

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


Часть 3

Контроль доступа

Аннотация

Руководство содержит описание настройки и конфигурирования модуля «Efros Network Access Control» (далее – модуль «Efros NAC»).

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

Для перехода в раздел необходимо выбрать в панели главного меню раздел «Контроль доступа», или, если панель свернута, нажать на пиктограмму , панель автоматически раскроется и отобразятся все подразделы.

Раздел «Контроль доступа» позволяет:

- задавать параметры и протоколы доступа к сетевому оборудованию с использованием механизма AAA, создавать группы сетевых устройств;
- создавать собственные конечные точки/группы конечных точек, просматривать данные, полученные в результате профилирования, управлять аутентификацией устройств, подключаемых к сети по MAC-адресам (MAC Authentication Bypass (MAB));
- создавать учетные записи пользователей/группы пользователей для разграничения доступа к сетевому оборудованию/группам сетевого оборудования;
- формировать правила доступа к сети на основе условий подключения, правил аутентификации и авторизации;
- создавать профили сетевого оборудования с возможностью указать сценарии доступа к сети, используемые протоколы, атрибуты RADIUS-словарей, значения параметров Change of Authorization (CoA);
- формировать профили авторизации сетевого оборудования, которые можно использовать в правилах наборов политик;
- добавлять загружаемые списки управления доступом;
- конфигурировать список политик доступа и основных правил аутентификации пользователей к контролируемому сетевому оборудованию;
- создавать шаблоны условий для использования в политиках доступа.

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.....	6
2	Работа с ПК «Efros DO». Раздел «Контроль доступа»	7
2.1	Настройка политик доступа	7
2.2	Рекомендуемая последовательность работы с локальными и сторонними сертификатами.....	10
2.3	Работа со списком сущностей модуля «Efros NAC» ПК «Efros DO». Общие сведения	10
2.3.1	Выбор сортировки записей таблиц.....	12
2.3.2	Поиск данных в таблицах списков сущностей	12
2.3.3	Фильтрация данных в таблицах сущностей.....	12
2.3.4	Настройка состава отображаемых колонок в таблицах списков сущностей.....	13
2.3.5	Копирование сущностей.....	14
2.3.6	Редактирование сущностей	14
2.3.7	Удаление сущностей	14
2.4	Сетевое оборудование	16
2.4.1	Вкладка «Устройства»	16
2.4.2	Вкладка «Группы»	20
2.5	Сетевые пользователи	23
2.5.1	Вкладка «Пользователи»	23
2.5.2	Вкладка «Группы»	28
2.5.3	Вкладка «Парольная политика»	30
2.6	Наборы политик.....	34
2.6.1	Вкладка «Доступ в сеть»	35
2.6.2	Вкладка «Доступ на оборудование»	42
2.6.3	Вкладка «Профилирование».....	50
2.6.4	Вкладка «Шаблоны условий».....	53
2.7	Профили оборудования	62
2.7.1	Добавление профиля сетевого оборудования	63
2.8	Профили авторизации	68
2.8.1	Вкладка «Доступ в сеть»	68

2.8.2	Вкладка «Доступ на оборудование»	71
2.9	Загружаемые ACL	77
2.9.1	Создание загружаемых ACL	78
2.9.2	Создание правила доступа для загружаемого ACL	79
2.10	Наборы команд	82
2.10.1	Создание набора команд	82
2.11	Разрешенные протоколы	87
2.11.1	Создание списка разрешенных протоколов	87
2.12	Разрешенные MAC-адреса	90
2.12.1	Создание разрешенного MAC-адреса	90
2.13	Словари	92
2.13.1	Вкладка «Системные»	95
2.13.2	Вкладка «Пользовательские»	95
2.13.3	Создание пользовательского словаря	97
2.14	Гостевые порталы	100
2.14.1	Создание нового гостевого портала	101
	Перечень сокращений	109
	Приложение А	111
	Приложение Б	146
	Приложение В	155


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:

1. Настроить подключение к AD (LDAP).
2. Добавить сертификаты для установки доверенного соединения при доступе устройств в сеть.
3. При необходимости, вручную добавить конечные точки сети.
4. Добавить учетные записи сетевых пользователей (более подробно об этом написано в п. 2.5.1).

 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.

2 Работа с ПК «Efros DO». Раздел «Контроль доступа»

2.1 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 2.7 «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


Протокол, используемый при доступе к сети	Логическая операция	Выбранные значения			
		ГАЗИНФОРМ	Тип	Сравнение	Протокол
TTLS_CHAP	И	Gazinformservice	GisEapType	равно	TTLS
		Gazinformservice	GisAuthType	равно	CHAP
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.

- кнопка «Колонки» () позволяет определить отображение необходимых колонок на странице.

Таблицы, кроме колонок с данными сущностей, содержат столбец с полями для флага. После установки флага в одной строке над таблицей отображается выбор операций, выполняемых с одной сущностью (рис. 2, рис. 3).

Выбрано: 1 |  Создать копию |  Добавить в группу |  Удалить

Рисунок 2 – Строка выбора операции, выполняемой с одной сущностью

Выбрано: 1 |  Разрешить МАВ |  Запретить МАВ |  Создать копию |  Добавить в группу |  Удалить

Рисунок 3 – Строка выбора операции, выполняемой с одной конечной точкой

Пользователь имеет возможность:

- в списках устройств, конечных точек, сетевых пользователей – создать копию сущности, добавить в группу сущностей, удалить выбранную сущность;
- в списках набора политик, профилей оборудования, профилей авторизации, набора команд – создать копию сущности, удалить выбранную сущность.
- в списках конечных точек – разрешить МАВ, запретить МАВ, создать копию сущности, добавить в группу сущностей, удалить выбранную сущность;
- в списках групп устройств, групп конечных точек, групп сетевых пользователей, групп набора политик, групп профилей оборудования, групп профилей авторизации, групп набора команд – создать копию группы сущностей, удалить выбранную группу сущностей.

После установки флага для двух и более строк или в поле в заголовке над таблицей отображается строка выбора операции, выполняемой с несколькими сущностями (рис. 4)

Выбрано: 3 |  Создать группу |  Добавить в группу |  Удалить

Рисунок 4 – Строка выбора операции, выполняемой с несколькими записями



Пользователь имеет возможность:

- в списках устройств, конечных точек, сетевых пользователей – создать группу сущностей, добавить выбранные сущности в группу или удалить выбранные сущности;
- в списках набора политик, профилей оборудования, профилей авторизации, набора команд – удалить выбранные сущности;

- в списках конечных точек – разрешить MAB, запретить MAB, создать группу сущностей, добавить выбранные сущности в группу или удалить выбранные сущности;
- в списках групп устройств, групп конечных точек, групп сетевых пользователей, групп набора политик, групп профилей оборудования, групп профилей авторизации, групп набора команд – удалить выбранные группы сущностей.


2.3.1 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 «».

2.3.2 Поиск данных в таблицах списков сущностей

Для поиска в списке сущностей требуемых записей необходимо ввести в поле поиска последовательность символов из искомой записи. После чего в списке отобразятся записи сущностей, в данных которых содержатся введенные символы.

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

2.3.3 Фильтрация данных в таблицах сущностей


Для фильтрации данных в списках сущностей необходимо нажать кнопку «Фильтр» ( **Фильтр**). Откроется окно фильтрации. Состав полей окна для разных подразделов раздела «Контроль доступа» отличается. На рис. 5 приведен пример окна фильтрации списка АСО.

Рисунок 5 – Окно фильтрации списка АСО

Необходимо заполнить параметры фильтрации и нажать кнопку «Применить».

После чего окно фильтрации закроется, на странице отобразятся записи с устройствами, соответствующими заданным параметрам фильтрации. Для отмены заданных правил фильтрации и отображения в списке всех записей, необходимо повторно нажать кнопку «Фильтр», затем кнопку «Сбросить».

2.3.4 Настройка состава 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. 6 приведено окно для списка конечных точек.

Рисунок 6 – Окно выбора колонок списка конечных точек

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.


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

установки/отмены флагов.


2.3.5 Копирование сущностей

Копирование сущности из списка может быть выполнено двумя способами:

1) Способ 1:

- нажать в строке копируемой записи 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».

Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности копируемой сущности.

При обнаружении незаполненных обязательных полей под полем появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Сохранить».

2.3.6 Редактирование сущностей

Редактирование сущностей выполняется следующим способом:

- 1) Пользователю необходимо в соответствующей вкладке кликнуть на название сущности.
- 2) Откроется страница редактирования сущности. Страница содержит внесенные ранее данные.
- 3) Пользователю необходимо внести требуемые изменения на странице редактирования и нажать кнопку «Сохранить».

Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности редактируемой сущности.

При обнаружении незаполненных обязательных полей под полем появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Сохранить».


2.3.7 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:

- нажать в строке удаляемой записи кнопку «Удалить» ();
- нажать в открывшемся окне подтверждения кнопку «ОК».


2) Способ 2:

- установить флаг в строке удаляемой записи;
- нажать в строке операций над списком сущностей (см. рис. 2) кнопку «Удалить» ( Удалить);
- нажать в открывшемся окне подтверждения кнопку «ОК».

В результате будет запущен процесс удаления сущности.

Для удаления нескольких сущностей из списка необходимо:

- 1) Установить флаг в соответствующих удаляемым записям полям. Для выбора всех записей на активной странице – установить флаг в заголовке таблицы. В верхней части таблицы отобразится строка выбора операций (см. рис. 4).





- Нажать в строке кнопку «Удалить» ().
- Нажать в открывшемся окне подтверждения кнопку «ОК». Будет запущен процесс удаления выбранных сущностей.

После успешного завершения процесса удаления:




- сущности удаляются из списка сущностей;
- в журнал событий ПК «Efros DO» в подразделе «Аудит» для каждой удаленной сущности вносится сообщение типа «Удаление».

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

Над списком АСО располагаются:

- поле поиска ( Введите запрос для поиска);
- кнопка «Фильтр» ( Фильтр) для фильтрации списка АСО;
- кнопка «Устройство» ( Устройство) позволяет добавить новое устройство (см. п. 2.4.1.1);
- 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.

2.4.1.1 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. Страница состоит из четырех вкладок:
- «Свойства» – вкладка активна по умолчанию;
 - «Группы».

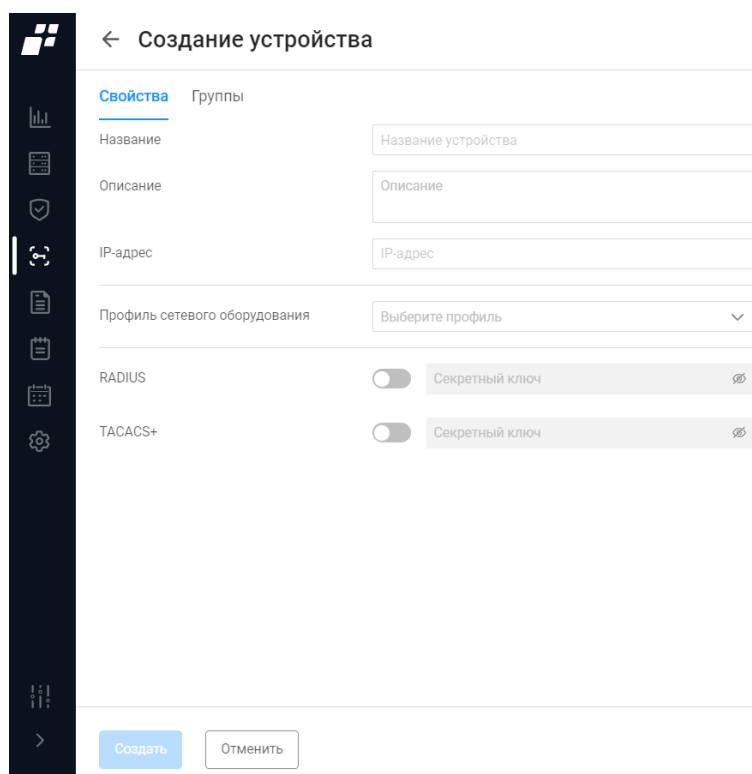


Рисунок 8 – Страница «Создание устройства»

Состав и описание элементов вкладки «Свойства» приведены в таблице 3.

Таблица 3 – Состав и описание элементов вкладки «Свойства»

Элемент	Описание
Поле «Название»	Текстовое поле для ввода имени устройства. Параметры ввода текста: от 1 до 250 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «-»
Поле «Описание»	Текстовое поле для ввода описания устройства. Параметры ввода текста: от 1 до 4000 любых символов
Поле «IP-адрес»	Текстовое поле для ввода IP-адреса устройства. 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 2.7)
Поле «Тип протокола»	Переключатели: — «RADIUS»; — «TACACS+». Активация переключателя означает, что устройство работает с использованием соответствующего протокола. Для активированного протокола необходимо ввести заданный на устройстве разделяемый ключ. При вводе символы ключа заменяются знаком «●». Для просмотра введенного значения необходимо нажать в поле ввода кнопку «Просмотр» (🔍)
Элементы управления	
Создать	При нажатии кнопки выполняется создание устройства
Отменить	При нажатии кнопки выполняется переход на страницу без сохранения внесенных данных

- 3) Заполнить поля вкладки соответствующими параметрами.
- 4) Перейти на вкладку «Группы» (рис. 9). Состав и описание элементов окна приведены в таблице 4.

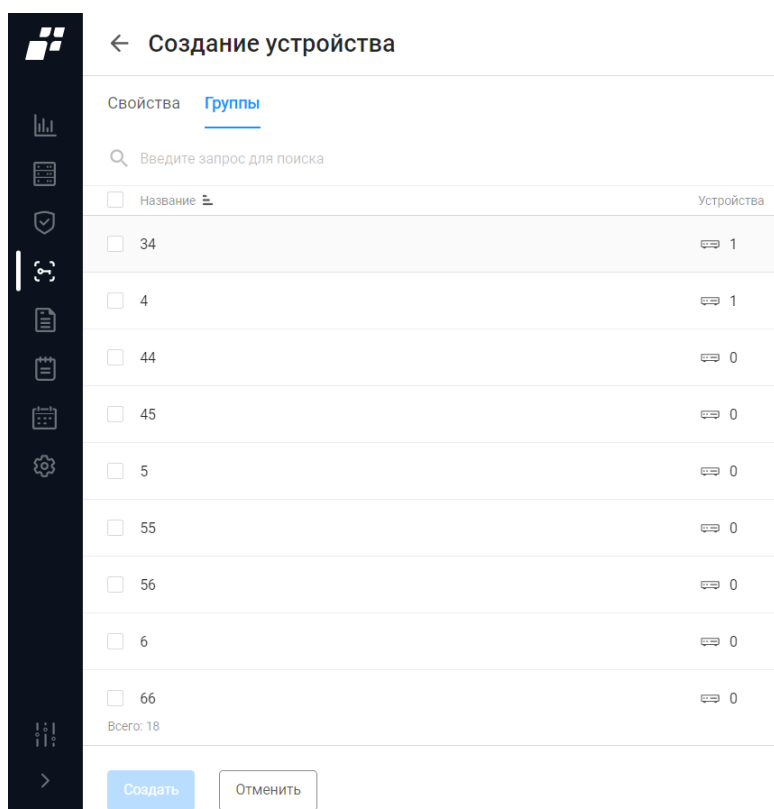


Рисунок 9 – Вкладка «Группы»

Таблица 4 – Состав и описание элементов вкладки «Группы»

Элемент	Описание
Поле для флага	Выбор определенной группы устройств
Поле «Название»	Содержит следующую информацию: — Название группы устройств; — Описание
Поле «Устройства»	Содержит информацию о количестве устройств в группе
Элементы управления	
Поле «Поиск»	Ввод 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

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

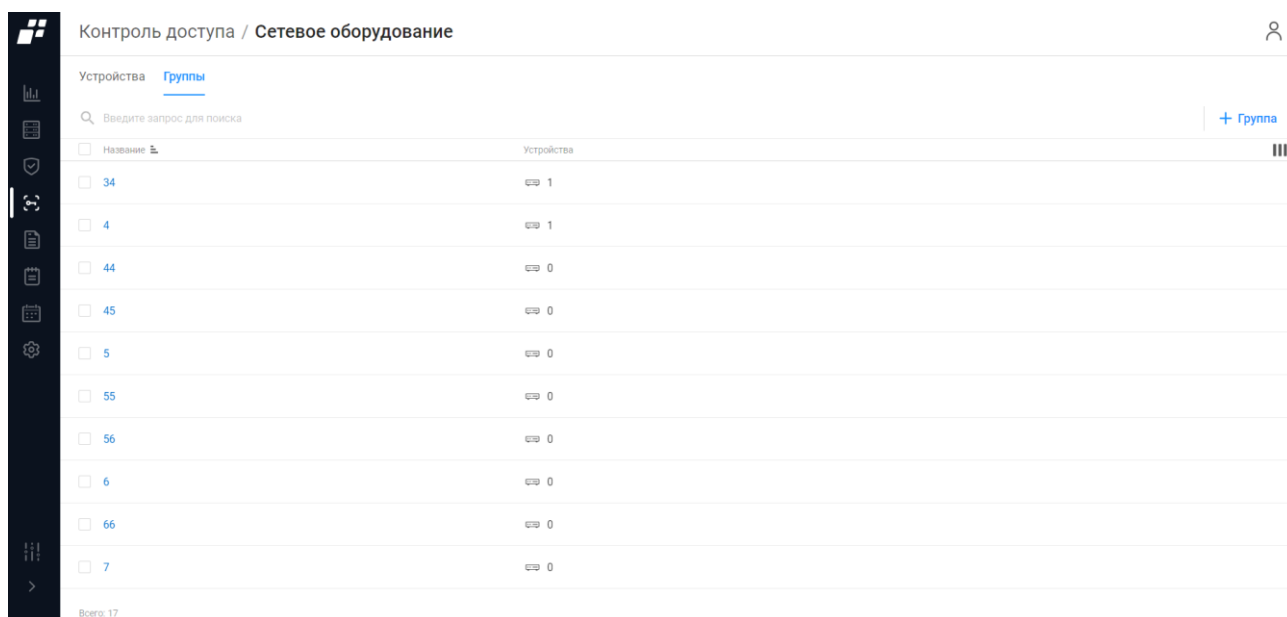
6) Нажать кнопку «Создать».

Автоматически запускается процесс проверки заполнения всех обязательных полей и уникальности добавляемого АСО по названию и IP-адресу.

При обнаружении незаполненных полей под полем появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить поля страницы и повторно нажать кнопку «Создать».

2.4.2 Вкладка «Группы»

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



Контроль доступа / Сетевое оборудование		👤
Устройства <u>Группы</u>		
🔍 Введите запрос для поиска		+ Группа
<input type="checkbox"/> Название	Устройства	☰
<input type="checkbox"/> 34	🔌 1	
<input type="checkbox"/> 4	🔌 1	
<input type="checkbox"/> 44	🔌 0	
<input type="checkbox"/> 45	🔌 0	
<input type="checkbox"/> 5	🔌 0	
<input type="checkbox"/> 55	🔌 0	
<input type="checkbox"/> 56	🔌 0	
<input type="checkbox"/> 6	🔌 0	
<input type="checkbox"/> 66	🔌 0	
<input type="checkbox"/> 7	🔌 0	
Всего: 17		

Рисунок 10 – Вкладка «Группы»

Для каждой записи списка отображаются следующие данные:

- поле для флага;
- название – является ссылкой, при переходе открывается окно редактирования группы (более подробно см. п. 2.3.6);
- 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.

2.4.2.1 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). Состав и описание элементов страницы приведены в таблице 5.

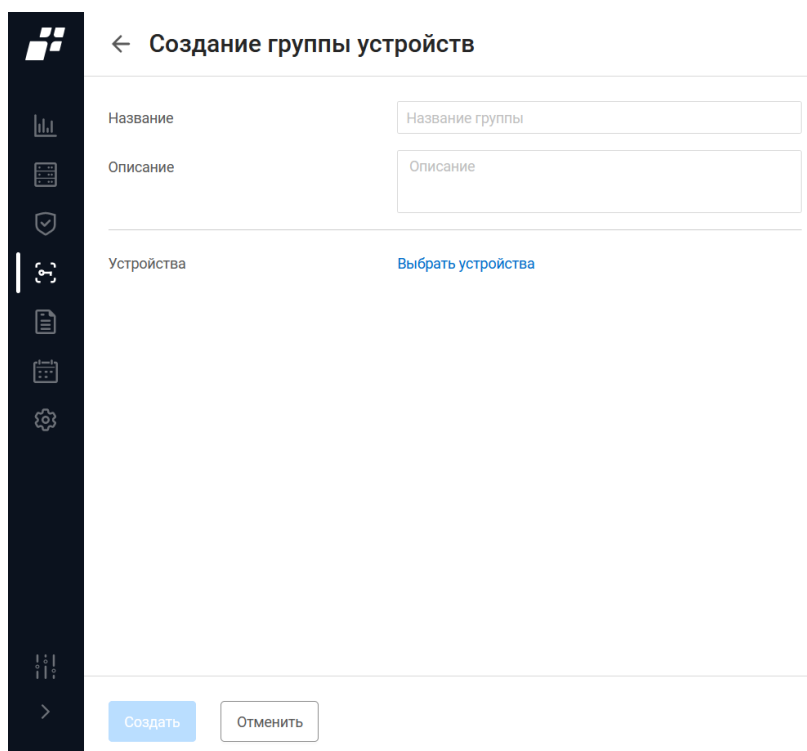


Рисунок 11 – Страница «Создание группы устройств»

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

Элемент	Описание
Поле «Название»	Текстовое поле для ввода названия группы устройств. Параметры ввода текста: от 1 до 250 символов. Допустимые символы: буквы латинского и кириллического алфавитов, цифры, знак «пробел», «_», «-»
Поле «Описание»	Текстовое поле для ввода описания группы устройств. 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

Элемент	Описание
Отменить	При нажатии кнопки выполняется переход без сохранения внесенных данных

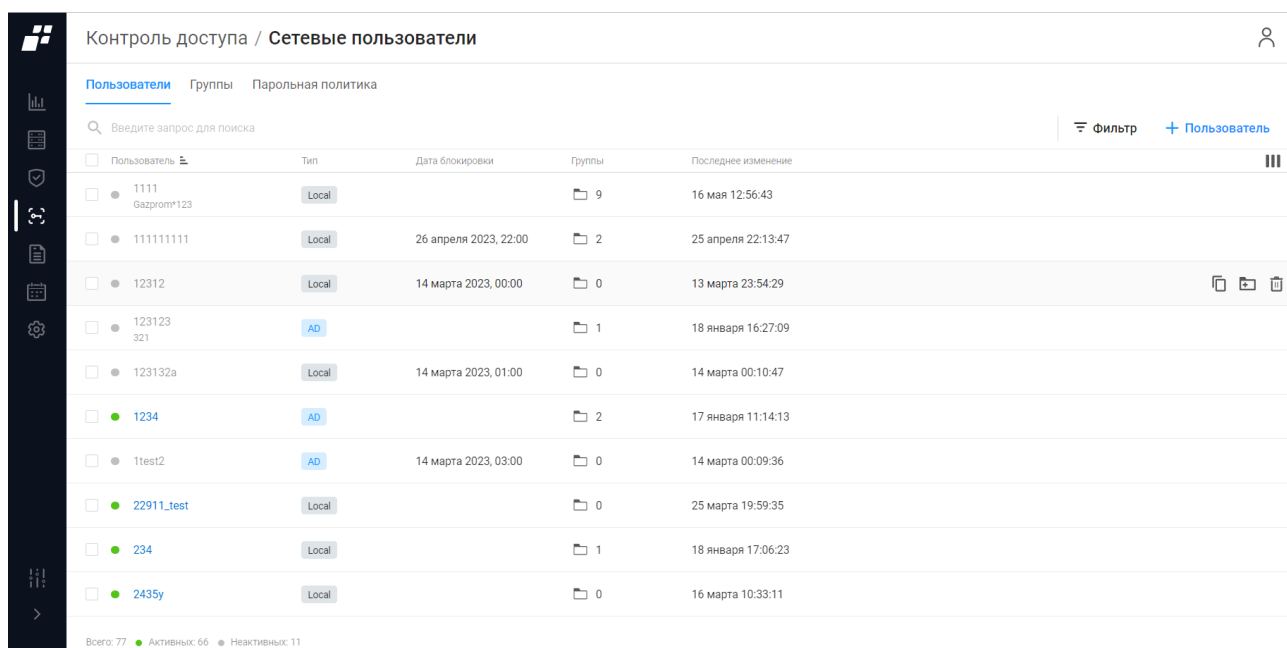
Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности добавляемой группы АСО по названию.




При обнаружении незаполненных полей под полем появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Создать».

2.5 Сетевые пользователи

Данный подраздел 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 «Парольная политика». Сетевые пользователи добавляются, редактируются или удаляются в списке вручную пользователем ПК «Efros DO» с соответствующей привилегией. По умолчанию активной является вкладка «Пользователи» (рис. 12).




<input type="checkbox"/>	Пользователь	Тип	Дата блокировки	Группы	Последнее изменение	
<input type="checkbox"/>	1111 Gazprom123	Local		9	16 мая 12:56:43	
<input type="checkbox"/>	1111111111	Local	26 апреля 2023, 22:00	2	25 апреля 22:13:47	
<input type="checkbox"/>	12312	Local	14 марта 2023, 00:00	0	13 марта 23:54:29	  
<input type="checkbox"/>	123123 321	AD		1	18 января 16:27:09	
<input type="checkbox"/>	123132a	Local	14 марта 2023, 01:00	0	14 марта 00:10:47	
<input type="checkbox"/>	1234	AD		2	17 января 11:14:13	
<input type="checkbox"/>	1test2	AD	14 марта 2023, 03:00	0	14 марта 00:09:36	
<input type="checkbox"/>	22911_test	Local		0	25 марта 19:59:35	
<input type="checkbox"/>	234	Local		1	18 января 17:06:23	
<input type="checkbox"/>	2435y	Local		0	16 марта 10:33:11	


Всего: 77 ● Активных: 66 ● Неактивных: 11

Рисунок 12 – Вкладка «Пользователи»

2.5.1 Вкладка «Пользователи»





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

- поле для флага – выбор сетевого пользователя, чтобы создать копию, добавить в группу или удалить;
- статус:
 - «зеленый круг» – пользователь активен;
 - «серый круг» – пользователь неактивен.
- логин – является ссылкой, при переходе по которой открывается окно для редактирования данных сетевого пользователя (более подробно см. п.п. 2.5.1.1);
- тип – содержит информацию об учетной записи сетевого пользователя:
 - «» – учетная запись сетевого пользователя создана локально в базе данных ПК «Efros DO»;




- «  » – используется доменная учетная запись².

- дата блокировки – дата окончания действия учетной записи сетевого пользователя;
- 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 ( Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Фильтр» ( Фильтр) для фильтрации списка пользователей;
- кнопка «Пользователь» ( Пользователь) позволяет добавить нового сетевого пользователя (см. п.п. 2.5.1.1);
- кнопка «Колонки» () для изменения отображения колонок на странице.


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

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

Аналогичные кнопки появляются в правой части экрана в строке с выбранным сетевым пользователем.

2.5.1.1 Добавление сетевого пользователя

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

- 1) Нажать кнопку «Пользователь» ( Пользователь).
- 2) Откроется страница «Создание сетевого пользователя» (рис. 13). Состав и описание элементов страницы приведены в таблице 6.

² Для доменных пользователей кнопка отображает название домена

← Создание сетевого пользователя

Статус ☒

Тип ☒ Пользователь ☐ Пользователь LDAP ☐ Группа LDAP

Пользователь

Описание

Пароль



Период действия учетной записи ☒ Бессрочно ☐ Задать

Привилегированный режим

Группы пользователей [Выбрать группы](#)

Рисунок 13 – Страница «Создание сетевого пользователя»

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

Элемент	Описание
Поле «Статус»	Переключатель: — «Активен» () – сетевому пользователю разрешен доступ к устройствам; — «Неактивен» () – сетевому пользователю закрыт доступ к устройствам. По умолчанию переключатель установлен в положение «Активен»
Поле «Тип»	Переключатель: — «Пользователь»; — «Пользователь LDAP»; — «Группа LDAP». От выбранного в поле значения зависит состав полей страницы создания сетевого пользователя
Группа полей при выборе типа «Пользователь»	
Поле «Пользователь»	Текстовое поле для ввода имени (логина) сетевого пользователя. Параметры ввода текста: от 1 до 50 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «-»

Элемент	Описание
Поле «Описание»	Текстовое поле для ввода описания сетевого пользователя. Параметры ввода текста: от 1 до 250 любых символов
Поле «Пароль»	Текстовое поле для ввода пароля сетевого пользователя. Только для локальных сетевых пользователей. Параметры для ввода текста: см. п. 2.5.3
Поле «Период действия учетной записи»	Переключатель: — «Бессрочно» – учетная запись сетевого пользователя действует на устройстве без ограничений; — «Задать» – учетная запись сетевого пользователя действует на устройстве определенный период времени. При выборе «Задать» появляется поле «Дата блокировки»
Поле «Дата блокировки»	Поле для ввода даты блокировки учетной записи сетевого пользователя
Поле «Привилегированный режим»	Поле с раскрывающимся списком типов привилегированного режима работы с АСО. Содержит значения: — «Не задано» – привилегированный режим не задан; — «Установить пароль» – привилегированный режим доступен по заданному паролю для привилегированного доступа (см. ниже поле «Пароль»). Поле «Пароль» отображается при выборе значения «Установить пароль»; — «Использовать пароль пользователя» – привилегированный режим доступен по паролю пользователя от учетной записи пользователя; — «Разрешить без пароля» – привилегированный режим доступен без пароля; — «Запретить» – установка принудительного запрета на использование привилегированного режима пользователем
Поле «Пароль»	Поле отображается только после выбора в поле «Привилегированный режим» значения «Установить пароль». Предназначено для ввода пароля авторизации сетевого пользователя в привилегированном режиме
Поле «Группы пользователей»	По умолчанию поле содержит кнопку «Выбрать группы» для перехода в окно выбора одной или нескольких групп. Для выбора группы необходимо установить флаг в соответствующей строке и нажать кнопку «Выбрать»
Группа полей при выборе типа «Пользователь LDAP»	

Элемент	Описание
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 «Период действия учетной записи»	Переключатель: <ul style="list-style-type: none"> — «Бессрочно» – учетная запись пользователя LDAP действует на устройстве без ограничений; — «Задать» – учетная запись пользователя LDAP действует на устройстве определенный период времени. При выборе «Задать» появляется поле «Дата блокировки»
Поле «Дата блокировки»	Поле для ввода даты блокировки учетной записи пользователя LDAP
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 «Период действия учетной записи»	Переключатель: <ul style="list-style-type: none"> — «Бессрочно» – учетная запись пользователя из группы LDAP действует на устройстве без ограничений; — «Задать» – учетная запись пользователя из группы LDAP действует на устройстве определенный период времени. При выборе «Задать» появляется поле «Дата блокировки»
Поле «Дата блокировки»	Поле для ввода даты блокировки учетной записи сетевого пользователя
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) Заполнить форму необходимыми параметрами.

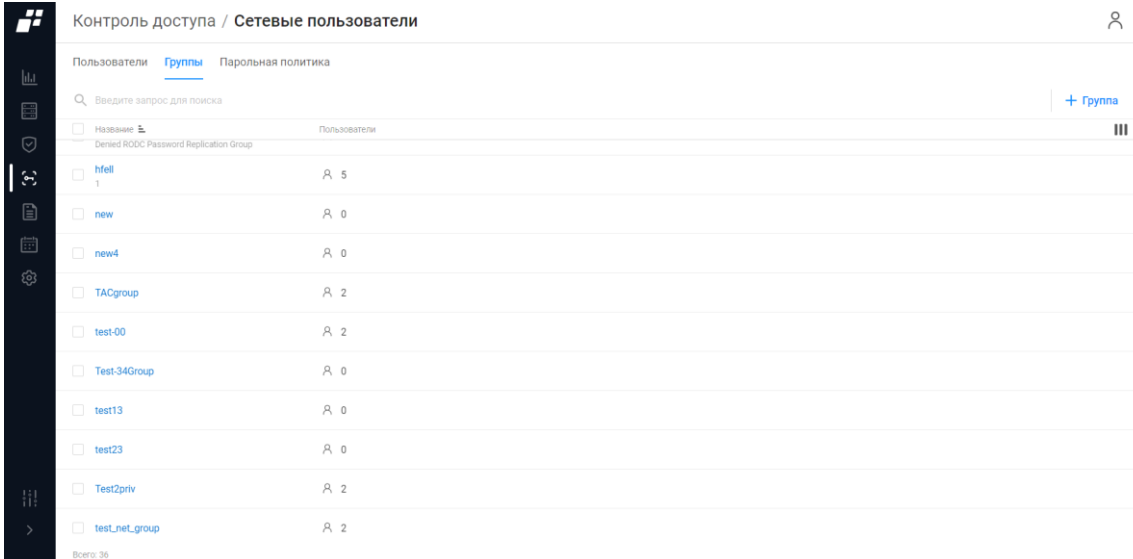
4) Нажать кнопку «Создать».

Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности добавляемого сетевого пользователя по имени.

При обнаружении незаполненных обязательных полей под полем появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Создать».

2.5.2 Вкладка «Группы»

На странице список групп сетевых пользователей реализован в виде таблицы (рис. 14).






Контроль доступа / Сетевые пользователи		
Пользователи Группы Парольная политика		
Введите запрос для поиска		
<input type="checkbox"/>	Message Denied RODC Password Replication Group	Пользователи
<input type="checkbox"/>	hfe1	5
<input type="checkbox"/>	new	0
<input type="checkbox"/>	new4	0
<input type="checkbox"/>	TACgroup	2
<input type="checkbox"/>	test-00	2
<input type="checkbox"/>	Test-34Group	0
<input type="checkbox"/>	test13	0
<input type="checkbox"/>	test23	0
<input type="checkbox"/>	Test2priv	2
<input type="checkbox"/>	test_net_group	2

Рисунок 14 – 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) для поиска искомой записи в списке;
- кнопка «Группа» () позволяет добавить новую группу;
- кнопка «Колонки» () для изменения отображения колонок на странице.

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.

! Группы, начинающиеся с «(GuestPortal)», создаются и удаляются автоматически и необходимы для корректной работы функции «Гостевой портал» (более подробно см. «Руководство пользователя. Часть 1. Администрирование»).

2.5.2.1 Добавление группы сетевых пользователей

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

- 1) Нажать кнопку «Группа» ([+ Группа](#)). Откроется страница «Создание группы сетевых пользователей», приведенная на рис. 15. Состав и описание элементов страницы приведены в таблице 7.

← Создание группы сетевых пользователей

Название	<input type="text" value="Название группы"/>
Описание	<input type="text" value="Описание"/>
Пользователи	Выбрать пользователей

Рисунок 15 – Страница «Создание группы сетевых пользователей»

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

Элемент	Описание
Поле «Название»	Текстовое поле для ввода названия группы пользователей. Параметры ввода текста: от 1 до 50 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «-»
Поле «Описание»	Текстовое поле для ввода описания группы пользователей. 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

Элемент	Описание
	пользователей. Для выбора сетевого пользователя необходимо установить флаг в соответствующих строках 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

Заполнить форму необходимыми параметрами.

Нажать кнопку «Создать».




Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности добавляемой группы сетевых пользователей по названию.






При обнаружении незаполненных обязательных полей под полем появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Создать».


2.5.3 Вкладка «Парольная политика»

Данная вкладка содержит список параметров парольной политики для сетевых пользователей (рис. 16). Состав и описание элементов вкладки приведены в таблице 8.

Рисунок 16 – Вкладка «Парольная политика»

Элемент	Описание
Группа полей «Сложность пароля»	
Поле «Минимальная длина пароля»	Числовое поле для ввода минимально допустимой длины пароля. Допустимые значения: от 8 до 30. Значение по умолчанию – 8
Поле «Цифры»	Переключатель: <ul style="list-style-type: none"> — «Да» () – пароль должен содержать хотя бы одну цифру; — «Нет» () – наличие в пароле цифр необязательно. По умолчанию переключатель установлен в положение «Да»
Поле «Буквы верхнего регистра»	Переключатель: <ul style="list-style-type: none"> — «Да» () – пароль должен содержать хотя бы одну

Элемент	Описание
	букву верхнего регистра латинского алфавита; — «Нет» () – наличие в пароле букв верхнего регистра необязательно. По умолчанию переключатель установлен в положение «Да»
Поле «Буквы нижнего регистра»	Переключатель: — «Да» () – пароль должен содержать хотя бы одну букву нижнего регистра латинского алфавита; — «Нет» () – наличие в пароле букв нижнего регистра необязательно. По умолчанию переключатель установлен в положение «Да»
Поле «Не буквенно–цифровые символы»	Переключатель: — «Да» () – пароль должен содержать хотя бы один не буквенно–цифровой символ (@#\$%&); — «Нет» () – наличие в пароле не буквенно–цифровых символов необязательно. По умолчанию переключатель установлен в положение «Нет»
Группа полей «Проверка по базе популярных паролей»	
Поле «База паролей»	Содержит ссылку. При переходе открывается окно со списком самых популярных паролей
Группа полей «Период действия пароля»	
Поле «Минимально дней»	Числовое поле для ввода времени (в днях) действия первого пароля пользователя (используемого им при первой авторизации в ПК «Efros DO»). После истечения указанного времени пароль необходимо изменить, пользователю при попытке запуска веб–приложения будет выведено соответствующее сообщение. Допустимые значения: от 0 до 60. Значение по умолчанию: 0
Поле «Максимально дней»	Числовое поле для ввода времени (в днях) действия пароля пользователя (второго и последующих). После истечения указанного времени пароль необходимо изменить, пользователю при попытке запуска веб–приложения будет выведено соответствующее сообщение. Допустимые значения: от 1 до 60. Значение по умолчанию: 60

Элемент	Описание
Группа полей «Блокировка пользователя, при неактивности»	
Поле «Количество дней неактивности»	Числовое поле, указывающее количество дней неактивности пользователя, по истечении которых производится блокировка учетной записи пользователя. Значение по умолчанию: 45. Недоступно для корректировки
Группа полей «Блокировка пользователя, при неверном вводе пароля»	
Поле «Неверных вводов пароля подряд»	Числовое поле для ввода количества неуспешных попыток ввода пароля. После превышения указанного количества неуспешных попыток авторизации пользователь блокируется на время, указанное в параметре «Временные ограничения. Время блокировки при неверном вводе пароля» (см. ниже в таблице). Допустимые значения: от 3 до 8. Значение по умолчанию: 4
Поле «Минут блокировки»	Числовое поле для ввода интервала времени (в минутах), на который блокируется учетная запись пользователя после превышения разрешенного количества неуспешных попыток авторизации. Допустимые значения: от 3 до 30 Значение по умолчанию: 26
Элементы управления	
Сохранить	При нажатии кнопки введенные изменения применяются
Отменить	При нажатии кнопки настройки остаются без применения изменений
При необходимости поля можно отключить, передвинув переключатель в положение «  » – поле будет недоступно для внесения изменений	

2.6 Наборы политик

Данный подраздел позволяет управлять различными сценариями доступа к сети и администрированию сетевого оборудования, с возможностью формирования списка разрешенных и запрещенных для выполнения команд с заданными аргументами (рис. 17). В одном наборе можно логически группировать правила аутентификации и авторизации.

При создании наборов политик настраиваются правила для выбора служб доступа к сети на уровне набора атрибутов (см. подраздел 2.12), источников идентификации на уровне политики аутентификации. Поддерживается определение условий, используя RADIUS-словари различных производителей.

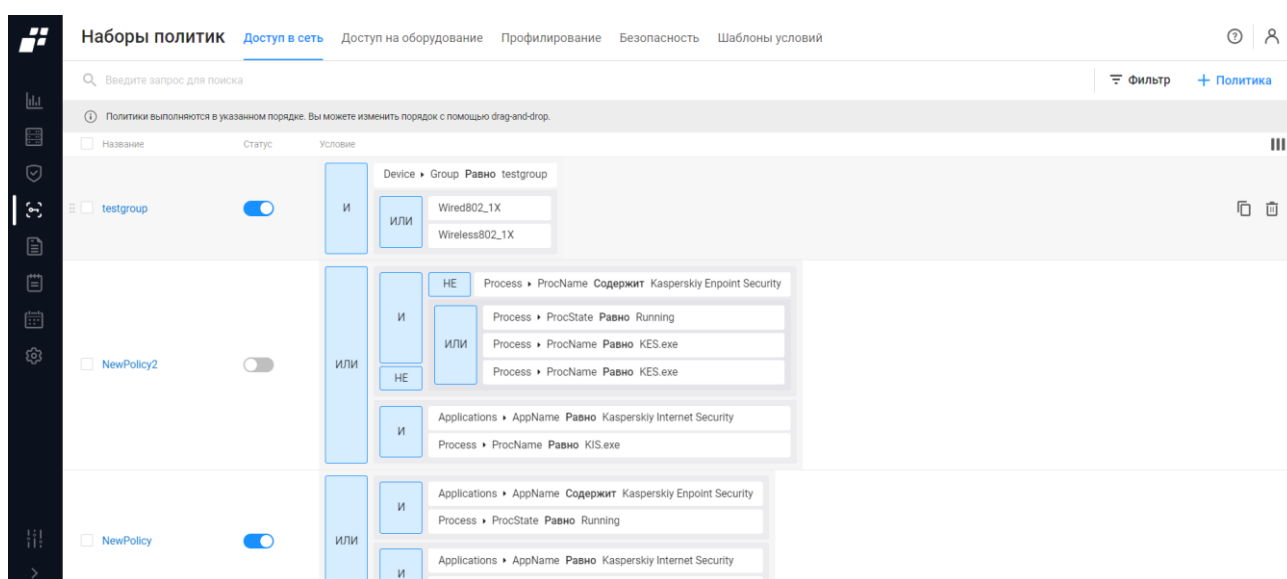


Рисунок 17 – Подраздел «Наборы политик»

i После установки ПК «Efros DO» список наборов политик пуст, на странице отображается сообщение «Список пуст. Вы можете создать политику при помощи кнопки ниже» и кнопка «Создать политику» для перехода на страницу создания нового набора политик.

Страница содержит вкладки:

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





2.6.1 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. 17). 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) для поиска искомой записи в списке;
- кнопка «Политика» ( Политика) для добавления новой политики;
- кнопка «Фильтр» ( Фильтр) для фильтрации списка политик;
- кнопка «Колонки» ().

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


- кнопка «Создать копию» ();
- кнопка «Удалить» () для удаления выбранной политики.

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, указанными 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.).

2.6.1.1 Создание политик «Доступ в сеть»

Для добавления в список новой политики необходимо:

- 1) Нажать над списком политик доступа кнопку «Политика» ( Политика).
- 2) Откроется страница «Создание политики (Доступ в сеть)», приведенная на рис. 18. Состав и описание элементов страницы приведены в таблице 9.

← Создание политики Доступ в сеть

Настройки Правила аутентификации - 1 Правила авторизации - 1

Статус ☒

Название

Описание

Условия срабатывания политики

☒ И ☐ ИЛИ ☐ НЕ Добавить

Выберите атрибут Введите значение ⋮ 📄 🗑️

Перенесите сюда условие

Создать Отменить

Введите запрос для поиска Все шаблоны условий

- 111111113234e34324355555555555553455435678...
- 123
- 20230505
- aaa2
- aaa21
- aaa212
- DeviceAdministration
DeviceAdministration
- dsds
dsds
- IF
IF
- Inner_IF
- Irina

Всего: 26

Рисунок 18 – Страница «Создание политики (Доступ в сеть)»

Таблица 9 – Состав и описание элементов вкладки «Настройки»

Элемент	Описание
Поле «Статус»	Переключатель: — «Активен»; — «Неактивен»
Поле «Название»	Текстовое поле для ввода названия политики. Параметры ввода текста: от 1 до 50 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «-»
Поле «Описание»	Текстовое поле для ввода описания политики. Параметры ввода текста: от 1 до 250 любых символов
Основное правило	
Формирование основного правила происходит на основе созданных правил аутентификации и авторизации на вкладках «Правила аутентификации» и «Правила авторизации» или стандартных шаблонов условий. 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

Элемент	Описание
	данных

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

Перейти на вкладку «Правила аутентификации» для определения правил аутентификации в рамках данного набора политик (рис. 19). 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. 2.6.1.2.

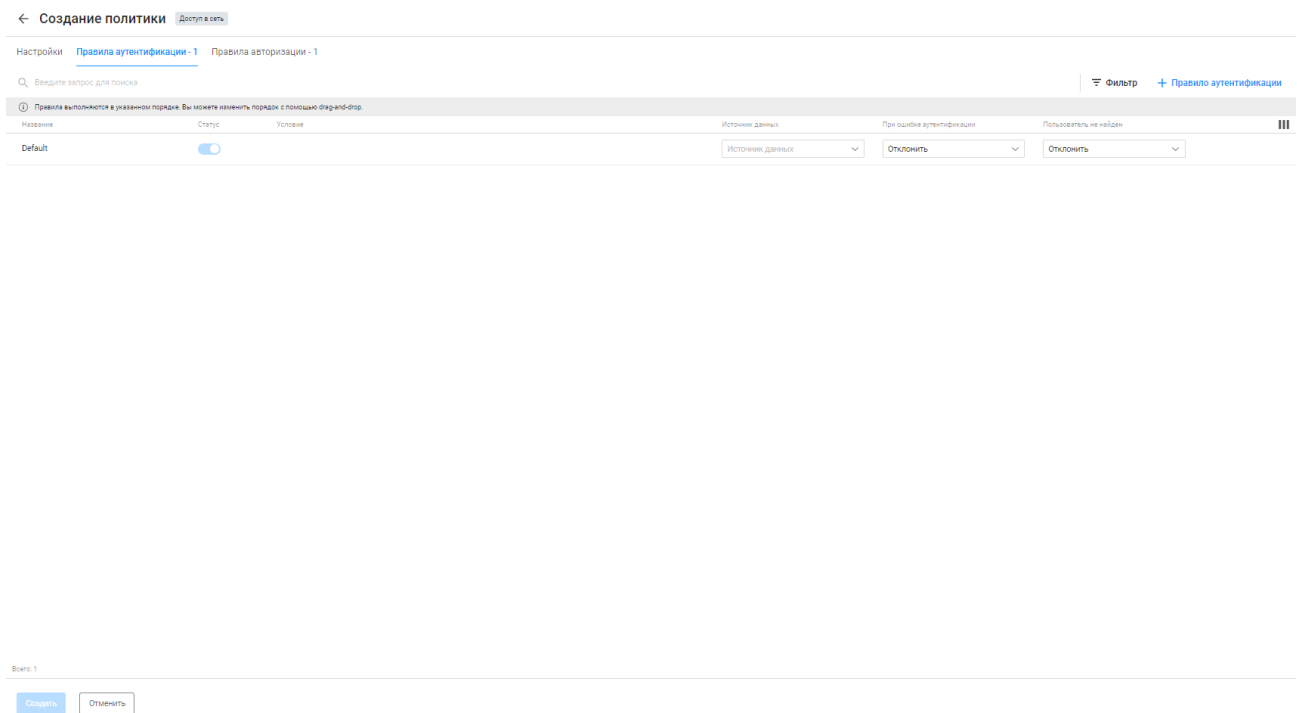


Рисунок 19 – Вкладка «Правила аутентификации»

Перейти на вкладку «Правила авторизации» для определения правил авторизации в рамках данного набора политик (рис. 20). 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. 2.6.1.3.

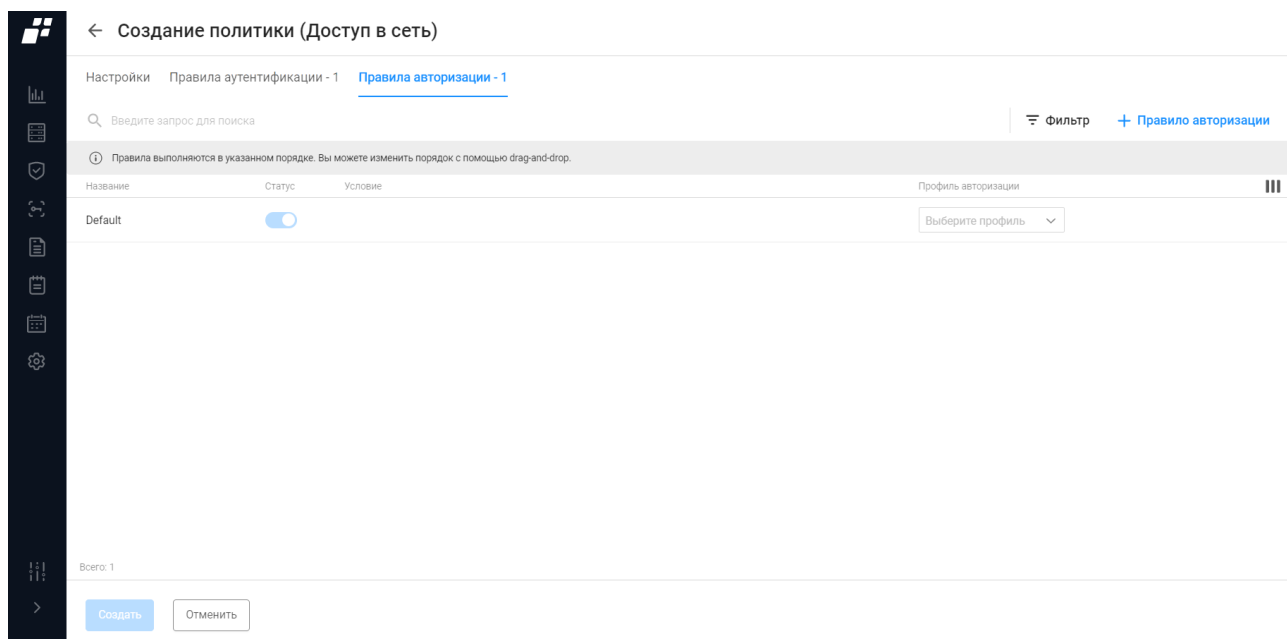


Рисунок 20 – Вкладка «Правила авторизации»

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

Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности добавляемого набора политик. При обнаружении незаполненных обязательных полей под полем появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Создать».

2.6.1.2 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 сверху 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. 21. Состав и описание элементов страницы приведены в таблице 10.

Рисунок 21 – Страница «Создание правила аутентификации (Доступ в сеть)»

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

Элемент	Описание
Поле «Статус»	Переключатель: «Включен», «Отключен» (статус может быть изменен как в окне редактирования параметров, так и непосредственно на вкладке «Правила аутентификации» у созданного правила).  В случае выбора статуса «Отключен», проверка на совпадение с условиями, заданными в данном правиле,

Элемент	Описание
	осуществляться не будет
Поле «Название»	Текстовое поле для ввода названия правила аутентификации. Параметры ввода текста: от 1 до 50 символов. 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 «Пользователь не найден»	Переключатель: — «Отклонить»; — «Продолжить»; — «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

Заполнить поле страницы соответствующими значениями.

Сформировать условия, определяющие правило аутентификации, или воспользоваться заранее сформированными шаблонами условий.

После настройки правила аутентификации нажать в окне добавления кнопку «Создать».

Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности добавляемого правила аутентификации.

При обнаружении незаполненных обязательных полей под полем появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Создать».

2.6.1.3 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 сверху 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)».

Нажать кнопку «Правило авторизации» ([+ Правило авторизации](#)).

Откроется страница «Создание правила авторизации (Доступ в сеть)», приведенное на рис. 22. Состав и описание элементов страницы приведены в таблице Таблица 11.

← Создание правила авторизации Доступ в сеть

Статус ☒

Название

Действия при выполнении условий

Профиль авторизации

Условия срабатывания правила

☒ И ☐ ИЛИ ☐ НЕ Добавить

Перенесите сюда условие

Введите запрос для поиска Системные

- DeviceAdministration
- RemoteAccessVPN
- Wired802_1X
- WiredMab
- WiredWebAuth
- Wireless802_1X
- WirelessMab
- WirelessWebAuth

Всего: 8

Создать Отменить

Рисунок 22 – Страница «Создание правила авторизации» (Доступ в сеть)

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

Элемент	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. Параметры ввода текста: от 1 до 50 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «-»
Группа поле «Действия при выполнении условий»	
Профиль авторизации	Раскрывающийся список с профилями авторизации, созданных в разделе 2.8
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

Заполнить поле страницы соответствующими значениями.

Сформировать условия, определяющие правило авторизации, или воспользоваться заранее сформированными шаблонами условий.

После настройки правила аутентификации нажать в окне добавления кнопку «Создать».

Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности добавляемого правила авторизации по названию.

При обнаружении незаполненных обязательных полей под полем появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Создать».

2.6.2 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. 23).

Рисунок 23 – Вкладка «Доступ на оборудование»

Для каждой записи списка отображаются следующие данные:

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

Над списком располагаются:

- поле поиска (Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Политики» (Политика) для добавления новой политики;
- кнопка «Фильтр» (Фильтр) для фильтрации списка политик;
- кнопка «Колонки» () для изменения отображения колонок на странице.

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, указанными в правилах

аутентификации, проверка разрешенных протоколов, а также на наличие учетных данных субъекта, запрашивающего доступ к сети, в выбранном источнике данных (локальные сетевые пользователи, пользователи подключенного LDAP и т.п.).

2.6.2.1 Создание политик «Доступ на оборудование»

Для добавления в список новой политики необходимо:

- 1) Нажать над списком политик доступа кнопку «Политика» ([+ Политика](#)).
- 2) Откроется страница «Создание политики (Доступ на оборудование)», приведенная на рис. 24. Состав и описание элементов вкладки приведены в таблице 12.

← Создание политики Доступ на оборудование

Настройки Правила аутентификации - 1 Правила авторизации - 1

Статус ☒

Название

Описание

Список разрешенных протоколов

Условия срабатывания политики

☒ И ☐ ИЛИ ☐ НЕ Добавить

Выберите атрибут Введите значение ⋮ 📄 🗑️

Перенесите сюда условие

Ничего не найдено
Измените запрос и повторите поиск

Всего: 0

Создать Отменить

Рисунок 24 – Страница «Создание политики (Доступ на оборудование)»

Таблица 12 – Состав и описание элементов вкладки «Настройки»

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

Элемент	Описание
разрешенных протоколов»	использоваться во время проверки аутентификации (см. подраздел 2.11)
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. 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.

Перейти на вкладку «Правила аутентификации» для определения правил аутентификации в рамках данного набора политик (рис. 25). 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. 2.6.2.2.

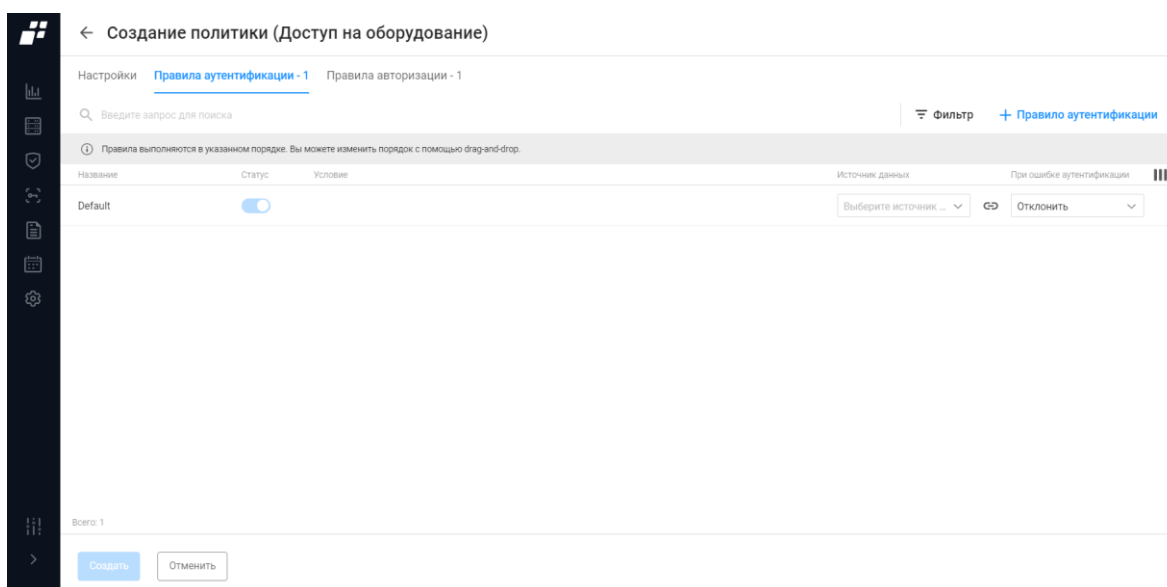


Рисунок 25 – Вкладка «Правила аутентификации»

Перейти на вкладку «Правила авторизации» для определения правил авторизации в рамках данного набора политик (рис. 26). 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. 2.6.2.3.

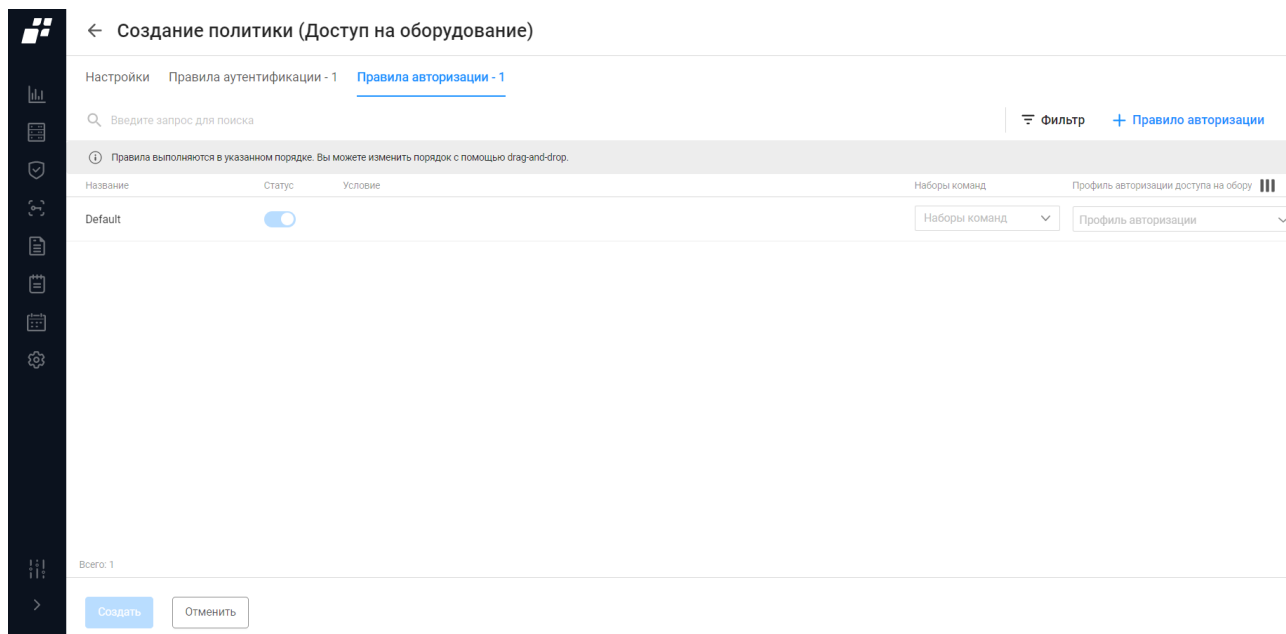


Рисунок 26 – Вкладка «Правила авторизации»

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

Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности добавляемого набора политик. При обнаружении незаполненных обязательных полей под полем появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Создать».

2.6.2.2 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. 27. Состав и описание элементов страницы приведены в таблице 13.

← Создание правила аутентификации Доступ на оборудование

Статус ☒

Название

Проверка учетных данных

Источник данных

При ошибке аутентификации

Условия срабатывания правила

И ИЛИ НЕ

НЕ Выберите атрибут

Перенесите сюда условие


Введите запрос для поиска Все шаблоны условий

new020202
new_1
new_3
test123

Всего: 4

Рисунок 27 – Страница «Создание правила аутентификации
(Доступ на оборудование)»

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

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

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

Заполнить поле страницы соответствующими значениями.

Сформировать условия, определяющие правило аутентификации, или воспользоваться заранее сформированными шаблонами условий.

После настройки правила аутентификации нажать в окне добавления кнопку «Создать».

Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности добавляемого правила аутентификации.

При обнаружении незаполненных обязательных полей под полем появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Создать».

2.6.2.3 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. 28. Состав и описание элементов страницы приведены в таблице 14.

← Создание правила авторизации Доступ на оборудование

Статус ☒

Название

Действия при выполнении условий

Назначить профиль авторизации ⓘ

Применить набор команд

Условия срабатывания правила

☒ И ☐ ИЛИ ☐ НЕ Добавить ▾

⋮ 📄 🗑️

Перенесите сюда условие

Введите запрос для поиска Системные ▾


Ничего не найдено
Измените запрос и повторите поиск

Всего: 0

Создать Отменить

Рисунок 28 – Страница «Создание правила авторизации (Доступ на оборудование)»

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

Элемент	Описание
Поле «Статус»	Переключатель: «Включен», «Отключен» (статус может быть изменен как в окне редактирования параметров, так и непосредственно на вкладке «Правила авторизации» у созданного правила).  В случае выбора статуса «Отключен», проверка на совпадение с условиями, заданными в данном правиле, осуществляться не будет
Поле «Название»	Текстовое поле для ввода названия политики. Параметры ввода текста: от 1 до 50 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «-»
Группа полей «Действия при выполнении условий»	
Поле «Назначить профиль авторизации»	Раскрывающийся список с профилями авторизации, созданных в разделе 2.10
Поле «Применить набор команд»	Раскрывающийся список наборами команд, созданных в разделе 2.8
Условия срабатывания политики	
Формирование основного правила происходит на основе выбранного шаблона	

Элемент	Описание
	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

- 4) Заполнить поле страницы соответствующими значениями.
- 5) Сформировать условия, определяющие правило авторизации, или воспользоваться заранее сформированными шаблонами условий.
- 6) Нажать кнопку «Создать».

Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности добавляемого правила авторизации по названию.

При обнаружении незаполненных обязательных полей под полем появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Создать».

2.6.3 Вкладка «Профилирование»

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

После классификации конечные точки проходят авторизацию в сети и им может быть предоставлен доступ на основе их профиля – набора политик доступа.

На странице список политик реализован в виде таблицы (рис. 29).

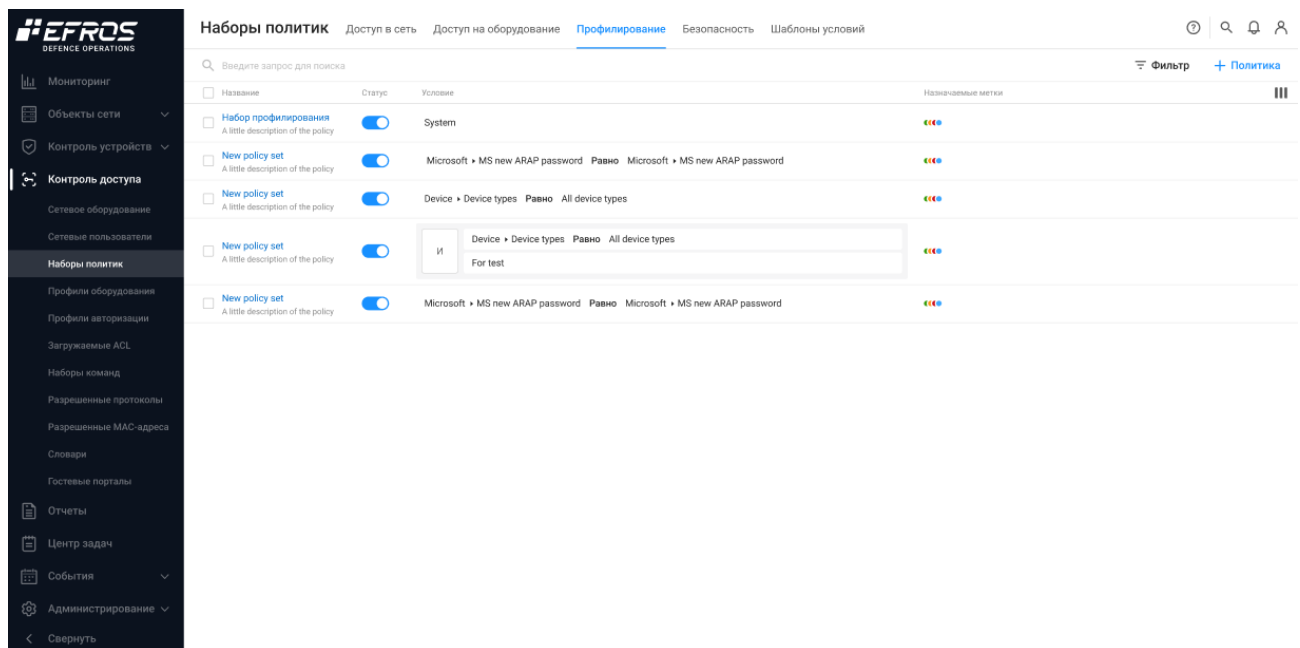


Рисунок 29 – Страница вкладки «Профилирование»

Для каждой записи списка отображаются следующие данные:

- поле для флага;
- название политики профилирования;
- статус – переключатель режима «Включен» / «Отключен»;
- условие – шаблон или набор шаблонов условий, входящих в политику профилирования;
- назначаемые метки.

Над списком располагаются:

- поле поиска (Введите запрос для поиска) для поиска искомой записи;
- кнопка «Политика профилирования» (Политика профилирования) для добавления новой политики;
- кнопка «Фильтр» (Фильтр) для фильтрации списка политик;
- кнопка «Колонки» () для изменения отображения колонок на странице.

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

- кнопка «Создать копию» (Создать копию) позволяет создать копию политики;
- кнопка «Удалить» (Удалить) позволяет удалить выбранную политику.

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

2.6.3.1 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. 30. Состав и описание элементов вкладки приведены в таблице 15.

Рисунок 30 – Страница «Создание политики профилирования»

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

Элемент	Описание
Поле «Статус»	Переключатель: — «Включен»; — «Отключен»
Поле «Название»	Текстовое поле для ввода названия политики. Параметры ввода текста: от 1 до 50 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «-»
Поле «Описание»	Текстовое поле для ввода описания политики. 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: — «Включен»; — «Отключен»
Условия профилирования	
Формирование основного правила происходит на основе выбранного шаблона	

Элемент	Описание
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.

Нажать кнопку «Создать».

Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности добавляемой политики профилирования. При обнаружении незаполненных обязательных полей под полем появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Создать».

2.6.4 Вкладка «Безопасность»

Вкладка «Безопасность» содержит список политик безопасности, которым должно соответствовать устройство, чтобы считаться надежным и безопасным для получения доступа к сетевым ресурсам организации. Политика безопасности может быть:

- базовой, которая используется для проверки устройства при запросе доступа в сеть;
- применимой к определенной ОС.

На странице список политик реализован в виде таблицы (рис. 31).

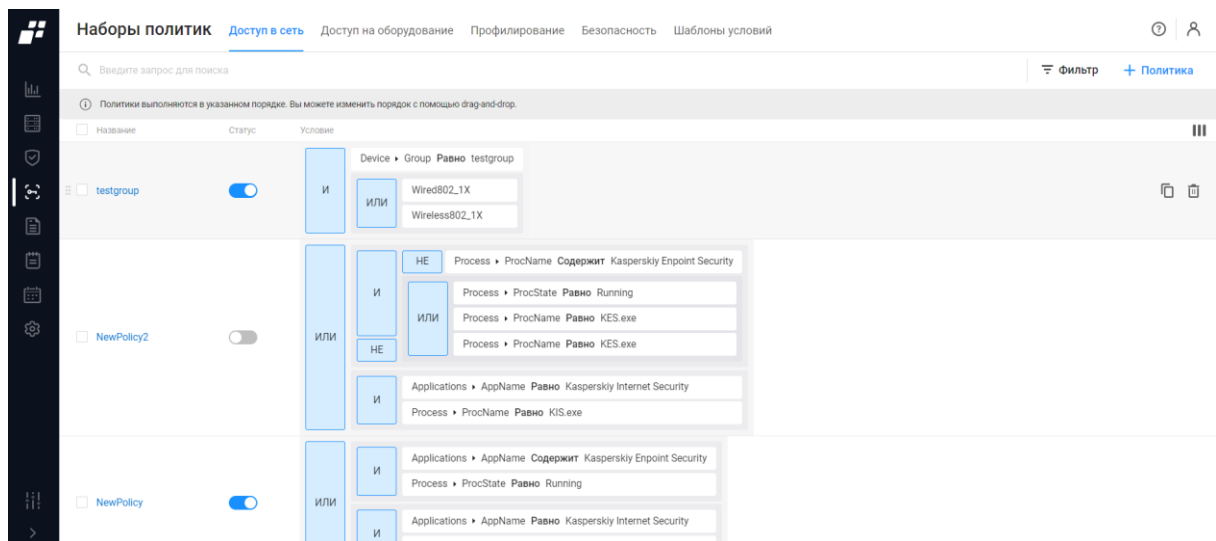






Рисунок 31 – Вкладка «Безопасность»



Для каждой записи списка отображаются следующие данные:

- поле для флага;
- название и описание;
- ОС;
- Требования для выполнения политики.

Над списком располагаются:

- поле поиска ( Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Политика» ( Политика) для добавления новой политики;
- кнопка «Фильтр» ( Фильтр) для фильтрации списка политик;
- кнопка «Колонки» ().


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

- кнопка «Создать копию» ();
- кнопка «Удалить» () для удаления выбранной политики.

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

2.6.4.1 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. 30. Состав и описание элементов вкладки приведены в таблице 15.

← Создание политики Безопасность

Статус ☒

Название

Описание

Семейство операционных систем i Linux Windows

i Для активации требований необходимо создать политику

Создать Отменить

Рисунок 32 – Страница «Создание политики (Безопасность)»

Таблица 16 – Состав и описание элементов страницы «Создание политики (Безопасность)»

Элемент	Описание
Поле «Статус»	Переключатель: — «Включен»; — «Отключен»
Поле «Название»	Текстовое поле для ввода названия политики. Параметры ввода текста: от 1 до 50 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «-»
Поле «Описание»	Текстовое поле для ввода описания политики. Параметры ввода текста: от 1 до 250 любых символов
Поле «Семейство операционных систем»	Переключатель: — «Linux»; — «Windows»
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) Нажать кнопку «Создать». Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности добавляемой политики профилирования. При обнаружении незаполненных обязательных полей под полем появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Создать».
- 5) Нажать на название-ссылку созданной политики. Перейти на вкладку «Требования» (рис. 33)

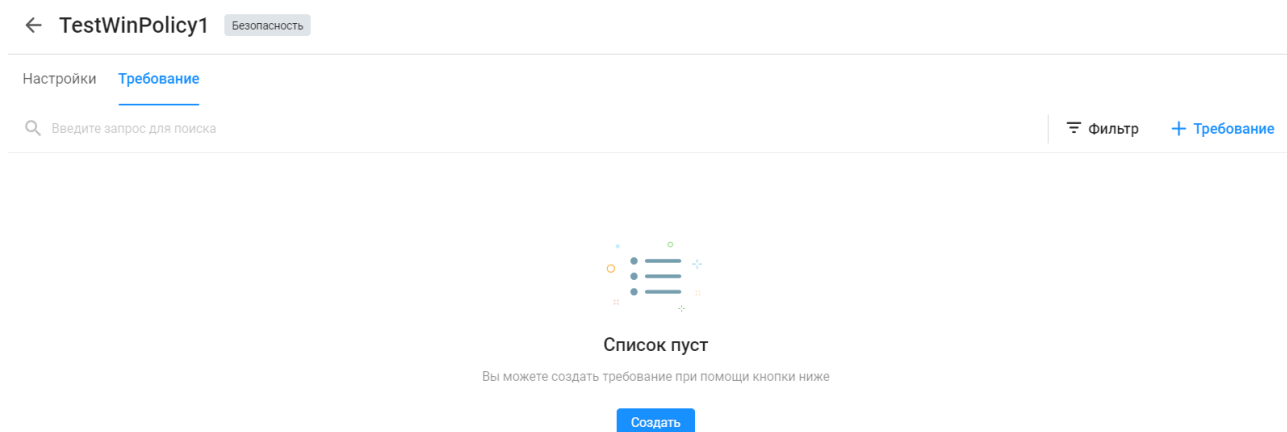
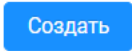



Рисунок 33 – Вкладка «Требования»

- 6) После создания политики безопасности вкладка «Требования» не содержит ни одного требования, на вкладке отображается сообщение «Список пуст. Вы можете создать требование при помощи кнопки ниже» и кнопка «Создать» для перехода в окно создания нового требования.
- 7) Нажать на кнопку «Создать» () или кнопку «Требование» ().
- 8) Откроется страница создания требования (рис. 36). Состав и описание элементов вкладки приведены в таблице 17.

← Создание требования **Безопасность**

Статус ☒

Название

Описание

Условия

и или

+ Объект

Объект

Атрибут Оператор Значение

Условия

и или

+ Условие

Атрибут Оператор Значение

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

Таблица 17 – Состав и описание элементов страницы «Создание политики (Безопасность)»

Элемент	Описание
Поле «Статус»	Переключатель: — «Активен»; — «Неактивен»
Поле «Название»	Текстовое поле для ввода названия политики. Параметры ввода текста: от 1 до 50 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «-»
Поле «Описание»	Текстовое поле для ввода описания политики. Параметры ввода текста: от 1 до 250 любых символов
Условия срабатывания политики	
Формирование условия происходит на основе выбора атрибута, оператора и значения	
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

9) Заполнить блок условий для объекта: выбрать объект, задать оператора и


значение.

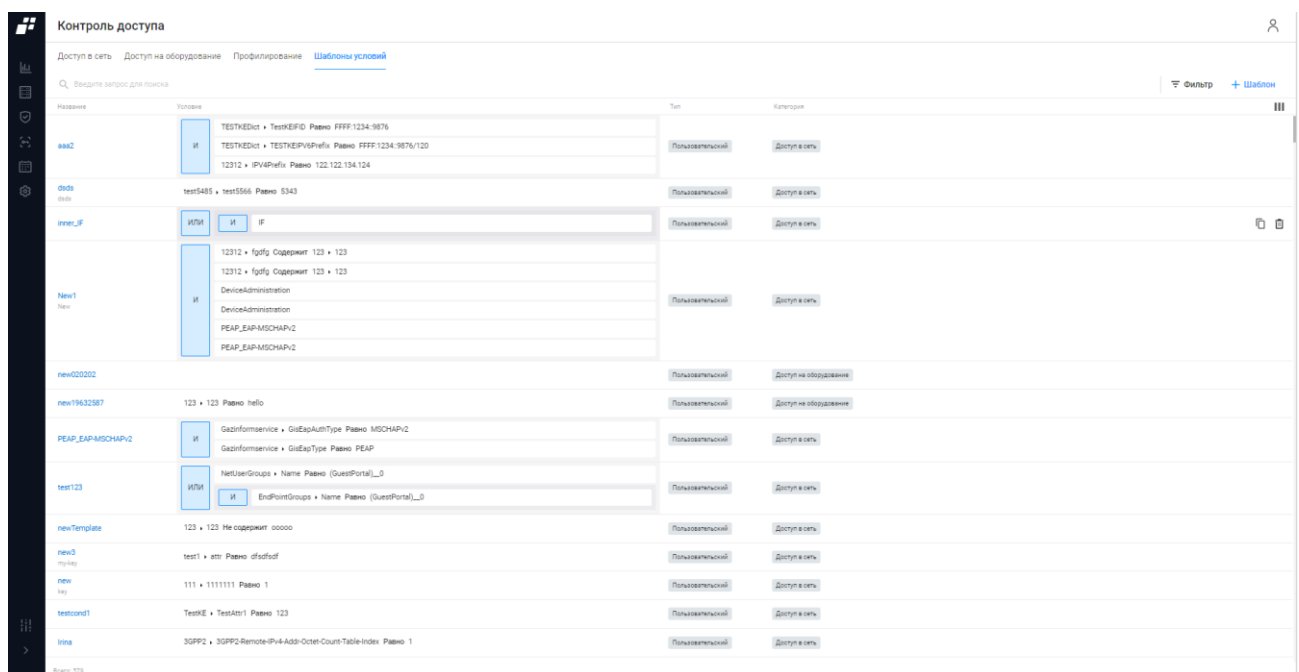
10) Заполнить список дополнительных условий для проверки объекта: указать атрибут, задать оператора и значение.

11) Нажать на кнопку «Создать».

2.6.5 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 (рис. 35).

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







Имя	Условие	Тип	Категория
aa62	И TESTKEYID = TESTKEYID Равно FFFF:1234:5676 TESTKEYID = TESTKEYID Равно FFFF:1234:5676/120 12312 = IPV4Prefix Равно 122.122.134.124	Пользовательский	Доступ в сеть
didb	test5485 = test5566 Равно 5343	Пользовательский	Доступ в сеть
inner_if	ИЛИ И IF	Пользовательский	Доступ в сеть
New1	И 12312 = IPv6p Содержит 123 = 123 12312 = IPv6p Содержит 123 = 123 DeviceAdministration DeviceAdministration PEAR_EAP-MSCHAPv2 PEAR_EAP-MSCHAPv2	Пользовательский	Доступ в сеть
new020202		Пользовательский	Доступ на оборудование
new19632987	123 = 123 Равно hello	Пользовательский	Доступ на оборудование
PEAR_EAP-MSCHAPv2	И GazInformService = GazAuthType Равно MSCHAPv2 GazInformService = GazAuthType Равно PEAR	Пользовательский	Доступ в сеть
test123	ИЛИ И NetUserGroup = Name Равно (GuestPort)_0 EndPointGroup = Name Равно (GuestPort)_0	Пользовательский	Доступ в сеть
newTemplate	123 = 123 Не содержит ooooo	Пользовательский	Доступ в сеть
new3	test1 = att Равно dfadfdf	Пользовательский	Доступ в сеть
new	111 = 11111111 Равно 1	Пользовательский	Доступ в сеть
testcond1	TestK = TestAtt1 Равно 123	Пользовательский	Доступ в сеть
lma	3GPP2 = 3GPP2-Remote-IPv4-Addr-Octet-Count-Table-Index Равно 1	Пользовательский	Доступ в сеть

Рисунок 35 – 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) для поиска искомой записи в списке;
- кнопка «Шаблон» ( Шаблон) для добавления нового пользовательского шаблона;
- кнопка «Фильтр» ( Фильтр) для фильтрации списка шаблонов;
- кнопка «Колонки» () для изменения отображения колонок на странице.

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.

2.6.5.1 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. 36 приведен пример создания шаблона «Доступ в сеть».

← Создание шаблона условий Доступ в сеть

Название	<input type="text" value="Название шаблона"/>
Описание	<input type="text" value="Описание"/>
Условия	
<div><div><div>И</div><div>ИЛИ</div><div>НЕ</div></div><div><div>НЕ</div><div>Выберите атрибут</div><div>Равно</div><div>Введите значение</div><div></div><div></div><div></div></div><div>Добавить</div></div>	
<div>Перенесите сюда условие</div>	

Введите запрос для поиска

Системные

DeviceAdministration

DeviceAdministration

RemoteAccessVPN

RemoteAccessVPN

Wired802_1X

Wired802_1X

WiredMab

WiredMab

WiredWebAuth

WiredWebAuth

Wireless802_1X

Wireless802_1X

WirelessMab

WirelessMab

WirelessWebAuth



WirelessWebAuth

Всего: 8

Сохранить

Отменить

Рисунок 36 – 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. п. 2.12) 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. 37). Для копирования условия в рамках одного уровня необходимо воспользоваться значком «Копировать» (), для удаления «Удалить» ().

← Создание шаблона условий Доступ в сеть

Название

Описание

Условия

И ИЛИ НЕ

HE DeviceAdministration
DeviceAdministration

HE WiredMab
WiredMab

Добавить ▾

Новое условие
Или
И

Перенесите сюда условие

Введите запрос для поиска Системные ▾

- DeviceAdministration
DeviceAdministration
- RemoteAccessVPN
RemoteAccessVPN
- Wired802_1X
Wired802_1X
- WiredMab
WiredMab
- WiredWebAuth
WiredWebAuth
- Wireless802_1X
Wireless802_1X
- WirelessMab
WirelessMab
- WirelessWebAuth
WirelessWebAuth

Всего: 8

Сохранить Отменить

Рисунок 37 – Поле для добавления нового условия в рамках одного уровня

Для добавления нового уровня вложенности нажать кнопку «Добавить». Из контекстного меню выбрать один из вариантов: «ИЛИ» или «И» (рис. 38).

← Создание шаблона условий Доступ в сеть

Описание

Условия

И ИЛИ НЕ

HE DeviceAdministration
DeviceAdministration

HE WiredMab
WiredMab

Добавить ▾

ИЛИ

HE Выберите атрибут ▾ Равно ▾ Введите значение ▾

Перенесите сюда условие

Перенесите сюда условие


Введите запрос для поиска Системные ▾

- DeviceAdministration
DeviceAdministration
- RemoteAccessVPN
RemoteAccessVPN
- Wired802_1X
Wired802_1X
- WiredMab
WiredMab
- WiredWebAuth
WiredWebAuth
- Wireless802_1X
Wireless802_1X
- WirelessMab
WirelessMab
- WirelessWebAuth
WirelessWebAuth

Всего: 8

Сохранить Отменить

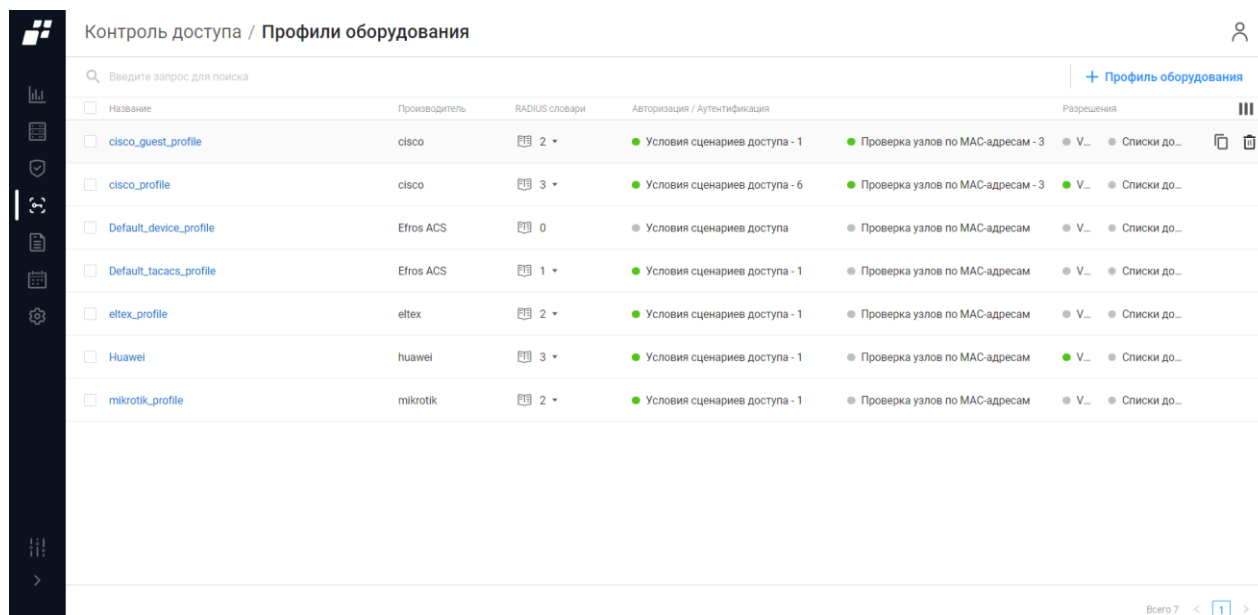
Рисунок 38 – Добавление условий с новым уровнем вложенности

-  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.

После определения необходимых условий для сохранения шаблона необходимо нажать «Создать». Созданный шаблон будет добавлен в набор условий.

2.7 Профили оборудования

Подраздел «Профили оборудования» (рис. 39) 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 ПК «Efros DO».






Название	Производитель	RADIUS словари	Авторизация / Аутентификация	Разрешения
<input type="checkbox"/> cisco_guest_profile	cisco	2	Условия сценариев доступа - 1	Проверка узлов по MAC-адресам - 3
<input type="checkbox"/> cisco_profile	cisco	3	Условия сценариев доступа - 6	Проверка узлов по MAC-адресам - 3
<input type="checkbox"/> Default_device_profile	Efros ACS	0	Условия сценариев доступа	Проверка узлов по MAC-адресам
<input type="checkbox"/> Default_tacacs_profile	Efros ACS	1	Условия сценариев доступа - 1	Проверка узлов по MAC-адресам
<input type="checkbox"/> eltex_profile	eltex	2	Условия сценариев доступа - 1	Проверка узлов по MAC-адресам
<input type="checkbox"/> Huawei	huawei	3	Условия сценариев доступа - 1	Проверка узлов по MAC-адресам
<input type="checkbox"/> mikrotik_profile	mikrotik	2	Условия сценариев доступа - 1	Проверка узлов по MAC-адресам

Рисунок 39 – Подраздел «Профили оборудования»


Для каждой записи списка отображаются данные:

- 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) для поиска искомой записи в списке;
- кнопка «Профиль оборудования» ( Профиль оборудования) для добавления нового профиля оборудования;
- кнопка «Колонки» () для изменения отображения колонок на странице.

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.

2.7.1 Добавление профиля сетевого оборудования

Для добавления нового профиля сетевого оборудования необходимо:

- 1) Нажать на странице кнопку «Профиль оборудования» ([+ Профиль оборудования](#)).
- 2) Откроется страница «Создание профиля сетевого оборудования», приведенная на рис. 40. Состав и описание элементов страницы приведены в таблице 18.

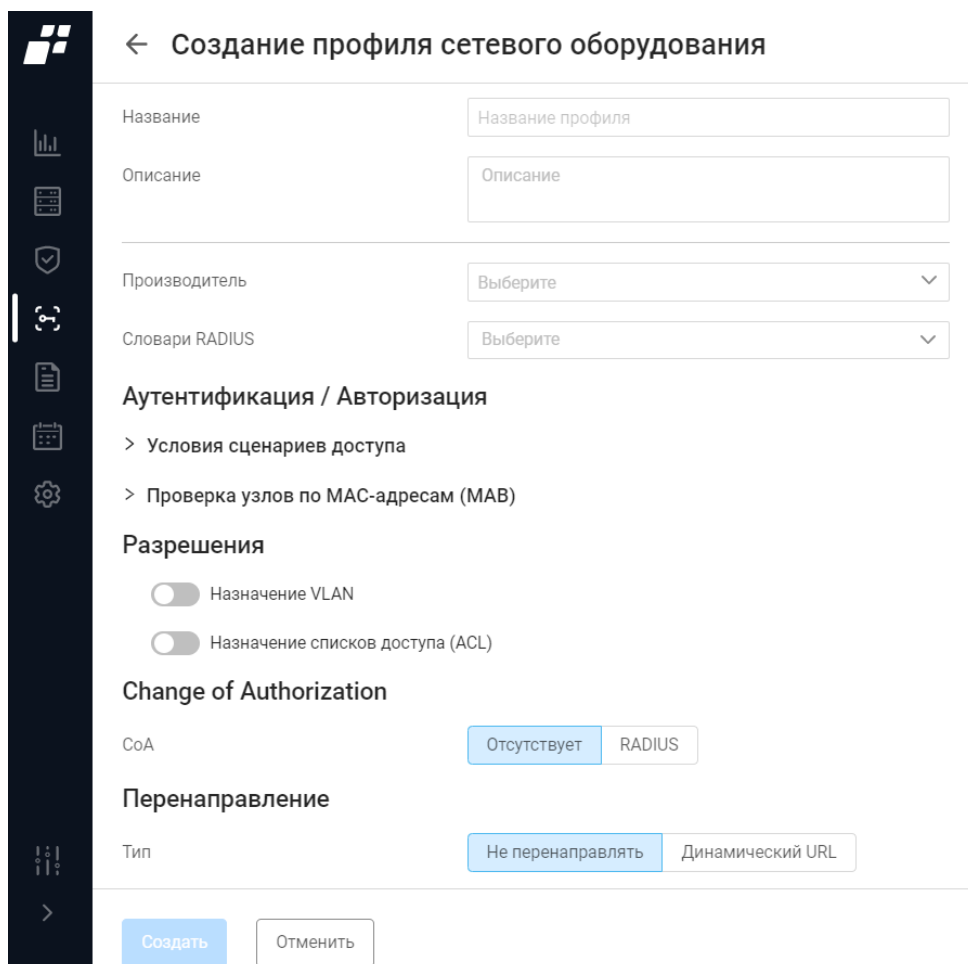










Рисунок 40 – Страница «Создание профиля сетевого оборудования»

Таблица 18 – Состав и описание элементов страницы «Создание профиля сетевого оборудования»

Элемент	Описание
Поле «Название»	Текстовое поле для ввода названия профиля сетевого оборудования. Параметры ввода текста: от 1 до 50 любых символов
Поле «Описание»	Текстовое поле для ввода описания профиля сетевого оборудования. Параметры ввода текста: от 1 до 250 любых символов
Поле «Производитель»	Раскрывающийся список для выбора производителя. В случае создания универсального профиля предлагается выбрать Efros ACS
Поле «Словари RADIUS»	Текстовое поле для выбора системных словарей и правил политик аутентификации и авторизации.  Не влияет на настройки сценария доступа по протоколу TACACS+. Выбирается любой
Аутентификация/Авторизация Данный блок полей предназначен для определения разрешенных сценариев доступа с указанием необходимых атрибутов и их значений (стандартные шаблоны условий, используемые при формировании набора политик).  Атрибуты, определяющие используемый сценарий доступа, могут различаться для разных производителей и типа оборудования (более подробно см. п. 2.13)	
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. 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)	

Элемент	Описание
Управление сетевыми устройствами (Device Administration)	
Удаленный доступ (VPN)	
Проверка узлов по MAC-адресам (MAB)	Переключатель «Метод проверки узлов», при включении отображаются три переключателя: <ul style="list-style-type: none"> — «С использованием PAP/ASCII»; — «С использованием CHAP»; — «С использованием EAP-MD5»
Разрешения	
Поле «Назначение VLAN»	Переключатель: <ul style="list-style-type: none"> — «Активен» () – разрешить использование VLAN; — «Неактивен» () – запретить использование VLAN. По умолчанию переключатель установлен в положение «Неактивен». При включении переключателя появляются следующие переключатели: <ul style="list-style-type: none"> — «Атрибуты IETF 802.1X»; — «Пользовательские атрибуты». При выборе данного поля необходимо указать атрибуты из раскрывающегося списка
Поле «Назначение списков доступа (ACL)»	Переключатель: <ul style="list-style-type: none"> — «Активен» () – разрешить использование ACL; — «Неактивен» () – запретить использование ACL. По умолчанию переключатель установлен в положение «Неактивен». При активации появляется поле для выбора атрибутов
Поле «CoA»	Содержит два переключателя: <ul style="list-style-type: none"> — «Отсутствует» – механизм «Change of Authorization» не применяется; — «RADIUS» – механизм «Change of Authorization» применяется с использованием сервера RADIUS. При активации переключателя «RADIUS» появляются дополнительные поля
Порт CoA	Порт для обмена CoA сообщениями между ПК «Efros DO» и сетевым оборудованием

Элемент	Описание
Группа полей «Отключение»	
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
Поле «Перенаправление»	<p> Использование данного параметра позволяет задать для пользователя, осуществляющего попытку доступа к сети, тип перенаправления на URL-адрес, который задается в профиле авторизации.</p> <p>Содержит следующие переключатели:</p> <ul style="list-style-type: none"> — «Не перенаправлять» – перенаправление не используется; — «Динамический URL». <p> При активации переключателя «Динамический URL», в профиле авторизации при выборе данного профиля сетевого оборудования появляется поле для выбора атрибута</p>
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

Заполнить поля страницы необходимыми параметрами.
Нажать кнопку «Создать».

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

2.8 Профили авторизации

Подраздел «Профили авторизации» (рис. 41) 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.

Название	Тип доступа	Профиль сетевого оборудования
00_auth_profile_bug_23567	Разрешен	Test bug 23567
111	Разрешен	_L_
123	Разрешен	1112dd
123-copy	Разрешен	1112dd
123321	Разрешен	cisco_guest
21	Разрешен	_L_
23	Разрешен	_L_
3333	Разрешен	cisco_guest
_aut_profile_	Разрешен	_net_device_
add	Разрешен	Default_cisco
allauthpol	Разрешен	epolauto
Allow-cisco-profile	Разрешен	Cisco IOS - тест
allow_idap_srv	Разрешен	Cisco IOS - тест
check_bug	Разрешен	Default_device_profile
ehack_bug0	Разрешен	

Рисунок 41 – Подраздел «Профили авторизации»

Страница состоит из вкладок:




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

2.8.1 Вкладка «Доступ в сеть»



На странице список профилей реализован в виде таблицы (см. рис. 41). 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) для поиска искомой записи в списке;
- кнопка «Профиль» ( Профиль) для добавления нового профиля;
- кнопка «Колонки» () для изменения отображения колонок на странице.


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.

2.8.1.1 Создание профиля авторизации доступа в сеть




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

- 1) Нажать кнопку «Профиль» ( Профиль). Откроется страница «Создание профиля авторизации доступа в сеть» (рис. 42). Состав и описание элементов страницы приведены в таблице 19.

← Создание профиля авторизации доступа в сеть

Название	<input type="text" value="Введите название"/>
Описание	<input type="text" value="Введите описание"/>
Тип доступа	<input checked="" type="button" value="Разрешен"/> <input type="button" value="Запрещен"/>
Профиль сетевого оборудования	<input type="text" value="Выберите профиль"/> ▾

Основные настройки

ACL 	<input type="checkbox"/>
Веб-переедресация 	<input type="checkbox"/>
VLAN 	<input type="checkbox"/>


Настройка дополнительных атрибутов

<input type="text" value="Выберите атрибут"/> ▾	<input type="text" value="Введите значение"/>	+
---	---	---

Передаваемые параметры

Рисунок 42 – Страница «Создание профиля авторизации доступа в сеть»

Таблица 19 – Состав и описание элементов страницы «Создание профиля авторизации доступа в сеть»

Элемент	Описание
Поле «Название»	Текстовое поле для ввода названия профиля авторизации. Параметры ввода текста: от 1 до 50 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «-»
Поле «Описание»	Текстовое поле для ввода описания профиля авторизации. Параметры ввода текста: от 1 до 250 любых символов
Переключатель «Тип доступа»	Переключатель: — «Разрешен»; — «Запрещен»
Поле «Профиль сетевого оборудования»	Поле содержит список созданных профилей сетевого оборудования (более подробно описано в подразделе 2.7)
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 2.9.)
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).  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

Элемент	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 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

2) Заполнить поля страницы необходимыми параметрами.

3) Нажать кнопку «Создать».

Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности создаваемого профиля авторизации по названию.

При обнаружении незаполненных обязательных полей под полем появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Создать».

2.8.2 Вкладка «Доступ на оборудование»

На странице список профилей реализован в виде таблицы (рис. 43).

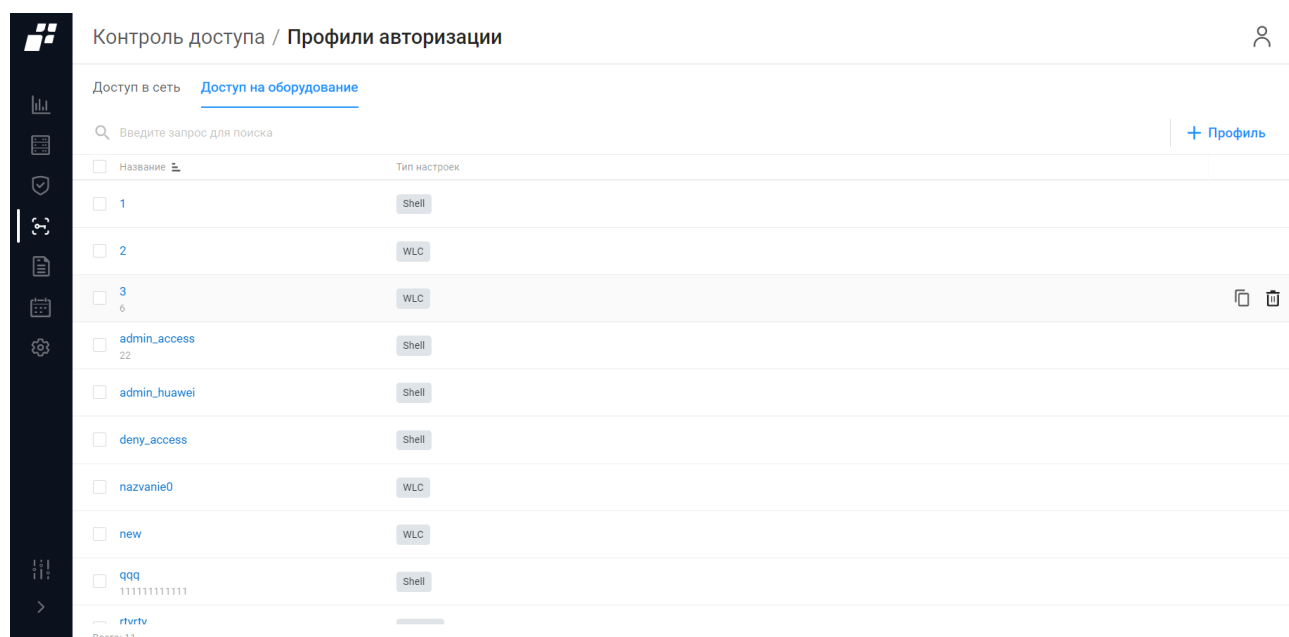





Рисунок 43 – Вкладка «Доступ на оборудование»



Для каждой записи списка отображаются данные:

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

Над списком располагаются:

- поле поиска ( Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Профиль» ( + Профиль) для добавления нового профиля;
- кнопка «Колонки» () для изменения отображения колонок на странице.


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.

2.8.2.1 Создание профиля авторизации доступа на оборудование

Для ручного добавления нового профиля авторизации пользователю необходимо:

- 1) Нажать кнопку «Профиль» ( + Профиль). Откроется страница «Создание профиля авторизации доступа на оборудование» (рис. 44). Состав и описание элементов страницы приведены в таблице 20.

Создание профиля авторизации доступа на оборудование

Название

Название профиля

Описание

Описание

Тип настроек

Shell

Основные настройки

Уровень привилегий по умолчанию

Не выбрано

Максимальный уровень привилегий

Не выбрано

Список контроля доступа

Список контроля доступа

Выполнение команды при подключении пользователя

Автокоманда

Запрет автоматического отключения после выполнения команды

Не задано

Да

Нет

Запрет использования управляющего символа

Не задано

Да

Нет

Время отключения при бездействии

0

Минут

Время отключения сеанса

0

Минут

Дополнительные атрибуты

Добавить атрибуты

Передаваемые параметры




Создать

Отменить

Рисунок 44 – Страница «Создание профиля авторизации доступа на оборудование»

Таблица 20 – Состав и описание элементов страницы «Создание профиля авторизации доступа на оборудование»

Элемент	Описание
Поле «Название»	Текстовое поле для ввода названия профиля авторизации. Параметры ввода текста: от 1 до 50 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «-»
Поле «Описание»	Текстовое поле для ввода описания профиля авторизации. Параметры ввода текста: от 1 до 250 любых символов
Поле «Тип настроек»	Раскрывающийся список: — «Shell» – базовый профиль, применимый к большинству

Элемент	Описание
	сетевых устройств; — «WLC» – применим для беспроводных LAN-контроллеров (Wireless LAN Controller); — «Nexus» – используется для коммутаторов Cisco Nexus; — «Generic» – полностью настраиваемый профиль без предустановленных значений
Группа полей «Основные настройки» при выборе типа настроек «Shell»	
Поле «Уровень привилегий по умолчанию»	Раскрывающийся список значений: от 0 до 15, «Не выбрано».  В случае, если задан уровень привилегий, необходимо проверить, что конкретная модель оборудования поддерживает выбранное значение. Передается в атрибуте "priv-lvl"
Поле «Максимальный уровень привилегий»	Раскрывающийся список значений: от 0 до 15, «Не выбрано».  В случае, если задан уровень привилегий, необходимо проверить, что конкретная модель оборудования поддерживает выбранное значение. Передается в атрибуте "max_priv_lvl"
Поле «Список контроля доступа»	Название ACL, который будет применен на интерфейсе сетевого оборудования. ACL предварительно должен быть создан локально на сетевом оборудовании. Передается в атрибуте "acl"
Поле «Выполнение команды при подключении пользователя»	Поле для ввода команды. Передается в атрибуте "autocmd"  Необходимо убедиться, что введенная команда поддерживается оборудованием
Поле «Запрет автоматического отключения после выполнения команды»	Переключатель: — «Не задано»; — «Да» – запретить использовать символ прерывания ввода; — «Нет» – разрешить использовать символ прерывания ввода. Передается в атрибуте "noescape"
Поле «Запрет использования управляющего символа»	Переключатель: — «Не задано»; — «Да» – запретить использовать символ прерывания ввода; — «Нет» – разрешить использовать символ прерывания

Элемент	Описание
	ввода. Передается в атрибуте "noescape"
Поле «Время отключения при бездействии»	Числовое значение в минутах. Допустимые значения: от 0 до 9999. Передается в атрибуте "idletime"
Поле «Время отключения сеанса»	Числовое значение в минутах. Допустимые значения: от 0 до 9999. Передается в атрибуте "timeout"
Группа полей «Основные настройки» при выборе типа настроек «WLC»	
Поле «Выбор роли»	Переключатель: <ul style="list-style-type: none"> — «All» – полный доступ ко всем вкладкам приложений WLC. Передается в атрибуте "role1"; — «Monitor» – доступ только для чтения к вкладкам приложения WLC. Передается в атрибуте "role1"; — «Lobby» – только ограниченные права на настройку. Передается в атрибуте "role1"; — «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: <ul style="list-style-type: none"> — «Обязательный»; — «Оptionальный»
Поле «Роль для NX-OS»	Предустановленные роли для управления NX-OS. Переключатель: <ul style="list-style-type: none"> — «Нет»; — «Оператор» — «Администратор»
Поле «Роль для VDC»	Предустановленные роли для управления. Переключатель: <ul style="list-style-type: none"> — «Нет»; — «Оператор»; — «Администратор»
Поле «Дополнительные атрибуты»	Поле обеспечивает ввод и сохранение параметров без шаблона. Поле раскрывается для ввода атрибутов при помощи кнопки «Добавить атрибуты»
Поле «Передаваемые параметры»	Поле для отображения результирующей информации о том, какие атрибуты и какие значения будут отправляться клиенту на основе данных текущего профиля авторизации. Для отображения информации необходимо нажать кнопку

Элемент	Описание
	«Показать»
Элементы управления	
Создать	При нажатии кнопки выполняется переход на страницу списка профилей авторизации с сохранением внесенных данных
Отменить	При нажатии кнопки выполняется переход на страницу списка без сохранения внесенных данных

2) Заполнить поля страницы необходимыми параметрами.

3) Нажать кнопку «Создать».

Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности создаваемого профиля авторизации по названию.

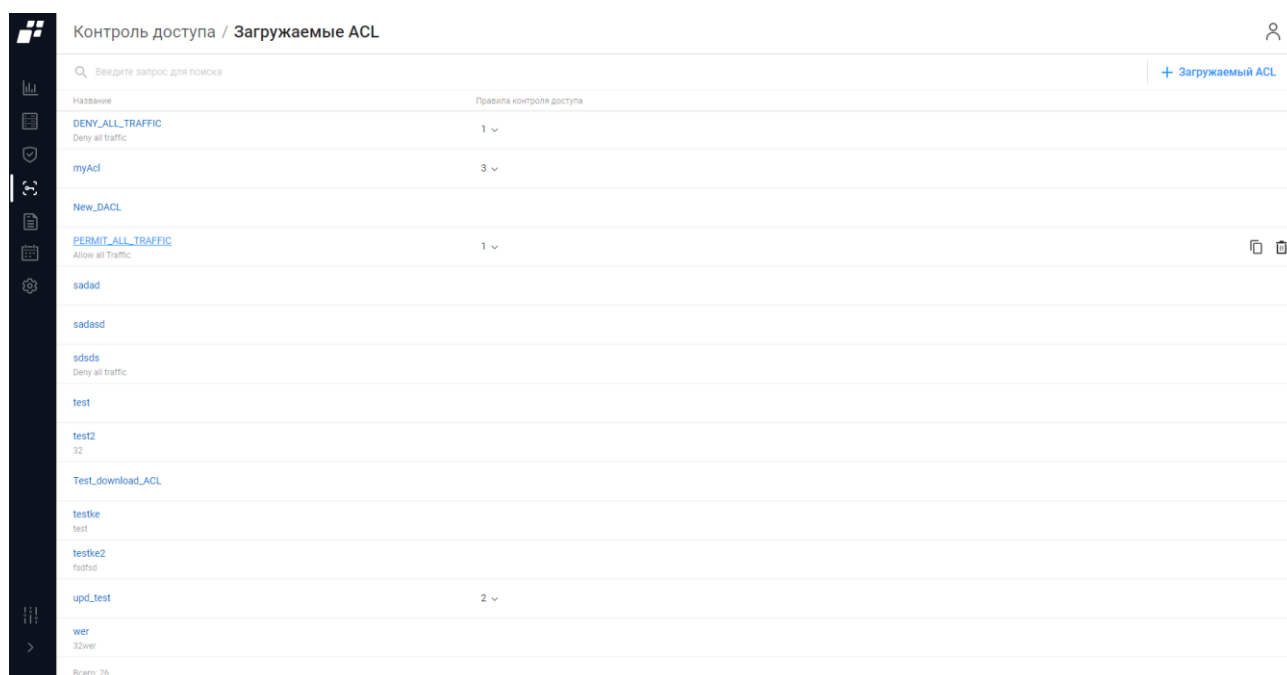
При обнаружении незаполненных обязательных полей под полем появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Создать».

2.9 Загружаемые ACL

 Загружаемые ACL работают только с оборудованием Cisco

В подразделе «Загружаемые ACL» (рис. 45) 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.

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






Название	Правила контроля доступа
DENY_ALL_TRAFFIC Deny all traffic	1
myAcl	3
New_DACL	
PERMIT_ALL_TRAFFIC Allow all Traffic	1
sadad	
sadesd	
sdsds Deny all traffic	
test	
test2 32	
Test_download_ACL	
testke test	
testke2 testad	
upd_test	2
wer 32wer	

Рисунок 45 – Страница «Загружаемые ACL»


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) для поиска искомой записи в списке;
- кнопка «Загружаемый ACL» ( + Загружаемый ACL) для добавления списка;
- кнопка «Колонки» () для изменения отображения колонок на странице.


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

- кнопка «Создать копию» ();

— кнопка «Удалить» ().

2.9.1 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. 46. Состав и описание элементов страницы приведены в таблице 21.

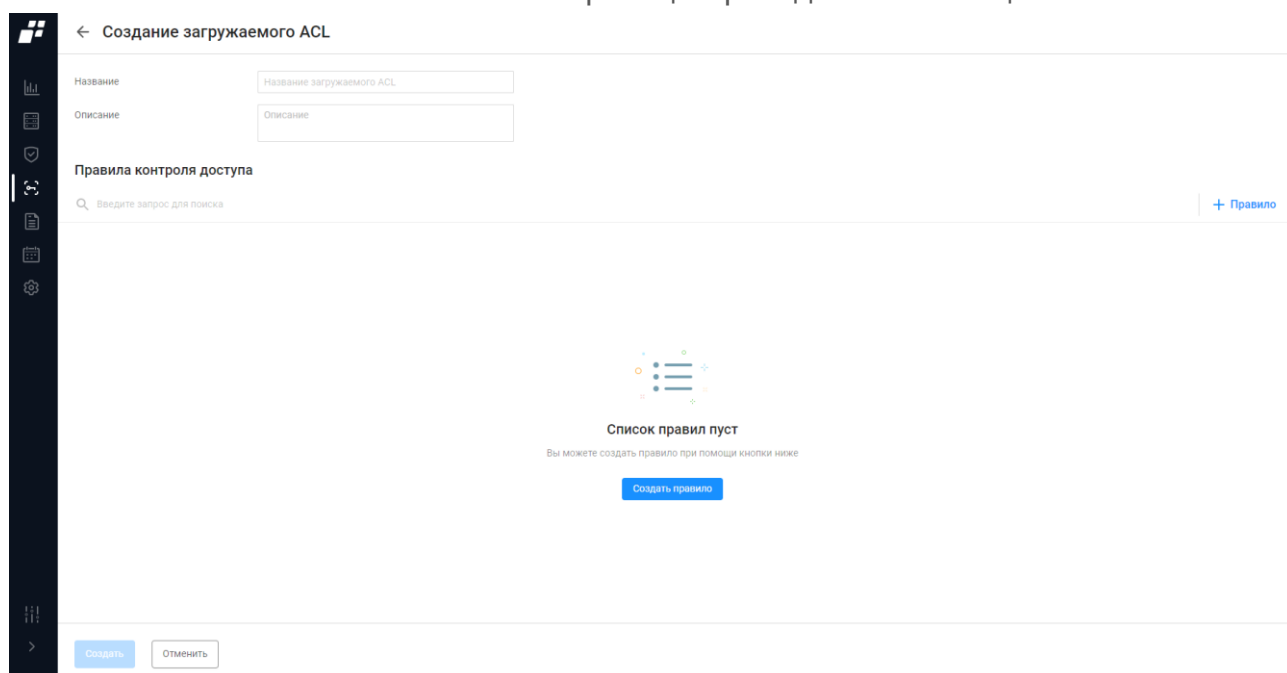
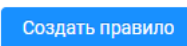




Рисунок 46 – Страница «Создание загружаемого ACL»

Таблица 21 – Состав и описание элементов страницы создания загружаемого ACL

Элемент	Описание
Поле «Название»	Текстовое поле для ввода названия ACL. Параметры ввода текста: от 1 до 50 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «-»
Поле «Описание»	Текстовое поле для ввода описания ACL. 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» (). Создание правила описано в п. 2.9.2

Элемент	Описание
	 Список представляет собой набор текстовых выражений, в каждом правиле определяется действие над пакетом: permit (разрешить) или deny (запретить).  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) Заполнить поля страницы необходимыми параметрами.

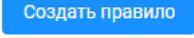
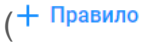
4) Нажать кнопку «Создать».

Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности создаваемого загружаемого ACL.

При обнаружении незаполненных обязательных полей под полем появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Создать».

2.9.2 Создание правила доступа для загружаемого ACL

Для создания нового правила доступа необходимо выполнить следующие действия:

- 1) Нажать кнопку «Создать правило» () или кнопку «Правило» ().
- 2) В открывшемся окне «Создание правила» (рис. 47) заполнить необходимые поля и нажать кнопку «Создать». Состав и описание полей страницы приведено в таблице 22.

← Создание правила

Действие

Протокол

Источник

Назначение

Результат

Рисунок 47 – Окно «Создание правила»

Таблица 22 – Состав и описание полей окна «Создание правила»

Элемент	Описание
Поле «Действие»	Переключатель: — «Разрешить»; — «Запретить»
Поле «Протокол»	Раскрывающийся список с протоколами. При выборе значения «Другой» появляется дополнительное поле «Номер IP протокола»
Группа полей, зависящих от типа протокола в поле «Протокол»	
Поле «Порт назначения»	Раскрывающийся список со значениями: — «Не выбрано»; — «Равен»; — «Неравен»; — «Диапазон»; — «Больше»; — «Меньше»
Поле «Номер порта»	Номер порта
Поле «Established»	Переключатель:

Элемент	Описание
	— «Вкл.»; — «Выкл.»
Поле «Дополнительные параметры»	Переключатель: — «Отсутствует»; — «Сообщение»; — «Тип»
Поле «Источник»	Переключатель: — «Все адреса»; — «Хост»; — «Подсеть». При выборе переключателей «Хост» появляется поле «Адрес хоста». При выборе переключателя «Подсеть» появляются поля «Адрес подсети», «Маска подсети», «Результирующая подсеть»
Поле «Назначение»	Переключатель: — «Все адреса»; — «Хост»; — «Подсеть». При выборе переключателей «Хост» появляется поле «Адрес хоста». При выборе переключателя «Подсеть» появляются поля «Адрес подсети», «Маска подсети», «Результирующая подсеть»
Элементы управления	
Показать	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

2.10 Наборы команд

С помощью подраздела «Наборы команд» (рис. 48) 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.

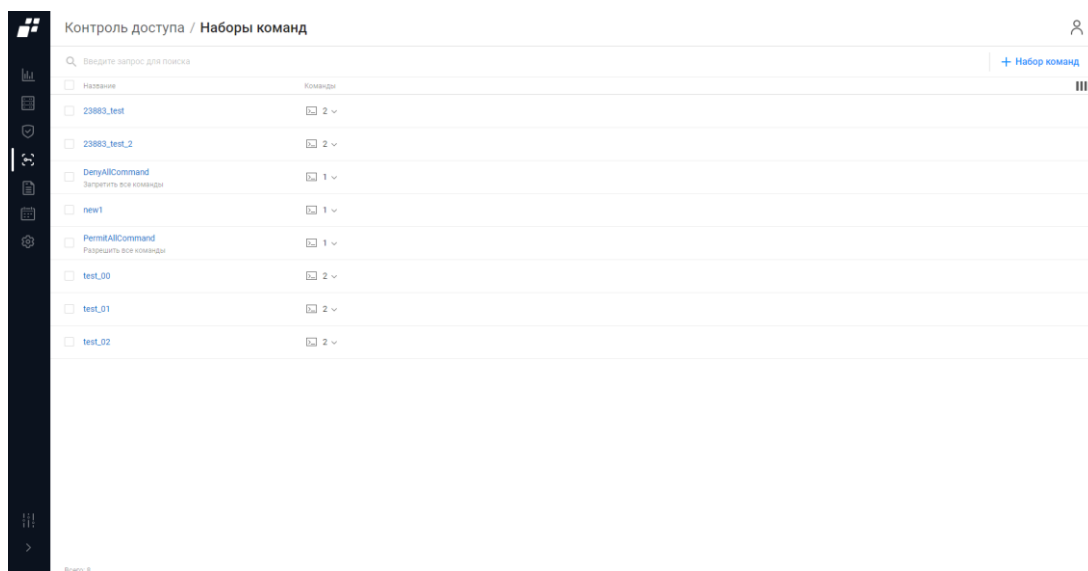





Рисунок 48 – Страница «Наборы команд»



Для каждой записи списка отображаются данные:

- поле для флага;
- название – является ссылкой, при нажатии откроется страница редактирование 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) для поиска искомой записи в списке;
- кнопка «Набор команд» ( Набор команд) для добавления нового набора команд;
- кнопка «Колонки» () для изменения отображения колонок на странице.

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

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

Аналогичная кнопка появляется в правой части экрана в строке с набором команд.

2.10.1 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. 49. Состав и описание элементов страницы приведены в таблице 23.

Рисунок 49 – Страница «Создание набора команд»

Таблица 23 – Состав и описание элементов окна создания набора команд

Элемент	Описание
Поле «Название»	Текстовое поле для ввода названия набора команд. Параметры ввода текста: от 1 до 50 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «-»
Поле «Описание»	Текстовое поле для ввода описания набора команд. Параметры ввода текста: от 1 до 250 любых символов
Таблица команд	Поле заполнения содержит список разрешенных (PERMIT) или запрещенных (DENY) для выполнения команд с указанными аргументами. После ввода команды и аргументов, необходимо кликнуть по


Элемент	Описание
	галочке справа от введенных значений для сохранения заданных параметров. Убедитесь, 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

2) Заполнить поля страницы необходимыми параметрами.

3) Нажать кнопку «Создать».

Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности создаваемого набора команд.

При обнаружении незаполненных обязательных полей под полем появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Создать».

 Для работы с набором команд на странице создания (см. рис. 49) или редактирования (рис. 50) необходимо:

1) Выбрать в поле «Действия» одно из действий: PERMIT (разрешить) или DENY (запретить).

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.

 Наименование команды не должно содержать пробелов. В значении аргумента допустимы любые символы. Суммарное количество символов в наименовании команды и значении аргумента не должно превышать 512 символов.

← test

Название: test

Описание: Описание



Команды - 1

Действие	Команда	Аргументы
Deny	show	user
Deny	Команда	Аргументы

Сохранить Отменить

Рисунок 50 – Редактирование набора команд

После сохранения внесенных изменений в таблице в соответствии с рис. 51 добавится строка с новой командой, в строке добавленной команды отобразятся кнопки:

- «Копировать» ();
- «Удалить» ().

The screenshot shows a web interface for configuring a user named 'deny_ver'. On the left is a dark sidebar with various icons. The main area has a header '← deny_ver'. Below it are two input fields: 'Название' (Name) containing 'deny_ver' and 'Описание' (Description). A section titled 'Команды - 2' (Commands - 2) contains a table with columns 'Действие' (Action), 'Команда' (Command), and 'Аргументы' (Arguments). The table has three rows: the first row has 'Deny' selected, command 'show', and argument 'ver'; the second row has 'Permit' selected, command 'show', and argument '.*'; the third row has 'Deny' selected, an empty 'Команда' field, and an empty 'Аргументы' field. At the bottom are 'Сохранить' (Save) and 'Отменить' (Cancel) buttons.

Действие	Команда	Аргументы
<input type="radio"/> Permit <input checked="" type="radio"/> Deny	show	ver
<input checked="" type="radio"/> Permit <input type="radio"/> Deny	show	.*
<input type="radio"/> Permit <input checked="" type="radio"/> Deny		

Рисунок 51 – 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 каким-то аргументом задано значение «PERMIT», то разрешено будет выполнять только эту команду с таким аргументом. Остальные аргументы – запрещены.
- Если в наборе команд для команды с аргументом задано значение «DENY», то правило будет наложено. Чтобы разрешить выполнение этой же команды с другими аргументами необходимо в одной из строк ниже в списке команд указать действие «PERMIT» с аргументом «.*».

2.11 Разрешенные протоколы

С помощью подраздела «Разрешенные протоколы» (рис. 52) можно создать список разрешенных протоколов, которые будут использоваться во время проверки правил аутентификации в политиках доступа на оборудование.

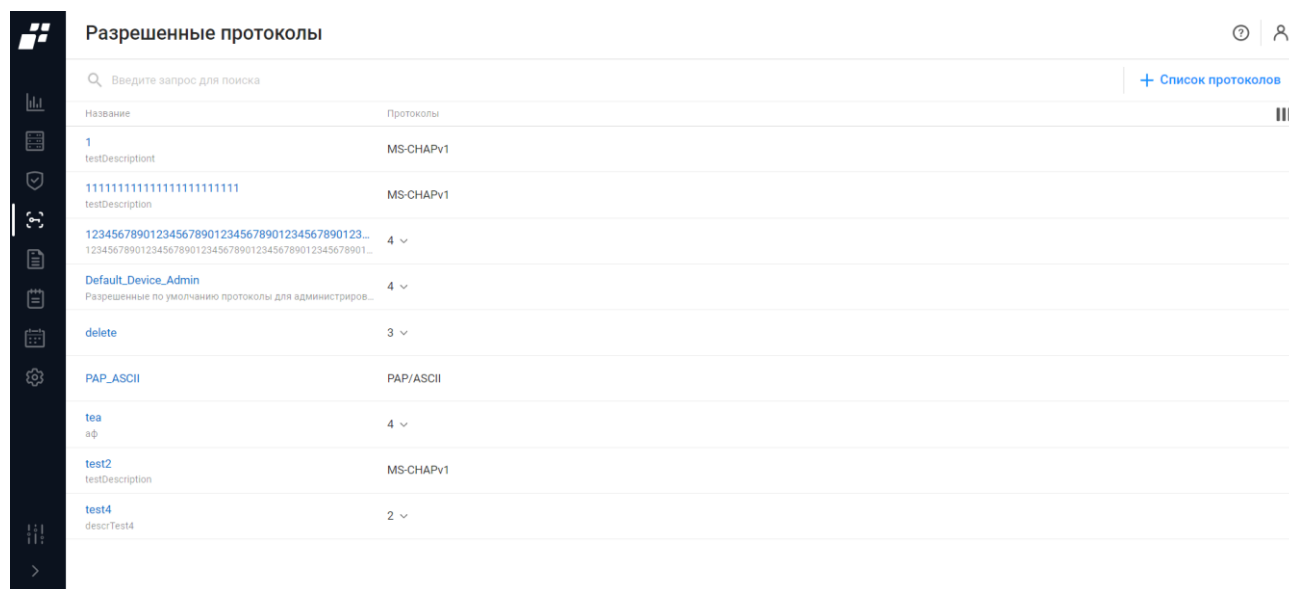




Рисунок 52 – Подраздел «Разрешенные протоколы»



Для каждой записи списка отображаются данные:

- название – является ссылкой, при нажатии откроется страница редактирования протоколов;
- количество протоколов – является раскрывающимся списком протоколов.

Над списком располагаются:


- поле поиска ( Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Список протоколов» ( Список протоколов) для добавления нового списка протоколов.

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

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

2.11.1 Создание списка разрешенных протоколов

Для создания нового списка пользователю ПК «Efros DO» необходимо:

- 1) Нажать кнопку «Список протоколов» ( Список протоколов). Откроется страница «Создание списка разрешенных протоколов», приведенная на рис. 53. Состав и описание элементов страницы приведены в таблице 24.

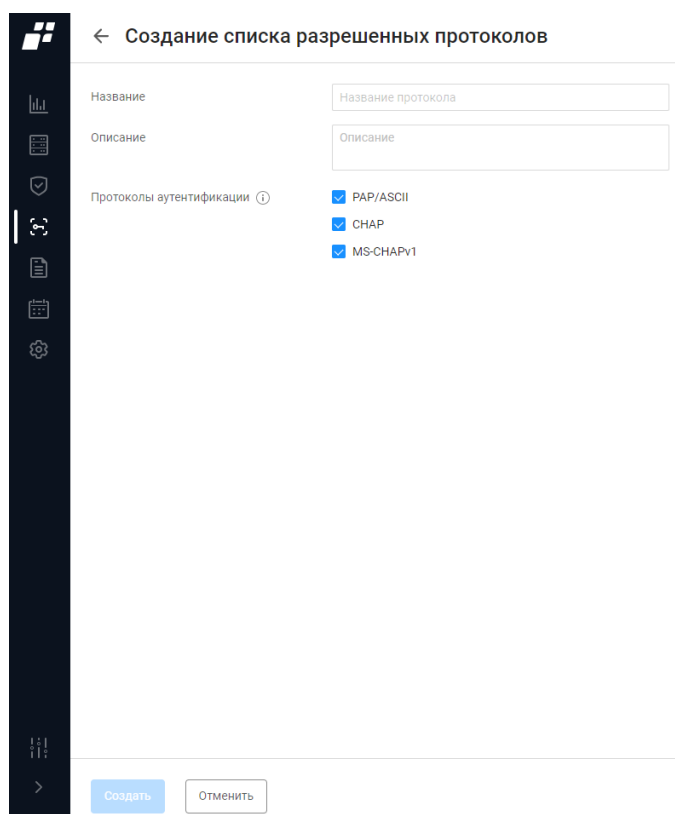


Рисунок 53 – Страница «Создание списка разрешенных протоколов»

Таблица 24 – Состав и описание элементов страницы создания списка разрешенных протоколов

Элемент	Описание
Поле «Название»	Текстовое поле для ввода названия списка разрешенных протоколов. Параметры ввода текста: от 1 до 50 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «-»
Поле «Описание»	Текстовое поле для ввода описания списка разрешенных протоколов. Параметры ввода текста: от 1 до 250 любых символов
Поле «Протоколы аутентификации»	Список протоколов аутентификации
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

- 2) Заполнить поля страницы необходимыми параметрами.
- 3) Нажать кнопку «Создать».

Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности создаваемого списка протоколов.

При обнаружении незаполненных обязательных полей под полем появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Создать».

2.12 Разрешенные MAC-адреса

С помощью подраздела «Разрешенные MAC-адреса» (рис. 54) можно вести список MAC-адресов, которым разрешена аутентификация по MAC-адресу.

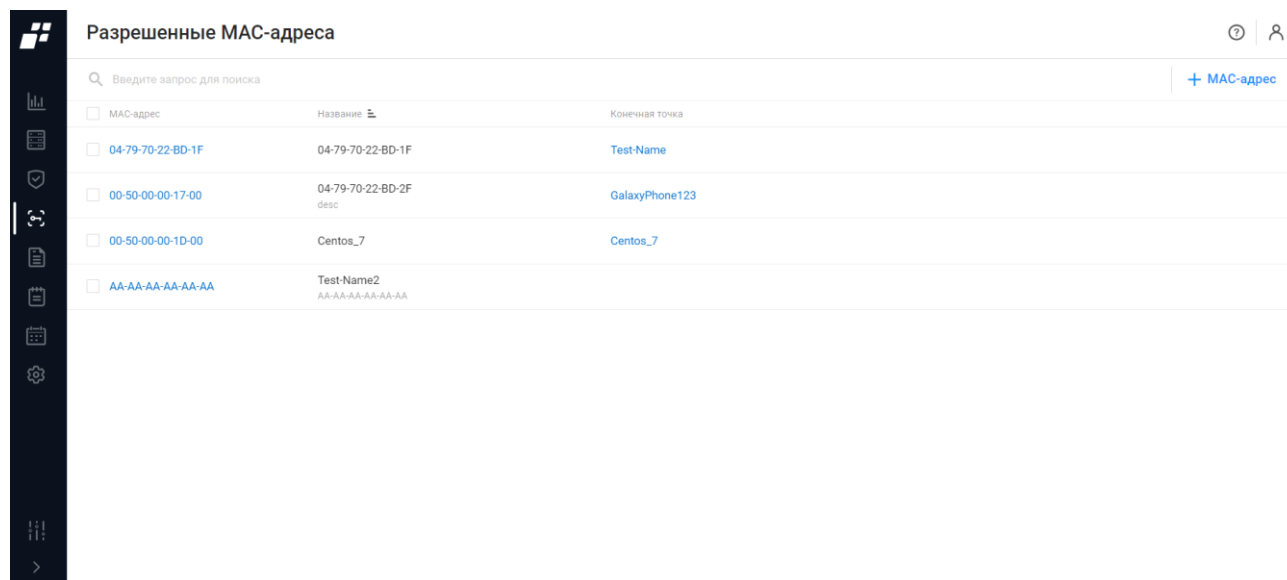


Рисунок 54 – Страница «Разрешенные MAC-адреса»

Для каждой записи списка отображаются данные:

- поле для флага;
- MAC-адрес – является ссылкой, при нажатии откроется страница редактирования MAC-адреса конечной точки;
- название – MAC-адрес конечной точки.

Над списком располагаются:

- поле поиска (Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «MAC-адрес» () для добавления нового MAC-адреса.

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.

2.12.1 Создание разрешенного MAC-адреса

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

- 1) Нажать кнопку «MAC-адрес» (). Откроется страница «Создание разрешенного MAC-адреса», приведенная на рис. 55. Состав и описание элементов страницы приведены в таблице 25.

← Создание разрешенного MAC-адреса

MAC-адрес	<input type="text" value="MAC-адрес"/>
Название	<input type="text" value="Название"/>
Описание	<input type="text" value="Описание"/>

Рисунок 55 – Страница «Создание разрешенного MAC-адреса»

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

Элемент	Описание
Поле «MAC-адрес»	Поле для ввода MAC-адреса
Поле «Название»	Текстовое поле для ввода названия MAC-адреса. Параметры ввода текста: от 1 до 50 символов. Допустимые символы: буквы латинского алфавита, цифры, «_», «-»
Поле «Описание»	Текстовое поле для ввода описания MAC-адреса. 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

- 2) Заполнить поля страницы необходимыми параметрами.

3) Нажать кнопку «Создать».

Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности создаваемого MAC-адреса.

При обнаружении незаполненных обязательных полей под полем появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Создать».

2.13 Словари

Для обеспечения взаимодействия аутентификатора (сетевого оборудования) с ПК «Efros DO» используются двоичные данные. В комплексе данные представлены в текстовой форме в виде словарей (рис. 56).

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:

- «Системные»;
- «Пользовательские»;
- «Псевдословари».

1) Системные словари – это предустановленные словари, необходимые для обеспечения работоспособности протоколов RADIUS и TACACS+.

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.
- `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;
 - а) `Administrative` – пользователю предоставляется доступ к административному интерфейсу NAS, с которого могут выполняться привилегированные команды;
 - б) `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.

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 формируемыми значениями атрибутов.

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.

Словари, используемые для RADIUS:

- EDO;
- Device – сетевое оборудование;
- NetUserGroups – группы сетевых пользователей;
- NetUsers – сетевой пользователь.

Словари, используемые для профилирования:

- DHCP;
- UserAgent.

Рисунок 56 – Подраздел «Словари»

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.

2.13.1 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.

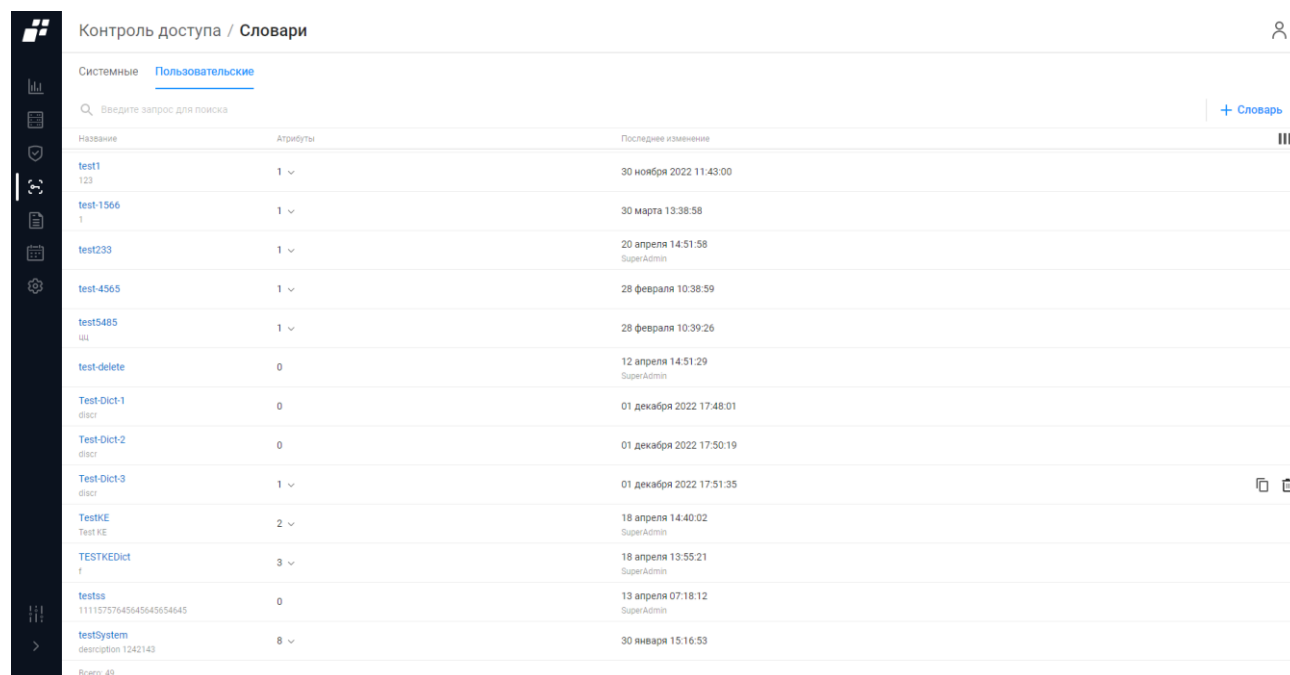
Над списком с системными словарями располагаются:

- поле поиска (🔍 Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Колонки» (☰) для изменения отображения колонок на странице.

2.13.2 Вкладка «Пользовательские»

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

комплекса.



Контроль доступа / Словари			
Системные Пользовательские			
Введите запрос для поиска			+ Словарь
Название	Атрибуты	Последнее изменение	
test1 123	1	30 ноября 2022 11:43:00	
test-1566 1	1	30 марта 13:38:58	
test233	1	20 апреля 14:51:58 SuperAdmin	
test-4565	1	28 февраля 10:38:59	
test5485 uu	1	28 февраля 10:39:26	
test-delete	0	12 апреля 14:51:29 SuperAdmin	
Test-Dict-1 descr	0	01 декабря 2022 17:48:01	
Test-Dict-2 descr	0	01 декабря 2022 17:50:19	
Test-Dict-3 descr	1	01 декабря 2022 17:51:35	
TestKE Test KE	2	18 апреля 14:40:02 SuperAdmin	
TESTKEDict f	3	18 апреля 13:55:21 SuperAdmin	
testes 11115757645645645645645	0	13 апреля 07:18:12 SuperAdmin	
testSystem description 1242143	8	30 января 15:16:53	

Всего: 49

Рисунок 57 – Вкладка «Пользовательские»






После установки ПК «Efros DO» список словарей пуст, на странице отображается сообщение «Список пуст. Вы можете добавить новый словарь» и кнопка «Добавить словарь».



На странице список пользовательских словарей реализован в виде таблицы. 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) для поиска искомой записи в списке;
- кнопка «Словарь» ( Словарь) для добавления нового пользовательского словаря;
- кнопка «Колонки» () для изменения отображения колонок на странице.

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

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

2.13.3 Создание пользовательского словаря

Для создания пользовательского словаря необходимо выполнить следующее:

- 1) Нажать над списком кнопку «Словарь» ([+ Словарь](#)). Откроется страница создания нового словаря (рис. 58). Состав и описание элементов страницы приведены в таблице 26.

Рисунок 58 – Страница создания нового пользовательского словаря

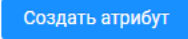

Таблица 26 – Состав и описание элементов окна создания нового словаря

Элемент	Описание
Поле «Название»	Текстовое поле для ввода названия словаря. 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. Требования, которым должно соответствовать содержание поля: цифры от 0 до 9
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

- 2) Заполнить поля страницы необходимыми параметрами.

3) Нажать кнопку «Создать». Произойдет автоматический переход на страницу добавления атрибутов в созданный словарь (рис. 59).

Атрибуты можно добавить двумя способами:

- через кнопку «Добавить атрибут» () (см. рис. 59) в центре страницы;
- через кнопку «Атрибут» ().

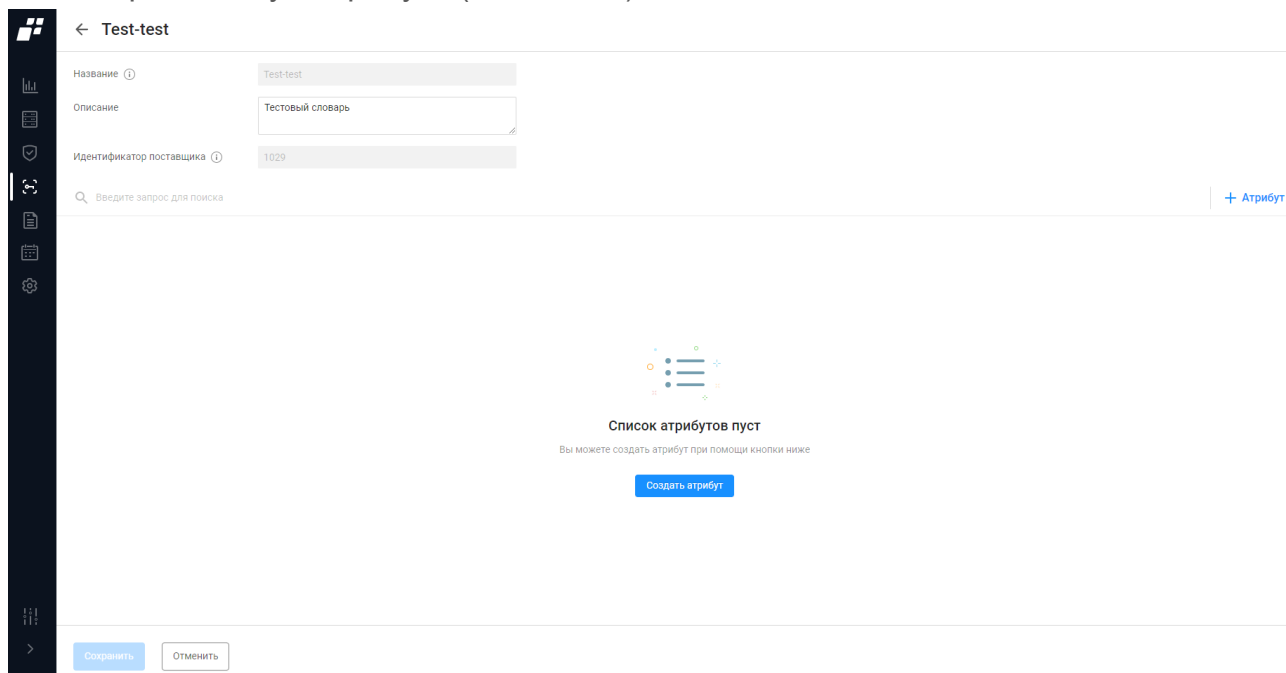


Рисунок 59 – Страница добавления атрибутов в созданный словарь

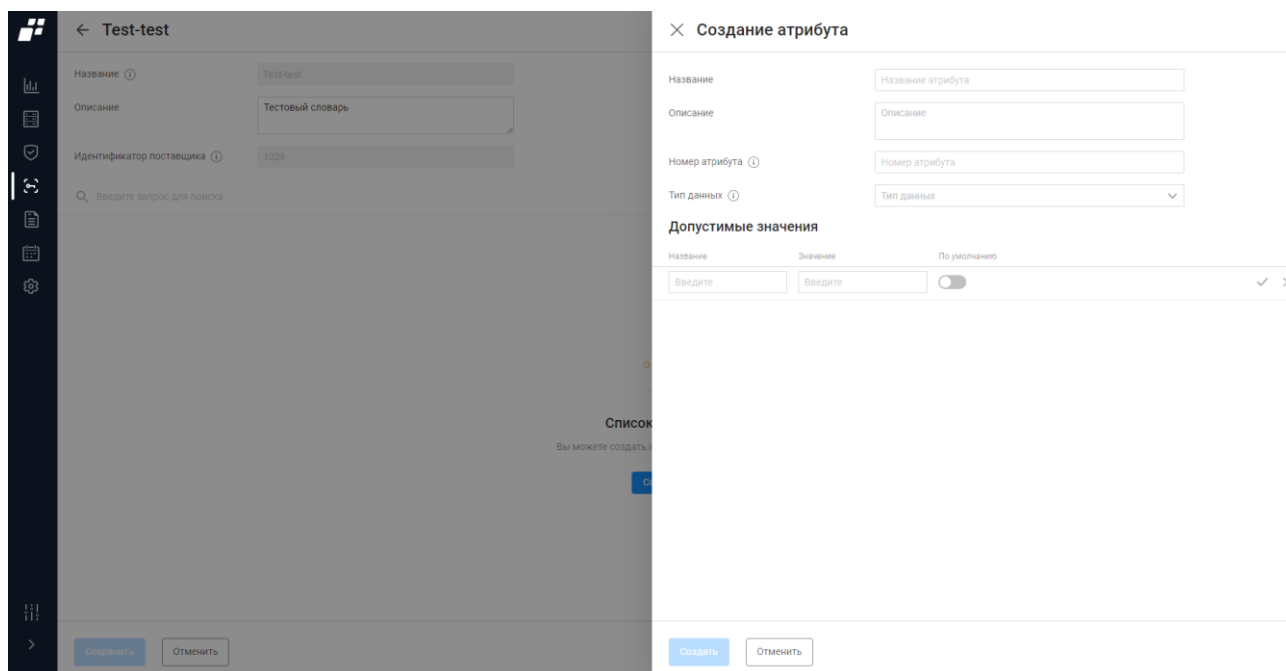




Рисунок 60 – Страница «Создание атрибута»

Откроется страница «Создание атрибута» (рис. 60). Состав и описание элементов страницы приведены в таблице 27.

Таблица 27 – Состав и описание элементов окна создания нового атрибута

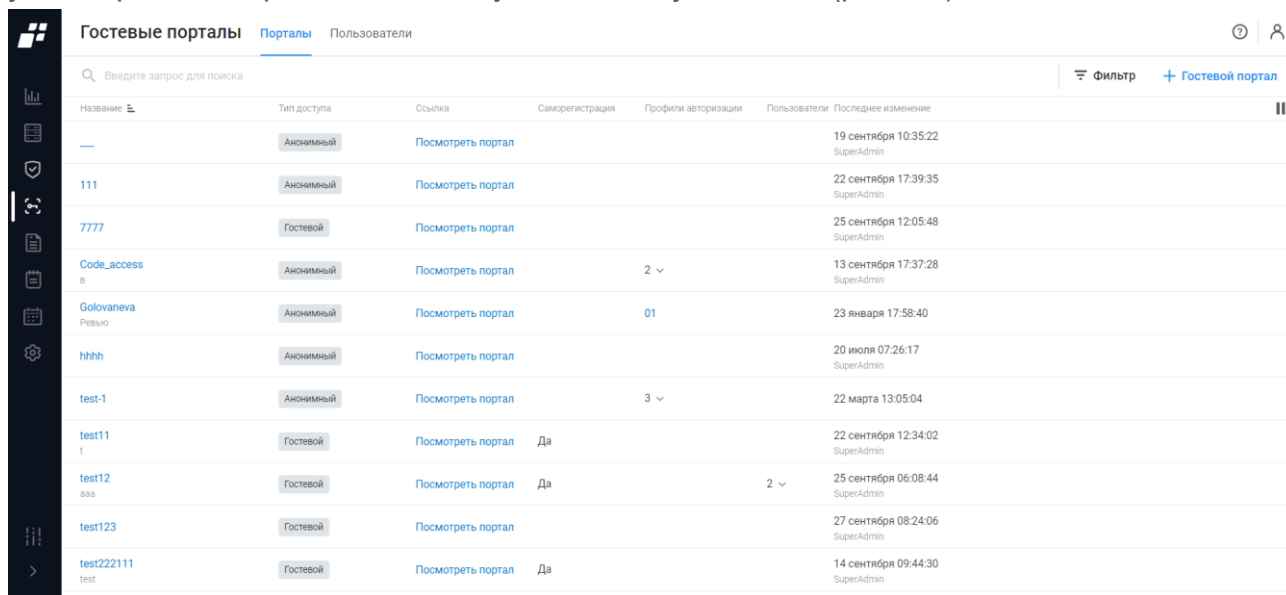
Элемент	Описание
Поле «Название»	Название атрибута
Поле «Описание»	Краткое описание атрибута
Поле «Номер атрибута»	Уникальный номер в рамках словаря
Поле «Тип данных»	Поле с раскрывающимся списком
Поле «Допустимые значения»	Список допустимых значений атрибутов словаря RADIUS, их описание и возможные принимаемые значения приведены в документе «RFC 2865 Remote Authentication Dial In User Service (RADIUS)». 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

Нажать кнопку «Создать». Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности создаваемого словаря.

При обнаружении незаполненных обязательных полей под полем появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Создать».

2.14 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 (рис. 61).



Гостевые порталы						
Порталы						
Пользователи						
Введите запрос для поиска						
Фильтр + Гостевой портал						
Название	Тип доступа	Ссылка	Саморегистрация	Профили авторизации	Пользователи	Последнее изменение
—	Анонимный	Посмотреть портал				19 сентября 10:35:22 SuperAdmin
111	Анонимный	Посмотреть портал				22 сентября 17:39:35 SuperAdmin
7777	Гостевой	Посмотреть портал				25 сентября 12:05:48 SuperAdmin
Code_access 8	Анонимный	Посмотреть портал		2		13 сентября 17:37:28 SuperAdmin
Golovaneva Резюме	Анонимный	Посмотреть портал		01		23 января 17:58:40
hhhh	Анонимный	Посмотреть портал				20 июля 07:26:17 SuperAdmin
test-1	Анонимный	Посмотреть портал		3		22 марта 13:05:04
test11 !	Гостевой	Посмотреть портал	Да			22 сентября 12:34:02 SuperAdmin
test12 aaa	Гостевой	Посмотреть портал	Да		2	25 сентября 06:08:44 SuperAdmin
test123	Гостевой	Посмотреть портал				27 сентября 08:24:06 SuperAdmin
test222111 test	Гостевой	Посмотреть портал	Да			14 сентября 09:44:30 SuperAdmin

Рисунок 61 – Подраздел «Гостевой портал»

Страница состоит из вкладок:




- «Порталы»;
- «Пользователи»

2.14.1 Вкладка «Порталы»

На странице список созданных гостевых порталов реализован в виде таблицы (см. рис. 61). Для каждой записи таблицы отображаются данные:

- название – является ссылкой, при переходе по которой открывается окно редактирования настроек гостевого портала;
- тип доступа;
- ссылка на страницу гостевого портала;
- профили авторизации. Раскрывающийся список профилей, которые являются ссылками.
- дата изменения гостевого портала.

Над таблицей располагаются:

- поле поиска ( Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Гостевой портал» ( Гостевой портал);
- кнопка «Фильтр» ( Фильтр) для фильтрации списка гостевых порталов;

— кнопка «Колонки» () для изменения отображения колонок на странице.


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

— кнопка «Создать копию» ( Создать копию);

— кнопка «Удалить» ( Удалить).

2.14.1.1 Создание нового 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» ( Гостевой портал). Откроется страница создания гостевого портала, приведенная на рис. 62. Состав и описание элементов страницы приведены в таблице 28.
- 2) Заполнить поля страницы соответствующими данными.

← Создание гостевого портала

Название

Описание

Настройки портала

Тип доступа ⓘ Анонимный Сетевые пользователи

Политика использования сети ☒

Текст политики

Брендирование портала ☒

Логотип ⓘ или перетащите файл сюда

Задний фон ⓘ или перетащите файл сюда

Корпоративный цвет







Требовать код доступа ☒

Код доступа

Рисунок 62 – Страница создания гостевого портала

Таблица 28 – Состав и описание элементов страницы создания нового гостевого портала


Элемент		Описание
Поле «Название»		Текстовое поле для ввода названия гостевого портала
Поле «Описание»		Текстовое поле для ввода описания гостевого портала
Группа полей «Настройки портала»		
Поле доступа	«Тип»	Переключатель: — «Анонимный»; — «Сетевой пользователь»


Элемент	Описание
Поле «Политика использования сети»	Переключатель: <ul style="list-style-type: none"> — «Активен» () – политика использования (лицензионное соглашение) активирована. При активации появляется поле «Текст политики»; — «Неактивен» () – политика использования (лицензионное соглашение) не активирована. По умолчанию установлено положение «Неактивен»
Поле «Текст политики»	Содержит кнопку «Добавить» при нажатии на которую открывается окно для добавления текста политики
Поле «Брендирование портала»	Переключатель: <ul style="list-style-type: none"> — «Активен» () – позволяет настроить внешний вид портала. При активации появляются дополнительные поля; — «Неактивен» () – отключает дополнительные поля для настройки внешнего вида гостевого портала. По умолчанию установлено положение «Неактивен»
Поле «Логотип»	Позволяет загрузить логотип портала. Рекомендуемое разрешение: 200x160px. Поддерживаемые форматы: png, svg, jpeg. Максимальный размер: 5 Мб
Поле «Задний фон»	Позволяет загрузить задний фон портала в виде картинки. Рекомендуемый размер 1920x1080px. Поддерживаемые форматы: png, jpeg. Максимальный размер: 5 Мб
Поле «Корпоративный цвет»	Цветовая шкала для выбора корпоративного цвета портала
Поле «Требовать код доступа»	Переключатель: <ul style="list-style-type: none"> — «Активен» () . При активации появляется поле «Код доступа»; — «Неактивен» () . По умолчанию установлено положение «Неактивен»
Поле «Код доступа»	Поле для ввода кода из буквенно-цифровых символов и знаков. Код можно сгенерировать при помощи кнопки «Сгенерировать»
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

3) Нажать кнопку «Создать».

Автоматически запускается процесс проверки заполнения всех обязательных полей и уникальности добавляемого гостевого портала.

При обнаружении незаполненных полей под полем появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить поля страницы и повторно нажать кнопку «Создать».

 После создания гостевого портала автоматически создается группа конечных точек, содержащая имя портала, и группа «Сетевые пользователи» (при выборе типа доступа «Сетевые пользователи»).

 При удалении гостевого портала автоматически удаляется группа конечных точек и группа сетевых пользователей, связанные с удаляемой сущностью.

Для редактирования существующего гостевого портала пользователю необходимо сделать следующее:

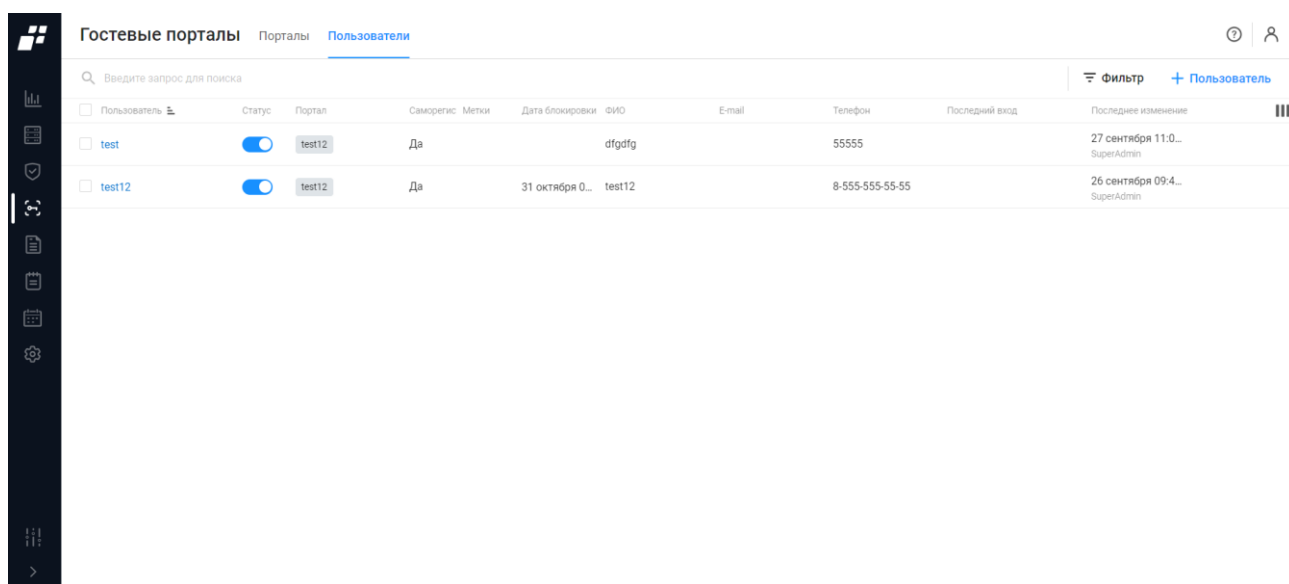
- 1) Нажать на название гостевого портала, который необходимо изменить.
- 2) Откроется страница редактирования гостевого портала (рис. 62).
- 3) Отредактировать необходимые поля.
- 4) Нажать кнопку «Сохранить».

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

Настройка гостевого портала приведена в приложении В.

2.14.2 Вкладка «Пользователи»

На странице список пользователей гостевых порталов реализован в виде таблицы (рис. 63).







Пользователь	Статус	Портал	Саморегис.	Метки	Дата блокировки	ФИО	E-mail	Телефон	Последний вход	Последнее изменение
test	<input checked="" type="checkbox"/>	test12	Да			dfgdfg		55555		27 сентября 11:0... SuperAdmin
test12	<input checked="" type="checkbox"/>	test12	Да		31 октября 0...	test12		8-555-555-55-55		26 сентября 09:4... SuperAdmin

Рисунок 63 – Вкладка «Пользователи»





Для каждой записи таблицы отображаются данные:

- пользователь – является ссылкой, при переходе по которой открывается окно для редактирования данных пользователя;
- статус – переключатель:
 - « ☒ » – пользователь активен;
 - « ☐ » – пользователь неактивен.
- портал – название портала, к которому у пользователя есть доступ;
- саморегистрация. Значение «Да» в случае, если регистрация осуществлялась пользователем самостоятельно. В противном случае, если пользователь создавался в комплексе, значение остается пустым;
- метки;
- дата блокировки учетной записи пользователя;
- Ф.И.О. пользователя;
- e-mail пользователя;
- телефон пользователя;
- дата последнего входа;
- дата последнего изменения;
- компания, где работает пользователь;
- комментарий.




Над таблицей располагаются:

- поле поиска ( Введите запрос для поиска) для поиска искомой записи в списке;
- кнопка «Пользователь» ( Пользователь);
- кнопка «Фильтр» ( Фильтр) для фильтрации списка пользователей;
- кнопка «Колонки» () для изменения отображения колонок на странице.

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

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

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

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

2.14.2.1 Создание пользователя гостевого портала

Для создания пользователя необходимо выполнить следующие действия:



- 1) Нажать на странице «Пользователи» кнопку «Пользователь» ([+ Пользователь](#)).
- 2) Откроется страница «Создание пользователя портала» (рис. 64). Состав и описание полей страницы приведены в таблице 29.

← Создание пользователя портала

Статус	<input checked="" type="checkbox"/>
Портал ^①	<input type="text" value="Портал"/>
Пользователь ^①	<input type="text" value="Пользователь"/>
Описание	<input type="text" value="Описание"/>
Пароль	<input type="password" value="Пароль"/>
Метки	Выбрать метки
ФИО	<input type="text" value="ФИО"/>
Компания	<input type="text" value="Компания"/>
E-mail	<input type="text" value="E-mail"/>
Телефон	<input type="text" value="Телефон"/>
Комментарий	<input type="text" value="Комментарий"/>
Период действия учетной записи	<input checked="" type="button" value="Бессрочно"/> <input type="button" value="Задать"/>
<input type="button" value="Создать"/> <input type="button" value="Отменить"/>	

Рисунок 64 – Страница «Создание пользователя портала»

Таблица 29 – Состав и описание полей страницы создания пользователей

Поле	Описание
Поле «Статус»	Переключатель: <ul style="list-style-type: none"> — «Активен» () – пользователю разрешен доступ к portalу; — «Неактивен» () – пользователю запрещен доступ к portalу. По умолчанию переключатель установлен в положение «Активен»
Поле «Портал»	Раскрывающийся список доступных порталов
Поле «Пользователь»	Текстовое поле для ввода логина пользователя. Параметры ввода текста: от 1 до 32 символов. Дополнительные символы: буквы латинского алфавита, цифры, «_», «-»
Поле «Описание»	Текстовое поле для ввода описания пользователя. Параметры ввода текста: от 1 до 250 любых символов
Поле «Пароль»	Текстовое поле для ввода пароля пользователя
Поле «Метки»	Ссылка для выбора меток
Поле «Email»	В поле указывается почтовый адрес пользователя для привязки к почте аккаунта пользователя ПК
Поле «ФИО»	Текстовое поле для ввода фамилии, имени и отчества пользователя. Параметры ввода текста: от 1 до 250 любых символов
Поле «Компания»	Текстовое поле для ввода названия компании, где работает пользователь. Параметры ввода текста: от 1 до 250 любых символов
Поле «Телефон»	Текстовое поле для ввода номера телефона пользователя. Параметры ввода текста: от 1 до 50 символов. Допустимые символы: цифры и символы «-», «+», «()»
Поле «Комментарий»	Текстовое поле для ввода комментария. Параметры ввода текста: от 1 до 250 любых символов
Поле «Период действия учетной записи»	Переключатель: <ul style="list-style-type: none"> — «Бессрочно» – учетная запись сетевого пользователя действует на устройстве без ограничений; — «Задать» – учетная запись сетевого пользователя действует на устройстве определенный период времени. При выборе «Задать» появляется поле «Дата блокировки»
Элементы управления	

Поле	Описание
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

3) Заполнить форму необходимыми параметрами.

4) Нажать кнопку «Создать».

Автоматически запускается процесс проверки заполненности всех обязательных полей и уникальности добавляемого пользователя по имени.

При обнаружении незаполненных обязательных полей под полем появится сообщение красного цвета: «Обязательное поле». Пользователю необходимо корректно заполнить поля окна и повторно нажать кнопку «Создать».

Перечень сокращений

AAA	—	Authentication, Authorization, Accounting
ACL	—	Access Control List
AD	—	Active Directory
ASCII	—	American Standard Code for Information Interchange
AUP	—	Acceptable Use Policy
CN	—	Common Name
CoA	—	Change of Authorization
DNS	—	Domain Name System
EAP	—	Extensible Authentication Protocol
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
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
TACACS+	—	Terminal Access Controller Access Control System plus
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
Ф.И.О.	—	Фамилия, имя, отчество
ЦС	—	Центр сертификации
ЭВМ	—	Электронно–вычислительная машина


Приложение А

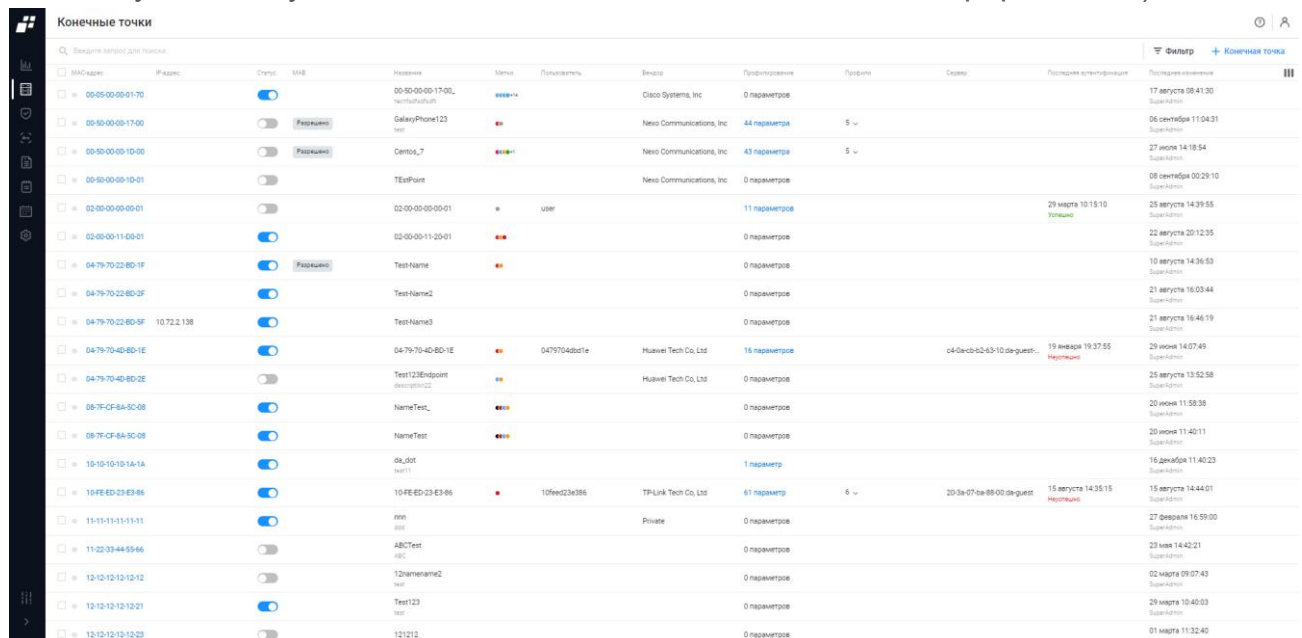
Рекомендуемая последовательность действий для настройки типового сценария взаимодействия с использованием протокола RADIUS

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:
 - конечные точки/группы конечных точек, добавленные в БД комплекса;
 - локальные пользователи, созданные в БД комплекса;
 - LDAP;
 - домен;
 - сертификаты.

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. 65);
- нажать кнопку « Конечная точка»;
- заполнить поля страницы создания конечной точки сети необходимыми параметрами (рис. 66) (более подробно о конечной точке сети написано в документе «Руководство пользователя. Часть 1. Администрирование»).



MAC-адрес	Имя	Статус	Имя	Вендор	Параметры	Профиль	Сервис	Последняя аутентификация	Последнее событие
00:05:00:00:01:70		Включен	00:05:00:00:01:70-00, Huawei	Cisco Systems, Inc	0 параметров			17 августа 08:41:30	Судитесь
00:05:00:00:01:70		Включен	GalaxyPhone123	Nexo Communications, Inc	44 параметра	5		06 сентября 11:04:31	Судитесь
00:05:00:00:01:70		Включен	Centos_7	Nexo Communications, Inc	43 параметра	5		27 июня 14:18:54	Судитесь
00:05:00:00:01:70		Включен	TEKPoint	Nexo Communications, Inc	0 параметров			08 сентября 00:28:10	Судитесь
02:00:00:00:00:01		Включен	02:00:00:00:00:01		11 параметров			29 марта 10:15:10	Судитесь
02:00:00:00:00:01		Включен	02:00:00:00:00:01		0 параметров			22 августа 20:12:35	Судитесь
04:79:70:22:8D:1F		Включен	TestName1		0 параметров			10 августа 14:36:53	Судитесь
04:79:70:22:8D:2F		Включен	TestName2		0 параметров			21 августа 16:03:44	Судитесь
04:79:70:22:8D:5F	10.72.2.138	Включен	TestName3		0 параметров			21 августа 16:46:19	Судитесь
04:79:70:4D:8D:1E		Включен	04:79:70:4D:8D:1E	Huawei Tech Co, Ltd	16 параметров		04:0a:cb:02:63:10:0a:quest...	19 января 19:37:55	Судитесь
04:79:70:4D:8D:2E		Включен	Test123Endpoint	Huawei Tech Co, Ltd	0 параметров			25 августа 13:52:58	Судитесь
08:7F:CF:8A:5C:08		Включен	NameTest_		0 параметров			20 июня 11:58:36	Судитесь
08:7F:CF:8A:5C:08		Включен	NameTest		0 параметров			20 июня 11:40:11	Судитесь
10:10:10:10:1A:1A		Включен	0a_00t		1 параметр			16 декабря 11:40:23	Судитесь
10:FE:ED:C3:E3:86		Включен	10:FE:ED:C3:E3:86	TP-Link Tech Co, Ltd	61 параметр	6	20:3a:07:0a:88:00:0a:quest...	15 августа 14:35:15	Судитесь
11:15:15:15:15:15		Включен	mm	Private	0 параметров			27 февраля 16:59:00	Судитесь
11:22:33:44:55:66		Включен	ABCTest		0 параметров			23 мая 14:42:21	Судитесь
12:12:12:12:12:12		Включен	12чипелам2		0 параметров			02 марта 09:07:43	Судитесь
12:12:12:12:12:21		Включен	Test123		0 параметров			29 марта 10:40:03	Судитесь
12:12:12:12:12:23		Включен	121212		0 параметров			01 марта 11:32:40	Судитесь

Рисунок 65 – Конечные точки как источник данных

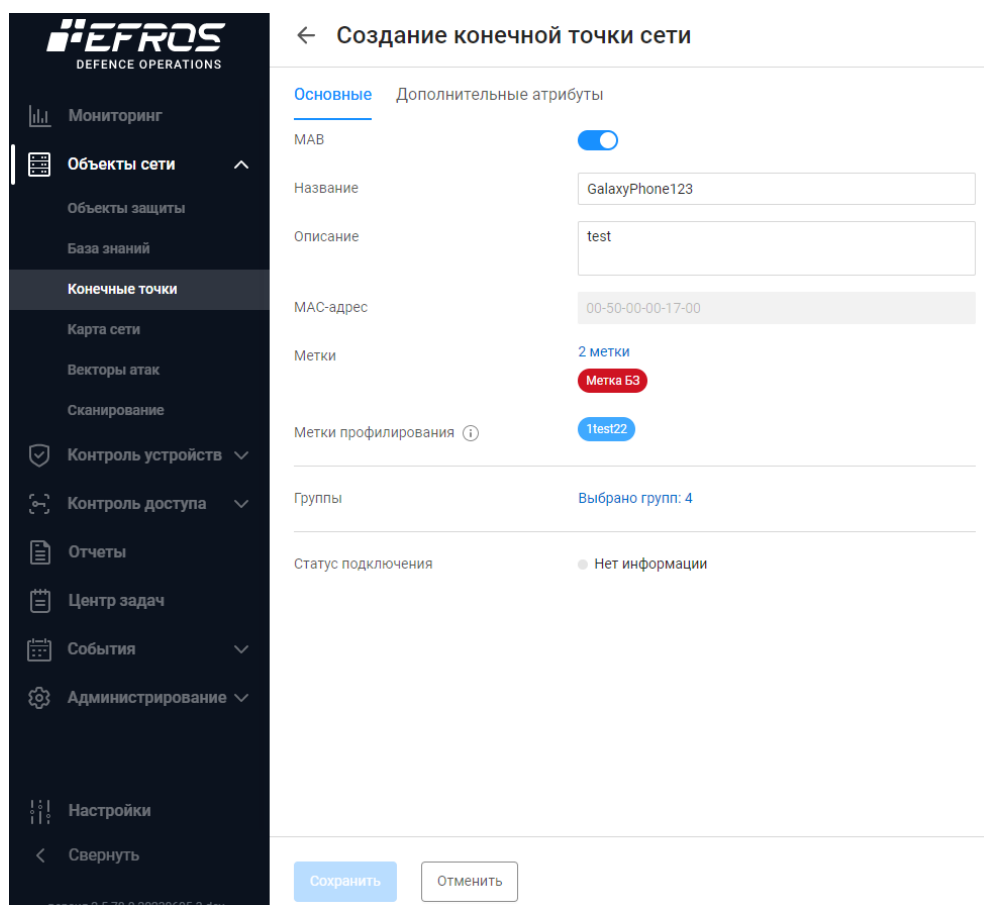


Рисунок 66 – Создание конечной точки

Если в качестве источника выбраны локальные пользователи, то необходимо сделать следующее:

- перейти в раздел «Контроль доступа», подраздел «Сетевые пользователи», вкладка «Пользователи»;
- нажать кнопку «**+ Пользователь**» (рис. 67);
- заполнить поля страницы необходимыми параметрами и нажать кнопку «Создать» (более подробно о создании локального сетевого пользователя написано в п.п. 2.5.1.1) (рис. 68).

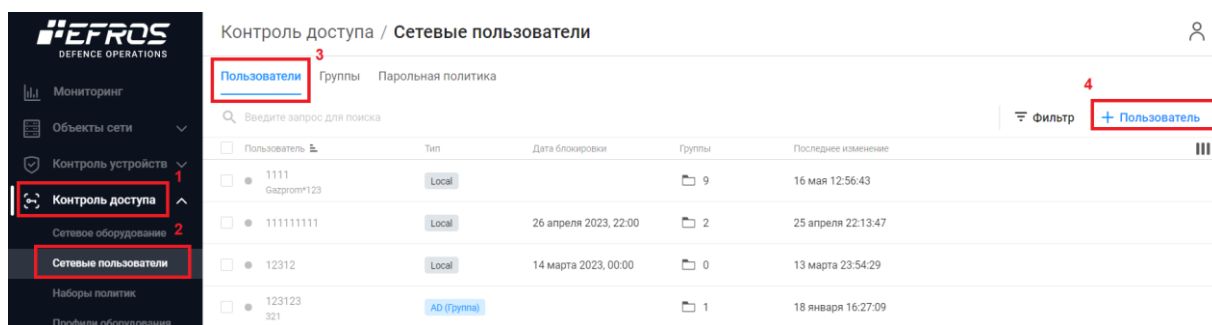


Рисунок 67 – Источник данных – локальный сетевой пользователь

← Создание сетевого пользователя

Статус ☒

Тип ☒ Пользователь ☐ Пользователь LDAP ☐ Группа LDAP

Пользователь

Описание

Пароль

Период действия учетной записи ☐ Бессрочно ☒ Задать

Дата блокировки

Привилегированный режим

Группы пользователей [Выбрано групп: 1](#)

Рисунок 68 – 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. 69);
- нажать кнопку «[+ Соединение](#)»;
- заполнить поля страницы соответствующими параметрами и нажать кнопку «Создать» (более подробно об LDAP соединении написано в документе «Руководство пользователя. Часть 1. Администрирование») (рис. 70);
- перейти в раздел «Контроль доступа», подраздел «Сетевые пользователи», вкладка «Пользователи»;
- создать сетевого пользователя LDAP (более подробно о создании пользователя LDAP написано в п.п. 2.5.1.1) (рис. 71).

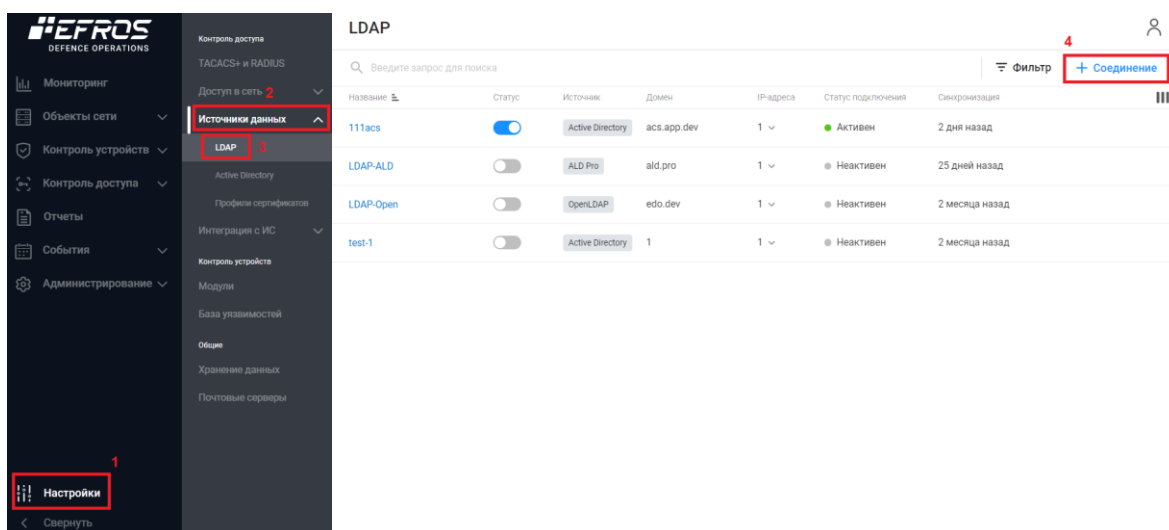


Рисунок 69 – Источник данных – служба каталогов LDAP

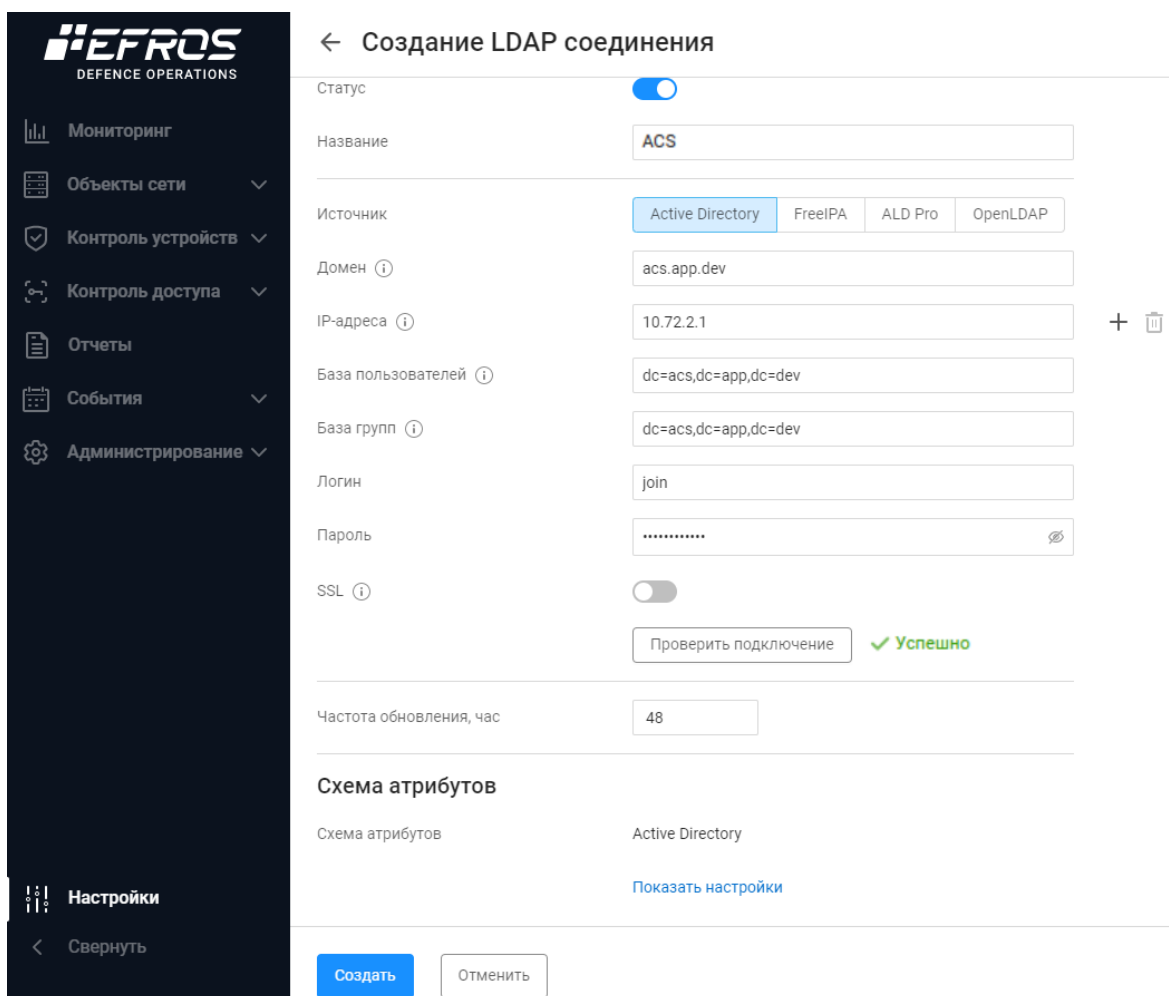


Рисунок 70 – Создание нового соединения

← Создание сетевого пользователя

Статус ☒

Тип Пользователь Пользователь LDAP Группа LDAP

Пользователь

Описание

Период действия учетной записи Бессрочно Задать

Дата блокировки

Привилегированный режим Не задано

Создать Отменить

Рисунок 71 – Создание сетевого пользователя LDAP

Если в качестве источника выбран домен, то необходимо сделать следующее:

- перейти в раздел «Настройки», подраздел «Источники данных», вкладка «Active Directory»;
- нажать кнопку «**+ Соединение**» (рис. 72);
- заполнить поля страницы необходимыми параметрами и нажать кнопку «Создать» (более подробно о создании нового соединения описано в документе «Руководство пользователя. Часть 1. Администрирование») (рис. 73).

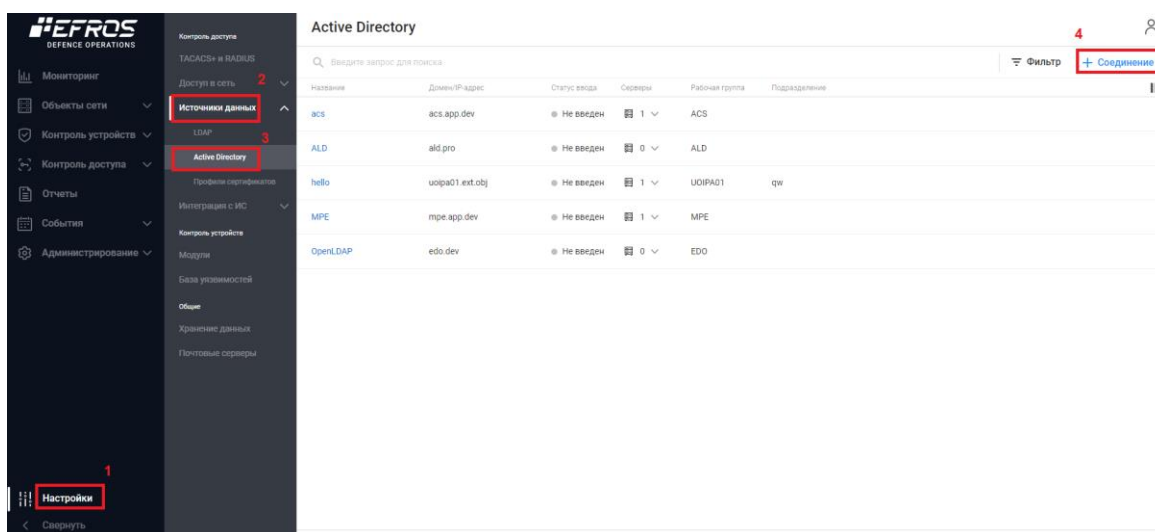


Рисунок 72 – Источник данных Active Directory

← Создание Active Directory соединения

Название	<input type="text" value="Название соединения"/>
Домен / IP-адрес	<input type="text" value="Домен / IP-адрес"/>
Подразделение (OU)	<input type="text" value="Название подразделения"/>
Серверы аутентификации	<input type="text" value="IP-адрес или DNS имя сервера"/> +
Альтернативное имя группы Имя рабочей группы (NetBIOS)	<input type="checkbox"/>

Ввод в домен

Для активации ввода в домен необходимо заполнить «Название» и «Домен / IP-адрес», а после нажать кнопку «Создать»

Логин	<input type="text" value="domain\username"/>
Пароль	<input type="password" value="Пароль"/>
	<input type="button" value="Ввести в домен"/>

Для активации выбора "Группы домена" необходимо ввести в домен

Группы домена	<input type="text" value="Выберите группу"/>
---------------	--

Рисунок 73 – 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 (более подробно о выпуске клиентского сертификата написано в приложении Б);
- установить корневой и клиентский сертификаты на устройство.

Более подробно о сертификатах написано в документе «Руководство пользователя. Часть 1. Администрирование».

2) Создать профиль сетевого оборудования⁴:

- перейти в раздел «Контроль доступа», подраздел «Профили оборудования»;
- нажать кнопку «**+ Профиль оборудования**» (рис. 74);

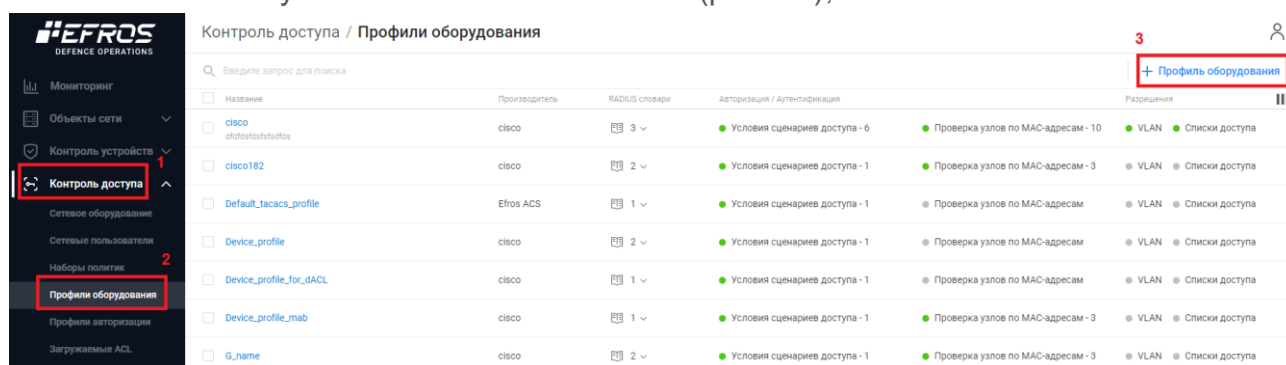


Рисунок 74 – Создание профиля сетевого оборудования

- заполнить поля страницы необходимыми параметрами (более подробно о создании профиля написано в п. 2.7.1) (рис. 75).

⁴ Профиль сетевого оборудования необходим для назначения общих правил аутентификации и авторизации на оборудовании для сетевых пользователей

← Создание профиля сетевого оборудования

Название: Device_profile

Описание:

Производитель: cisco

Словари RADIUS: Выбрано: 2 (Cisco, Radius)

Аутентификация / Авторизация

Условия сценариев доступа

Проводная аутентификация по MAC-адресам (Wired MAB)

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)

Radius / Service-Type = Administrative-User

Radius / NAS-Port-Type = Virtual

Удаленный доступ (VPN)

Проверка узлов по MAC-адресам (MAB)

Разрешения

Назначение VLAN

Назначение списков доступа (ACL)

Change of Authorization

CoA: Отсутствует, RADIUS

Перенаправление

Тип: Не перенаправлять, Динамический URL

Сохранить Отменить

Рисунок 75 – 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 требуемые изменения.
- Рекомендуется активировать следующие словари:
- RADIUS;
 - Gazinformservice;
 - Словарь, соответствующий названию производителя оборудования.

3) Создать профиль авторизации «Доступ в сеть» (для оборудования,

- выбрать на странице «Профиль авторизации» вкладку «Доступ в сеть»;
- нажать кнопку «**+ Профиль**» (рис. 76);



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

← Создание профиля авторизации доступа в сеть

Название: auth_mab

Описание: Введите описание

Тип доступа: Разрешен / Запрещен

Профиль сетевого оборудования: Device_profile_mab

Основные настройки

Загружаемый ACL: ☐

ACL: ☐

ACL контроллера точек доступа: ☐

Веб-перенадресация: ☐

VLAN: ☐

Настройка дополнительных атрибутов

Выберите атрибут = Введите значение +

Передаваемые параметры

Показать

Сохранить Отменить

Рисунок 77 – Создание профиля авторизации доступа в сеть

- 4) Создать требуемый набор политик доступа (более подробно о наборе политик написано в подразделе 2.6). 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. 78);

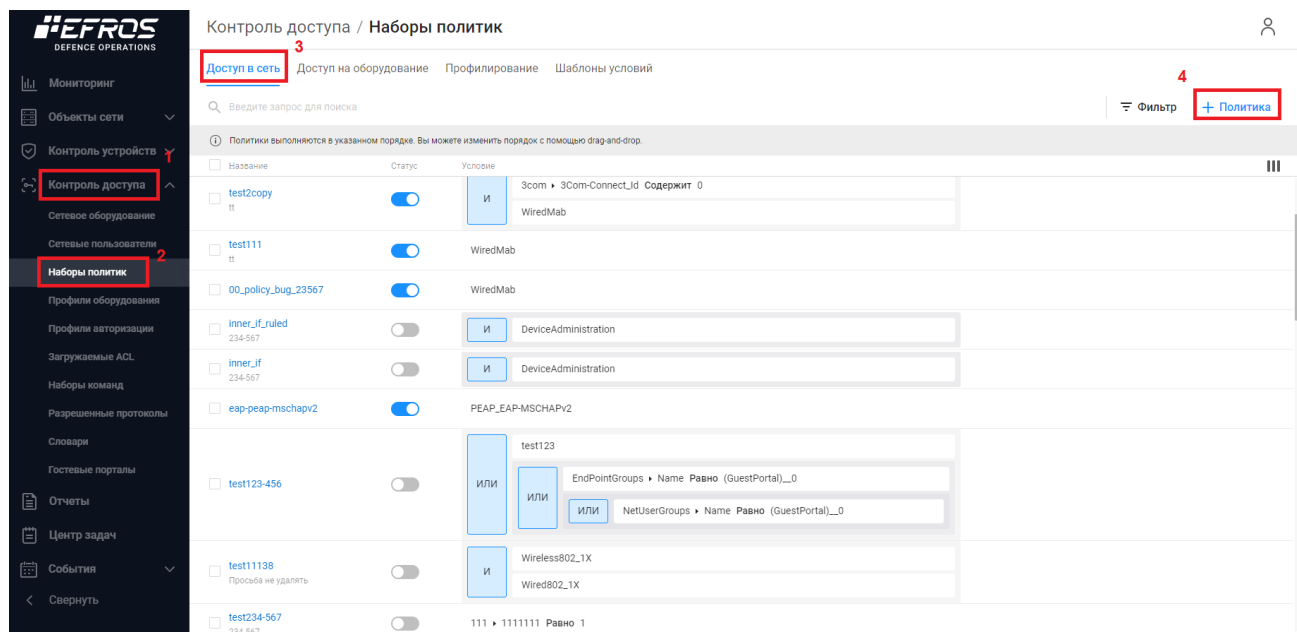


Рисунок 78 – Создание набора политик «Доступ в сеть»

— на вкладке «Настройки» создать условия срабатывания политики⁵ или выбрать условие из шаблона условий (рис. 79);



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

⁵ Это условия, которым в первую очередь должно соответствовать устройство при попытке получения доступа в сеть



- 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».

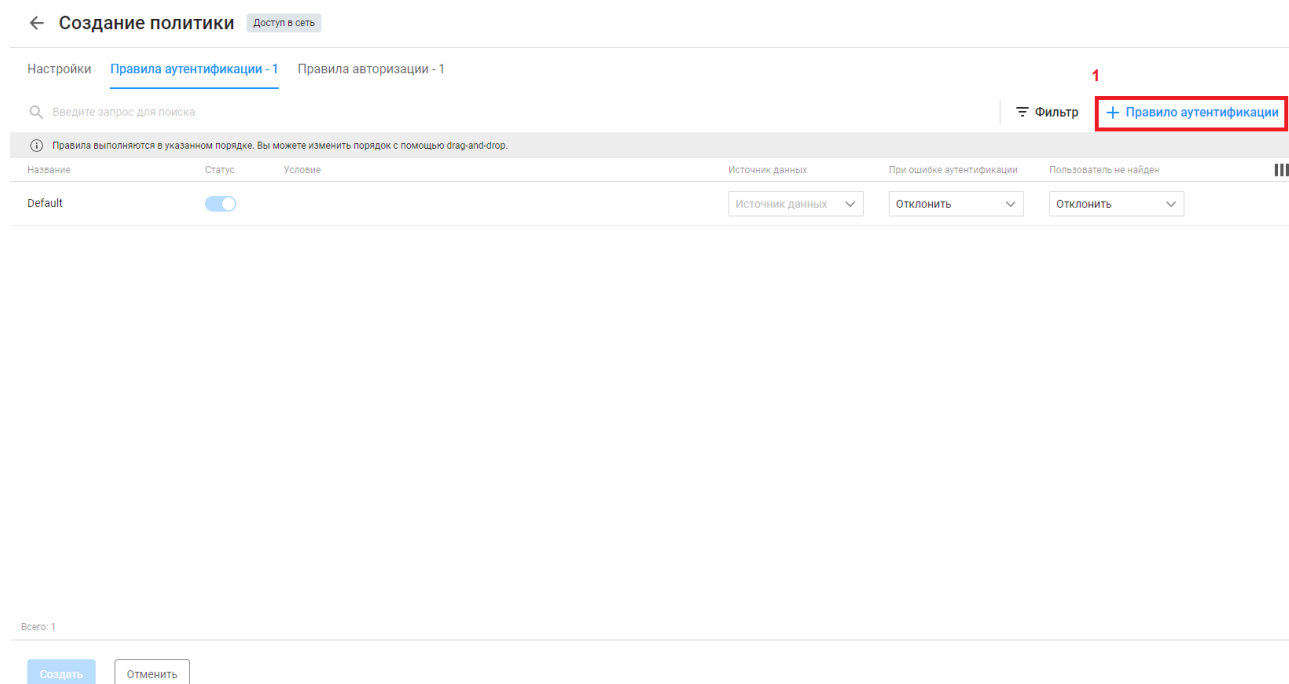


Рисунок 80 – Создание правила аутентификации

— нажать кнопку «**+ Правило аутентификации**» (см. рис. 80). Заполнить поля необходимыми данными (рис. 81):

- 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 81 – Создание правила аутентификации

- выбрать созданный ранее профиль авторизации.

Версия ПК «Efros DO» – 2.7

Рисунок 82 – Создание правила авторизации

- на вкладке нажать кнопку «[+ Правило авторизации](#)» (см. рис. 82). Заполнить поля необходимыми данными (рис. 83):
- 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.*

← Создание правила авторизации Доступ в сеть

Статус ☒

Название

Действия при выполнении условий

Профиль авторизации

Условия срабатывания правила

И или НЕ

Добавить

НЕ Выберите атрибут Равно Введите значение

Перенесите сюда условие

Введите запрос для поиска

Все шаблоны условий

11111113234e34324355555555555553455435678465755555

1

123

20230505

aaa2

aaa21

aaa212

DeviceAdministration

DeviceAdministration

dsds

dsds

IF

IF

inner_IF

Irina

new

key

New1

New

Всего: 28

Создать

Отменить

Рисунок 83 – Создание правила авторизации

- нажать кнопку «Сохранить».
- 5) Перейти в раздел «Контроль доступа», подраздел «Сетевое оборудование».
- Создать сетевое оборудование. Для этого необходимо:
- на вкладке «Устройства» нажать кнопку «[+ Устройство](#)» (рис. 84);
 - заполнить поля необходимыми данными (указать профиль сетевого оборудования, созданный в шаге 2) (рис. 85);
 - указать RADIUS Shared key.

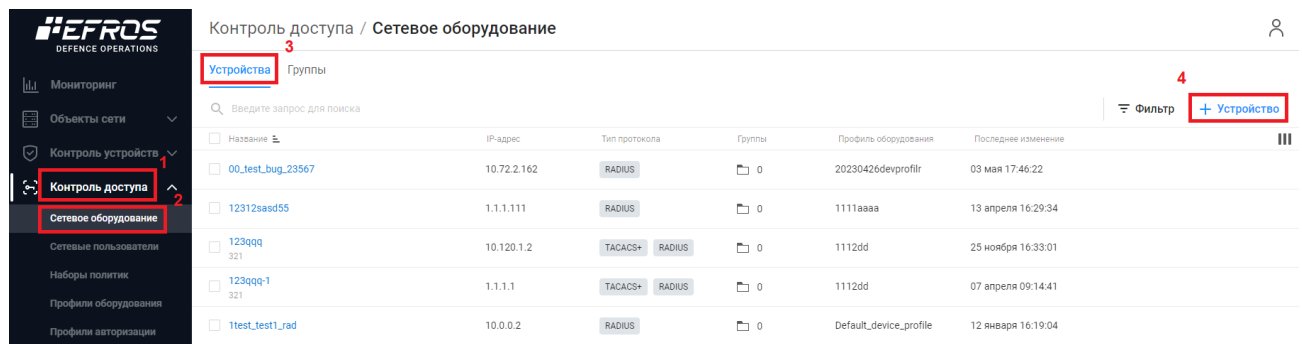


Рисунок 84 – Создание устройства

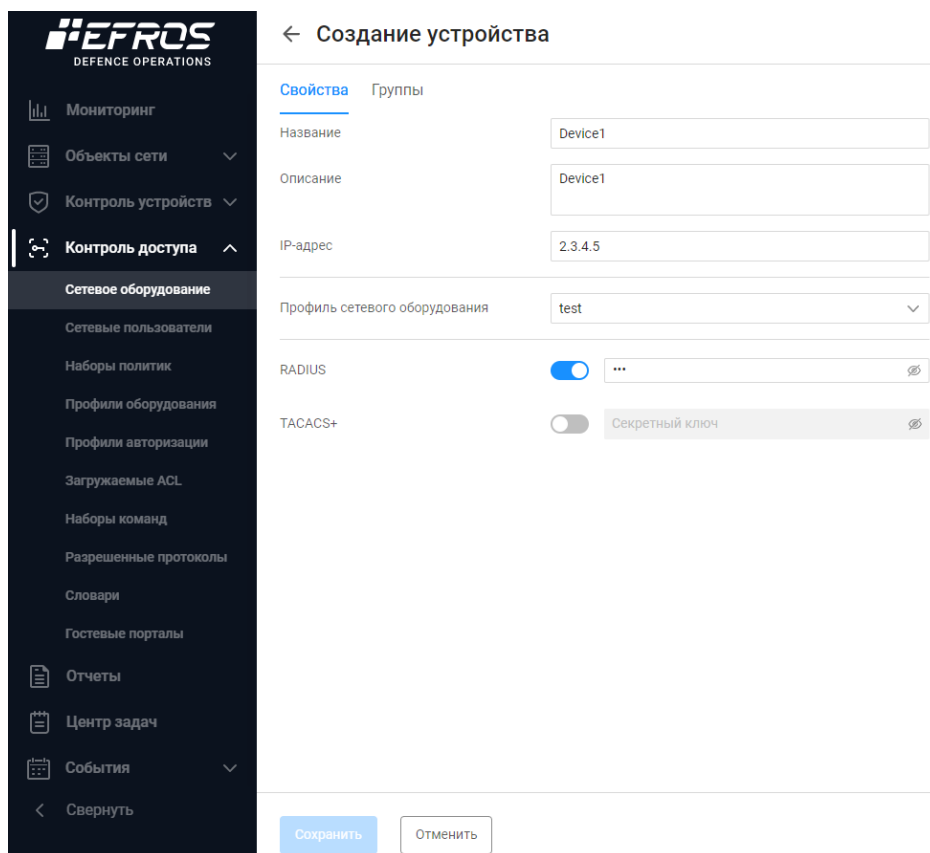


Рисунок 85 – Создание устройства

Таблица 30 – Краткая последовательность действий для настройки типового сценария взаимодействия с RADIUS

№ п/п	Действие	Описано в разделе документа
1	Создать/добавить/подключить необходимые источники данных ⁶ : <ul style="list-style-type: none">• конечные точки;• локальные сетевые пользователи/группы;• LDAP;• домен;	
		-
		2.5.1.1
		-
		-

	• сертификаты	-
2	Создать профиль сетевого оборудования	2.7.1
3	Создать профиль авторизации	2.8
4.1	Создать набор политик	2.6.1.1
4.2	Создать правила аутентификации	2.6.1.2
4.3	Создать правила авторизации	2.6.1.3
5	Создать сетевое оборудование	2.4.1.1



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

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

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:
 - локальные пользователи, созданные в БД комплекса;
 - пользователи LDAP;
 - домен (как пользователи, так и устройства).

Если в качестве источника выбраны локальные пользователи, то необходимо сделать следующее:

- перейти в раздел «Контроль доступа», подраздел «Сетевые пользователи»;
- выбрать вкладку «Пользователи»;
- нажать кнопку «+ Пользователь» (рис. 87);
- заполнить поля страницы необходимыми параметрами и нажать кнопку «Создать» (рис. 88) (более подробно о создании локального сетевого пользователя написано в п.п. 2.5.1.1).

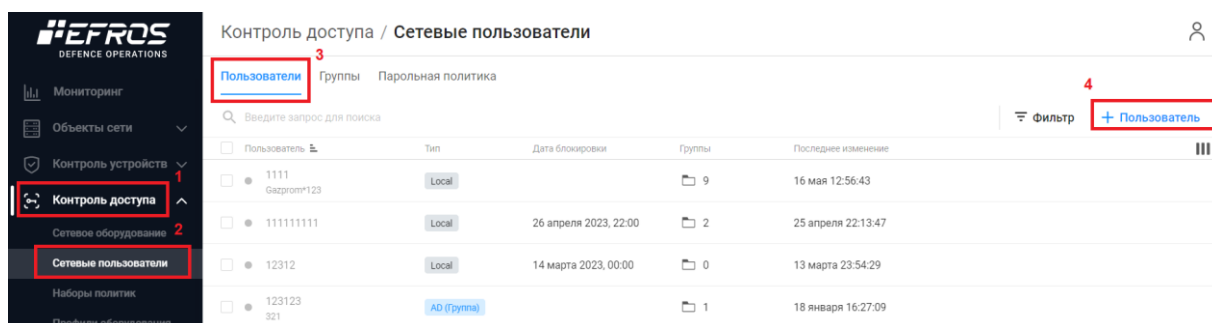


Рисунок 87 – Источник данных – локальный сетевой пользователь

← Создание сетевого пользователя

Статус ☒

Тип ☒ Пользователь ☐ Пользователь LDAP ☐ Группа LDAP

Пользователь

Описание

Пароль

Период действия учетной записи ☐ Бессрочно ☒ Задать

Дата блокировки

Привилегированный режим

Группы пользователей [Выбрано групп: 1](#)

Рисунок 88 – 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. 89);
- нажать кнопку «[+ Соединение](#)»;
- заполнить поля страницы соответствующими параметрами и нажать кнопку «Создать» (более подробно об LDAP соединении написано в документе «Руководство пользователя. Часть 1. Администрирование») (рис. 90);
- перейти в раздел «Контроль доступа», подраздел «Сетевые пользователи», вкладка «Пользователи»;
- создать пользователя LDAP (более подробно о создании пользователя LDAP написано в п.п. 2.5.1.1) (рис. 91).

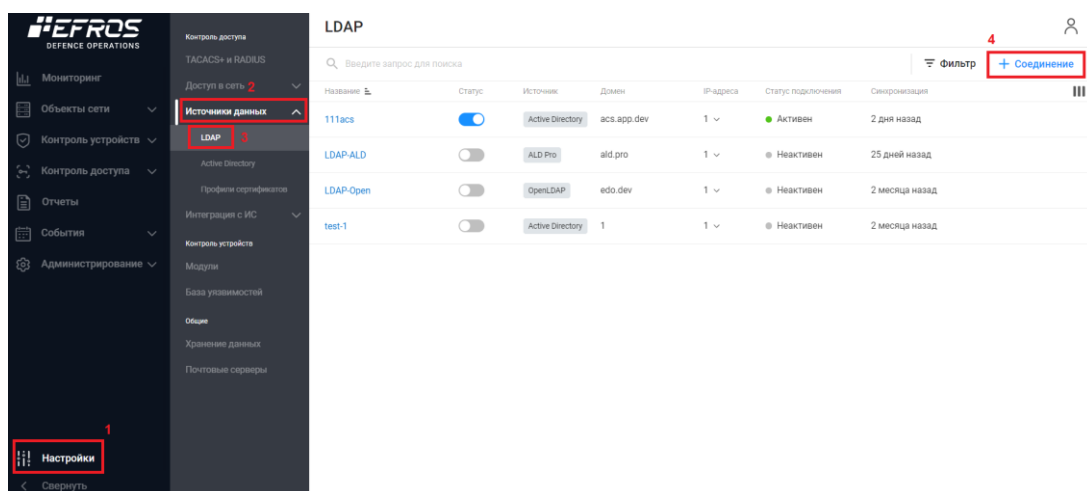


Рисунок 89 – Источник данных – служба каталогов LDAP

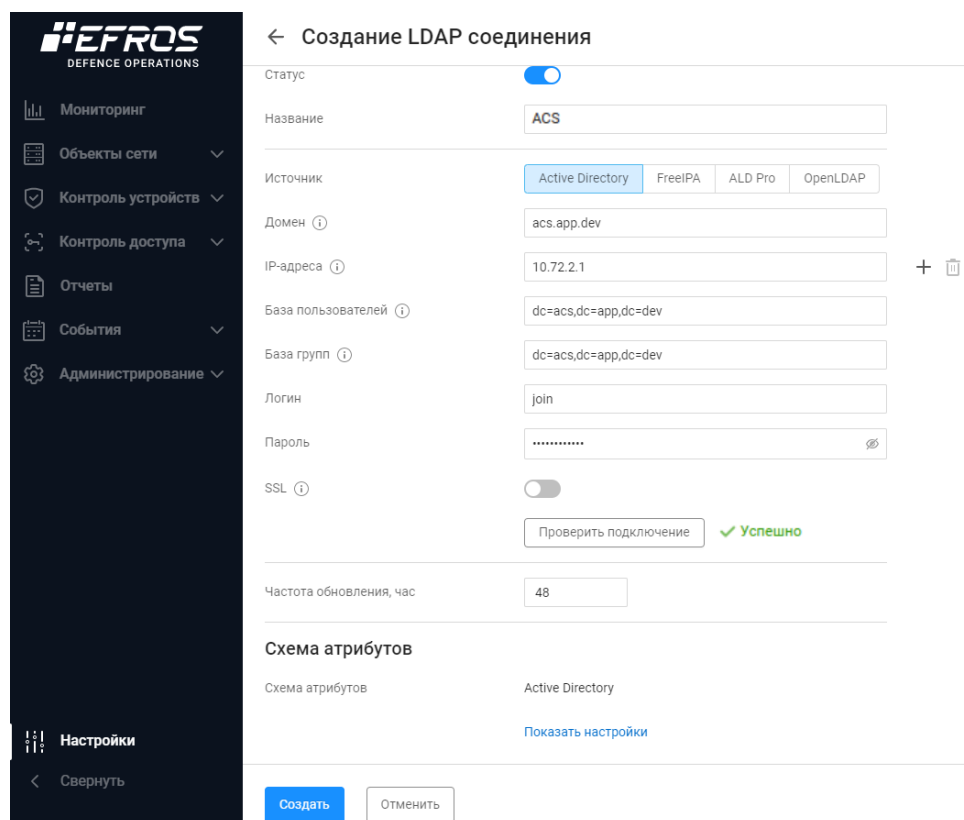


Рисунок 90 – Создание нового соединения

← Создание сетевого пользователя

Статус ☒

Тип Пользователь Пользователь LDAP Группа LDAP

Пользователь AaronAdams

Описание AaronAdams

Период действия учетной записи Бессрочно Задать

Дата блокировки 09 июня 2023, 12:00

Привилегированный режим Не задано

Создать Отменить

Рисунок 91 – Создание пользователя LDAP

Если в качестве источника выбран домен, то необходимо сделать следующее:

- перейти в раздел «Настройки», подраздел «Источники данных», вкладка «Active Directory»;
- нажать кнопку «+ Соединение» (рис. 92);
- заполнить поля страницы необходимыми параметрами и нажать кнопку «Создать» (более подробно о создании нового соединения описано в документе «Руководство пользователя. Часть 1. Администрирование») (рис. 93).

Active Directory

Введите запрос для поиска

Фильтр + Соединение

Имя	Домен/ИП-адрес	Статус ввода	Серверы	Рабочая группа	Подразделение
acs	acs.app.dev	Не введен	1	ACS	
ALD	ald.pro	Не введен	0	ALD	
hebo	uopad1.ext.obj	Не введен	1	UOPAD1	qn
MPE	mpe.app.dev	Не введен	1	MPE	
OpenLDAP	edo.dev	Не введен	0	EDO	

Рисунок 92 – Источник данных Active Directory

← Создание Active Directory соединения

Название: acs

Домен / IP-адрес: acs.app.dev

Подразделение (OU): Название подразделения

Серверы аутентификации: 10.72.2.1

Альтернативное имя группы / Имя рабочей группы (NetBIOS): ☐

Ввод в домен: ☒ Не введен

Логин: join

Пароль:

Ввести в домен

Для активации выбора "Группы домена", Вам необходимо ввести в домен

Группы домена: Выберите группу

Сохранить Отменить

Рисунок 93 – Создание Active Directory соединения

3) Создать список разрешенных протоколов для аутентификации:

— перейти в раздел «Контроль доступа», подраздел «Разрешенные протоколы» (рис. 94);

Контроль доступа / Разрешенные протоколы

Введите запрос для поиска

+ Список протоколов

Название	Протоколы
Default_Device_Admin	4
Разрешенные по умолчанию протоколы для администрирования...	
PAP_ASCI	1
просьба не использовать	

Рисунок 94 – Разрешенные протоколы

- на странице нажать кнопку «[+ Список протоколов](#)»;
- заполнить поля страницы необходимыми параметрами (рис. 95) (более подробно о создании списка протоколов написано в п. 2.11).

← Создание списка разрешенных протоколов

Название: PAP_ASCII

Описание:

Протоколы аутентификации ①

- ☒ PAP/ASCII
- ☐ CHAP
- ☐ MS-CHAPv1
- ☐ MS-CHAPv2

Создать Отменить

Рисунок 95 – Создание списка разрешенных протоколов

4) Создать набор команд:

- перейти в раздел «Контроль доступа», подраздел «Разрешенные протоколы» (рис. 96)

Контроль доступа / Наборы команд

Введите запрос для поиска

+ Набор команд

Название	Команды
111	2
23883_test	2
23883_test_2	2
DenyAllCommand Запретить все команды	1
new1	1
PermitAllCommand Разрешить все команды	1
test_00	2
test_01	2
test_02	2

Рисунок 96 – Набор команд

- на странице нажать кнопку «**+ Набор команд**»;
- заполнить поля страницы необходимыми параметрами (рис. 97) (более подробно о наборе команд написано в п. 2.10).

← Создание набора команд

1 Название test_00

2 Описание

3 Команды - 2

Действие	Команда	Аргументы
Permit Deny	show	version
Permit Deny	show	ip route
Permit Deny	Команда	Аргументы

Создать Отменить

Рисунок 97 – Набор 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. 98);

Контроль доступа / Профили оборудования

3 + Профиль оборудования

Название	Производитель	RADIUS словари	Авторизация / Аутентификация	Разрешения		
cisco	cisco	3	Условия сценариев доступа - 6	Проверка узлов по MAC-адресам - 10	VLAN	Списки доступа
cisco182	cisco	2	Условия сценариев доступа - 1	Проверка узлов по MAC-адресам - 3	VLAN	Списки доступа
Default_tacacs_profile	Efros ACS	1	Условия сценариев доступа - 1	Проверка узлов по MAC-адресам	VLAN	Списки доступа
Device_profile	cisco	2	Условия сценариев доступа - 1	Проверка узлов по MAC-адресам	VLAN	Списки доступа
Device_profile_for_dACL	cisco	1	Условия сценариев доступа - 1	Проверка узлов по MAC-адресам	VLAN	Списки доступа
Device_profile_mab	cisco	1	Условия сценариев доступа - 1	Проверка узлов по MAC-адресам - 3	VLAN	Списки доступа
G_name	cisco	2	Условия сценариев доступа - 1	Проверка узлов по MAC-адресам - 3	VLAN	Списки доступа

Рисунок 98 – Создание сетевого профиля оборудования

- заполнить поля страницы создания профиля сетевого оборудования необходимыми параметрами (рис. 99) (более подробно о профиле оборудования написано в п. 2.7.1).

← Создание профиля сетевого оборудования

Название: huawei

Описание:

Производитель: huawei

Словари RADIUS: Выбрано: 2

Аутентификация / Авторизация

Условия сценариев доступа

☐ Проводная аутентификация по MAC-адресам (Wired MAB)

☐ 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)

Radius / Service-Type = Administrative-User

Radius / NAS-Port-Type = Virtual

☐ Удаленный доступ (VPN)

> Проверка узлов по MAC-адресам (MAB)

Разрешения

☐ Назначение VLAN

☐ Назначение списков доступа (ACL)

Change of Authorization

CoA: Отсутствует, RADIUS

Перенаправление

Тип: Не перенаправлять, Динамический URL

Сохранить, Отменить

Рисунок 99 – 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. 100);
- заполнить поля необходимыми данными, указать профиль сетевого

- оборудования, созданный на шаге 5 (рис. 101);
- указать TACACS+ Shared key.

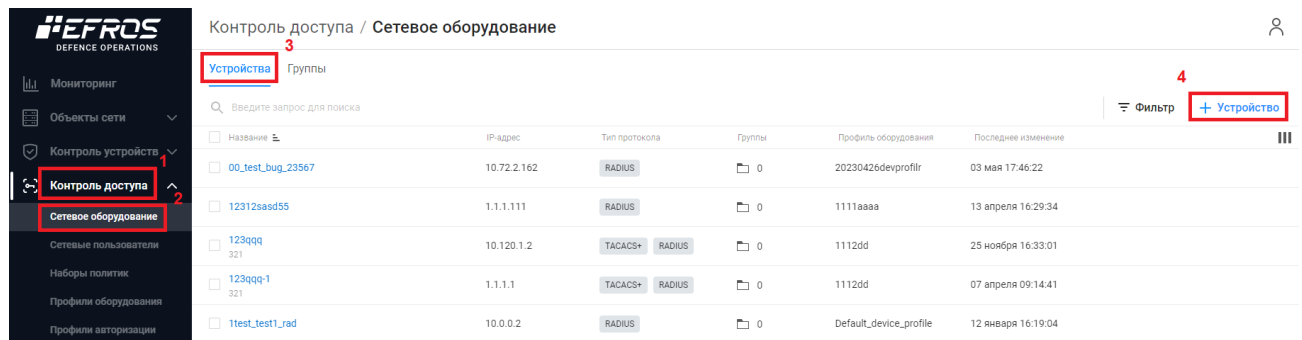


Рисунок 100 – Создание устройства

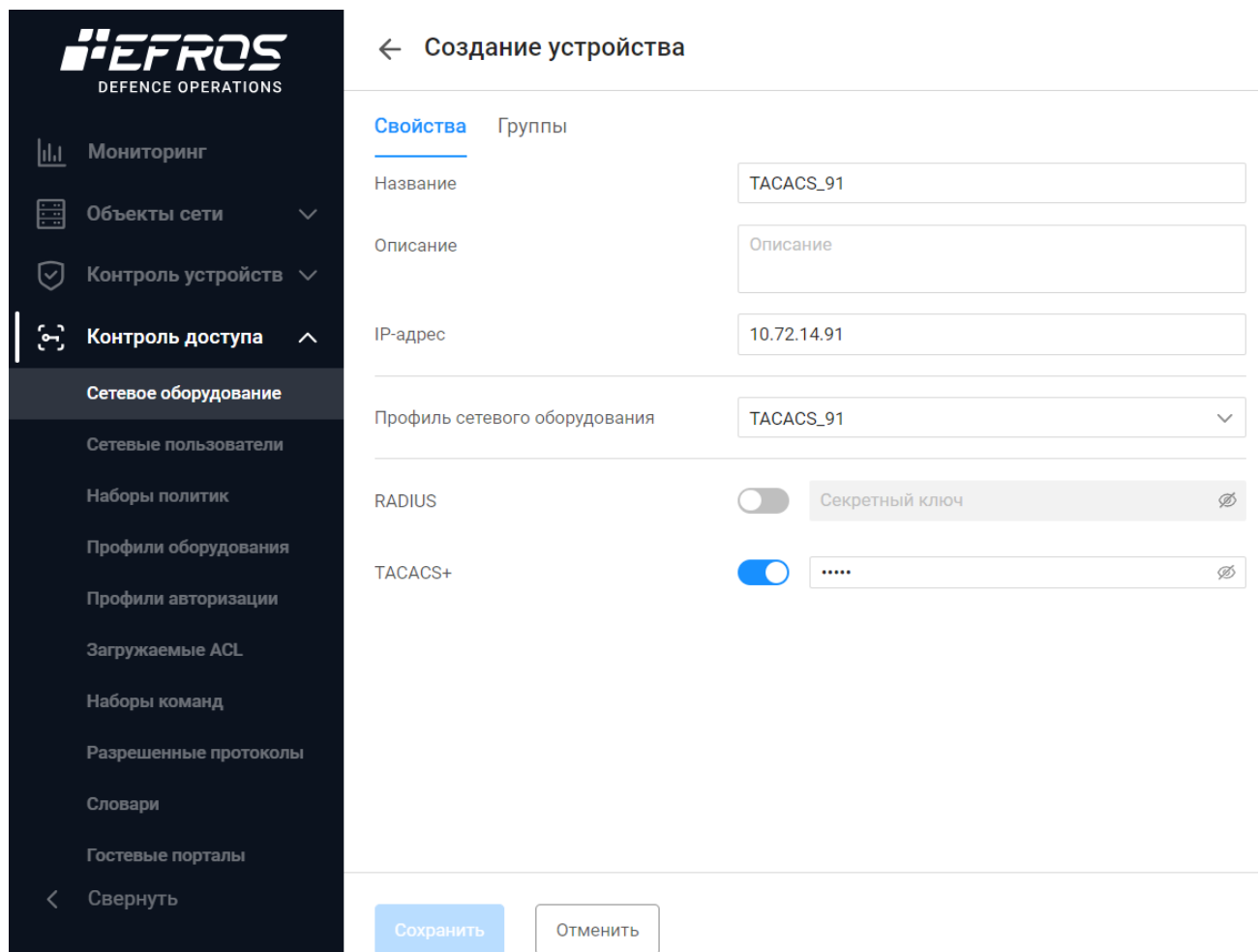


Рисунок 101 – Создание устройства

- 7) Создать сетевого пользователя.
- перейти в раздел «Контроль доступа», подраздел «Сетевые пользователи», вкладка «Пользователи»;
 - нажать кнопку «+ Пользователь» (рис. 102);
 - заполнить поля страницы необходимыми параметрами и нажать кнопку

«Создать» (более подробно о сетевом пользователе написано в п.п. 2.5.1.1). Примеры создания сетевого пользователя представлены на рис. 103 – рис. 105.

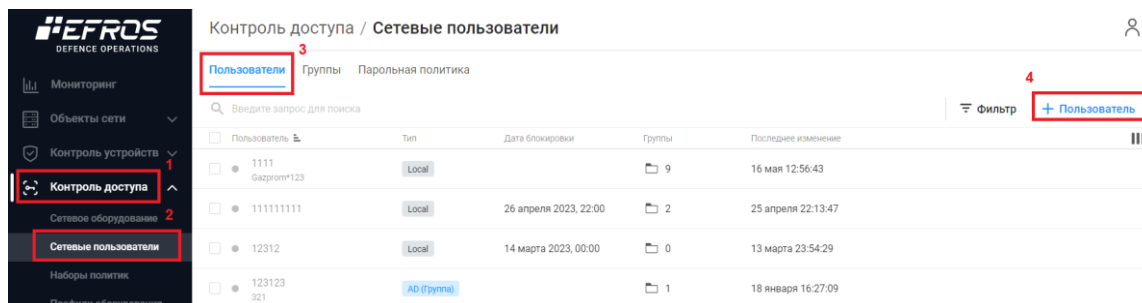


Рисунок 102 – Создание сетевого пользователя

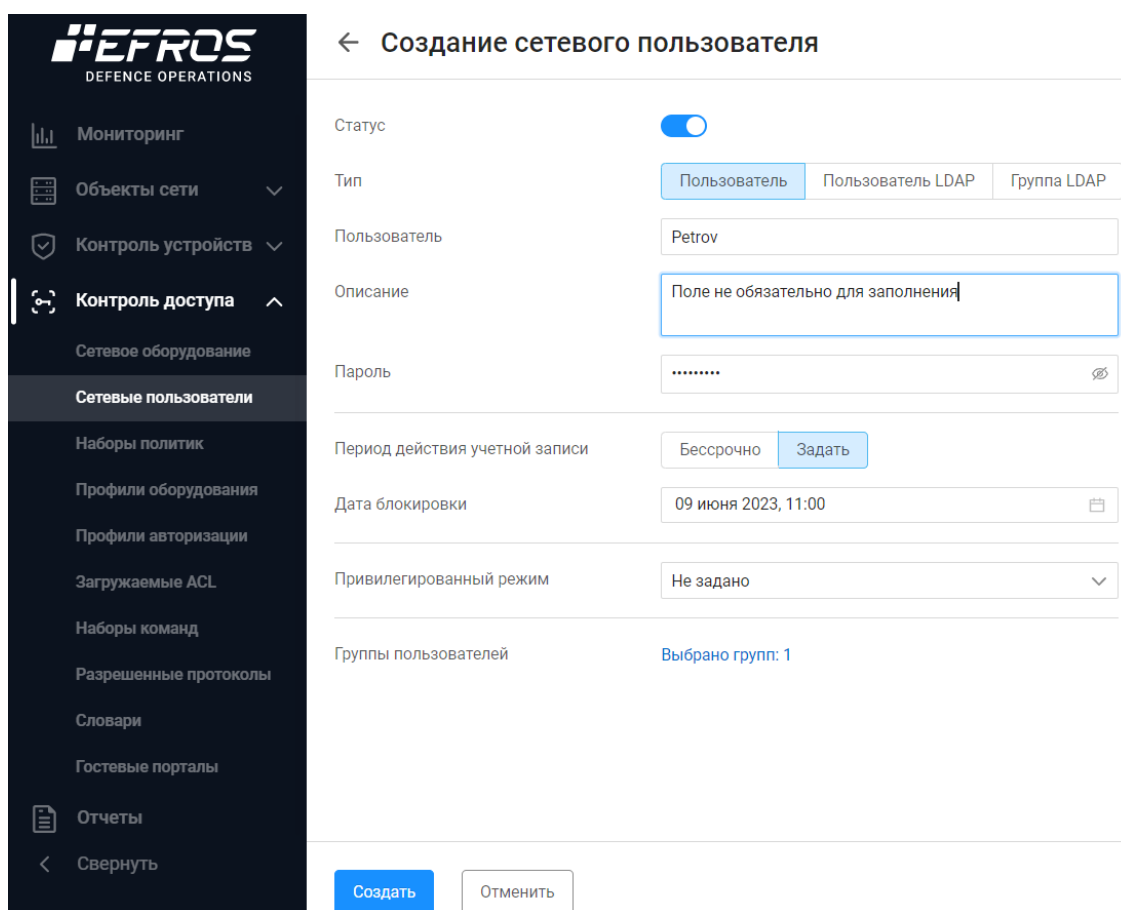


Рисунок 103 – Создание локального сетевого пользователя

← Создание сетевого пользователя

Статус ☒

Тип: Пользователь | **Пользователь LDAP** | Группа LDAP

Пользователь: sidorov

Описание: Сидор С. Сидоров

Период действия учетной записи: **Бессрочно** | Задать

Привилегированный режим: Не задано

Создать **Отменить**

Рисунок 104 – Создание сетевого пользователя LDAP

← Создание сетевого пользователя

Статус ☒

Тип: Пользователь | Пользователь LDAP | **Группа LDAP**

Группа: New4

Описание: New4

Период действия учетной записи: **Бессрочно** | Задать

Привилегированный режим: Не задано

Состав группы: 1 пользователь

Создать **Отменить**

Рисунок 105 – Создание группы LDAP

-
- Скриншот веб-интерфейса EPROS Defence Operations, страница «Контроль доступа / Профили авторизации».
- В левом меню (1) выделен пункт «Контроль доступа». В основном меню (2) выделен пункт «Профили авторизации».
- В заголовке страницы (3) выделен пункт «Доступ в сеть».
- В правом верхнем углу (4) выделен значок «+ Профиль».
- Таблица данных:
- | Название | Тип доступа | Профиль сетевого оборудования |
|---------------------------------|-------------|-------------------------------|
| 11138fff
куекуекуеуеуекуекуе | Запрещен | Device_profile_for_dACL |
| auth_mab | Разрешен | Device_profile_mab |
| AuthorizationProfile | Запрещен | Device_profile |
| Authorized_profile_for_dACL | Разрешен | Device_profile_for_dACL |
| cisco
куекуекуекуеуеуекуекуе | Запрещен | cisco |
| Deny45 | Разрешен | G_name |
| G1_profileAred
1 | Разрешен | G_name |
| G2_profileAfull | Разрешен | G_name |
| N0000000 | Запрещен | G_name |
| preview_test | Запрещен | New_G |

- заполнить необходимые поля на странице создания профиля авторизации (более подробно о профилях авторизации доступа на оборудование написано в п. 2.8.2) (рис. 107).

← Создание профиля авторизации на оборудование

Название

Описание

Тип настроек

Основные настройки ⓘ

Уровень привилегий по умолчанию ⓘ

Максимальный уровень привилегий

Список контроля доступа ⓘ

Выполнение команды при подключении пользователя

Запрет автоматического отключения после выполнения команды ⓘ Да Нет

Запрет использования управляющего символа ⓘ Да Нет

Время отключения при бездействии Минут

Время отключения сеанса Минут

Дополнительные атрибуты ⓘ

Передаваемые параметры ⓘ

Рисунок 107 – Создание профиля авторизации доступа в сеть

- 9) Создать требуемый набор политик доступа (более подробно о создании набора политик написано в подразделе 2.1). 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 элементов, 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. 108);

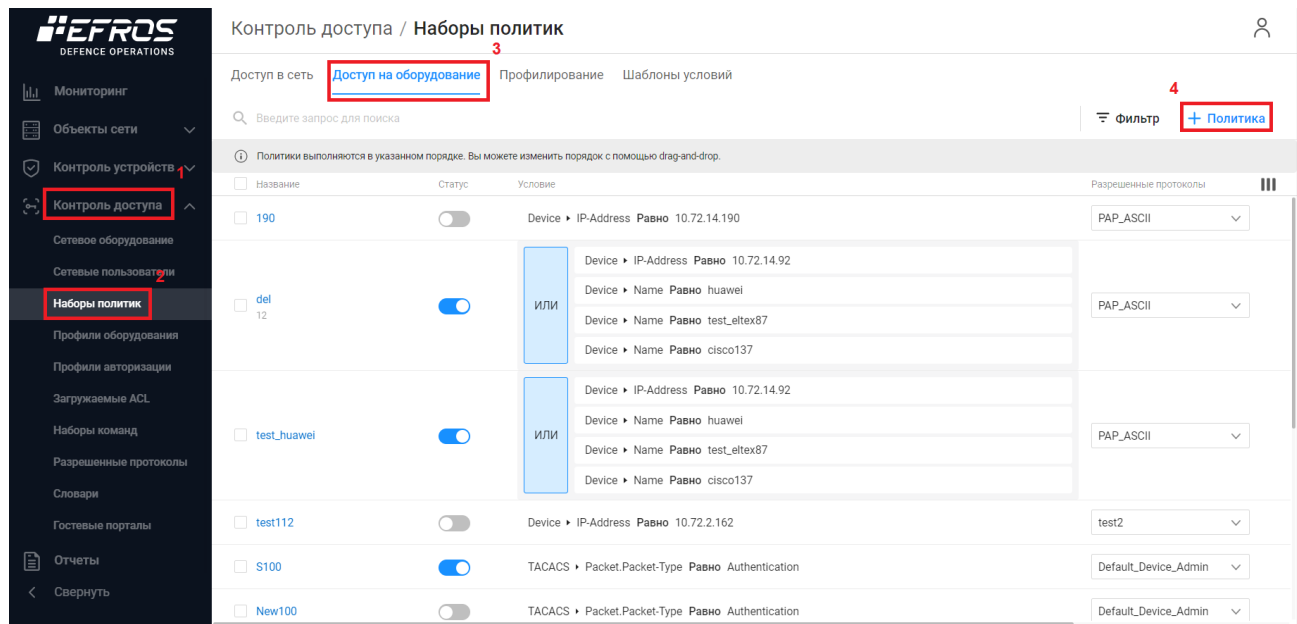


Рисунок 108 – Создание набора политик «Доступ на оборудование»

— указать название/описание политики, выбрать статус, выбрать список разрешенных протоколов (из созданных выше или выбрать стандартный Default_Device_Admin), создать условия срабатывания политики⁷ или выбрать условие из шаблона условий (рис. 109);

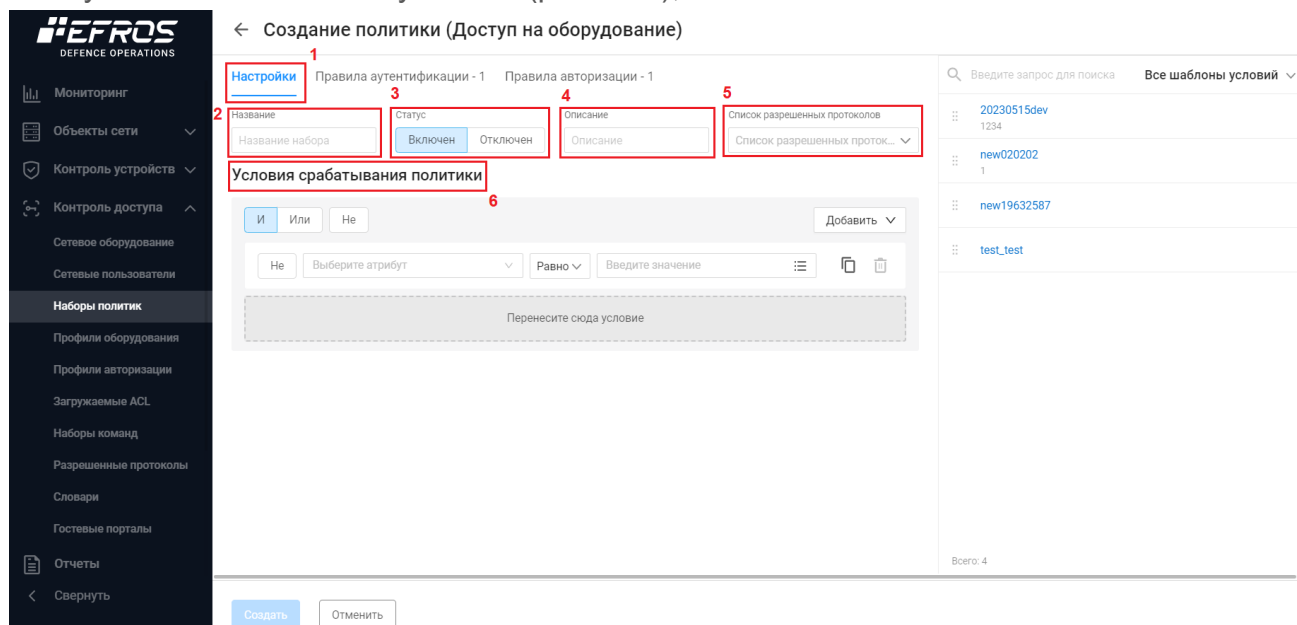


Рисунок 109 – Создание условия срабатывания политики

⁷ Это условия, которым в первую очередь должен соответствовать пользователь при попытке получения доступа на оборудование

- на вкладке «Правила аутентификации» нужно определить, каким образом и где происходит аутентификация устройства (рис. 110). 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 источник данных. Для правила по умолчанию рекомендуется выбрать «DenyAccess»;
 - выбрать действие при ошибке аутентификации. Для правила по умолчанию рекомендуется выбрать «Отклонить».

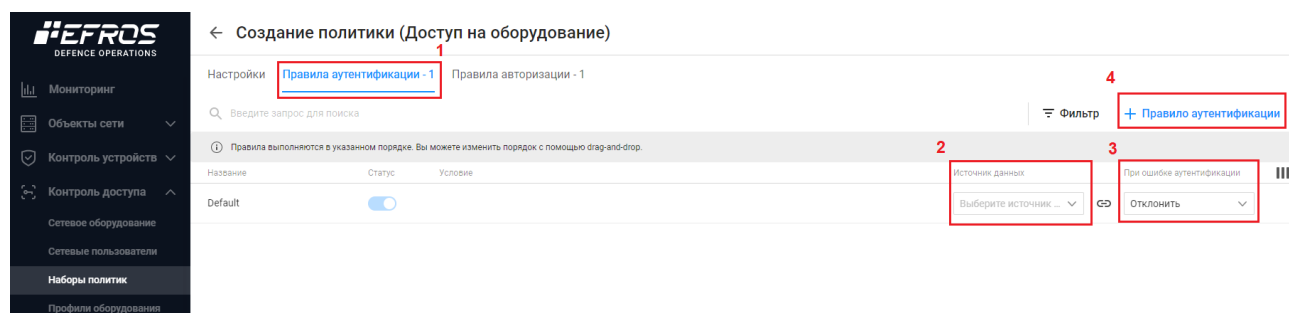


Рисунок 110 – Создание правила аутентификации

- нажать кнопку « **+ Правило аутентификации** »;
- заполнить поля необходимыми данными (рис. 111):
- указать название правила;
 - выбрать статус «Включен»;
 - 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 111 – Создание правила аутентификации

— перейти на вкладку «Правила авторизации» (рис. 112). 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 112 – Создание правила авторизации

- на вкладке нажать кнопку « + Правило авторизации »;
- заполнить поля необходимыми данными (рис. 113):
 - указать название правила;
 - выбрать статус «Включен»;
 - 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 113 – Создание правила авторизации

10) Нажать кнопку «Создать».



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

Таблица 31 – Краткая последовательность действий для настройки типового сценария взаимодействия с TACACS+

№ п/п	Действие	Описано в разделе документа
1	Создать/добавить/подключить необходимые источники данных ⁸ : <ul style="list-style-type: none">• конечные точки;• локальные сетевые пользователи/группы;• LDAP;• домен;• сертификаты	—

⁸ Добавление сертификатов, настройка подключения к AD (LDAP) и создание конечной точки описано в документе «Руководство пользователя. Часть 1. Администрирование»

№ п/п	Действие	Описано в разделе документа
2	Создать набор команд	2.10
3	Создать список разрешенных протоколов	2.11
4	Создать профиль оборудования	2.7
5	Создать сетевое оборудование	2.4
6	Создать профиль авторизации	2.8
7	Создать набор политик	2.6
7.1	Создать правила аутентификации	2.6.2
7.2	Создать правила авторизации	2.6.2

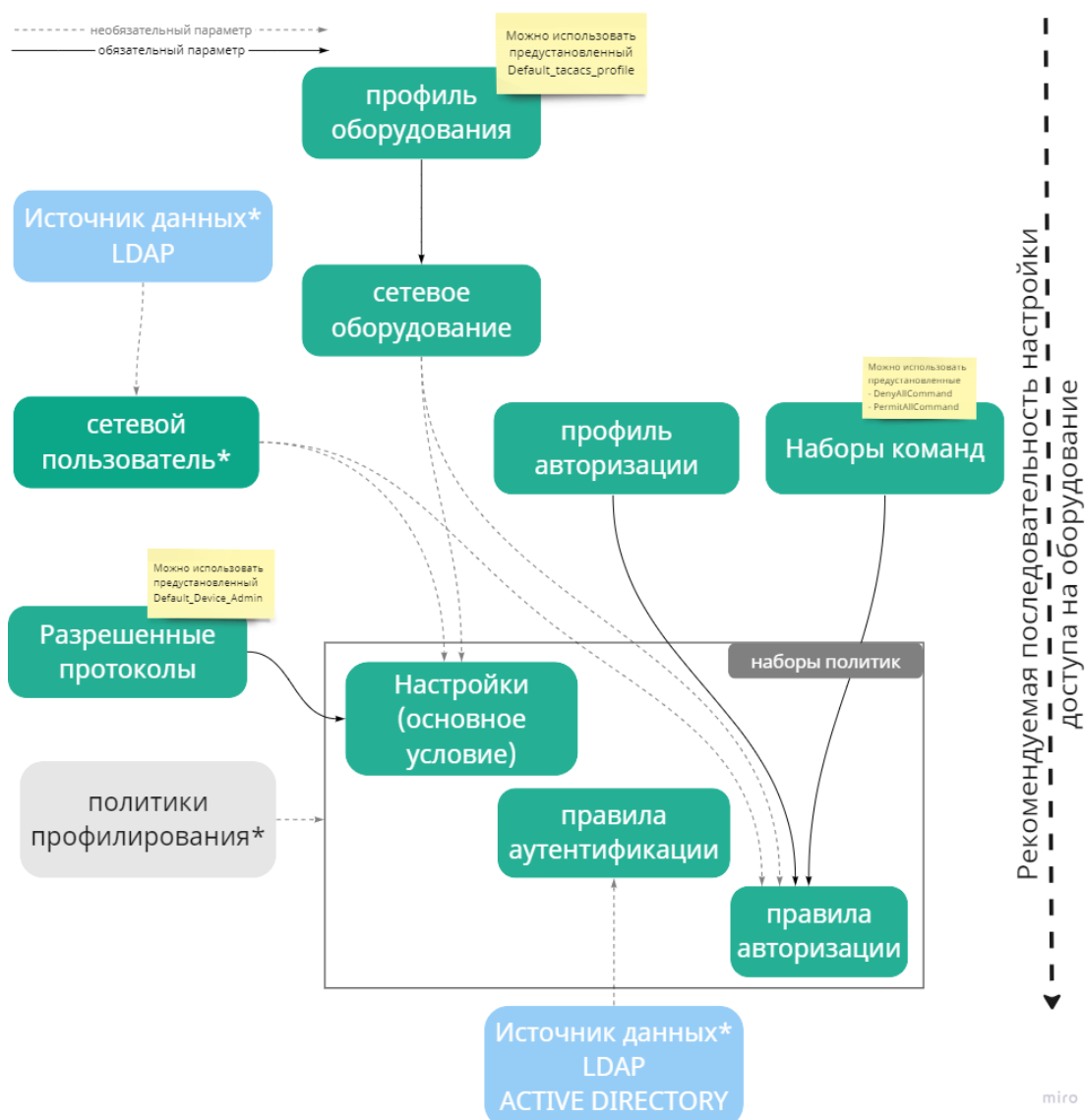


Рисунок 114 – Схема с кратким алгоритмом настройки типового сценария взаимодействия с протоколом TACACS+

Приложение Б

Рекомендуемая последовательность работы с локальными сертификатами

- 1) Перейти в раздел «Администрирование», подраздел «Сертификаты», вкладка «Корневые» (рис. 115).

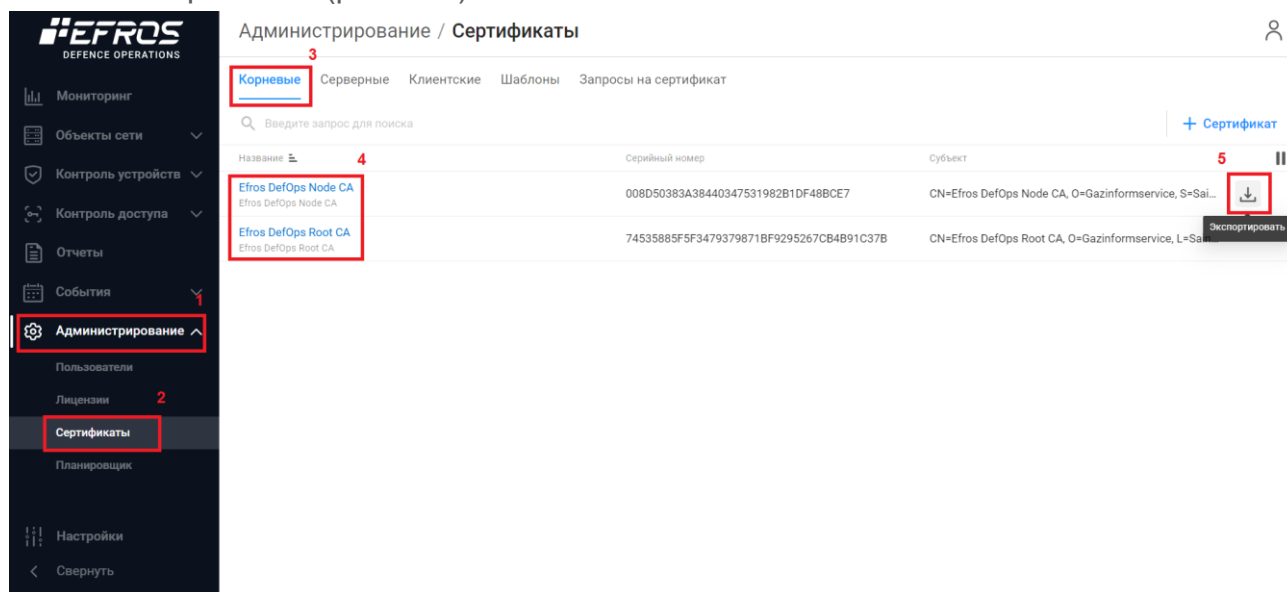


Рисунок 115 – Корневые сертификаты

Скачать предустановленные корневой и промежуточный сертификаты («Efros DefOps Node CA» и «Efros DefOps Root CA»).

Установить корневой и промежуточный сертификаты на устройство.

Перейти на вкладку «Шаблоны» (рис. 116).

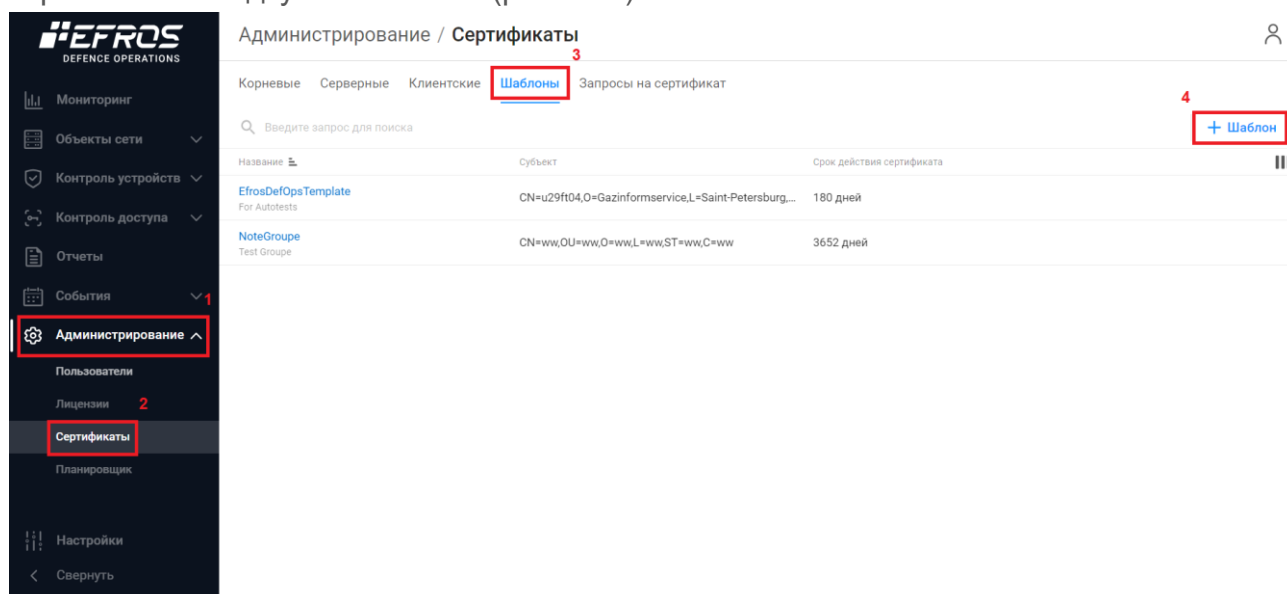


Рисунок 116 – Вкладка «Шаблоны»

Создать шаблон клиентского сертификата, заполнив поля необходимыми данными (рис. 117).

← Создание шаблона

Название: EfrosDefOpsTemplate

Описание: For Autotests

Срок действия сертификата (дней): 180

Субъект

Общее имя (CN): u29ft04

Страна (C): RU

Область (ST): Saint-Petersburg

Город (L): Saint-Petersburg

Организация (O): Gazinformservice

Подразделение (OU): Подразделение

Создать Отменить

Рисунок 117 – Создание шаблона

Перейти на вкладку «Клиентские». Нажать кнопку « Сертификат» (рис. 118)

Администрирование / Сертификаты

Корневые Серверные **Клиентские** Шаблоны Запросы на сертификат

Введите запрос для поиска

Фильтр + Сертификат

Субъект	Статус	Издатель	Альтернативное имя	Серийный номер	Дата создания	Дата окончания
CN=ww, OU=ww, O=ww, L=ww, S=ww, C=ww	Активен	CN=Efros DefOps Node CA, O=G...	DNS:10.72.22.63	00A85B71341B85DA48	23.08.2022 18:21	19.02.2023 00:00
CN=u29ft09, O=Gazinformservice, L=Saint-P...	Активен	CN=Efros DefOps Node CA, O=G...	DNS:u29ft09.mpe.app.dev	00A66C63F85634DB48	03.04.2023 18:20	30.09.2023 00:00
CN=u29ft05, O=Gazinformservice, L=Saint-P...	Активен	CN=Efros DefOps Node CA, O=G...	DNS:u29ft05.mpe.app.dev	00C0E00EB3E846DB48	27.04.2023 09:29	24.10.2023 00:00
CN=u29ft05, O=Gazinformservice, L=Saint-P...	Активен	CN=Efros DefOps Node CA, O=G...	DNS:u29ft05.mpe.app.dev	00FC5814C6EA46DB48	27.04.2023 09:43	24.10.2023 00:00
CN=u29ft05, O=Gazinformservice, L=Saint-P...	Активен	CN=Efros DefOps Node CA, O=G...	DNS:u29ft05.mpe.app.dev	00F4764CD4EA46DB48	27.04.2023 09:44	24.10.2023 00:00
CN=u29ft05, O=Gazinformservice, L=Saint-P...	Активен	CN=Efros DefOps Node CA, O=G...	DNS:u29ft05.mpe.app.dev	2972DCE1EA46DB48	27.04.2023 09:44	24.10.2023 00:00
CN=u29ft05, O=Gazinformservice, L=Saint-P...	Активен	CN=Efros DefOps Node CA, O=G...	DNS:u41ft72.mpe.app.dev	5437711EEB46DB48	27.04.2023 09:46	24.10.2023 00:00
CN=u29ft04, O=Gazinformservice, L=Saint-P...	Активен	CN=Efros DefOps Node CA, O=G...	DNS:u29ft04.mpe.app.dev	44B562FB2C47DB48	27.04.2023 17:37	24.10.2023 00:00

Рисунок 118 – Вкладка «Клиентские»

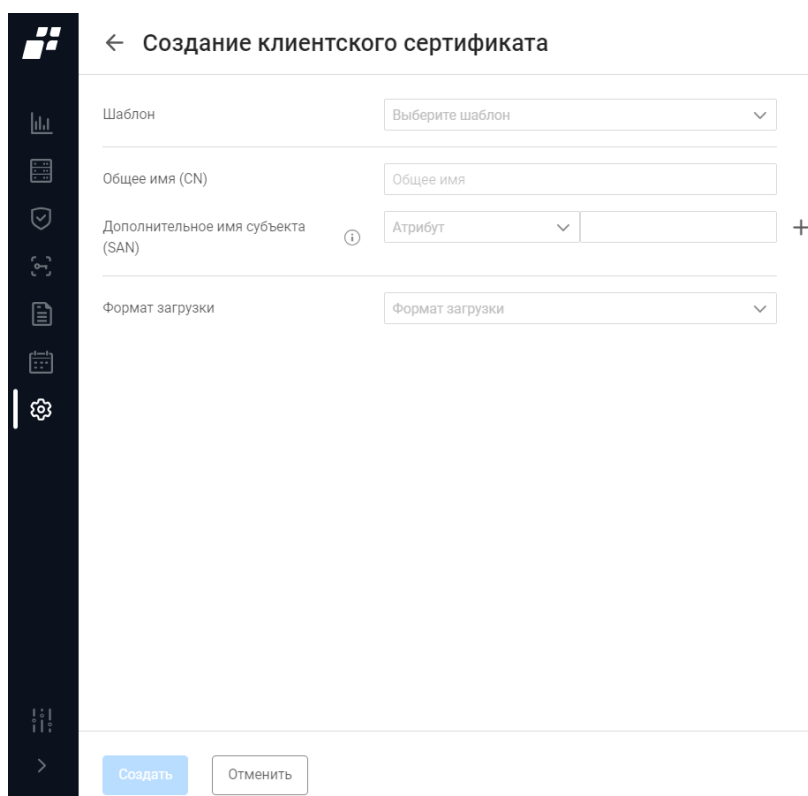


Рисунок 119 – Создание клиентского сертификата


Выбрать в поле «Шаблон» название требуемого шаблона.

Если в выбранном шаблоне заполнено поле «Общее имя (CN)», то это значение отобразится в поле «Общее имя (CN)» формы выпуска сертификата, иначе – заполнить поле вручную.

Указать альтернативное имя (одно или несколько) клиентской ЭВМ, для чего в группе «Альтернативное имя (SAN)»:


- выбрать в поле со списком тип дополнительного параметра: «MAC-адрес», «Имя участника–пользователя», «DNS»;
- ввести проверяемое при проверке сертификата значение параметра;
- в автоматически добавленной строке группы указать тип и значение второго альтернативного имени при необходимости.

Выбрать формат сертификата.

 Выбор формата загрузки определяется требованиями ПО, установленного на клиентской ЭВМ, для экспорта клиентского сертификата и публичной части корневого сертификата. Например, IIS принимает сертификаты в формате PKCS12, файл «client.p12» содержит в себе сам клиентский сертификат и закрытый ключ сертификата, файл «ca.pem» является файлом-контейнером, который хранит в себе открытую, публичную часть корневого сертификата.

Для обеспечения взаимной аутентификации клиентских ЭВМ и сервера ПК «Efros DO» выпустить клиентский сертификат.

Установить клиентский сертификат на устройство.

-  Использование шаблонов позволяет унифицировать и ускорить процесс выпуска сертификатов, поскольку параметры субъекта сертификата "Организация", "Подразделение", "Страна", "Город", "Область" могут быть одинаковыми для клиентских ЭВМ.

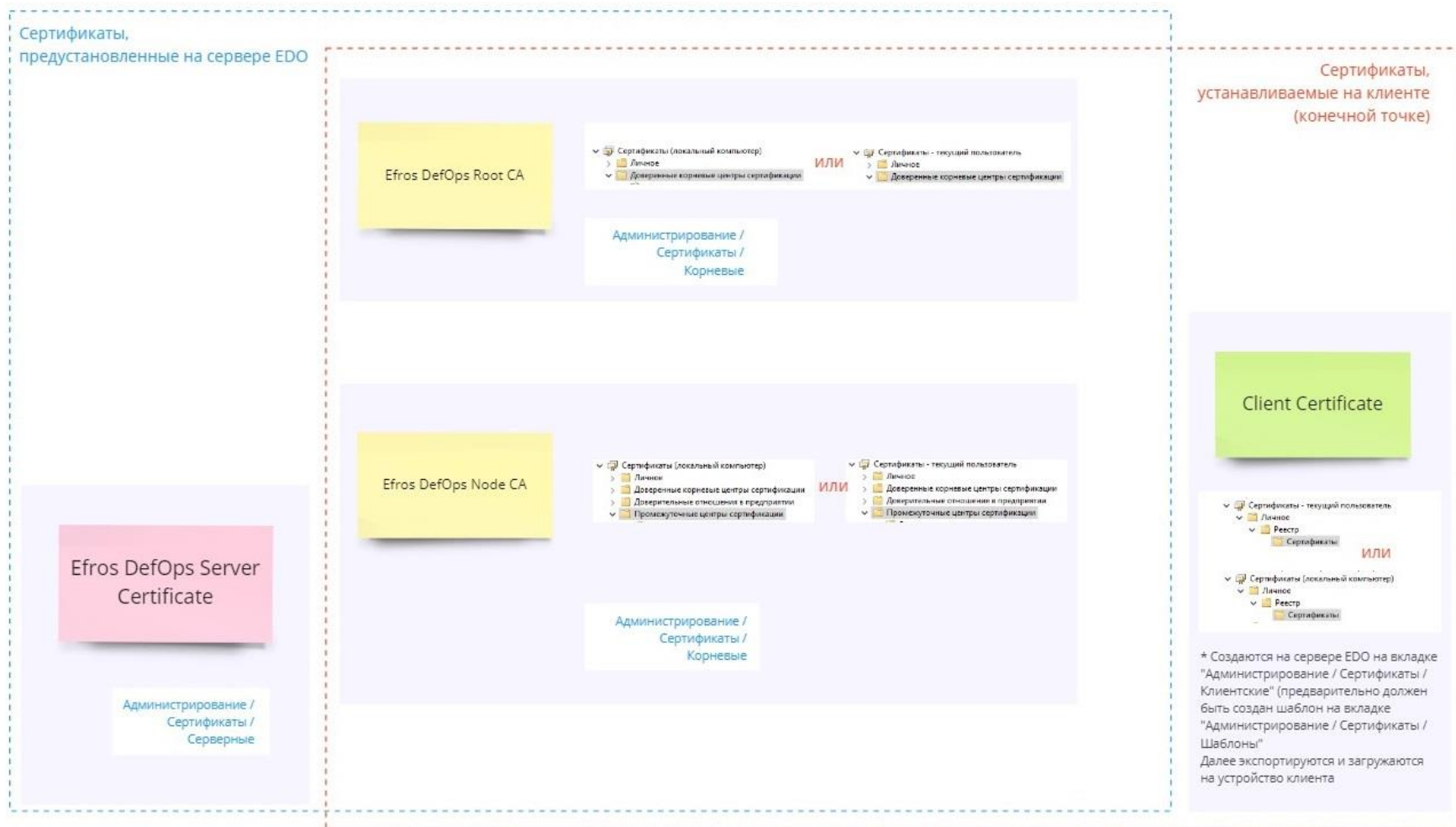


Рисунок 120 – Краткая схема по работе с локальными сертификатами⁹

⁹ Расположение сертификатов на клиенте приведено для ОС Windows и зависит от особенностей реализации конкретного сценария доступа в сеть и используемой версии ОС. Рекомендуется руководствоваться документацией производителя ОС

Рекомендуемая последовательность работы со сторонними сертификатами

- 1) Перейти в раздел «Администрирование», подраздел «Сертификаты», вкладка «Корневые» (рис. 121).

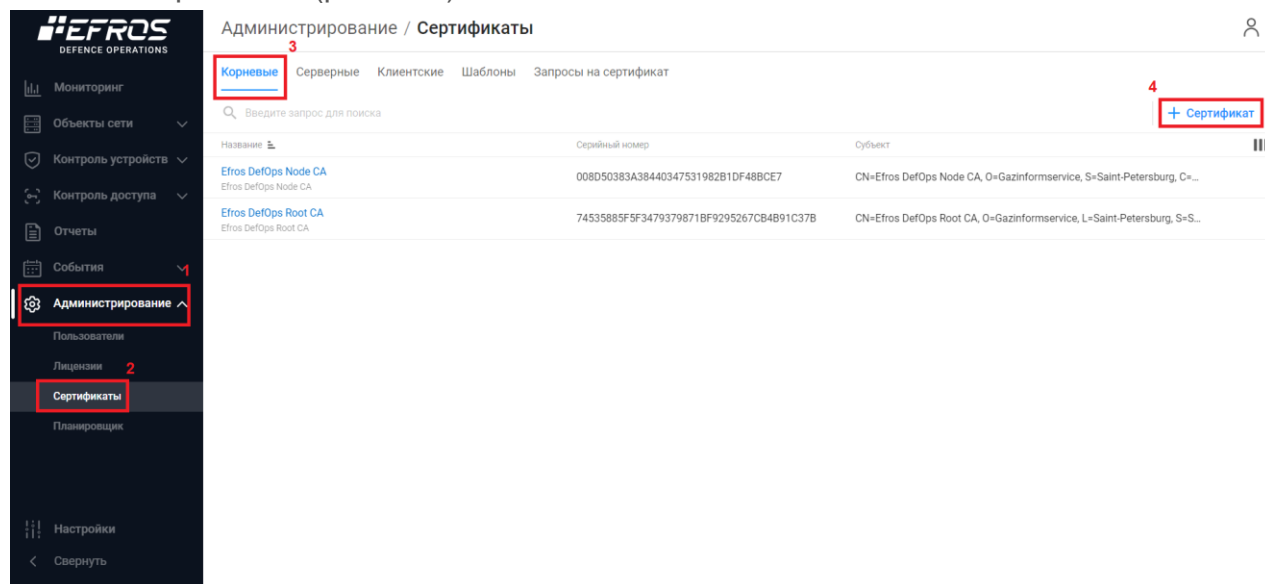


Рисунок 121 – Корневые сертификаты

- 2) Загрузить корневой сертификат, выданный сторонним Центром Сертификации (далее - ЦС).
- 3) Перейти на вкладку «Серверные» (рис. 122).

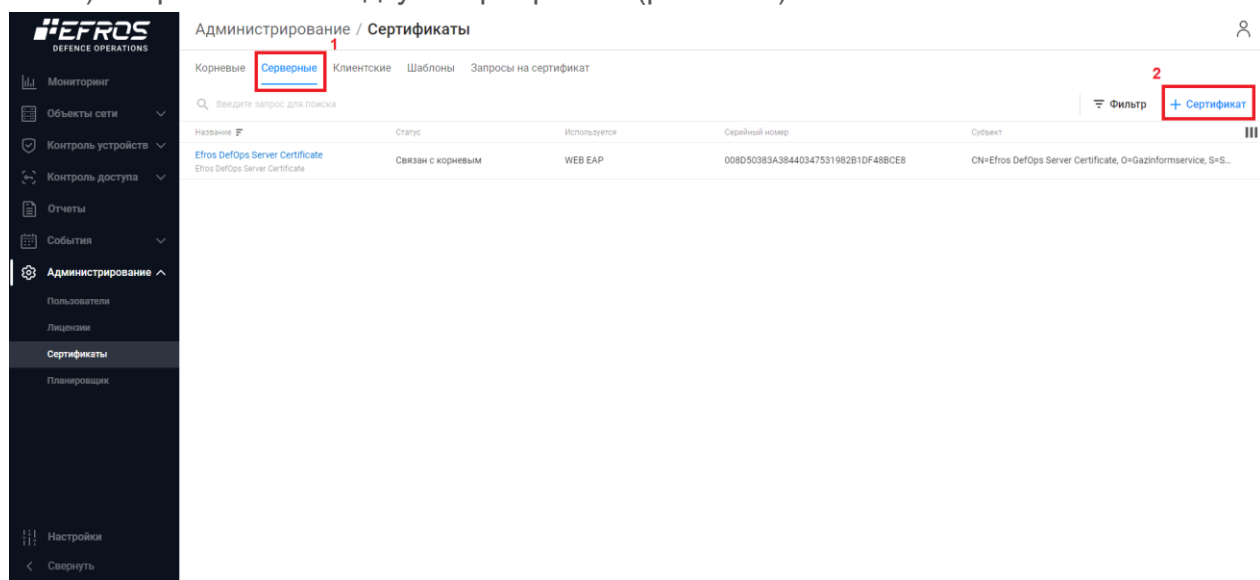


Рисунок 122 – Серверный сертификат

- 4) Загрузить серверный сертификат, выданный сторонним ЦС.

При импорте серверного сертификата автоматически определяется соответствующий ему корневой сертификат. Если в БД комплекса не обнаружен соответствующий корневой сертификат, то серверный сертификат добавляется в список подраздела «Сертификаты» вкладка «Серверные». Такой серверный сертификат не доступен для

выбора в настройках доступа в сеть (настройки TLS) в качестве серверного сертификата, используемого при аутентификации устройств на сервере аутентификации. При этом соответствующий корневой сертификат может быть добавлен в список подраздела «Сертификаты», вкладка «Корневые» после добавления серверного сертификата. В процессе добавления будет выполнена автоматическая привязка серверного сертификата к добавленному корневому, после чего серверный сертификат будет доступен для выбора при настройке доступа в сеть в качестве серверного сертификата, используемого при аутентификации устройств на сервере аутентификации.

Если необходимо создать новые корневой/промежуточный и серверный сертификаты, то:

- 1) Перейти на вкладку «Запросы на сертификат». Нажать кнопку «Запрос на сертификат» (рис. 123, 124).

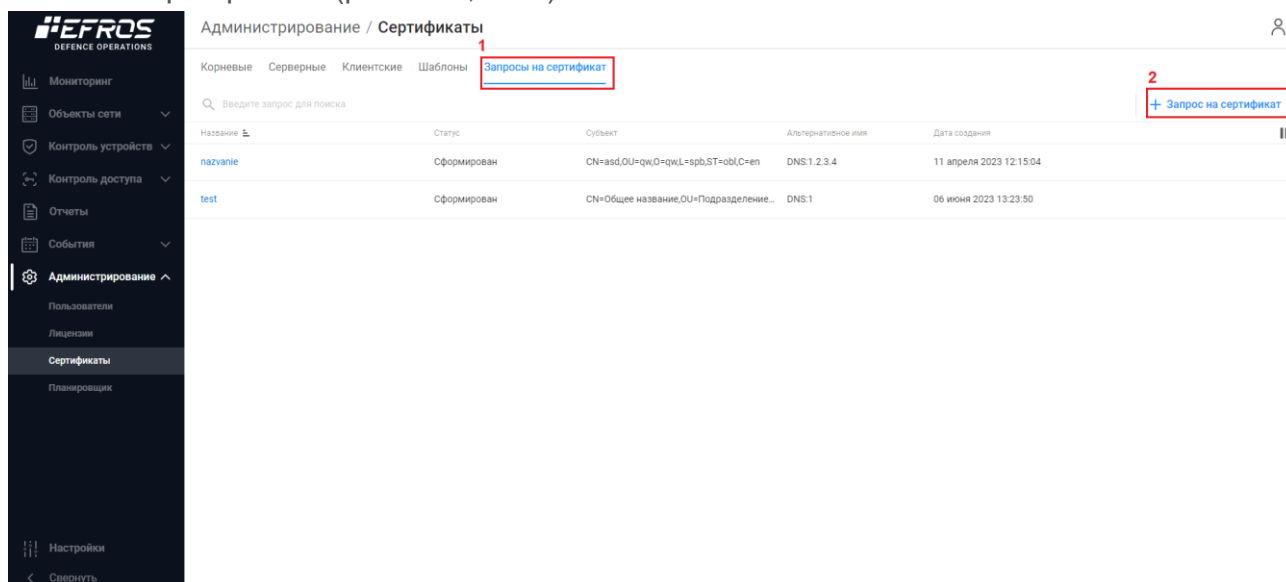
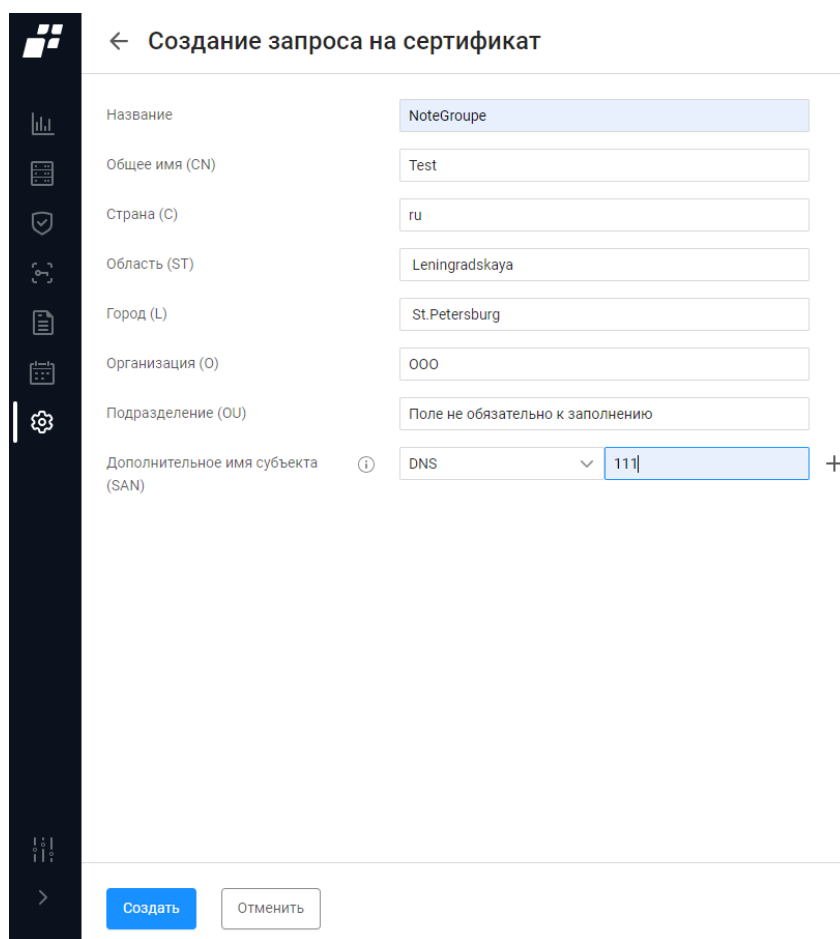


Рисунок 123 – Запросы на сертификат

- 2) Создать запрос на сертификат (рис. 124).



← Создание запроса на сертификат

Название	NoteGroupe
Общее имя (CN)	Test
Страна (C)	ru
Область (ST)	Leningradskaya
Город (L)	St.Petersburg
Организация (O)	ООО
Подразделение (OU)	Поле не обязательно к заполнению
Дополнительное имя субъекта (SAN)	DNS 111 +

Создать **Отменить**

Рисунок 124 – Создание запроса на сертификат

- 3) Заполнить поля необходимыми данными.
- 4) Экспортировать сертификат в сторонний ЦС.
- 5) Получить от ЦС серверный и корневой сертификаты.
- 6) Загрузить серверный и коревой сертификаты в БД комплекса.
- 7) Привязать серверный сертификат к запросу на сертификат. Корневой сертификат автоматически свяжется с серверным.

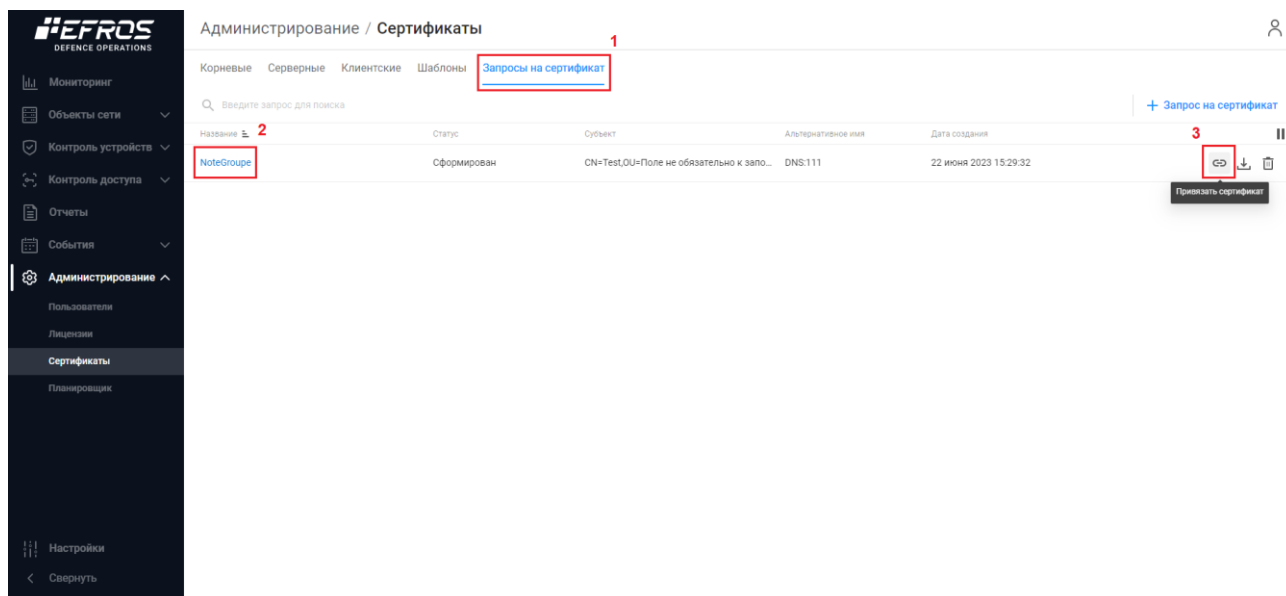



Рисунок 125 – Привязка запроса на серверный сертификат



При загрузке сторонних корневых и серверных сертификатов выдача локальных клиентских сертификатов, созданных в БД ПК «Efros DO», не требуется. Сторонние клиентские сертификаты контролируются сторонними корневым и серверным сертификатами.

Приложение В

Рекомендуемая последовательность действий для настройки и работы с гостевым порталом

-  В инструкции пример заполнения минимально необходимых полей для корректной работы гостевого портала и политик доступа.

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 оборудование поддерживает механизм RADIUS Change of Authorization, а также настроен CoA в профиле оборудования контроллера, 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.

1) Настроить точку доступа и контроллер точек доступа.

2) Создать страницу гостевого портала:

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

— нажать кнопку « Гостевой портал» или «» (рис. 126).

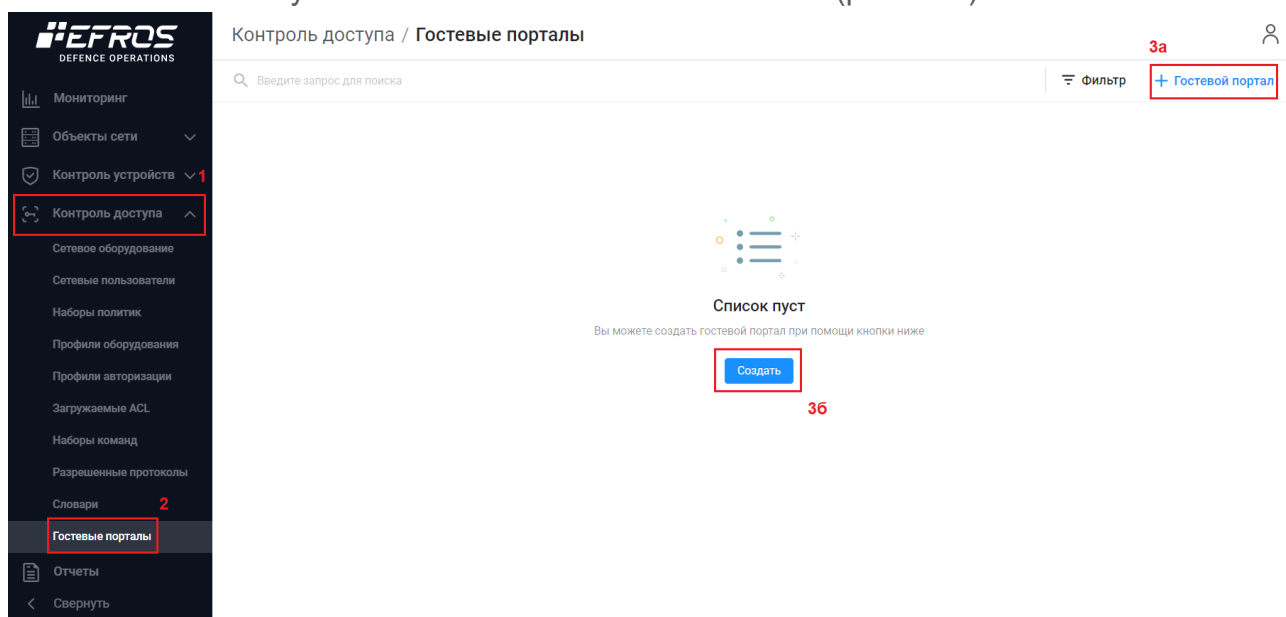


Рисунок 126 – Создание гостевого портала

← Создание гостевого портала

Название

Описание

Настройки портала

Тип доступа ☒ Анонимный ☐ Сетевые пользователи

Политика использования (AUP) ☒

Текст политики (AUP)

Брендирование портала ☒

Логотип или перетащите файл сюда

Задний фон или перетащите файл сюда

Корпоративный цвет

Требуется код доступа ☒

Код доступа

Рисунок 127 – Создание гостевого портала

Особенности заполнения полей (рис. 127) описаны ниже:

- поле «Название»: любое;
- поле «Описание»: любое;
- блок полей «Настройки портала»:
 - тип доступа: «Анонимный» или «Сетевой пользователь».
 - переключатель «Политика использования (AUP)». При включении данного параметра, на веб-странице гостевого портала появляется поле для флага - ознакомление и согласие с политикой использования сети, и ссылка на текст политики. По ссылке отображается текст, введенный в поле «Текст политики (AUP)». Кнопка «Подключиться» блокируется до простановки гостевым пользователем флага в поле.
- переключатель «Брендирование портала» позволяет загрузить логотип, выбрать задний фон и корпоративный цвет портала.
- переключатель «Требуется код доступа».
- поле «Код доступа».



При выборе типа доступа «Сетевой пользователь» переключатель «Требуется код доступа» и поле «Код доступа» отсутствуют.

После создания гостевого портала автоматически создается группа конечных точек, содержащая имя портала. Также автоматически создается группа сетевых пользователей с именем гостевого портала.

❗ Доступ на гостевой портал разрешен только для пользователей, входящих в соответствующую группу.

❗ Группы автоматически удаляются при удалении портала. Список конечных точек, входящих в группу конечных точек, очищается ежедневно в 00.00. Это необходимо для того, чтобы авторизованные пользователи проходили повторную процедуру аутентификации для получения доступа к сети.

3) Перейти к настройке политик доступа к portalу. Создать профиль сетевого оборудования для контроллера точек доступа (рис. 128):

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

— нажать кнопку «**+ Профиль оборудования**».

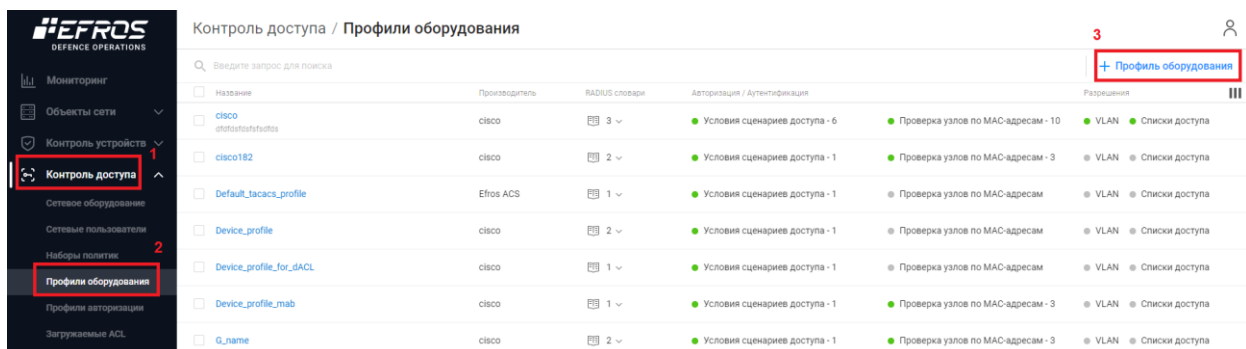


Рисунок 128 – Создание профиля сетевого оборудования

← Создание профиля сетевого оборудования

Название	<input type="text" value="cisco"/>
Описание	<input type="text" value="Описание"/>
Производитель	<input type="text" value="cisco"/>
Словари RADIUS	Выбрано: 2 ✕

Аутентификация / Авторизация

▼ Условия сценариев доступа

- ☐ Проводная аутентификация по MAC-адресам (Wired MAB)
- ☒ Беспроводная аутентификация по MAC-адресам (Wireless MAB)
- | | | | |
|------------------------|---|-----------------|-------------------------------|
| Radius / NAS-Port-Type | = | Wireless-802.11 | + ✕ |
| Radius / Service-Type | = | Call-Check | + ✕ |
- ☐ 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)

Сохранить

Отменить

Рисунок 129 – Создание профиля сетевого оборудования

← Создание профиля сетевого оборудования

▼ Проверка узлов по MAC-адресам (MAB)

- ☒ Метод проверки узлов
- ☒ С использованием PAP/ASCII
- ☐ Проверить пароль
- ☒ Проверить атрибут Calling-Station-Id на соответствие MAC-адресу
- ☐ С использованием CHAP
- ☐ С использованием EAP-MD5

Разрешения

- ☐ Назначение VLAN
- ☐ Назначение списков доступа (ACL)

Change of Authorization

CoA	<input type="text" value="Отсутствует"/> <input type="text" value="RADIUS"/>
Порт CoA	<input type="text" value="1700"/>

ⓘ Хотя бы один из параметров для Отключения или Повторной аутентификации должен быть активен

> Отключение

Сохранить

Отменить

Рисунок 130 – Создание профиля сетевого оборудования

← Создание профиля сетевого оборудования

Порт CoA

ⓘ Хотя бы один из параметров для Отключения или Повторной аутентификации должен быть активен

> Отключение

▼ Повторная аутентификация

Basic ⓘ ☒

= +

Rerun ⓘ ☐

Last ⓘ ☒

= +

Перенаправление

Тип

=

Рисунок 131 – Создание профиля сетевого оборудования

Особенности заполнения полей (рис. 129, 130, 131) описаны ниже:

- поле «Производитель»: Cisco;
- поле «Словари RADIUS»: Radius, Cisco;
- группа 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 позицию «Активен» с использованием PAP/ASCII:
 1. *Проверять атрибут Calling-Station-Id на соответствие MAC-адресу.*
- Блок полей «Разрешения» не заполняется;
- 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:reauthenticate–type=last.

— Поле «Перенаправление»:

- Тип: Динамический URL;
- Атрибуты: Cisco / Cisco–AVPair = url–redirect=\${URL}.

5) Создать сетевое оборудование – контроллер точек доступа:

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

— нажать кнопку «**+ Устройство**» (рис. 132).

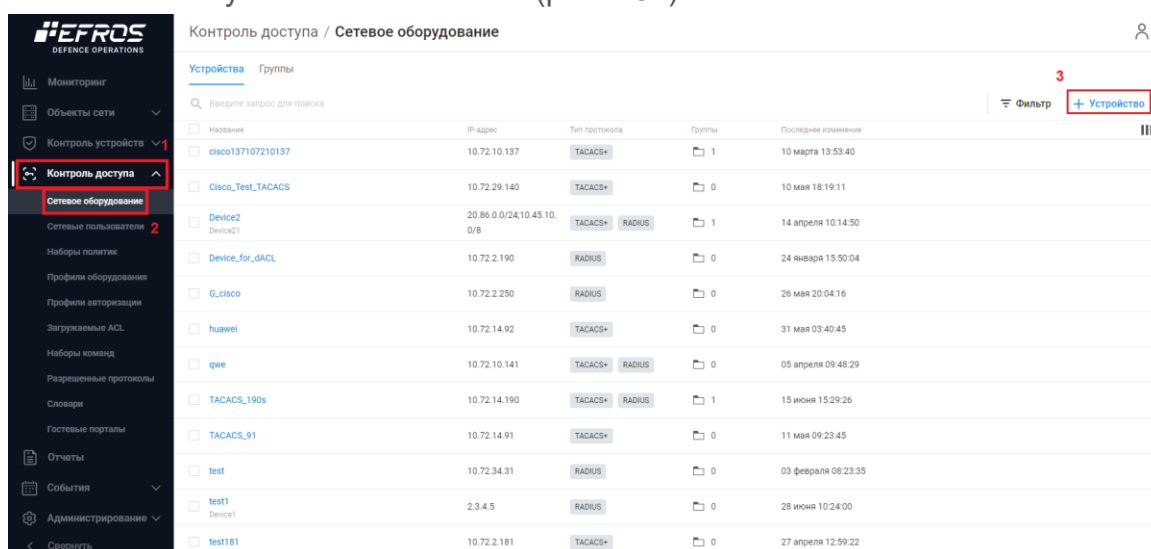


Рисунок 132 – Создание сетевого оборудования

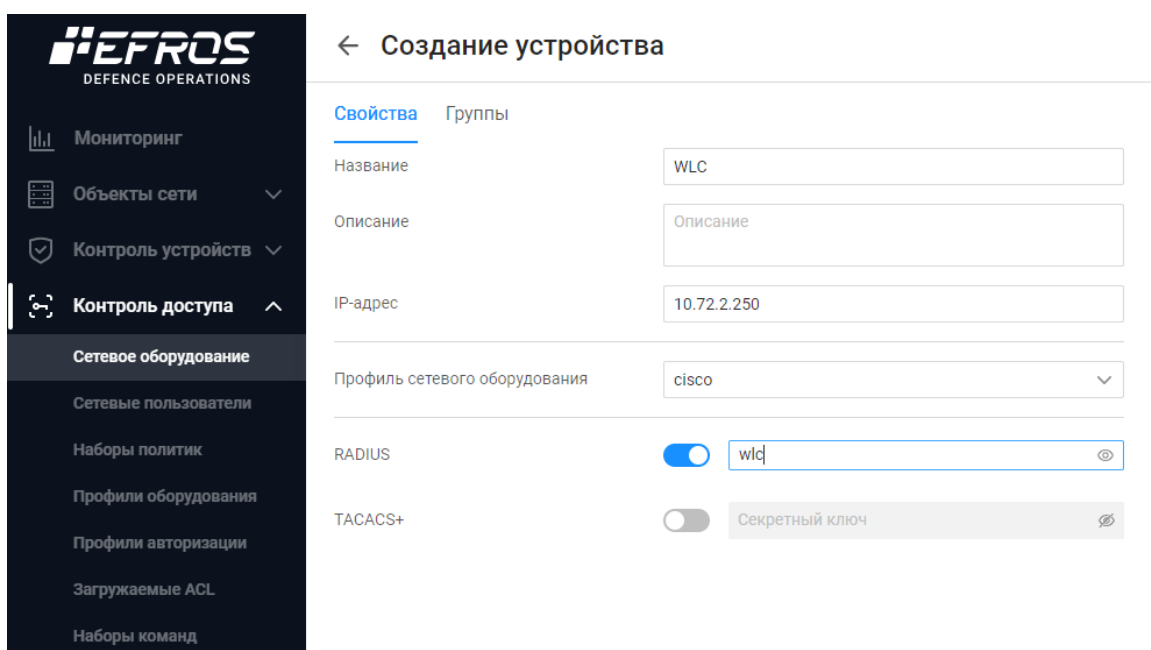




Рисунок 133 – Создание сетевого оборудования

Особенности заполнения полей (рис. 133) описаны ниже:

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

 Данный профиль используется для перенаправления внешнего пользователя (пользователя гостевого портала) на гостевой портал для ввода логина и пароля, 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.

- перейти в раздел «Контроль доступа», подраздел «Профили авторизации», вкладка «Доступ в сеть»;
- нажать кнопку « Профиль» (рис. 134).

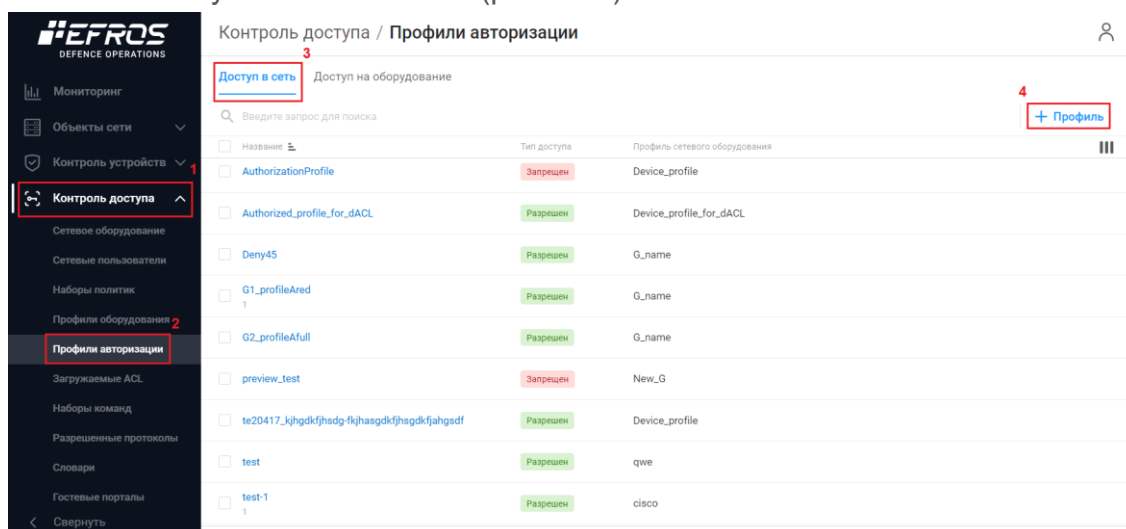


Рисунок 134 – Создание профиля авторизации

← Создание профиля авторизации доступа в сеть

Название	<input type="text" value="guest_redirect"/>
Описание	<input type="text" value="Введите описание"/>
Тип доступа	<input checked="" type="button" value="Разрешен"/> <input type="button" value="Запрещен"/>
Профиль сетевого оборудования	<input type="text" value="cisco"/>

Основные настройки

Загружаемый ACL	<input type="checkbox"/>
ACL	<input type="checkbox"/>
ACL контроллера точек доступа	<input type="checkbox"/>
Веб-перенадресация	<input checked="" type="checkbox"/>
Гостевой портал	<input type="text" value="guest-portal"/>
Название ACL	<input type="text" value="ACL_WEBAUTH_REDIRECT"/>
Статический IP / Имя хоста / FQDN	<input type="text" value="https://10.72.29.36:5802/"/>
VLAN	<input type="checkbox"/>

Настройка дополнительных атрибутов

Выберите атрибут	=	Введите значение	+
------------------	---	------------------	---

Передаваемые параметры

Рисунок 135 – Создание профиля авторизации

Особенности заполнения полей (рис. 135) описаны ниже:

- поле «Название»: любое;
- поле «Описание»: любое;
- поле «Тип доступа»: разрешен;
- поле «Профиль сетевого оборудования»: созданный в шаге 3;
- блок полей «Основные настройки»:
 - поле «Загружаемый ACL» не активировать;
 - поле «ACL» не активировать;
 - поле «ACL контроллера точек доступа» – название ACL, созданного на контроллере точек доступа.
- поле «Веб-перенадресация», перевести переключатель в положение «Активно»:
 - поле «Гостевой портал» – название ранее созданного гостевого портала;
 - поле «Название ACL» – название ACL. Созданного на контроллере точек доступа;
 - поле «Статический IP/имя хоста/FQDN» – адрес гостевого портала в формате `https://{адрес сервера EDO}:5802`.



В данном ACL описываются правила расширенного доступа, которые будут применены к устройству гостевого пользователя после его успешной авторизации.

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

— перейти в раздел «Контроль доступа», подраздел «Профили авторизации», вкладка «Доступ в сеть».

— нажать кнопку «**+ Профиль**» (рис. 136).

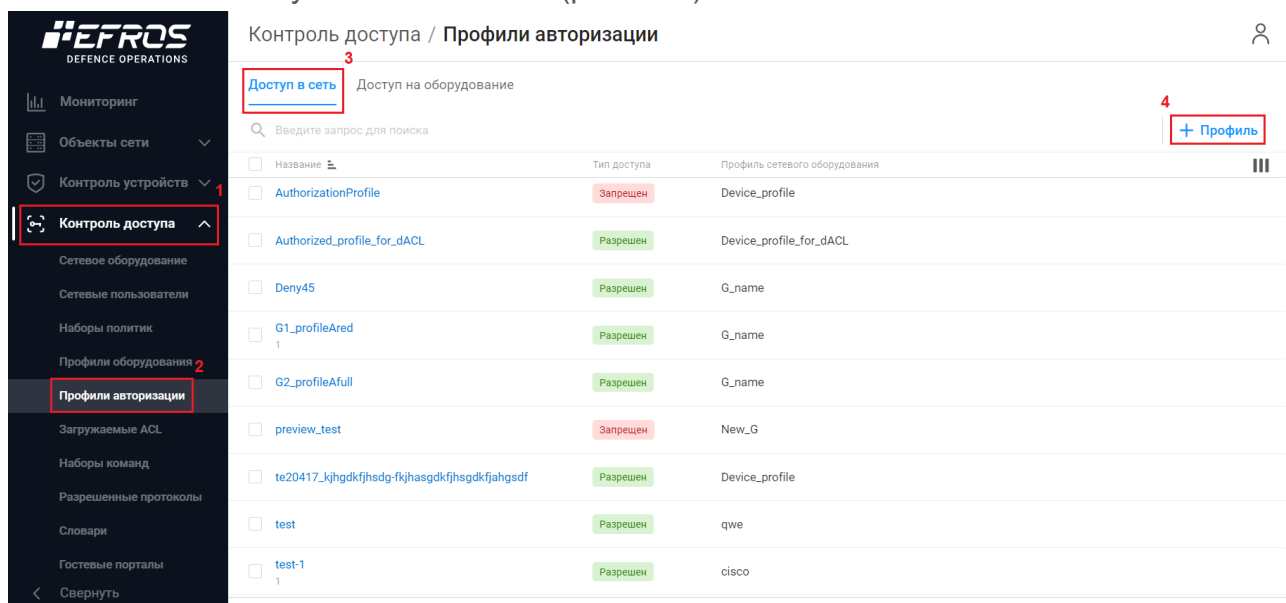


Рисунок 136 – Создание профиля авторизации

← Создание профиля авторизации доступа в сеть

Название	<input type="text" value="guest_full"/>
Описание	<input type="text" value="Введите описание"/>
Тип доступа	<input checked="" type="button" value="Разрешен"/> <input type="button" value="Запрещен"/>
Профиль сетевого оборудования	<input type="text" value="cisco"/> ▼

Основные настройки

Загружаемый ACL ⓘ	<input type="checkbox"/>
ACL ⓘ	<input type="checkbox"/>
ACL контроллера точек доступа ⓘ	<input checked="" type="checkbox"/>
Название ACL	<input type="text" value="FULL_ACL"/>
Веб-перееадресация ⓘ	<input type="checkbox"/>
VLAN ⓘ	<input type="checkbox"/>

Настройка дополнительных атрибутов

Выберите атрибут ▼	=	<input type="text" value="Введите значение"/>	+
--------------------	---	---	---

Передаваемые параметры

Рисунок 137 – Создание профиля авторизации

Особенности заполнения полей (рис. 137) описаны ниже:

- Поле «Название»: любое;
 - Поле «Описание»: любое;
 - Поле «Тип доступа»: разрешен;
 - Поле «Профиль сетевого оборудования»: созданный в шаге 3;
 - Блок полей «Основные настройки»:
 - поле «Загружаемый ACL» не активируем;
 - поле «ACL» не активируем;
 - поле «ACL контроллера точек доступа» – название ACL, созданного на контроллере точек доступа.
 - Поле «Веб-перееадресация», переключатель не активируем;
 - Поле «VLAN» не активируем.
- 8) Создать набор политик.
- перейти в подраздел «Профили авторизации», вкладка «Доступ в сеть»;
 - нажать кнопку «+ **Политика**» (рис. 138).

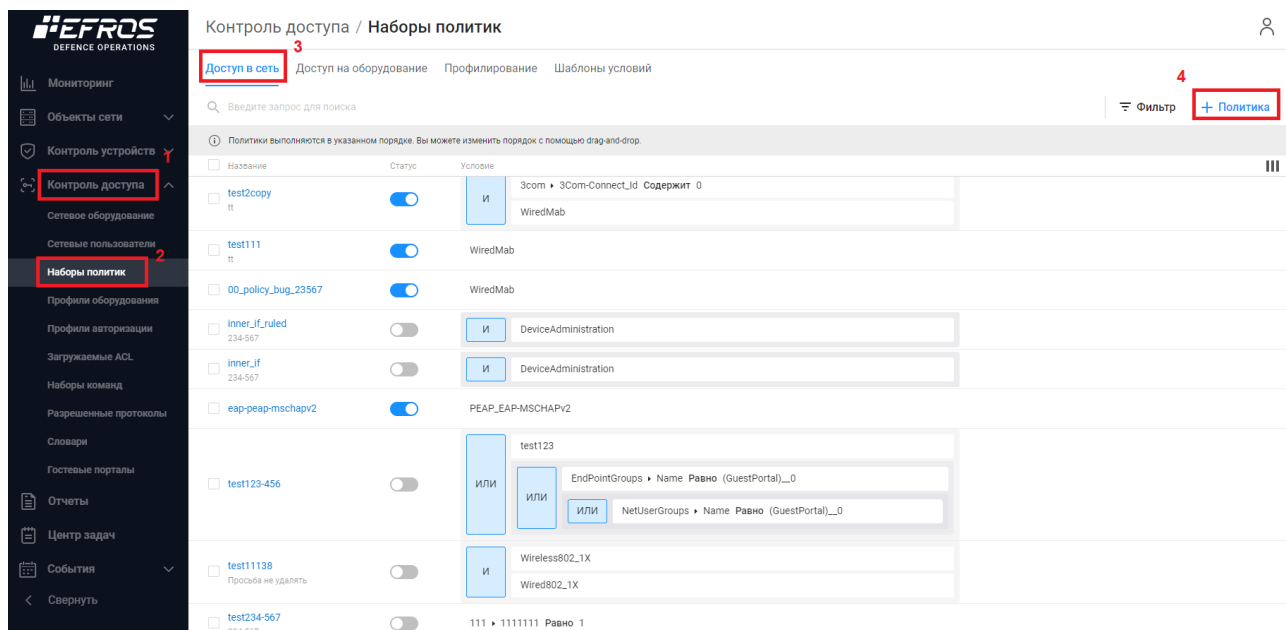


Рисунок 138 – Создание набора политик

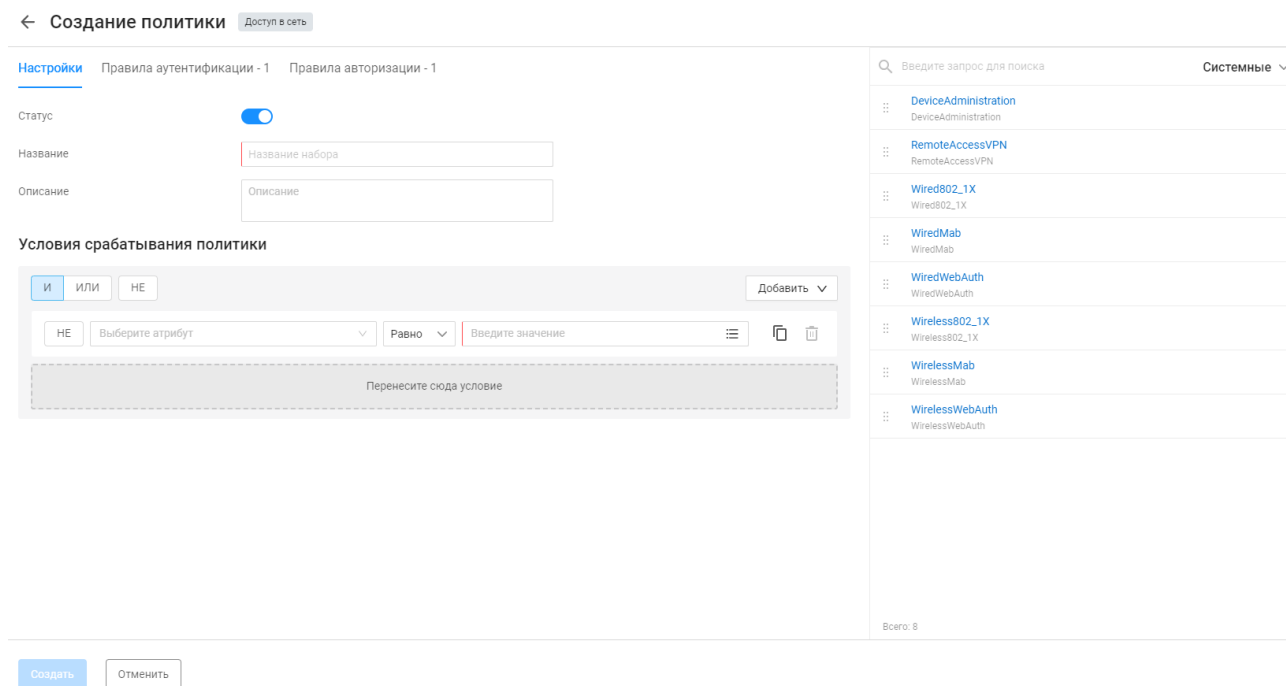


Рисунок 139 – Создание основного правила

Особенности заполнения полей (рис.) описаны ниже:

- Поле «Статус»: включен;
- Поле «Название»: любое;
- Поле «Описание»: любое
- Поле «Основное правило»: Wireless MAB.

- ❗ Для указания основного правила рекомендуется использовать предустановленный шаблон «Wireless MAB». Шаблон правил «Wireless MAB» – это набор правил для аутентификации устройств, подключенных к беспроводной сети по MAC-адресам.

Создать основное правило аутентификации (рис. 140):

- на странице создания набора политик перейти на вкладку «Правила аутентификации»;
- указать параметры для предустановленного правила.

Особенности заполнения полей описаны ниже:

- Поле «Источник данных»: DenyAccess.
- Поле «При ошибке аутентификации»: «Отклонить».

← Создание политики Доступ в сеть

Настройки **Правила аутентификации - 1** Правила авторизации - 1

🔍 Введите запрос для поиска

🔼 Фильтр + Правило аутентификации

❗ Правила выполняются в указанном порядке. Вы можете изменить порядок с помощью drag-and-drop.

Название	Статус	Условие	Источник данных	При ошибке аутентификации	Пользователь не найден	
Default	<input checked="" type="checkbox"/>		Источник данных	Отклонить	Отклонить	⋮

Всего: 1

Создать Отменить

Рисунок 140 – Создание правила аутентификации

- нажать кнопку « + Правило аутентификации ».

← Создание правила аутентификации Доступ в сеть

Статус ☒

Название

Проверка учетных данных

Источник данных

При ошибке аутентификации

Пользователь не найден

Условия срабатывания правила

Перенесите сюда условие

Введите запрос для поиска Системные

- DeviceAdministration
- RemoteAccessVPN
- Wired802_1X
- WiredMab
- WiredWebAuth
- Wireless802_1X
- WirelessMab
- WirelessWebAuth

Всего: 8

Рисунок 141 – Создание правил аутентификации

Особенности заполнения полей (рис. 141) описаны ниже:

- Поле «Название»: любое;
- Поле «Статус»: включен;
- Поле «Источник данных»: InternalEndpoints;
- Поле «При ошибке аутентификации»: продолжить;
- Поле «Основное правило»: WirelessMAB.

i При подключении гостевого устройства к сети, автоматически создается конечная точка (в случае ее отсутствия) с активным свойством «разрешить MAB».

i Аутентификация пользователя будет осуществляться после ввода логина и пароля на веб-странице гостевого портала.

← Создание политики Доступ в сеть

Настройки Правила аутентификации - 2 Правила авторизации - 1

Введите запрос для поиска Фильтр + Правило аутентификации

i Правила выполняются в указанном порядке. Вы можете изменить порядок с помощью drag-and-drop.

Название	Статус	Условие	Источник данных	При ошибке аутентификации	Пользователь не найден
Device1	<input checked="" type="checkbox"/>	WiredMab	InternalEndpoints	Продолжить	Отклонить
Default	<input checked="" type="checkbox"/>		Источник данных	Отклонить	Отклонить

Рисунок 142 – Созданные правила аутентификации

Создать правила авторизации.

- на странице создания набора политик перейти на вкладку «Правила авторизации» (рис. 143).

! Необходимо соблюдать порядок правил. Выше по списку должно находиться правило авторизации, осуществляющее проверку на нахождение конечной точки в группе конечных точек, созданной автоматически при создании гостевого портала.

Особенности заполнения полей (рис. 143) для доступа неавторизованных пользователей описаны ниже:

- Поле «Название»: default (создано по умолчанию);
- Поле «Профиль авторизации»: профиль авторизации, созданный в шаге 5.

← Создание политики (Доступ в сеть)

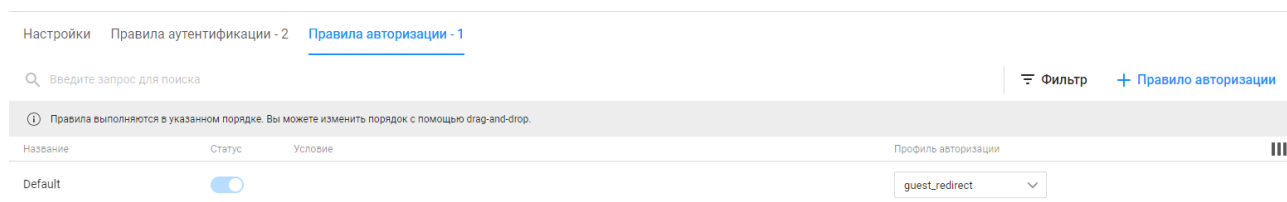


Рисунок 143 – Правило авторизации для доступа
неавторизованных пользователей

Правило авторизации для доступа авторизованных пользователей описаны ниже:

- на вкладке «Правила авторизации» нажать кнопку «+ Правило авторизации» (рис. 144).

← Создание политики (Доступ в сеть)

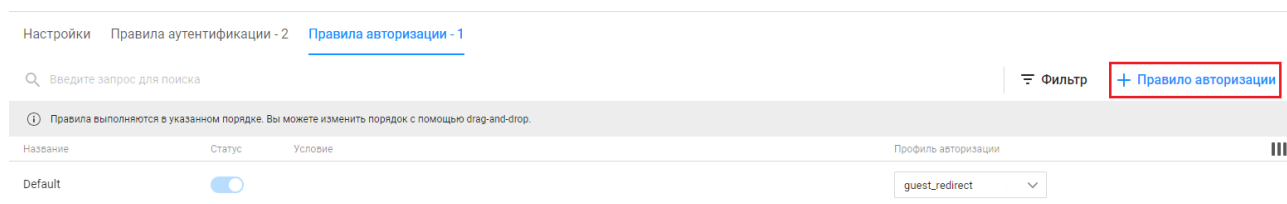


Рисунок 144 – Правило авторизации для доступа
авторизованных пользователей

← Создание правила авторизации Доступ в сеть

Статус ☒

Название

Действия при выполнении условий

Профиль авторизации

Условия срабатывания правила

☒ И ☐ ИЛИ ☐ НЕ

☐ НЕ

Перенесите сюда условие

Всего: 8

Введите запрос для поиска Системные

- DeviceAdministration
- RemoteAccessVPN
- Wired802_1X
- WiredMab
- WiredWebAuth
- Wireless802_1X
- WirelessMab
- WirelessWebAuth

Рисунок 145 – Правило авторизации для доступа
авторизованных пользователей

Особенности заполнения полей (рис. 145) для доступа авторизованных пользователей описаны ниже:

- Поле «Название»: любое;
 - Поле «Статус»: активен;
 - Поле «Профиль авторизации»: профиль авторизации, созданный в шаге 5;
 - Поле «Основное правило»: EndPointGroups / Name Равно (GuestPortal) {название созданного ранее портала}.
- 9) Создать внешнего пользователя.
- перейти в раздел «Контроль доступа», подраздел «Сетевые пользователи».
 - нажать кнопку «**+ Пользователь**» (рис. 146).

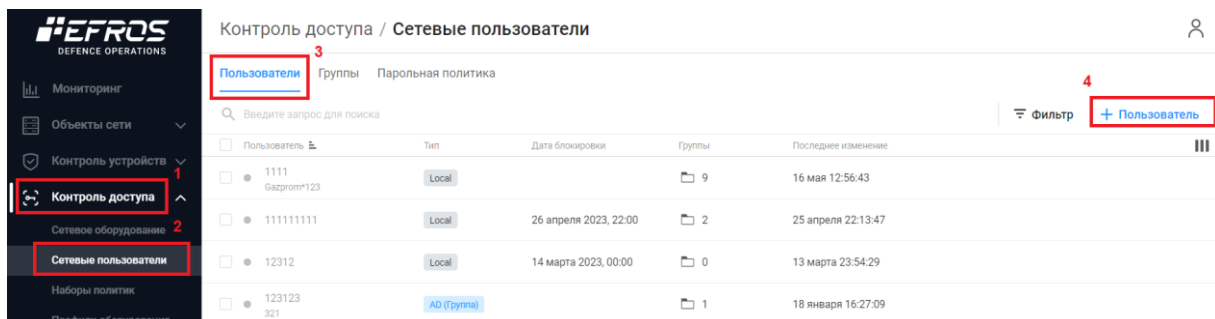


Рисунок 146 – Создание внешнего пользователя

← Создание сетевого пользователя

Статус ☒

Тип Пользователь Пользователь LDAP Группа LDAP

Пользователь

Описание

Пароль

Период действия учетной записи Бессрочно Задать

Дата блокировки

Привилегированный режим Не задано

Группы пользователей Выбрано групп: 1

Создать Отменить

Рисунок 147 – Создание внешнего пользователя

Особенности заполнения полей (рис. 147) описаны ниже:

- Переключатель «Статус пользователя»: положение «Активно».
- Тип пользователя: «Пользователь».
- Логин: любой.
- Пароль: любой.

Добавить пользователя в группу, соответствующую названию гостевого портала, на котором ему разрешена аутентификация.