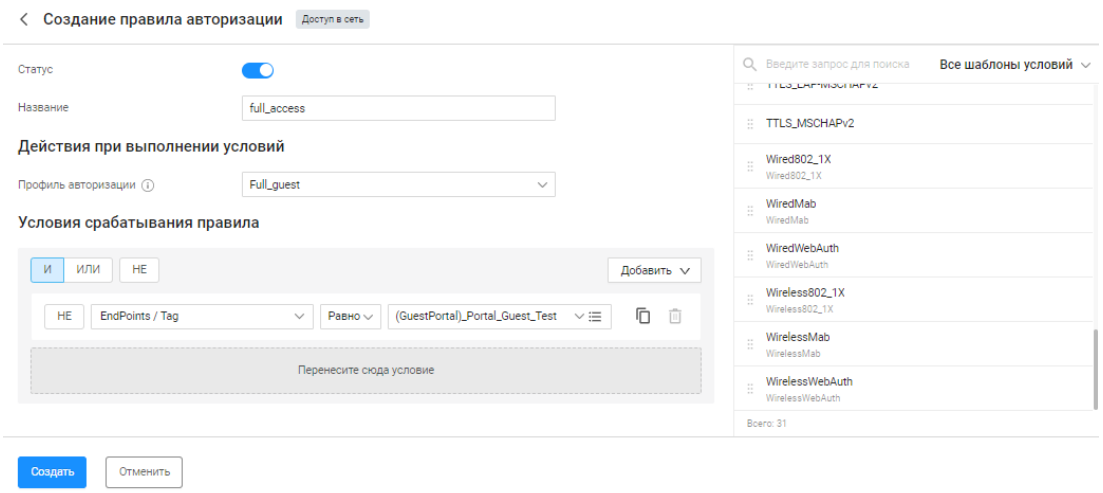



Рисунок 175 – Создание правила авторизации

Особенности заполнения полей описаны ниже:

— поле «Статус»: активен;
— поле «Название»: любое;
— поле «Профиль авторизации»: профиль авторизации, созданный в п. 6;
— поле «Условия срабатывания правила»:
  - EndPoints / Tag Равно (GuestPortal)_{название созданного ранее портала}.

Пользователи, не соответствующие ранее созданным правилам авторизации, должны переадресовываться на гостевой портал для аутентификации. Для этого необходимо в строке правила «Default» указать профиль авторизации, созданный в п. 5 (рис. 176).

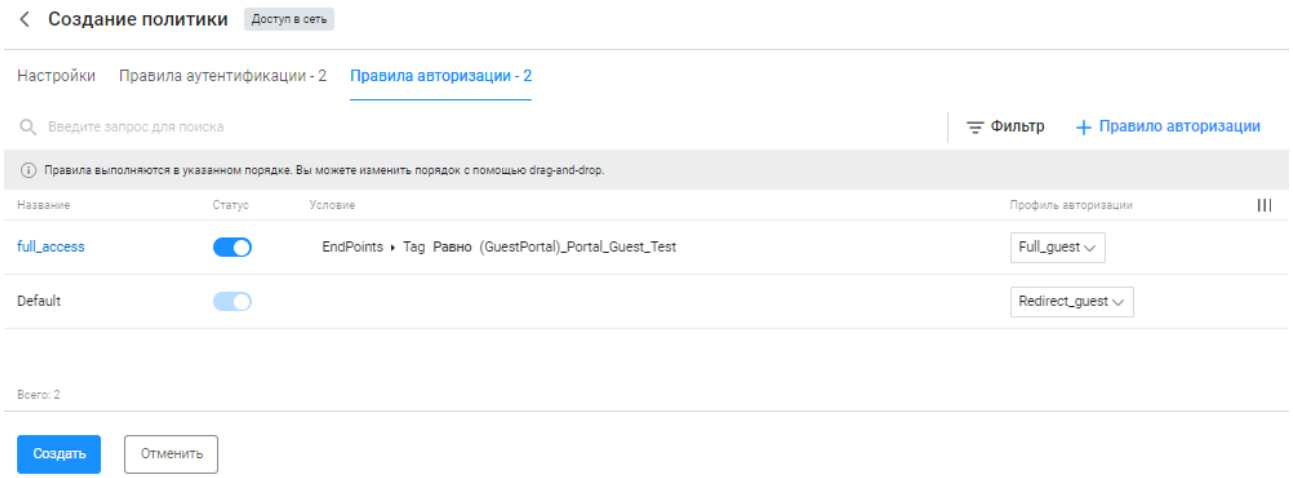



Рисунок 176 – Редактирование правила авторизации «Default» для переадресации пользователей на гостевой портал для аутентификации

10) Создать пользователей гостевого портала:

— перейти в раздел «Контроль доступа», подраздел «Гостевые порталы», вкладка «Пользователи»;

— нажать кнопку « + Пользователь » (рис. 177);

— заполнить поля страницы необходимыми параметрами (рис. 178).

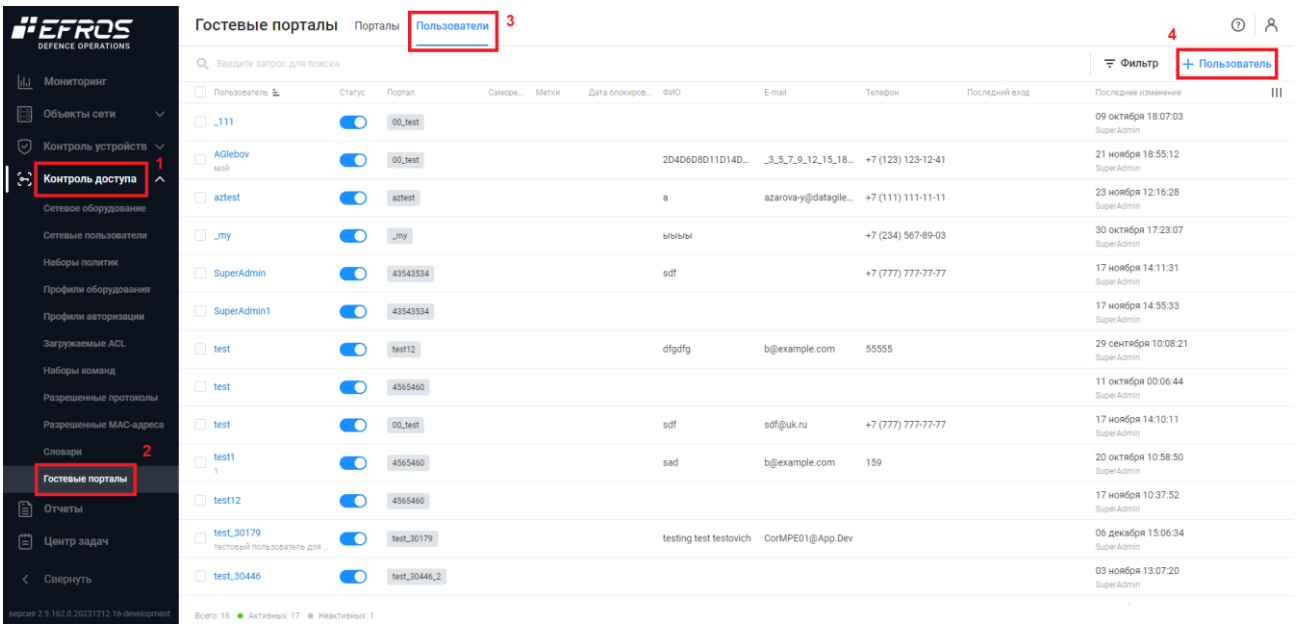



Рисунок 177 – Вкладка «Пользователи» в подразделе «Гостевые порталы»

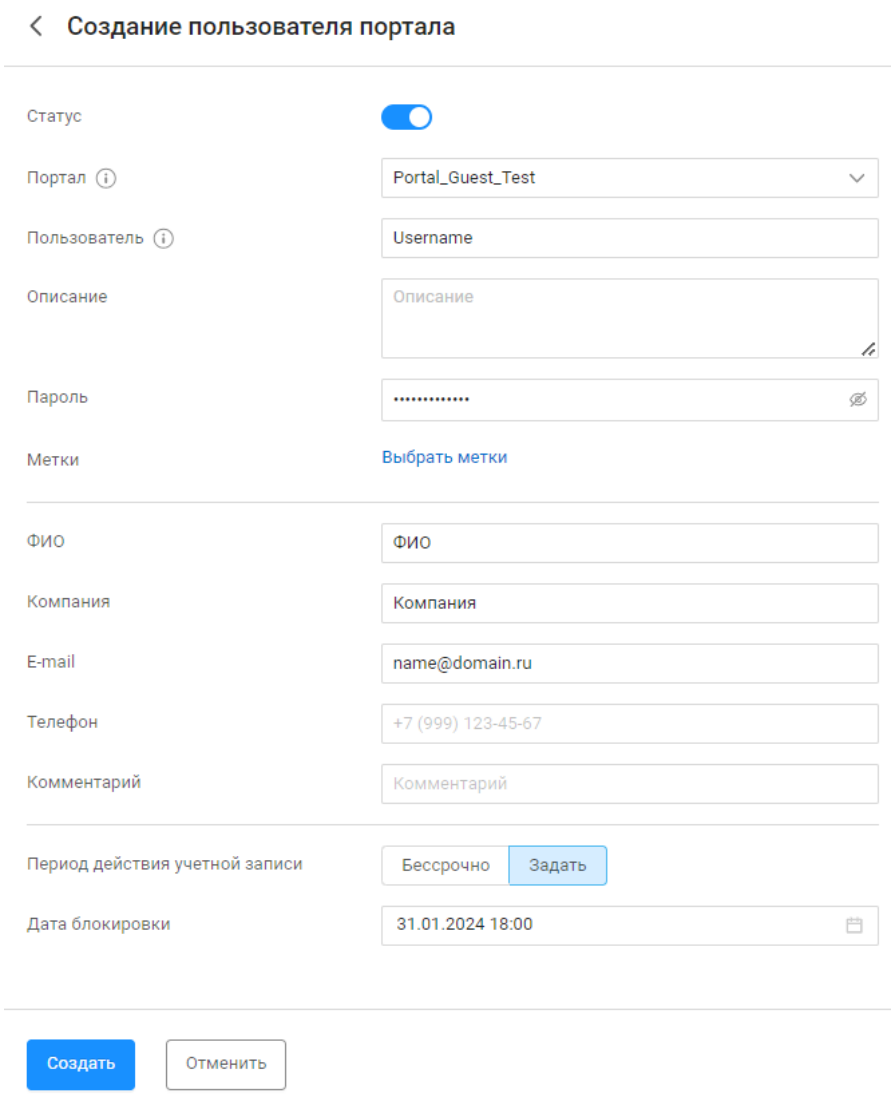



Рисунок 178 – Создание пользователя гостевого портала

Особенности заполнения полей описаны ниже:

- поле «Статус»: активен;
- поле «Портал»: созданный в п. 2 (с типом доступа «Гостевой»);
- поле «Пользователь»: уникальный логин в рамках гостевого портала;
- поле «Пароль»: заполняется согласно парольной политике, заданной в настройках портала при выбранном варианте входа на портал «Логин и пароль»;
- поля «ФИО», «Компания», «E-mail»: заполняются обязательно, как было задано в настройках портала (см. рис. 159);
- поля «Телефон», «Комментарий»: не заполняется в случае, если не задано в настройках портала.

Создать пользователя гостевого портала также можно при редактировании созданного гостевого портала на вкладке «Пользователи» (рис. 179).

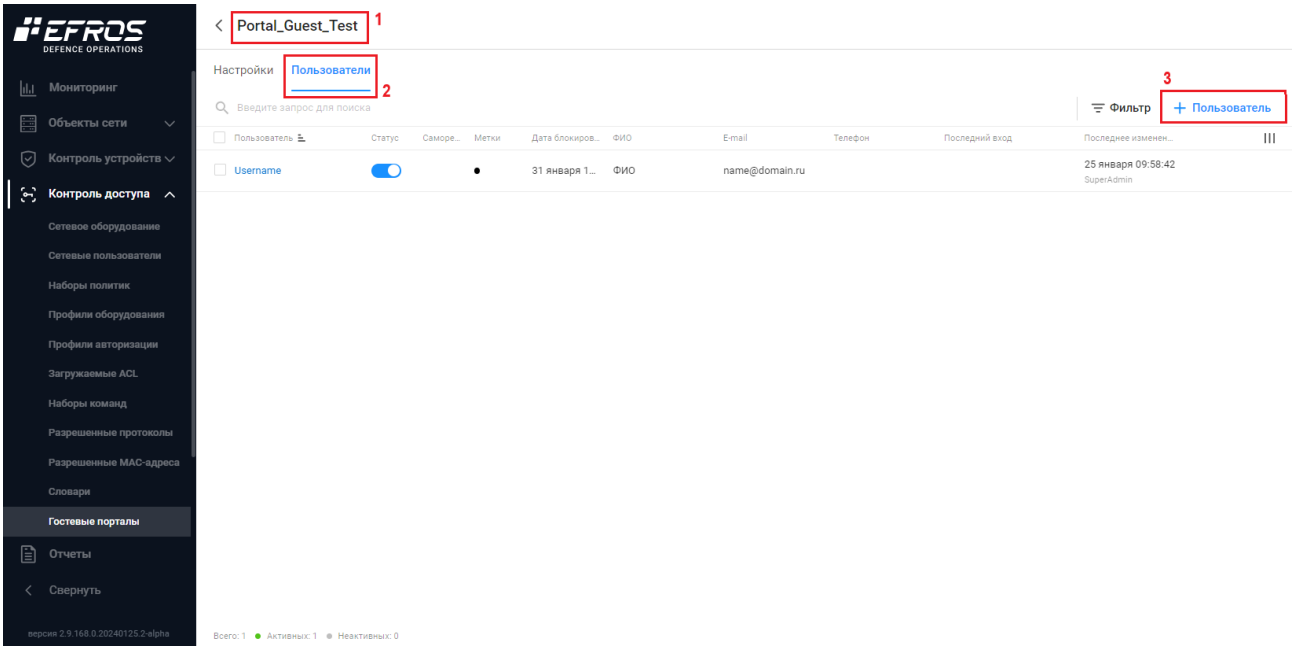



Рисунок 179 – Редактирование вкладки «Пользователи» гостевого портала

## Г.2 Рекомендуемая последовательность действий для настройки контроллера точек доступа

В инструкции пример приведен заполнения минимально необходимых полей для настройки контроллера точек доступа оборудования Cisco.

Последовательность действий для настройки доступа контроллера точек доступа оборудования Cisco:

1) Подключиться к точке доступа и открыть интерфейс настройки оборудования в разделе «Monitor». В строке «All APs» нажать кнопку «Detail» (рис. 180).

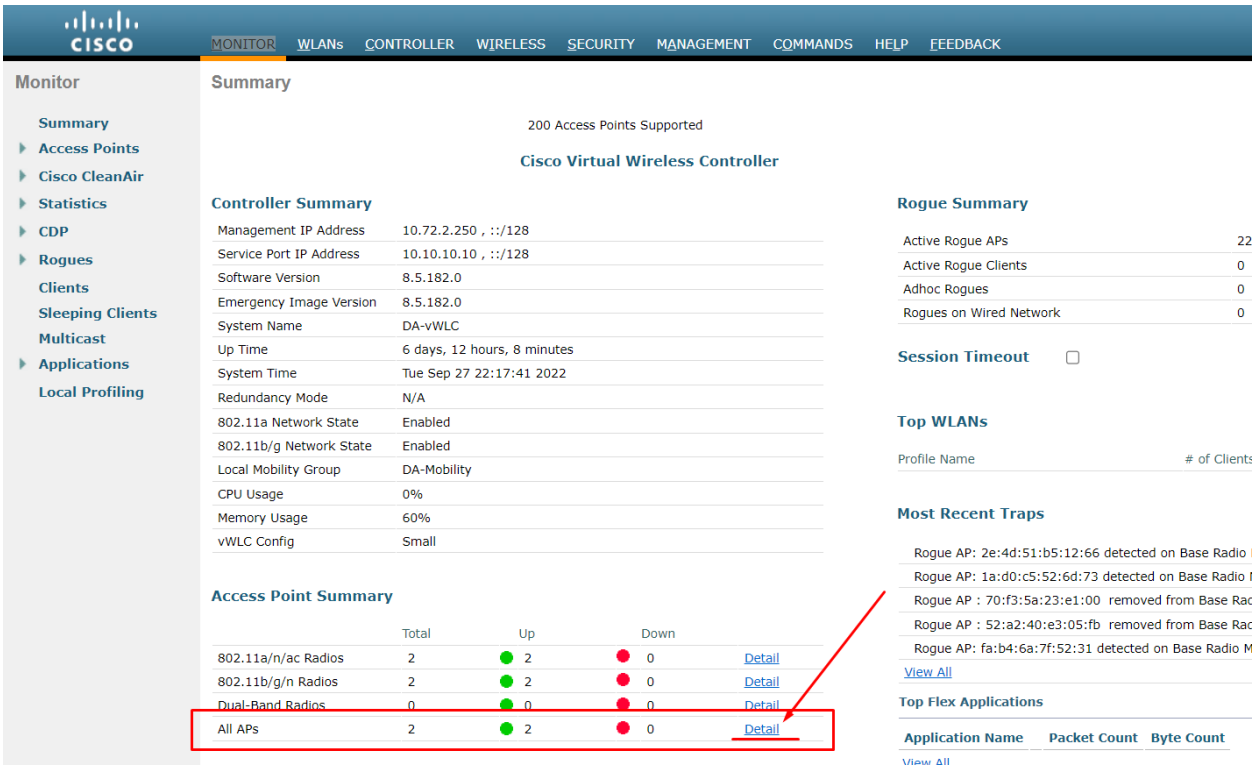



Рисунок 180 – Раздел «Monitor»

2) Убедиться, что точка доступа успешно добавлена и отображается на странице «All APs» (рис. 181). Нажать на название точки доступа, в открывшейся вкладке «General» настроить общие настройки (рис. 182).

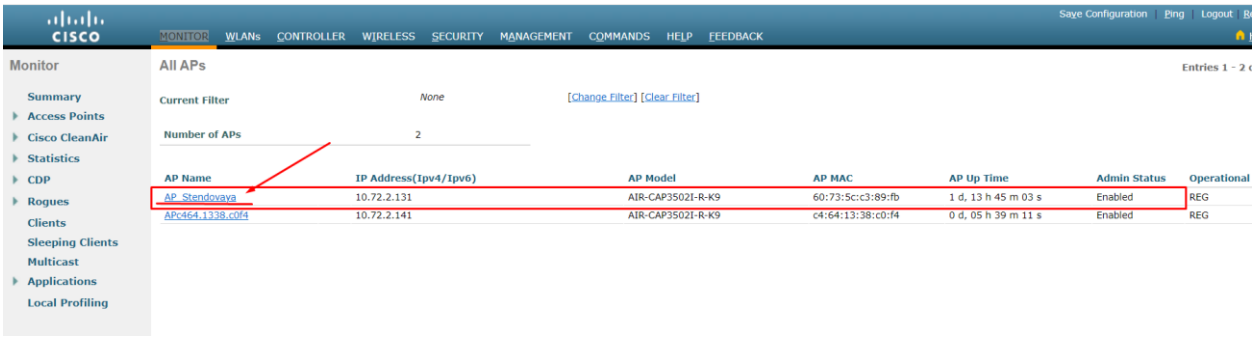



Рисунок 181 – Страница «All APs»

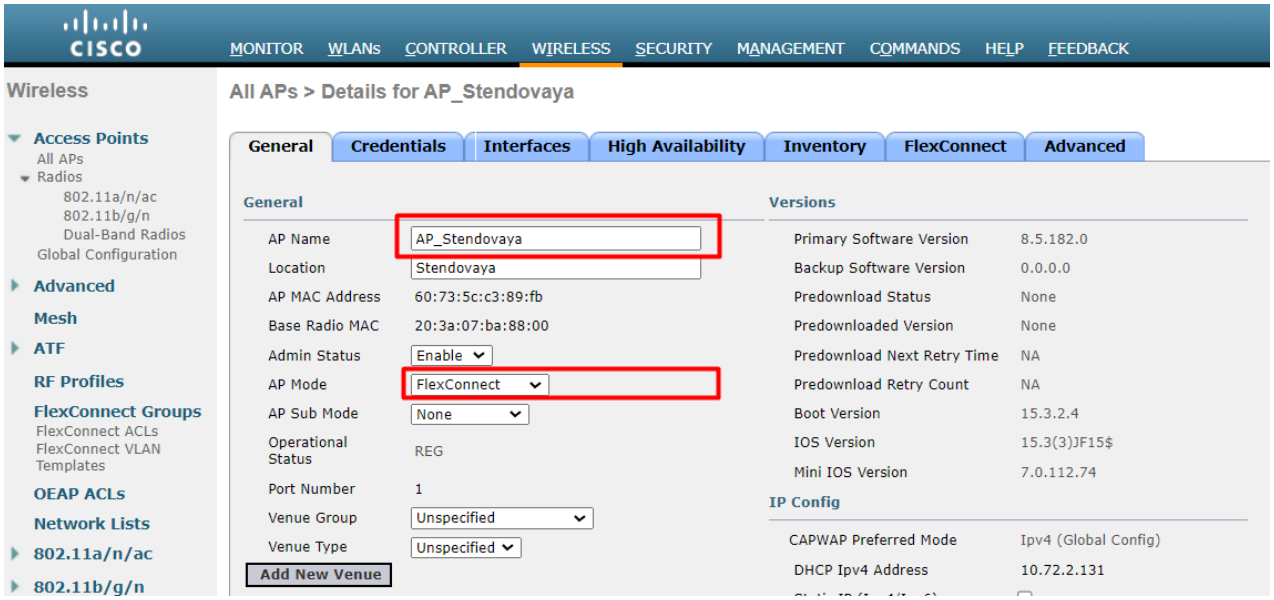



Рисунок 182 – Вкладка «General» в разделе «Wirelless»

Особенности заполнения полей вкладки «General» для настройки конечной точки (рис. 182) описаны ниже:

- поле «AP Name»: имя конечной точки;
- поле «AP Mode»: FlexConnect – режим работы точки доступа для подключения через публичный канал связи (например, если точка доступа развернута в филиале головного офиса, без развертывания контроллера в каждом офисе).

3) Настроить работу с сервером аутентификации. В разделе «Security» перейти на страницу «RADIUS Authentication Servers» (рис. 183).

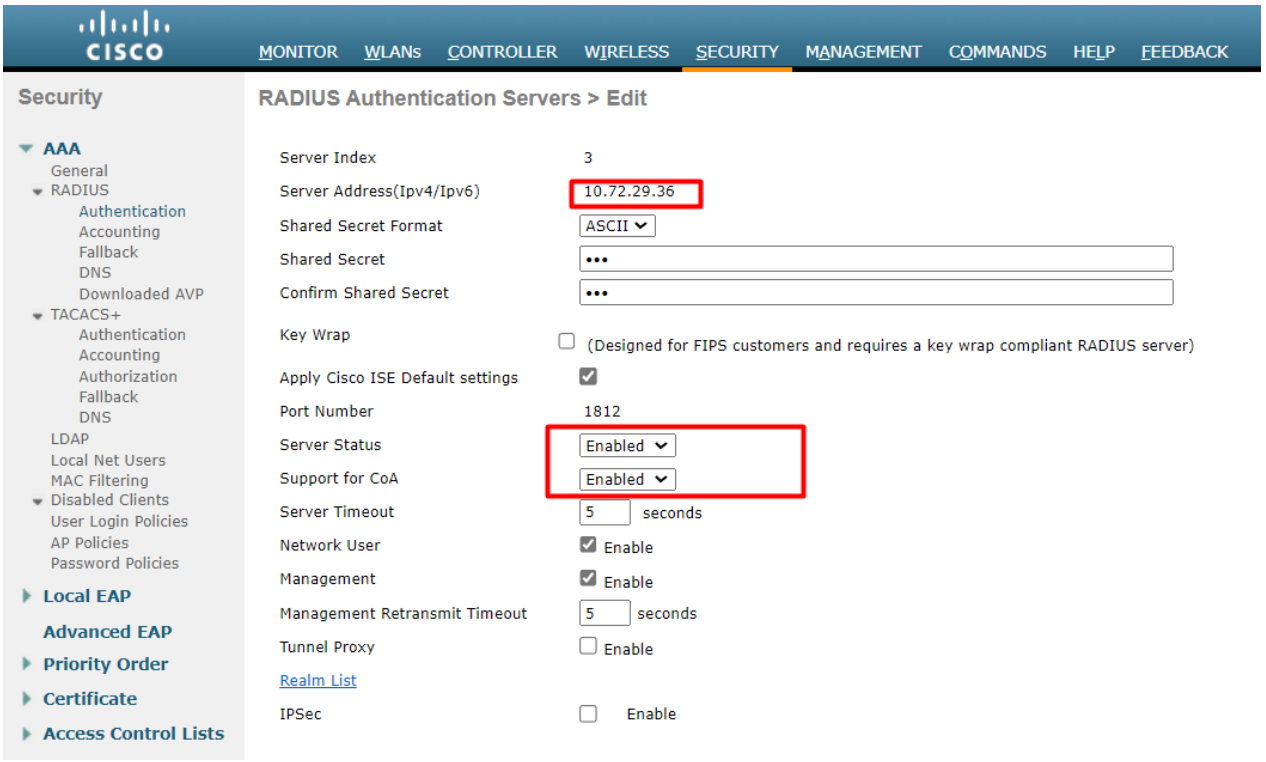



Рисунок 183 – Страница «RADIUS Authentication Servers»

Особенности заполнения полей (рис. 183) описаны ниже:

- поле «Server Address»: IP-адрес сервера;
- поле «Shared secret»: ключ RADIUS-сервера;
- поле «Server Status»: Enabled – включение отображения статуса сервера;
- поле «Support of CoA»: Enabled – включение поддержки CoA;
- поле «Network User»: Enable – включение поддержки авторизации пользователей по беспроводной сети;
- поле «Management»: Enable – включение поддержки авторизации администраторов контроллера.

4) Задать адрес сервера для целей учета. Адрес аналогичен указанному в предыдущем шаге. В разделе «Security» перейти на страницу «RADIUS Accounting Servers» (рис. 184).

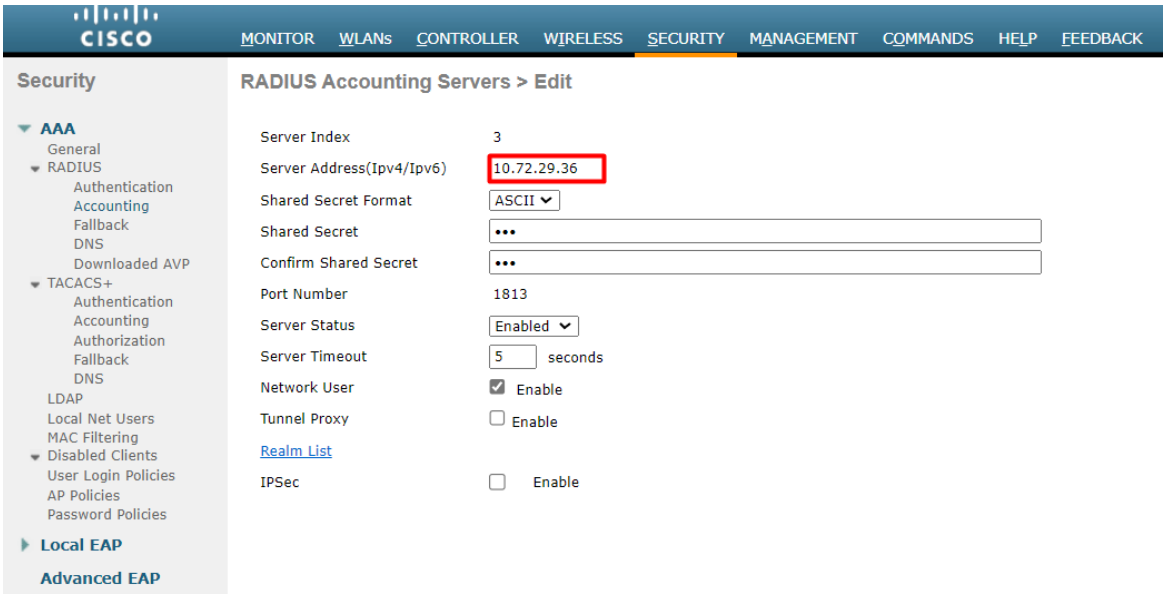



Рисунок 184 – Страница «RADIUS Accounting Servers»

5) Создать WLAN и SSID в разделе «WLANs» (рис. 185).


Рисунок 185 – Создание WLAN и SSID в разделе «WLANs»

6) Зайти в настройки созданного WLAN (рис. 186).


Рисунок 186 – Раздел «WLANs»

7) Настроить параметры на вкладке «Security» → «Layer 2» (рис. 187).

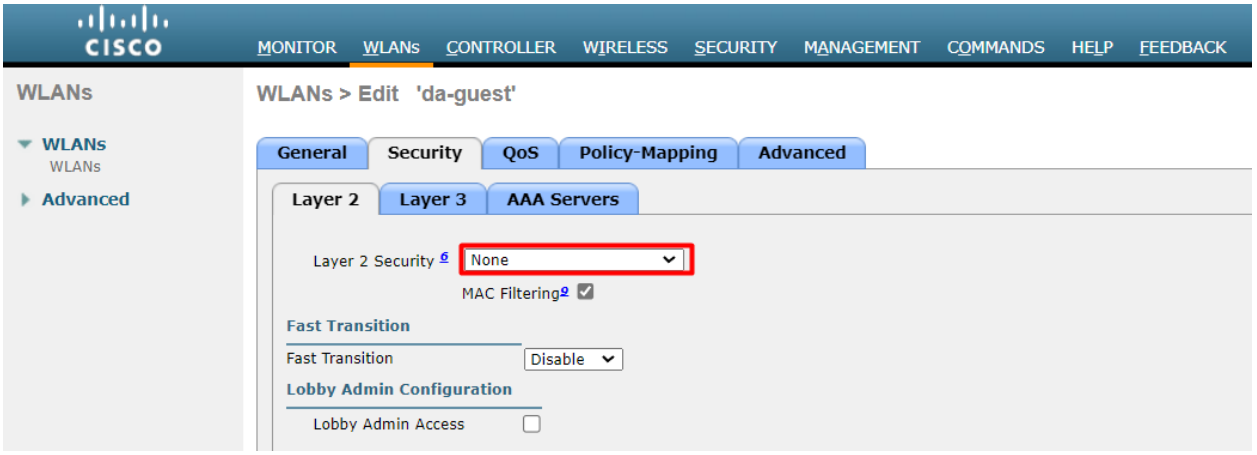



Рисунок 187 – Вкладка «Layer 2»

8) Настроить параметры на вкладке «Security» → «Layer 3» (рис. 188).

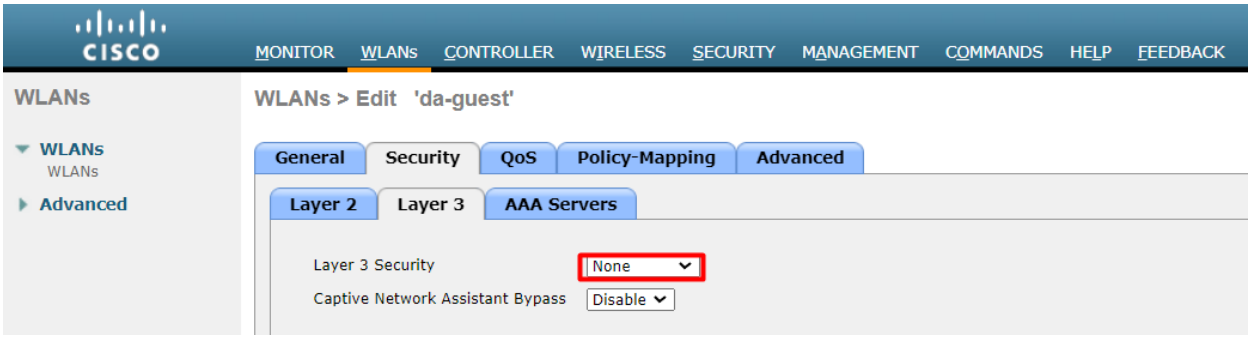



Рисунок 188 – Вкладка «Layer 2»

9) На вкладке «Security» → «AAA Servers» прописать параметры сервера для авторизации, аутентификации и учета (рис. 189).

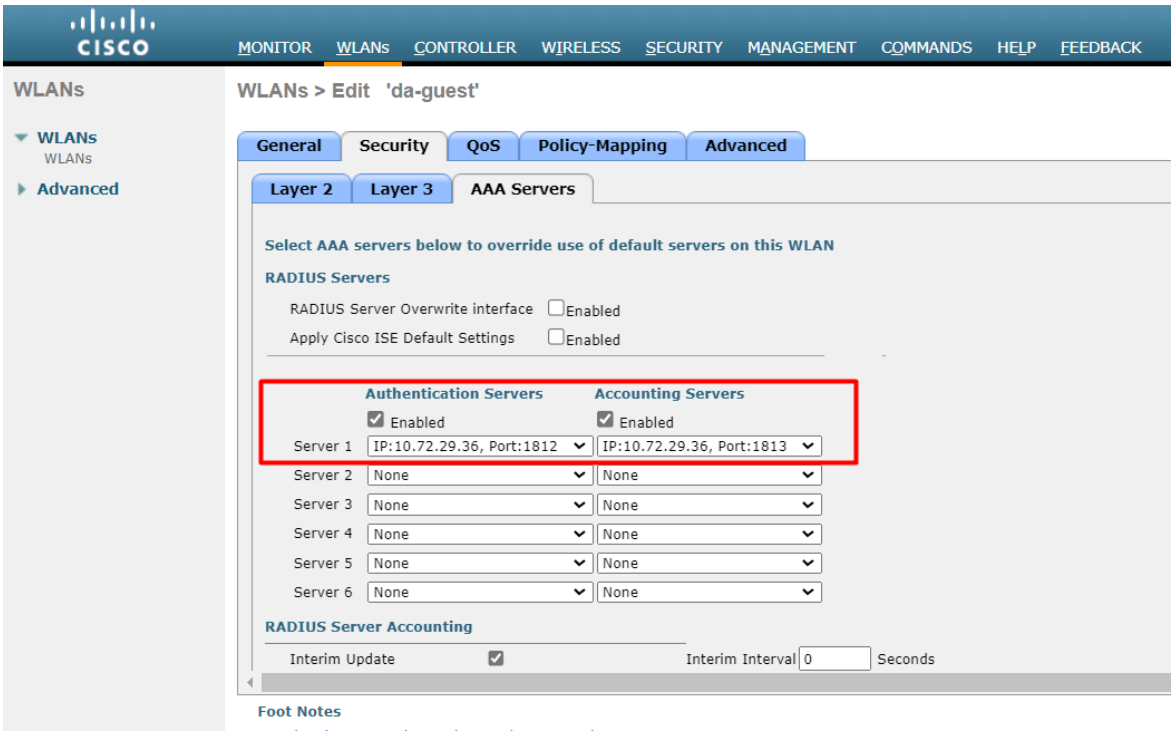



Рисунок 189 – Вкладка «AAA Servers»

10) Настроить параметры на вкладке «Advanced» (рис. 190).

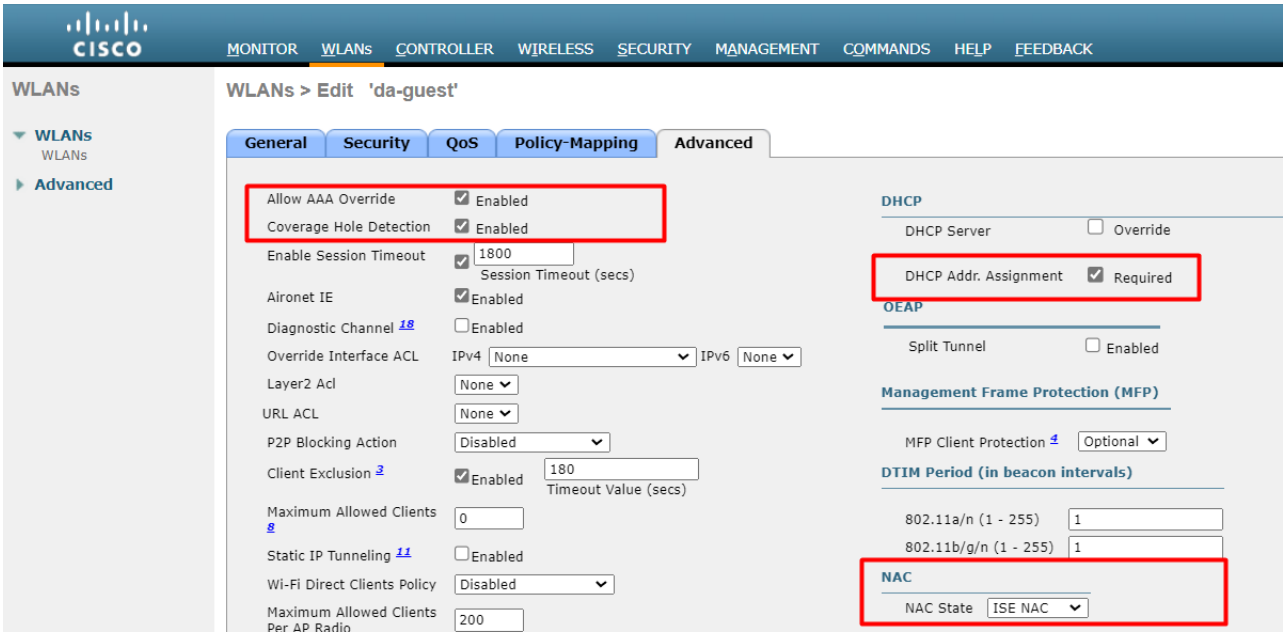



Рисунок 190 – Вкладка «Advanced»

Особенности заполнения полей описаны ниже:

— поле «Allow AAA Override»: Enabled – включение передачи дополнительных параметров от RADIUS-сервера в момент успешной авторизации клиента;

— поле «Coverage Hole Detection»: Enabled – включение применения дополнительных параметров, передаваемых определенному клиенту от RADIUS-

сервера;

— поле «DHCP Addr. Assignment»: Required – включение функции передачи траффика от клиентов, получивших IP-адрес по DHCP;
— поле «NAC State»: ISE NAC – передача управления серверу ISE.

11) Создать два вида ACL. В разделе «Security» перейти на страницу «Access Control List» в (рис. 191).

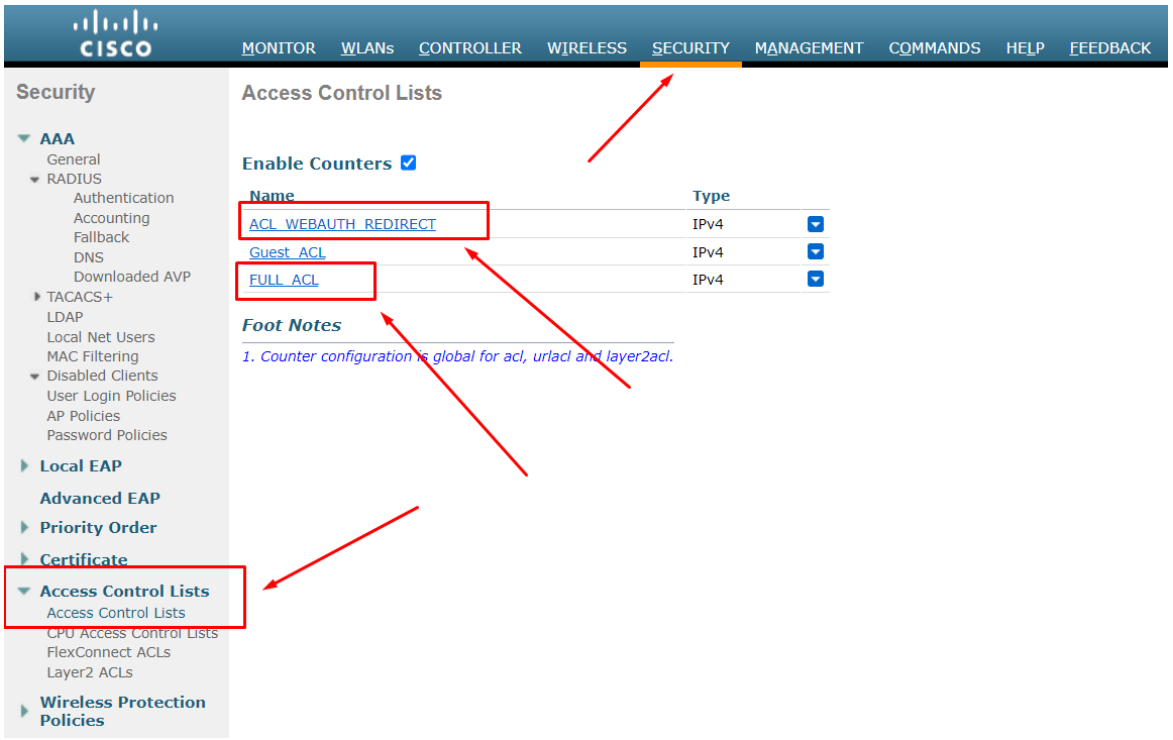
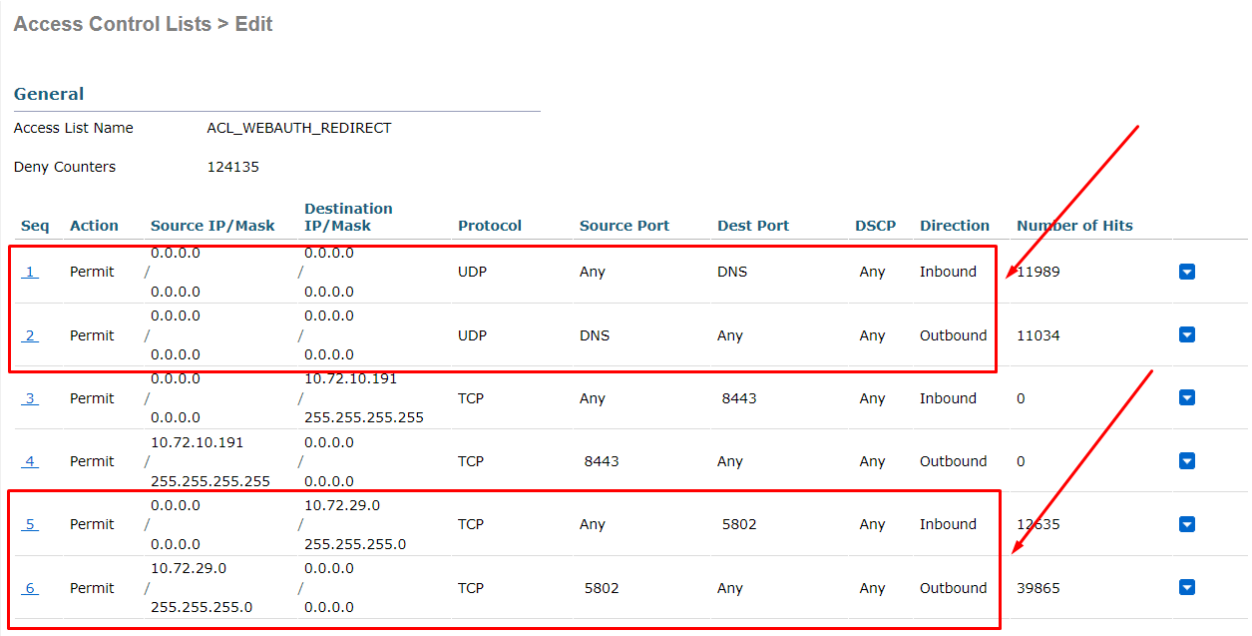



Рисунок 191 – Страница «Access Control List»

Особенности полей описаны ниже:

— (ACL_WEBAUTH_REDIRECT) – ACL с ограниченным доступом для неавторизованных пользователей. Предназначен для доступа к гостевому порталу, DHCP-серверу, серверу DNS. Пример приведен на рис. 192;
— (FULL_ACL) – ACL для авторизованных пользователей. Пример приведен на рис. 193.



Access Control Lists > Edit

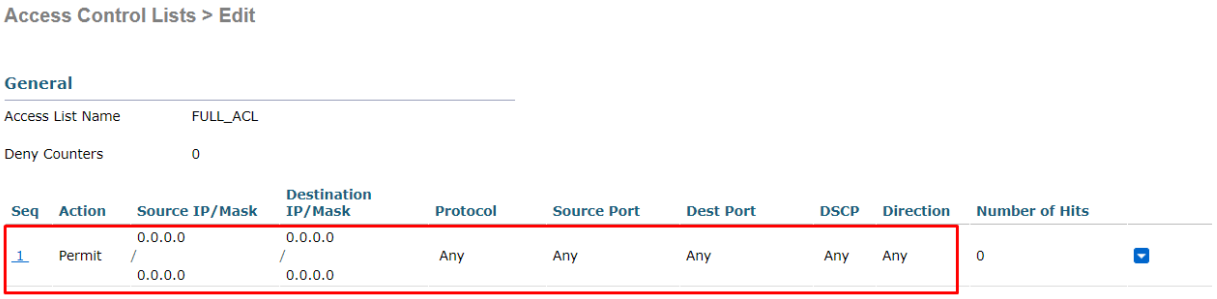
General

Access List Name ACL_WEBAUTH_REDIRECT

Deny Counters 124135

| Seq | Action | Source IP/Mask | Destination IP/Mask | Protocol | Source Port | Dest Port | DSCP | Direction | Number of Hits |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Permit | 0.0.0.0 / 0.0.0.0 | 0.0.0.0 / 0.0.0.0 | UDP | Any | DNS | Any | Inbound | 11989 |
| 2 | Permit | 0.0.0.0 / 0.0.0.0 | 0.0.0.0 / 0.0.0.0 | UDP | DNS | Any | Any | Outbound | 11034 |
| 3 | Permit | 0.0.0.0 / 0.0.0.0 | 10.72.10.191 / 255.255.255.255 | TCP | Any | 8443 | Any | Inbound | 0 |
| 4 | Permit | 10.72.10.191 / 255.255.255.255 | 0.0.0.0 / 0.0.0.0 | TCP | 8443 | Any | Any | Outbound | 0 |
| 5 | Permit | 0.0.0.0 / 0.0.0.0 | 10.72.29.0 / 255.255.255.0 | TCP | Any | 5802 | Any | Inbound | 12635 |
| 6 | Permit | 10.72.29.0 / 255.255.255.0 | 0.0.0.0 / 0.0.0.0 | TCP | 5802 | Any | Any | Outbound | 39865 |

Рисунок 192 – ACL с ограниченным доступом для неавторизованных пользователей



Access Control Lists > Edit

General

Access List Name FULL_ACL

Deny Counters 0

| Seq | Action | Source IP/Mask | Destination IP/Mask | Protocol | Source Port | Dest Port | DSCP | Direction | Number of Hits |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Permit | 0.0.0.0 / 0.0.0.0 | 0.0.0.0 / 0.0.0.0 | Any | Any | Any | Any | Any | 0 |

Рисунок 193 – ACL для авторизованных пользователей

Схема взаимодействия подключаемого устройства, точки доступа и настроенного контроллера точек доступа для беспроводного доступа в сеть приведена на рис. 194.


Рисунок 194 – Схема взаимодействия с контроллером точек доступа

# Перечень сокращений

| | | |
|---|---|---|
| AAA | — | Authentication, Authorization, Accounting |
| ACL | — | Access Control List |
| AD | — | Active Directory |
| ASCII | — | American Standard Code for Information Interchange |
| AUP | — | Acceptable Use Policy |
| AV | — | AntiVirus |
| CDP | — | Cisco Discovery Protocol |
| CN | — | Common Name |
| CoA | — | Change of Authorization |
| DNS | — | Domain Name System |
| EAP | — | Extensible Authentication Protocol |
| FAST | — | Flexible Authentication via Secure Tunneling |
| FQDN | — | Fully Qualified Domain Name |
| GTC | — | Generic Token Card |
| IETF | — | Internet Engineering Task Force |
| IIS | — | Internet Information Services |
| IP | — | Internet Protocol |
| LAN | — | Local Area Network |
| LDAP | — | Lightweight Directory Access Protocol |
| LLDP | — | Link Layer Discovery Protocol |
| MAB | — | MAC Authentication Bypass |
| MAC | — | Media Access Control |
| MD5 | — | Message Digest 5 |
| MSCHAPv2 | — | Microsoft Challenge-Handshake Authentication Protocol v 2 |
| NAC | — | Network Access Control |
| PAP | — | Password Authentication Protocol |
| PEAP | — | Protected Extensible Authentication Protocol |
| RADIUS | — | Remote Authentication in Dial-In User Service |
| RFC | — | Request for Comments |
| SAN | — | Subject Alternative Name |
| SNMP | — | Simple Network Management Protocol |
| TACACS+ | — | Terminal Access Controller Access Control System plus |
| TEAP | — | Tunnel Extensible Authentication Protocol |
| TLS | — | Transport Layer Security |

| | | |
|---|---|---|
| TTLS | — | Tunneled Transport Layer Security |
| URL | — | Uniform Resource Locator |
| VDC | — | Virtual Device Context |
| VLAN | — | Virtual Local Area Network |
| VPN | — | Virtual Private Network |
| WLC | — | Wireless LAN Controller |
| АСО | — | Активное сетевое оборудование |
| БД | — | База данных |
| КО | — | Клиентское оборудование |
| ОЗ | — | Объект защиты |
| ОС | — | Операционная система |
| ПК | — | Программный комплекс |