Руководство администратора GM SMART SYSTEM NEW GENERATION

Версия GMSS New Gen Factory 3.18.0
Версия GM CORE KIT 2.6.1
Версия GMSS New Generation Client 1.4.0
Версия GM Monitoring 1.6.0
Версия документа 1.0

Оглавление

Термины и сокращения 6
1 О документе 8
2 Платформа GM SMART SYSTEM NEW GENERATION 9
2.1 Назначение платформы 9
2.2 Ключевые особенности платформы 12
3 Подготовка к развертыванию платформы GMSS NG 17
3.1 Доступ к «Личному кабинету» 18
3.2 Подготовка инфраструктуры 18
3.3 Проверка готовности инфраструктуры 18
4 Установка и базовая настройка СУ 20
4.1 Требования к СУ 20
4.2 Требования для работы GM-Box 21
4.3 Требования для работы устройств с установленным GMSS NG Client 21
4.4 Установка и запуск СУ 22
4.5 Быстрый старт, базовая настройка СУ 27
4.6 Базовые рекомендации по обеспечению информационной безопасности 37
5 Настройка и администрирование СУ 42
5.1 Сводка 43
5.2 Устройства 43
5.3 Группы устройств 46
5.4 Инвентаризация устройств 49
5.5 Пользователи 54
5.6 Шаблоны 79
5.7 Роли 83
5.8 Обновления 85
5.9 Приложения 87
5.10 Точки дистрибуции и распространяемые файлы 91

5.11 Задания 92
5.12 Сценарии 94
5.13 Команды 104
5.14 Организации 110
5.15 Журнал 110
5.16 Настройки 112
5.17 Удаленная поддержка пользователей 132
5.18 Работа с таблицами 132
6 Настройка сервиса мониторинга 134
6.1 Настройка ротации логов 134
6.2 Настройка ротации индексов Elasticsearch 136
6.3 Настраиваемые отсечки свободного места (watermarks) в Elasticsearch 136
7 Настройка и управление устройствами с установленным GMSS NG Client 138
7.1 Установка GMSS NG Client 138
7.2 Подключение и настройка RFID-карты к учетной записи пользователя 138
7.3 Настройка использования USB flash drive в VDI 139
8 Настройка и управление GM-Box 140
8.1 Загрузка обновления на GM-Box 140
8.2 Настройка гостевой учетной записи 141
8.3 Блокировка / разрешение подключения USB -устройств к GM-Box 142
8.4 Настройка использования принтеров 144
8.5 Настройка использования USB flash drive в VDI 150
9 Настройка интеграции с сервисами IP-телефонии 152
9.1 Настройка телефонной книги 152
9.2 Настройка поддержки аудиокодеков 154
9.3 Настройка отображения избранных контактов 155
9.4 Режим проверки и повторной регистрации VoIP клиента 156
9.5 Настройка высокой доступности IP телефонии 156
9.6 Описание сообщений VoIP клиента 157

9.7 Диагностика голосового VLAN 158
9.8 Регистрация GM-Box в Cisco Unified Communications Manager 159
9.9 Регистрация GM-Box в Avaya Aura 165
9.10 Настройка записи голосового трафика 170
10 Настройка удаленного подключения 171
10.1 Настройка удаленного подключения 171
10.2 Создание защищенного соединения с использованием OpenVPN 172
10.3 Создание защищенного удаленного соединения с использованием ViPNET 175
10.4 Создание защищенного удаленного соединения TLS VPN между GM-Box и сетевой инфраструктурой. 176
11 Диагностика и устранение неисправностей 180
11.1 Общие рекомендации по диагностике и устранению неисправностей 180
11.2 Сбор и анализ отладочной информации (логов) в сервисе мониторинга 181
11.3 Сервисный режим GM-Box 182
11.4 Режим диагностики СУ GMSS NG Factory 184
11.5 Режим восстановления прошивки GM-Box 188
12 Часто задаваемые вопросы 191
12.1 Рекомендации по обновлению ПО 191
12.2 Обновление СУ 192
12.3 Как вернуть GM-Box к заводским настройкам 192
12.4 Синхронизация со службой каталогов с использованием SSL 194
12.5 Первичная настройка веб-консоли сервиса мониторинга 195
12.6 Настройка аутентификации по протоколу Kerberos в VDI клиенте Citrix 199
12.7 Редактирование учетной записи суперпользователя LDAP 200
12.8 Редактирование учетной записи пользователя с системной ролью SUPER_ADMIN / ADMIN 200
12.9 Редактирование учетной записи пользователя с правами суперпользователя root в MongoDB 201

12.10 Настройка использования защищенного соединения между СУ и устройством ... 202

12.11 Подключение к корпоративной службе каталогов с ненадежным сертификатом TLS ... 202

12.12 Как установить безопасное соединение между смартфоном и GM-Box ... 203

12.13 В Citrix-сессии не работает переключение раскладки клавиатуры ... 203

12.14 Автоматическая блокировка и отключение сессии пользователя ... 203

12.15 Настройка политики требований к сложности паролей локальных пользователей ... 204

12.16 Настройка количества попыток неудачного входа в веб-интерфейс администратора ... 206

12.17 Указание прокси-сервера для веб-режима ... 207

Приложение А. Экран приветствия GM-Box ... 208

Приложение Б. Конфигурационный файл greeter.conf ... 209

Термины и сокращения

CA	Корневой сертификат
CPU	Central Processing Unit, центральный процессор
CUCM	Cisco Unified Communications Manager
CUPS	Common UNIX Printing System
DHCP	Dynamic Host Configuration Protocol
Distribution Point, DP	Модуль сервера управления GM Smart System New Generation. Distribution Point
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
GMSS	GM Smart System
HDD	Hard Disk Drive
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
LDAP	Lightweight Directory Access Protocol
NFC	Near Field Communication
NG Client	GM Smart System NG Client – ПО для управления устройствами сторонних производителей
NTP	Network Time Protocol
RAM	Random Access Memory
RDP	Remote Desktop Protocol
RFID	Radio Frequency IDentification
SASL	Simple Authentication and Security Layer
SD App-приложение	Smart Desktop Application
SIP	Session Initiation Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security

URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VDI	Virtual Desktop Infrastructure, виртуальный рабочий стол
ВМ	Виртуальная машина
ОС	Операционная система
ПО	Программное обеспечение
VoIP	IP-телефония
VPN	Virtual Private Network
АТС	Автоматическая телефонная станция
Базовое встроенное ПО, GM CORE KIT,	Базовое встроенное программное обеспечения для GM-Box не включающее дополнительные SD App-приложения
Витрина или SD	Smart Desktop – рабочий стол, режим «Витрина»
Режим GM-Box	Режим работы одного SD App-приложения
Реестр обновлений	Реестр на сервере управления для файлов обновлений встроенного базового ПО (GM CORE KIT)
Реестр приложений	Реестр на сервере управления для файлов SD App-приложений
СУ	Сервер управления GM FACTORY SERVER
Точка дистрибуции, ТД	см. Distribution Point
УЦ	Удостоверяющий Центр
Устройство, управляемое устройство	Устройство, управляемое сервером управления: GM-Box G1 или устройства других производителей с установленным GMSS NG Client
Шаблон	Унифицированная настройка режима/SD App-приложения на СУ для нескольких пользователей, объединенных общим признаком (атрибут, группа)
Шаблон SD	Специальный шаблон для «Витрины» (Smart Desktop)
SD App-приложение	Smart Desktop Application-приложения в формате плагинов (подключаемых модулей), выполняемые на устройствах пользователей

1 О документе

Руководство администратора содержит информацию:

- по установке сервера управления GM Smart System NEW GENERATION FACTORY (далее – СУ);
- по настройке и администрированию СУ с использованием веб-консоли.

Информация по установке, настройке и администрированию модуля GM Smart System New Generation. Distribution Point приводится в документе «**Руководство администратора. Модуль GM SMART SYSTEM NEW GENERATION. DISTRIBUTION POINT**»

Информация по установке ПО GM Smart System New Generation Client приводится в документе «**Руководство администратора по установке GM SMART SYSTEM NEW GENERATION CLIENT**»

При обнаружении опечаток или неточностей в настоящем руководстве, пожалуйста, сообщите о них, разместив заявку в Service Desk GETMOBIT.

2 Платформа GM SMART SYSTEM NEW GENERATION

2.1 Назначение платформы

GM SMART SYSTEM NEW GENERATION (далее – GMSS NG) – это единая доверенная платформа для построения и централизованного управления инфраструктурой рабочих пространств на базе док-станции GM-Box G1 (далее – GM-Box) со встроенным программным обеспечением (далее – ПО) GM CORE KIT, устройств сторонних производителей с установленным системным ПО GM SMART SYSTEM New Generation Client (далее – GMSS NG CLIENT) и собственного серверного ПО СУ.

В состав GMSS NG входят следующие компоненты:

- СУ GMSS NEW GEN FACTORY;
- отдельно устанавливаемый опциональный модуль GM Smart System New Generation. Distribution Point;
- веб-консоль;
- ПО для управления устройствами сторонних производителей GMSS NG CLIENT;
- агент, предустановленный в GMSS NG CLIENT и не требующий дополнительной настройки;
- Smart Desktop Application (далее – SD App-приложения), устанавливаемые на управляемые устройства.

Кроме того, платформа GMSS NG обеспечивает совместимость со следующими компонентами платформы GM SMART SYSTEM:

- док-станциями GM-Box со встроенным ПО GM CORE KIT;
- агент, предустановленный в GM CORE KIT и не требующий дополнительной настройки;
- сервис Global Discovery Service (далее – GDS), обеспечивающий автоматизированную инициализацию GM-Box для подключения к инфраструктуре заказчика;
- мобильное приложение GM Mobile Assistant, предназначенное для обеспечения возможности использования смартфона как средства аутентификации совместно с устройствами GM-Box.

Состав платформы GMSS NG приведен на Рисунок 1.

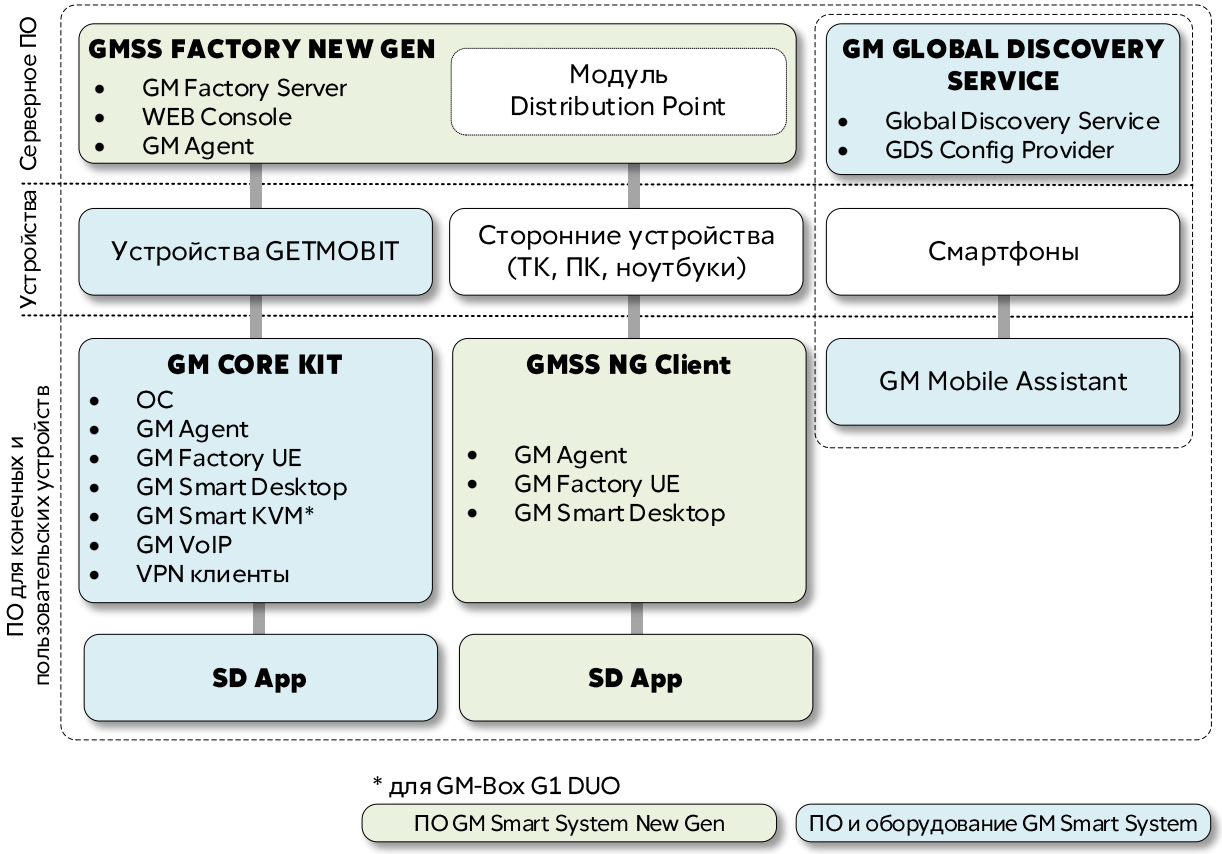


Рисунок 1 – Состав платформы GMSS NG

Типовая структурная схема организации единой доверенной рабочей среды приведена на Рисунок 2.

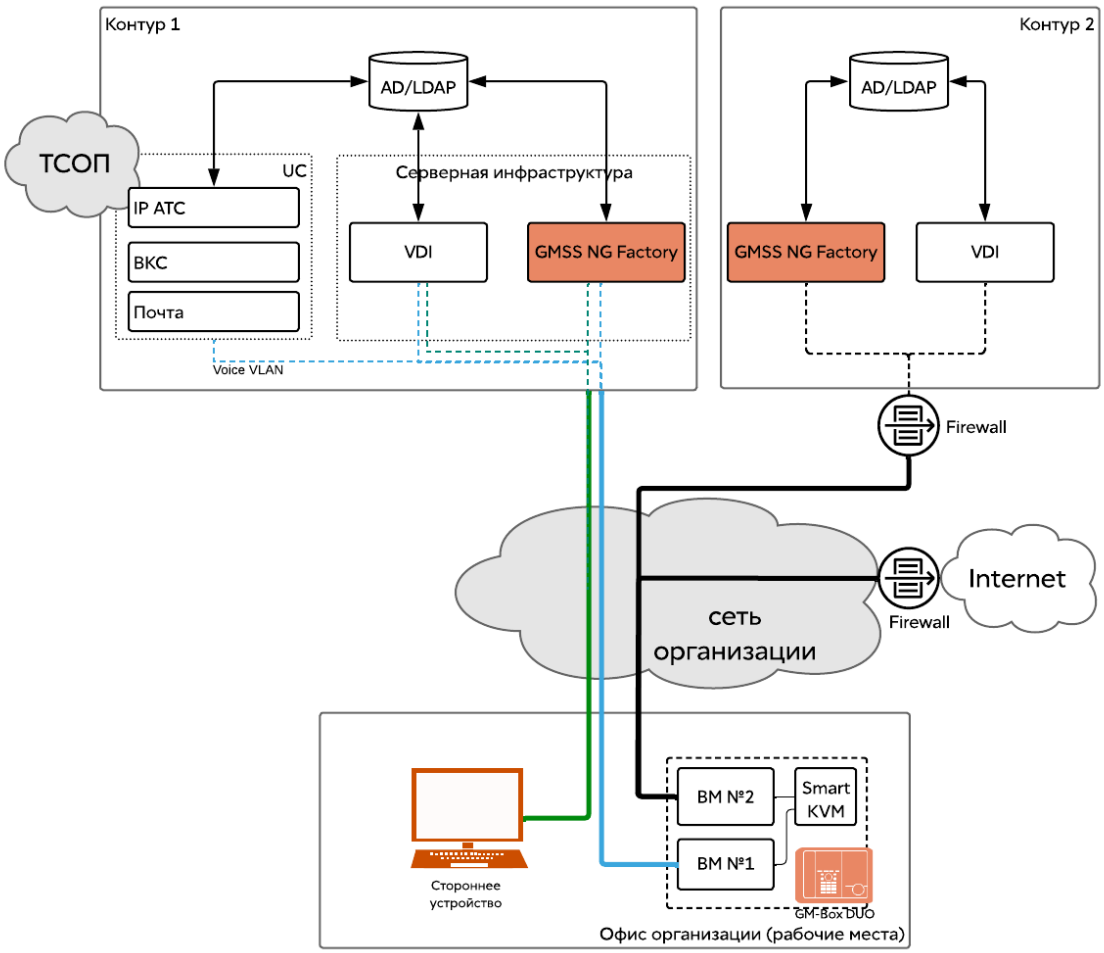


Рисунок 2 – Типовая структурная схема организации единой доверенной рабочей среды

Для функционирования GMSS NG в сетевой инфраструктуре компании необходимо установить СУ. Для работы в двухконтурной сети, например, при внедрении GM-Box DUO, необходимо установить два СУ – по одному в каждый контур. СУ обеспечивает управление профилями пользователей и устройств GM-Box, мониторинг и обновление устройств. Настройка и администрирование СУ выполняется из веб-консоли.

СУ позволяет:

- определить параметры доступа пользователей GM-Box:
  - к сервисам виртуальных рабочих столов (далее – VDI);
- к сервисам VoIP-телефонии с использованием протокола SIP;
  - к сервисам видеоконференцсвязи с использованием протокола SIP или штатными средствами в ВМ пользователя;
  - к веб-сервисам;

- определить параметры доступа пользователей сторонних устройств под управлением GMSS NG CLIENT:
  - к сервисам VDI;
  - к веб-сервисам;
- предоставить администраторам системы возможности:
  - управления пользовательским оборудованием;
  - оказания удалённой поддержки пользователям управляемых устройств;
  - управления учетными данными и профилями пользователей;
  - управления шаблонами настроек;
  - настройки синхронизации со службой каталогов;
  - мониторинга состояния пользовательского оборудования;
  - просмотра журналов событий;
  - централизованного обновления системного программного обеспечения пользовательского оборудования.

2.2 Ключевые особенности платформы

Для обеспечения гибкости настройки и предоставления различной функциональности конечным пользователям, платформа GMSS NG предлагает администраторам и специалистам службы эксплуатации удобные механизмы настройки, которые предоставляют доступ к инфраструктурным сервисам организации через управляемые устройства.

Гибкость обеспечивается:

- функциональным образом встроенного ПО – формируется администратором для пользовательских устройств;
- единым профилем пользователя – настройки определяются администратором для пользователей.

2.2.1 Функциональный образ встроенного ПО

2.2.1.1 Базовое встроенное ПО

Состав и полная доступная функциональность встроенного ПО на управляемых устройствах определяется комбинацией базового встроенного ПО GMSS NG CLIENT или GM CORE KIT и набором SD App-приложений. Администратор платформы формирует состав по своему усмотрению и на основе требований организации.

Например, если в организации необходимо подключаться к VDI ресурсам Citrix и VDI Space (Basis и др.), то администратор должен сформировать функциональный образ

встроенного ПО на основе GM CORE KIT или GMSS NG Client и двух SD App-приложений: Citrix и Space[1].

2.2.1.2 Режимы работы устройства и SD App-приложения

На платформе GMSS NG с использованием СУ, устройства GETMOBIT поддерживают динамически добавляемые режимы работы, которые реализуются через SD App-приложения. Работа с SD App-приложениями на устройстве GETMOBIT возможна с помощью режимов GM-Box.

Режим GM-Box – режим, в котором запускается единственное SD App-приложение, завершение данного приложения приводит к полному выходу из пользовательской сессии на устройстве. Все доступные режимы работы приведены в Таблица 4.

2.2.2 Единый профиль пользователя

2.2.2.1 Типы учетных записей пользователей

В платформе GMSS NG существуют два типа учетных записей пользователей:

- локальные учетные записи пользователей, созданные локально на СУ для тестовых целей. Такие пользователи в веб-консоли СУ обозначены иконкой (Рисунок 3);
- AD/LDAP учетные записи пользователей, созданные на основе синхронизации с AD/LDAP.

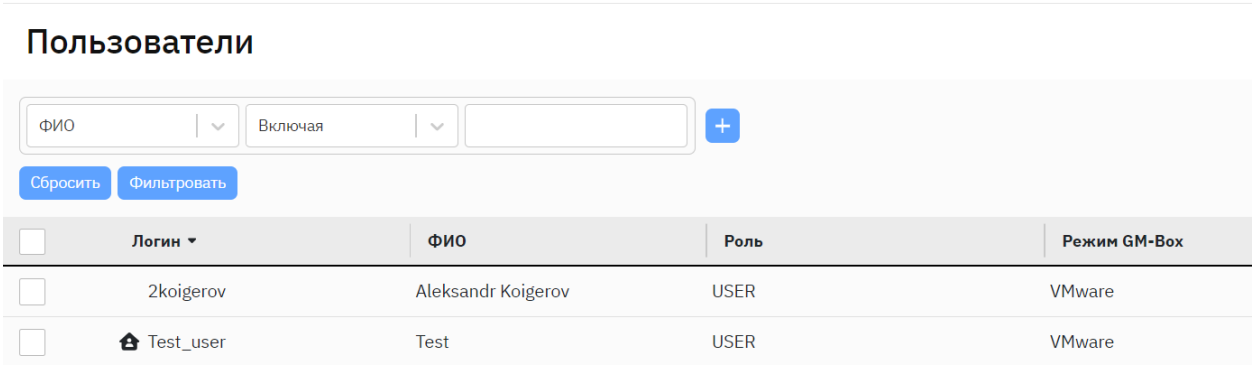


Рисунок 3 – Пример учетных записей пользователей: Test_user – локальная учетная запись, 2koigerov – доменная

2.2.2.2 Шаблоны режимов и приложений

Шаблон является унифицированной настройкой работы пользовательской сессии на устройстве для группы пользователей. Группа пользователей представлена

[1] В зависимости от характеристик устройства (объём носителя) и параметров SD App-приложений, количество одновременно устанавливаемых на устройство приложений может быть ограничено.

группой пользователей в Службе каталогов (AD/LDAP), с которой настроена синхронизация. Группа пользователей в Службе каталогов (AD/LDAP) объединена общим признаком: значением атрибута, группой в AD/LDAP и т.д. Существуют два вида шаблонов:

- шаблон режима GM-Box/SD App-приложения (далее – шаблон) – настройка режима GM-Box/SD App-приложения для группы пользователей (см. п. 5.6.1);
- режим «Витрина» – особый режим работы GM-Box для группы пользователей, позволяющий администратору настроить доступ к нескольким режимам GM-Box/SD App-приложениям (см. п. 5.6.3).

Примечание. *Шаблон настройки для режима GM-Box/SD App-приложения появляется на СУ только после добавления в реестр приложений СУ нового SD App-приложения.*

2.2.2.3 Профиль пользователя

В платформе GMSS NG для обеспечения доступа пользователя к целевым сервисам используется единый профиль пользователя. Единый профиль пользователя доставляется на управляемое устройство (GM-Box, управляемое устройство сторонних производителей) после успешной аутентификации пользователя.

Существуют два типа единого профиля пользователя: предварительный (далее – предварительный профиль) и единый финальный (далее – финальный профиль).

Предварительный профиль пользователя формируется на основе правил синхронизации с AD/LDAP или путем ручного создания локальной учетной записи пользователя.

Примечание. *Значения полей в предварительном профиле пользователя (кроме локальной учетной записи пользователя) зависят только от параметров настройки синхронизации с корпоративной службой каталогов AD/LDAP.*

Финальный профиль пользователя (Рисунок 4) формируется после аутентификации пользователя в пользовательской сессии при запросе к СУ со стороны устройства. Таким образом, если внести изменения в шаблон, то при повторном запросе (входе пользователем в сессию) финальный профиль пользователя будет сформирован на основе новых данных.

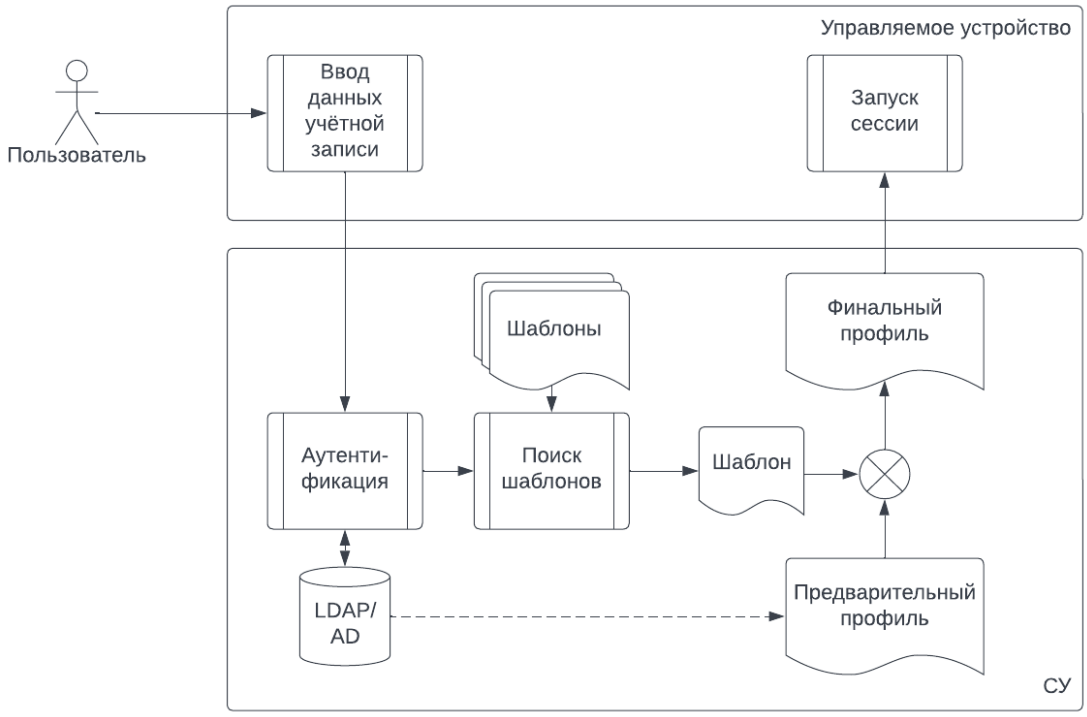


Рисунок 4 – Процесс формирования финального профиля пользователя

Примечание. *Значения полей в финальном профиле пользователя зависят только от значений полей в шаблоне, который применен в соответствии с правилами.*

Финальный профиль пользователя формируется на основе статических или динамических правил:

- статические правила – прямое указание в профиле пользователя шаблона, данные которого надо использовать;
- динамические правила формируются на основе правил сопоставления шаблонов. Как только будет найден первый шаблон, удовлетворяющий правилам, процесс поиска шаблона останавливается, и шаблон выбирается для формирования финального профиля пользователя.

Поиск подходящего шаблона для пользователя происходит по следующим правилам и приоритетам:

1) шаблон, указанный в профиле пользователя в поле **Шаблон профиля** (статическое правило);
2) первый шаблон, удовлетворяющий правилу сопоставления, с типом сопоставлений: **Атрибут**, **Группа** (динамическое правило);
3) шаблон с типом сопоставления: **По умолчанию** (динамическое правило).

Если подходящий шаблон найден, то финальный профиль пользователя будет составлен из предварительного профиля пользователя и параметров, заданных шаблоном. Если подходящий шаблон не найден, то финальный профиль пользователя будет составлен из предварительного профиля пользователя.

При заполнении значениями полей финального профиля пользователя применяются следующие приоритеты:

1) значение поля **Режим GM-Box** из профиля пользователя всегда игнорируется, и используется значение поля **Режим GM-Box**, указанного в шаблоне;
2) если в поле предварительного профиля пользователя указано значение, то его приоритет выше значения в одноименном поле шаблона;
3) если поле предварительного профиля пользователя не заполнено, то будет использовано значение из одноименного поля шаблона.

Примечание. *Веб-консоль СУ при просмотре учетных записей пользователей показывает предварительный вид финального профиля пользователя. Значения полей, которые были подставлены из шаблонов, показаны серым цветом.*

3 Подготовка к развертыванию платформы GMSS NG

Рекомендуемый процесс развертывания платформы GMSS NG приведен на Рисунок 5.

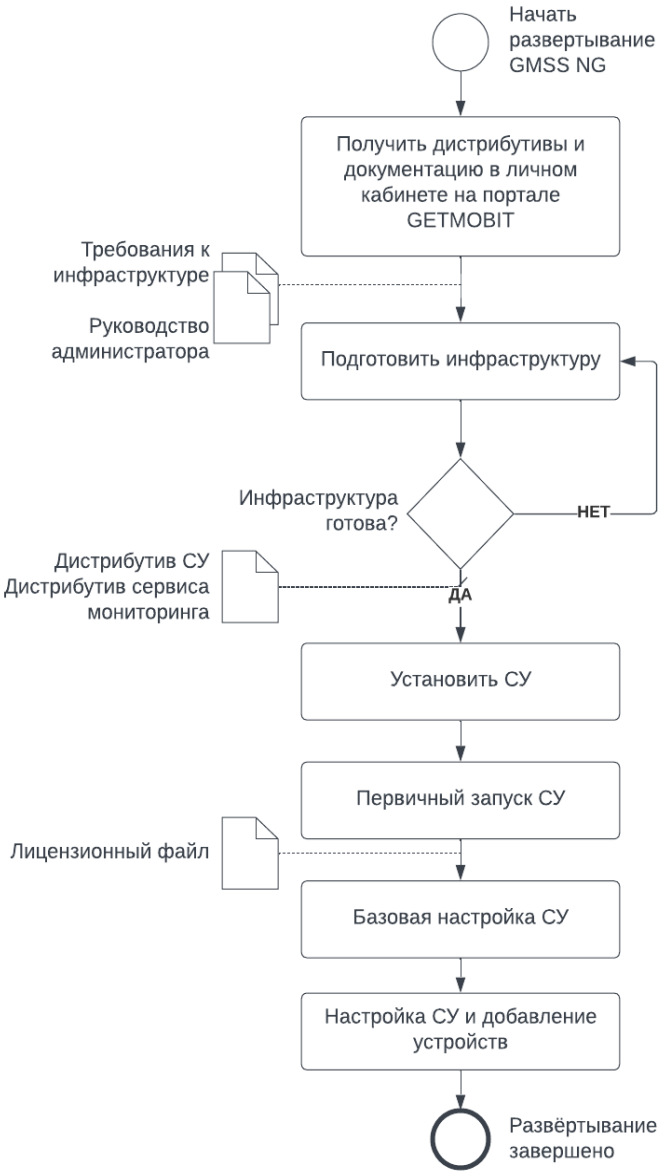


Рисунок 5 – Рекомендуемый процесс развертывания GMSS NG

Пошаговое описание процесса развертывания GMSS NG приведено в следующих разделах.

3.1 Доступ к «Личному кабинету»

Доступ к разделу «Личный кабинет» (далее – ЛК) на портале GETMOBIT (cp.getmobit.ru) предоставляется по заявке в службу технической поддержки GETMOBIT через вашего дистрибутора.

3.2 Подготовка инфраструктуры

Перед развертыванием GMSS NG, загрузите из ЛК документ «GM Smart System Требования к инфраструктуре». Ознакомьтесь и выполните требования к инфраструктуре с учетом особенностей архитектуры вашей автоматизированной информационной системы. Для удобства администратора, настоящее Руководство администратора частично дублирует информацию, приведенную в указанном документе.

3.3 Проверка готовности инфраструктуры

Приступайте к установке СУ и дальнейшему развертыванию системы только после того, как убедитесь в готовности инфраструктуры. Проверка готовности инфраструктуры позволит снизить риски возникновения ошибок при дальнейшей настройке системы и ускорить ввод ее в эксплуатацию.

Для проверки готовности инфраструктуры, воспользуйтесь контрольным списком критериев приведенным в Таблица 1.

Таблица 1 – Контрольный список критериев готовности инфраструктуры

№	Описание требования	Критерии готовности	✓/✗
1	Для установки СУ выделен физический или виртуальный сервер.	a. К консоли сервера можно подключиться по SSH или через консоль ВМ, проверен логин/пароль _____	☐
		b. На сервер можно загрузить дистрибутивы СУ	☐

№	Описание требования	Критерии готовности	✓/✗
2.1	Готовность инфраструктуры VDI/ Терминальных серверов	a. Клиентом _____версия ____можно подключиться к VDI/Терминальному серверу	☐
		b. IP-адрес или DNS-имя сервера VDI, терминального сервера или брокера _____	☐
		c. VDI логин/пароль тестового пользователя _____	☐
2.2	Веб-портал доступен (при использовании веб-режима)	a. Веб браузером _____ можно подключиться к порталу _____	☐
3	Настроена IP-АТС	a. Устройством/Клиентом _____ версия _____ можно подключиться к IP-АТС и произвести звонок на другого абонента	☐
		b. IP-адрес или DNS-имя сервера IP-телефонии (SIP-сервера) _____	☐
		c. SIP логин/пароль тестового пользователя _____	☐
4	Выполнены требования к пропускной способности сети.	a. Пропускная способность каналов связи между GM-Box и VDI/Телефонией/Сервером управления не менее _____ mbps	☐
5	Открыты порты и протоколы в соответствии с правилами сетевого взаимодействия	a. Порты и протоколы открыты и просканированы сторонними утилитами (например nmap)	☐
		b. Приложен отдельный чек лист по таблице портов и протоколов.	☐
6	Информация для интеграции со службой каталогов	a. IP-адрес или DNS-имя сервера службы каталогов, порт _____	☐
		b. Логин/пароль технического пользователя _____	☐
		c. base DN Корневая папка поиска _____	☐
		d. Фильтр пользователей _____	☐
		e. Фильтр администраторов _____	☐

4 Установка и базовая настройка СУ

4.1 Требования к СУ

СУ может быть установлен как на физически выделенном сервере, так и на ВМ. На ВМ или сервере должны быть установлены Docker CE (версия 20.10.1 или выше) и одна из приведенных ниже ОС:

- 64-bit Ubuntu (версия 16.04 или выше);
- Astra Linux SE (версия 1.7.5);
- РедОС (версия 7.3.4).

***Примечание**. Актуальная документация по ОС и Docker CE находится на сайтах соответствующих производителей. Приводимые ниже инструкции верны для конкретных указанных версий.*

***Внимание!** В случае, если в ОС настраивается встроенный межсетевой экран (iptables или другой), правила межсетевого взаимодействия должны соответствовать правилам, приведенным в «GM Smart System Требования к инфраструктуре».*

Минимальные требования к аппаратному обеспечению СУ:

- 4 vCPU;
- 16 GB RAM;
- 100 GB HDD.

Для автоматического поиска СУ необходимо настроить *DNS-запись* типа *A* или *CNAME* с именем *getmobit.**, например: **getmobit.*example.org*** и указать локальный домен в *DHCP option 119 - 'Domain Search List'*, например: ***example.org***

Если на *DNS-сервере* указано имя СУ ***getmobit.*домен*.ru*,** то устройство возьмет домен из *DHCP option 015*. В этом случае *DHCP option 119* не обязательна для заполнения.

Настройка и администрирование СУ осуществляется:

- с помощью командной строки (текстовой консоли) с доступом по ssh (openssh, putty и др. приложения) для низкоуровневых задач и базовой настройки СУ: установка deb-пакетов, обновление deb-пакетов, перезагрузка, установка сертификатов, изменение параметров ОС;
- с помощью веб-консоли осуществляются все остальные задачи по администрированию СУ и устройствами GM-Box.

Внимание! *После выполнения задач администрирования с помощью командной строки рекомендуется запретить доступ к СУ по протоколу SSH или ограничить доступ к СУ по протоколу SSH с определенных ресурсов.*

4.2 Требования для работы GM-Box

Для работы устройства GM-Box необходимо использовать сервис DHCP, предоставляющий следующую информацию:

- выдаваемый IP-адрес;
- IP-адрес сервера имен (DNS-сервер);
- IP-адрес сервера точного времени (NTP-сервер);
- локальный домен, указываемый в DHCP option 119 'Domain Search List';
- [опционально] временная зона, указываемая в DHCP option 101 в текстовом формате.

Внимание! *В случае выделения сервиса IP-телефонии в отдельный VLAN (voice VLAN), необходимо обеспечить функционирование сервиса DHCP и трансляцию DNS в voice VLAN.*

4.3 Требования для работы устройств с установленным GMSS NG Client

Для работы устройства с установленным GMSS NG Client необходимо использовать сервис DHCP, предоставляющий следующую информацию:

- выдаваемый IP-адрес;
- IP-адрес сервера имен (DNS-сервер);
- IP-адрес сервера точного времени (NTP-сервер);
- локальный домен, указываемый в DHCP option 119 – 'Domain Search List';
- [опционально] временная зона, указываемая в DHCP option 101 в текстовом формате.

4.4 Установка и запуск СУ

4.4.1 Установка СУ

Условия для выполнения этапа:
1. Выполнены Требования к инфраструктуре
2. Подготовлен сервер (ВМ) с минимальными требованиями
3. Выполнены требования для работы GM-Box и/или GMSS NG Client

Результат выполнения этапа:
Требуемые пакеты установлены

Для выполнения работ по инсталляции, обновлению и перезапуску СУ, установки TLS/SSL сертификатов и настройки параметров ОС, необходим доступ к ВМ по ssh (openssh, PUTTY и др. программы) с правами суперпользователя (root).

Штатная эксплуатация СУ осуществляется только с использованием веб-консоли.

Установку СУ можно выполнить из deb-пакета для 64-bit Ubuntu 20.04 или Astra Linux SE 1.7.5. Установка СУ на сервер с РедОС 7.3.4 осуществляется из rpm-пакета.

Внимание! *Для выполнения команд и настроек с правами суперпользователя (root) рекомендуется использовать команду* ***sudo****. В примерах ниже, предполагается, что перед выполнением команд выполнена команда* ***sudo su*** *или команда* ***sudo*** *добавляется индивидуально.*
Пароль для суперпользователя (root) должен формироваться, храниться и меняться в соответствии с парольными политиками, принятыми в организации.

4.4.1.1 Установка СУ на Ubuntu

1. Специальные требования к разбиению диска для установки ОС не предъявляются. В случае необходимости разбивки диска, необходимо обеспечить следующие размеры разделов:
    - **/tmp** – не менее 10 ГБ;
    - **/var/lib/docker** – не менее 50 ГБ.
2. Для установки Docker CE перейдите по ссылке https://download.docker.com/linux/ubuntu/dists/ и выберите версию Ubuntu, используемую для установки СУ.
3. Перейдите в каталог **pool/stable/amd64** и скачайте необходимые пакеты **docker-ce**, **docker-ce-cli** и **containerd.io**. Например:

```
containerd.io_1.4.6-1_amd64.deb;
```

```
docker-ce-cli_20.10.7~3-0~ubuntu-xenial_amd64.deb;
docker-ce_20.10.7~3-0~ubuntu-xenial_amd64.deb).
```

4. Скачанные пакеты скопируйте на сервер, на котором будет установлен СУ, и установите их последовательно с помощью команды:

```
dpkg -i /путь_до_пакета/имя_пакета.deb
```

Например:

```
dpkg -i containerd.io_1.4.6-1_amd64.deb
dpkg -i docker-ce-cli_20.10.7~3-0~ubuntu-xenial_amd64.deb
dpkg -i docker-ce_20.10.7~3-0~ubuntu-xenial_amd64.deb
```

После завершения установки необходимо проверить, что Docker CE запущен. Проверить состояние Docker CE после установки можно командой:

```
sudo systemctl status docker
```

Если Docker CE не запустился, выполните команду:

```
sudo systemctl start docker
```

Установите пакет СУ пользователем с правами суперпользователя (root):

```
dpkg -i gmserver_[VERSION]_amd64.deb
```

4.4.1.2 Установка СУ на Astra Linux

Для установки СУ на Astra Linux 1.7.5 требуется установка Docker CE из стороннего репозитория:

```
wget http://ftp.us.debian.org/debian/pool/main/libs/libseccomp/libseccomp2_2.5.4-1+b3_amd64.deb
wget https://download.docker.com/linux/ubuntu/dists/bionic/pool/stable/amd64/containerd.io_1.6.20-1_amd64.deb
wget https://download.docker.com/linux/ubuntu/dists/bionic/pool/stable/amd64/docker-ce-cli_23.0.3-1~ubuntu.18.04~bionic_amd64.deb
wget https://download.docker.com/linux/ubuntu/dists/bionic/pool/stable/amd64/docker-ce_20.10.9~3-0~ubuntu-bionic_amd64.deb

sudo apt install ./libseccomp2_2.5.4-1+b3_amd64.deb
sudo apt install ./containerd.io_1.6.20-1_amd64.deb
sudo apt install ./docker-ce-cli_23.0.3-1~ubuntu.18.04~bionic_amd64.deb
sudo apt install ./docker-ce_20.10.9~3-0~ubuntu-bionic_amd64.deb
```

Установите СУ:

```
sudo apt install gmserver*.deb
```

4.4.1.3 Установка СУ на РедОС

Для установки СУ на РедОС 7.3.4 требуется предварительное включение модуля SELinux и установка Docker CE из стороннего репозитория.

Для включения модуля SELinux создайте или отредактируйте файл ***/usr/local/etc/getmobit/meta.env***, внеся в него строку:

```
ENABLE_SELINUX_MODULE=true
```

Из репозитория:
https://mirrors.cloud.tencent.com/docker-ce/linux/centos/7/x86_64/stable/Packages/
скачайте следующие пакеты: ***containerd.io, docker-ce, docker-ce-cli***.

Установите скачанные пакеты, запустите Docker CE и проверьте его работоспособность:

```
dnf install ./*.rpm

systemctl enable docker --now
systemctl status
```

Установите СУ:

```
sudo dnf install gmserver*.rpm
```

4.4.2 Установка сервиса мониторинга и журналирования

Условия для выполнения этапа:
1. Выполнены условия для установки СУ
2. Установлены пакеты docker и СУ

Результат выполнения этапа:
Установлены пакеты сервиса мониторинга и журналирования

Примечание. *Ниже рассмотрен пример, когда сервис мониторинга разворачивается на том же сервере, где установлен СУ. Для получения инструкций по разворачиванию сервиса мониторинга на отдельном сервере, обратитесь в отдел техподдержки GETMOBIT.*

Для мониторинга вы можете использовать платформу Grafana, которая включена в пакет сервиса мониторинга и позволяет анализировать данные и визуализировать результаты с помощью диаграмм, таблиц и карт.

Установите пакет сервиса мониторинга gmserver-monitoring на тот же сервер, где развернут СУ. Убедитесь, что установка завершена успешно.

```
dpkg -i gmserver-monitoring_[VERSION]_amd64.deb
```

Откройте файл **/usr/local/etc/getmobit/monitoring/config.env**

Примечание. *Файл /usr/local/etc/GETMOBIT/monitoring/config.env предназначен для настройки отдельных параметров СУ в соответствии с настоящей инструкцией. Описание параметров файла приведено в Приложении «В. Конфигурационный файл сервера управления».*

Добавьте в **/usr/local/etc/getmobit/monitoring/config.env** строки:

```
PROM_TARGETS=http://gateway:8080
KIBANA_ROOT=/kibana
```

1. Перезапустите gmserver-monitoring. Убедитесь, что сервис перезапустился, выполнив команды:

```
systemctl restart gmserver-monitoring
systemctl status gmserver-monitoring
```

Добавьте/отредактируйте в **/usr/local/etc/getmobit/docker/config.env** строки:

```
KIBANA_HOST=kibana
GRAFANA_HOST=grafana
```

2. Перезапустите СУ. Убедитесь, что сервис перезапустился.

```
systemctl restart gmserver
systemctl status gmserver
```

Откройте браузер и подключитесь к веб-консоли СУ. Для перехода к сервисам мониторинга и логирования воспользуйтесь кнопками в веб-консоли (Рисунок 6).

В разделе **Сводка** так же отображена кнопка 

(рисунок 6) для настройки и управления системой оповещений. Она позволяет создавать правила мониторинга, которые будут отслеживать метрики в реальном времени и уведомлять администраторов или ответственных лиц, если значения метрик выходят за пределы заданных порогов или нарушаются определенные условия.

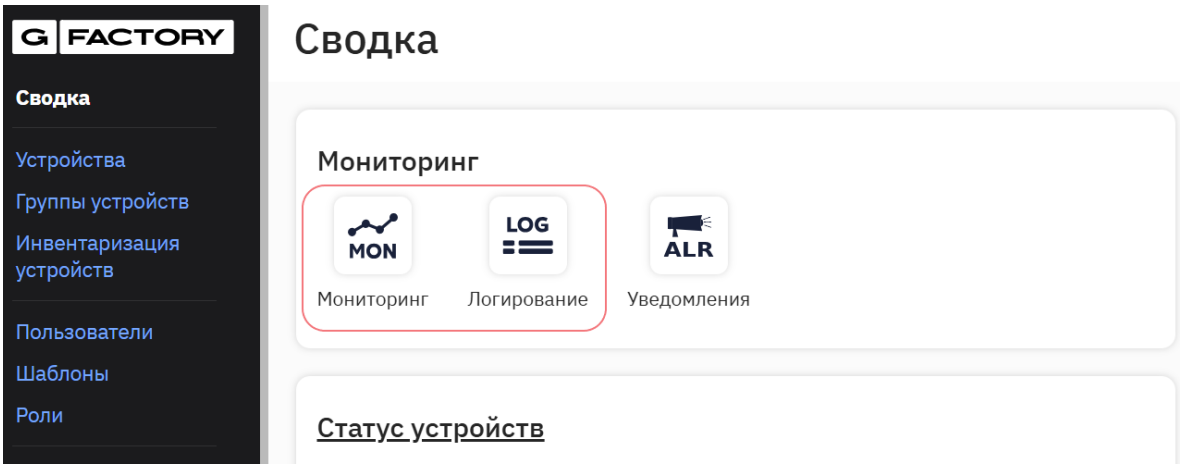


Рисунок 6 – Внешний вид кнопок мониторинга и логирования

Кнопки мониторинга и логирования отображаются при корректно выполненных настройках СУ в следующих разделах веб-консоли:

- «Сводка»;
- «Устройства» (в каждой строке для управляемых устройств с преднастроенными фильтрами для каждого устройства);
  - на странице устройства в карточке устройства;
- «Пользователи» (только сервис логирования, в каждой строке для пользователя в списке с преднастроенным фильтром по пользователю).

Для установки сервиса мониторинга на отдельном сервере обратитесь в службу технической поддержки ООО «ГЕТМОБИТ».

4.4.3 Первичный запуск СУ

Условия для выполнения этапа:
1. СУ установлен
2. Конфигурационный файл для сервисов мониторинга и журналирования отредактирован

Результат выполнения этапа:
СУ запущен

После установки СУ запускается автоматически. Убедитесь, что состояние сервисов активно, выполнив команду:

```
systemctl status gmserver
```

Если сервисы неактивны, запустите СУ командой:

```
systemctl start gmserver
```

Загрузка СУ может занимать до 5 минут. После запуска выполните настройку СУ в веб-консоли (см. подраздел 4.5).

Если СУ не запускается, убедитесь в корректности выполненных действий в подразделе 4.1, п. 4.4.1, п.п. 4.4.1.2. В случае, если все действия выполнены корректно, но СУ не запускается, обратитесь в службу технической поддержки в соответствии с вашим договором технической поддержки.

4.5 Быстрый старт, базовая настройка СУ

Условия для выполнения этапа:
СУ запущен

Результаты выполнения этапа:
1. Получен доступ к веб-консоли СУ
2. Установлен адрес агента СУ (Discovery адрес)
3. Применен лицензионный файл
4. Создан тестовый пользователь
5. Подключено устройство пользователя
6. Настроена синхронизация со службой каталогов

Для базовой настройки СУ выполните действия описанные в п. 4.5.1-4.5.6

4.5.1 Тестовое подключение к консоли СУ

1. Откройте браузер и введите адрес консоли СУ, например, ***getmobit.example.org*** (см. п. 4.1).
2. Дождитесь появления экрана приглашения с окном аутентификации (Рисунок 7).

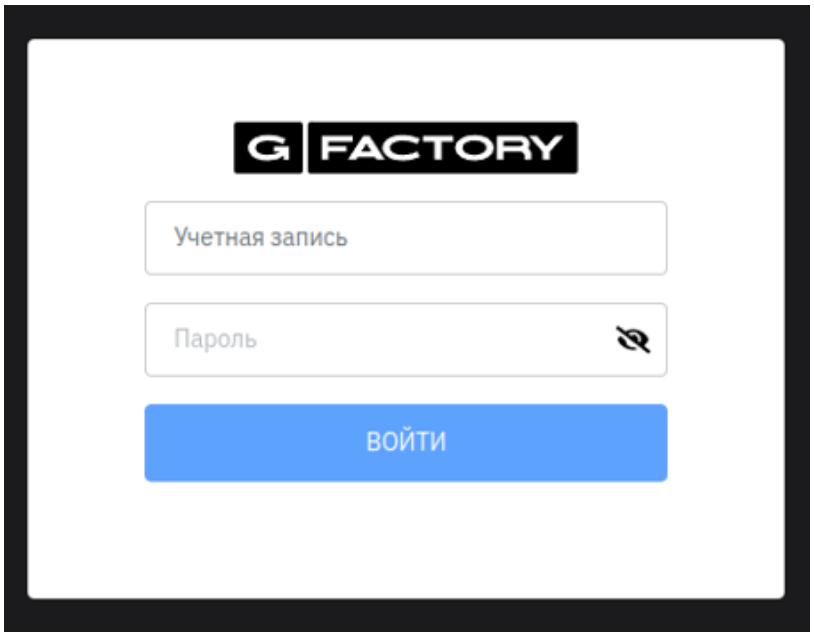


Рисунок 7 – Вид окна аутентификации

3. В открывшемся окне аутентификации введите логин и пароль администратора СУ (см. п. 5.5.1).

Значения по умолчанию:

```
Login/Password: superadmin/superadmin или
Login/Password: admin/admin
```

Внимание! *Примеры настроек и действий в настоящем документе описаны для пользователя с правами superadmin. Если на этапе эксплуатации для администрирования СУ определяются дополнительные роли, убедитесь в корректности назначения прав соответствующим ролям.*

После первого входа измените и запомните пароль администратора в файле **/usr/local/etc/getmobit/docker/config.env,** например:

```
LDAP_USER_LOGIN=admin
LDAP_USER_PASSWORD=mail123#
LDAP_SUPER_USER_LOGIN=superadmin
LDAP_SUPER_USER_PASSWORD=mail123#
```

Учетная запись администратора имеет доступ ко всей функциональности и используется для начальных настроек и восстановления доступа к веб-консоли для администрирования СУ.

Для выполнения регулярных задач по администрированию СУ следует использовать доменные учетные записи, включенные в список администраторов и суперадминистраторов (см. п. 4.5.6).

Результат шага

Открылась главная страница веб-консоли (Рисунок 8)

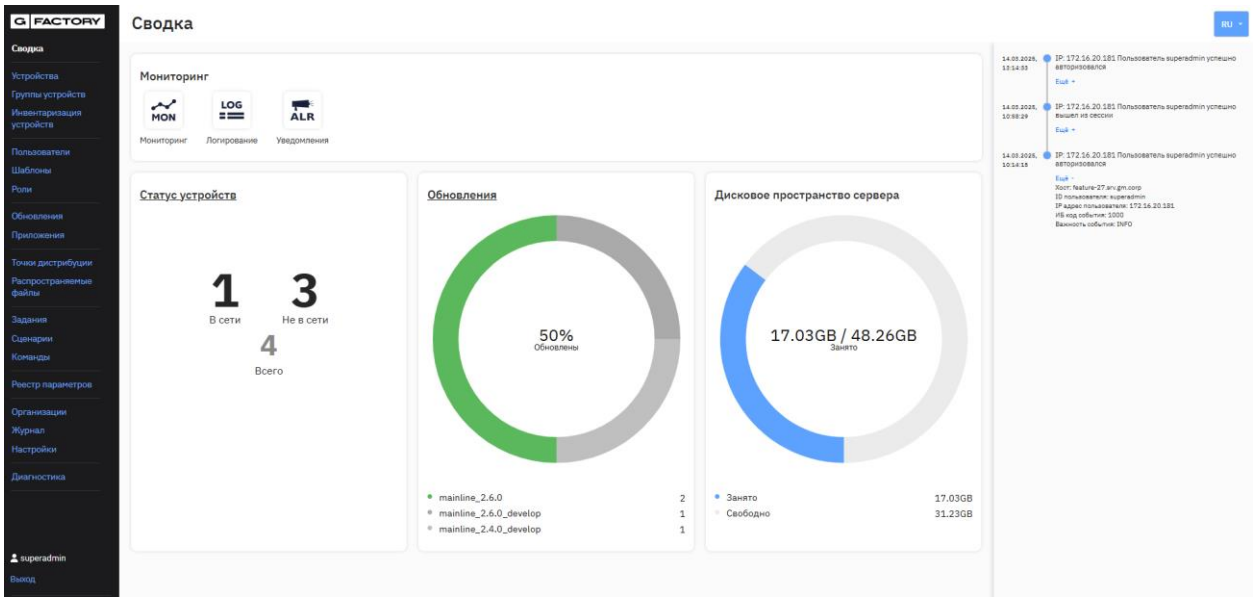


Рисунок 8 – Вид главной страницы веб-консоли

4.5.2 Установка Discovery адреса для СУ

1. В веб-консоли выберите раздел **Организации**. В поле **Первичный discovery адрес** задайте корректный Discovery адрес СУ. Указывать протокол подключения (http или https), начиная с версии сервера 3.7.1, не требуется.
   Например, getmobit.example.org
   Где ***getmobit.examlple.org*** - DNS имя СУ.

Примечание. *DHCP-сервер должен транслировать зону* ***example.org****.*

Внимание! *При отсутствии DNS-записи и настройки DHCP-сервера (включая DHCP option 119 - 'Domain Search List') устройство GM-Box не сможет обнаружить и подключиться к СУ автоматически.*

2. Нажмите кнопку **Сохранить изменения**.

Дополнительная информация приведена в подразделе 5.14

Результат шага

В веб-консоли задан первичный Discovery адрес СУ.

4.5.3 Установка лицензионного файла

Для активации лицензии скачайте лицензионный файл из личного кабинета по адресу: cp.getmobit.ru (логин и пароль для доступа в личный кабинет запросите в отделе технической поддержки ООО «ГЕТМОБИТ») или получите его у партнера ООО «ГЕТМОБИТ».

В веб-консоли выберите раздел **Настройки,** перейдите на вкладку **Лицензия** и загрузите лицензионный файл.

Примечание. *Если в лицензионном файле будет отсутствовать тип лицензии Приложение с ID: WEB, то при дальнейшей настройке использование режима Web на управляемых устройствах будет невозможно.*

Дополнительная информация приведена в п. 5.16.1.

Результат шага

Параметры активированной лицензии отображаются на вкладке **Лицензия** (Рисунок 9).

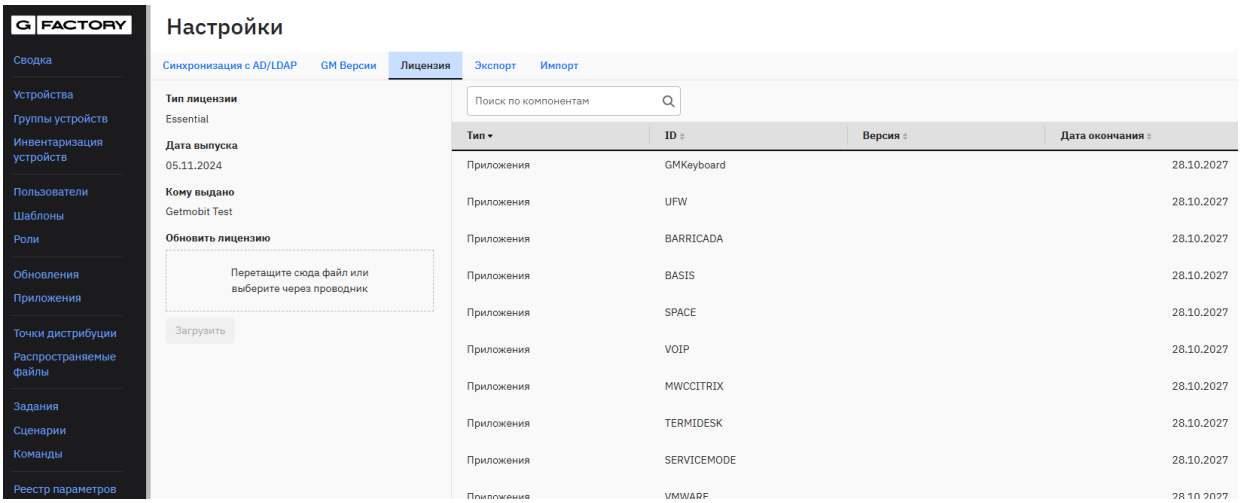


Рисунок 9 – Вид окна вкладки Лицензия

4.5.4 Создание тестового пользователя

В веб-консоли выберите раздел **Пользователи**, затем нажмите кнопку **Добавить**. В форме окна **Новый пользователь** заполните поля:

- Логин – webtest;
- Пароль и повторный ввод пароля;
- ФИО;

- Роль – USER;
- Режим GM-Box – Веб;
- Веб-адрес – URL-адрес сайта, который будет открываться после входа в систему. Например, www.getmobit.ru или другой веб-портал организации.

Нажмите кнопку **Создать**

Дополнительная информация приведена в подразделе 5.5.

Результат шага

В списке раздел **Пользователи** (Рисунок 10) отображается созданный тестовый пользователь с логином webtest

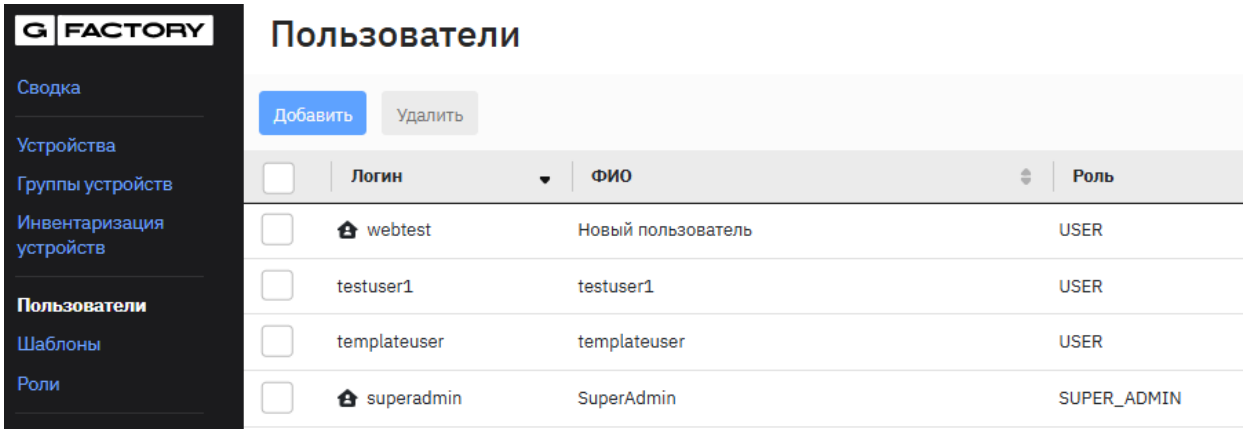


Рисунок 10 – Вид окна раздела **Пользователи**

4.5.5 Подключение устройства

Внимание! *При отсутствии DNS-записи и настройки DHCP-сервера (включая DHCP option 119 - 'Domain Search List') управляемое устройство не сможет обнаружить и подключиться к СУ автоматически. В этом случае для подключения к СУ потребуется ручная настройка на каждом управляемом устройстве.*
Для корректной работы DHCP-сервер должен раздавать корректные NTP и DNS-серверы.
До подключения устройства убедитесь в корректном выполнении п. 4.5.2.

1. Подключите управляемое устройство в сеть, включите его и дождитесь загрузки.

2. На экране приветствия GM-Box[2] нажмите пиктограмму  и выберите **Настройка агента** (Рисунок 11). Если автоматический выбор СУ не работает, введите адрес СУ. Убедитесь, что устройство подключилось к СУ.
3. Выполните несколько попыток входа/выхода пользователем webtest. Откроется экран сессии пользователя.

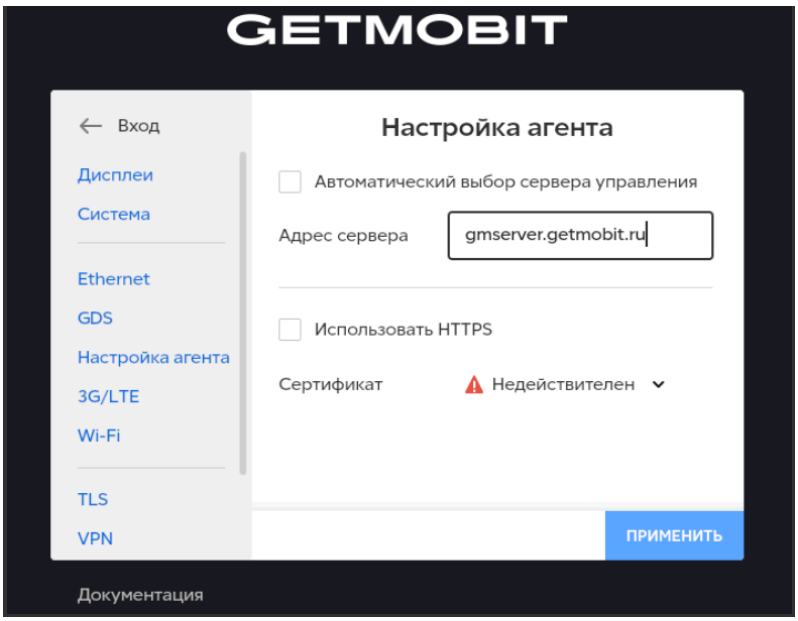


Рисунок 11– Вид окна **Настройка агента**

Результат шага

В веб-консоли устройство отображается в списке со статусом **В сети** (Рисунок 12).

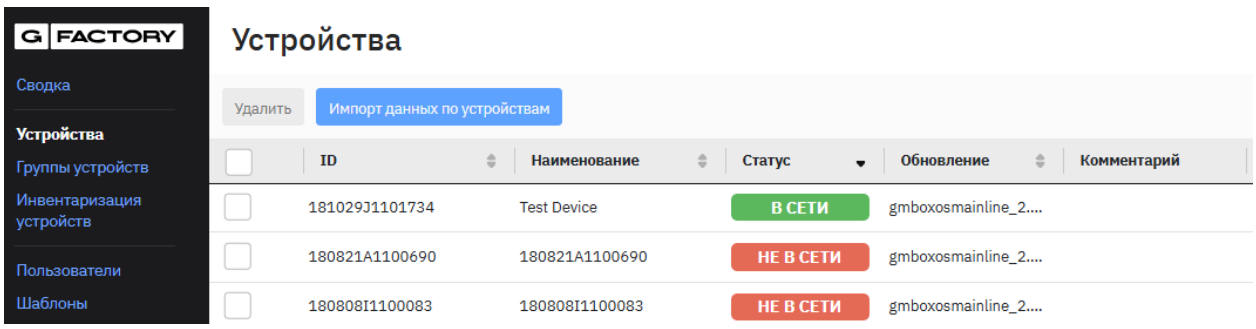


Рисунок 12 – Вид раздела Устройства

[2] Здесь и далее приводятся примеры настроек для устройств GM-Box G1. Настройки устройств с ПО GMSS NG Client выполняются идентично, если не указано иное.

4.5.5.1 Первичная настройка (инициализация) устройства

После первого подключения устройства к СУ, переподключения с другого СУ к данному, а также по факту подключения к СУ после проведенного сброса устройства к заводским настройкам, происходит **автоматическое** выполнение первичной настройки устройства.

Первичная настройка включает проведение процедуры Zero Deploy, а также сохранение данных о СУ на подключенном устройстве.

Запуск заданий и сценариев на устройстве возможен только после завершения первичной настройки.

Результат выполнения первичной настройки отображается на странице устройства на вкладке **Информация** в блоке **Конфигурация**. При корректной первичной настройке результат должен соответствовать значению **Finished** (Рисунок *13*).

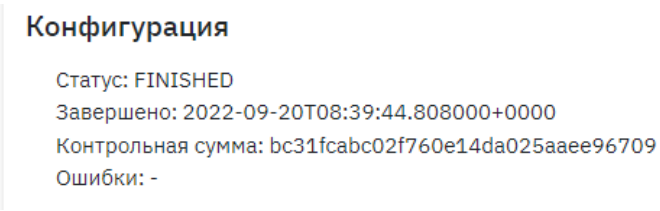


Рисунок 13 – Вид блока **Конфигурация**

4.5.6 Настройка синхронизации данных с корпоративной службой каталогов/LDAP

***Примечание**. Этот шаг можно пропустить, если вы хотите выполнить базовую настройку СУ только для локальной учетной записи пользователя.*

Настройка синхронизации данных с корпоративной службой каталогов необходима для того, чтобы пользователи могли выполнять аутентификацию на GM-Box с использованием доменных учетных записей.

Для настройки синхронизации с корпоративной службой каталогов в веб-консоли выберите раздел **Настройки**. В левой части страницы находятся поля настройки синхронизации, в которых необходимо указать значения в соответствии с Таблица 2.

Далее выполните действия, описанные ниже.

1. Установите флажок **Включить синхронизацию**.
2. Заполните поля **AD/LDAP Сервер** (укажите host без ldap:// и т.п.), **AD/LDAP Порт**, **Логин**, **Пароль**.

Таблица 2– Значение полей настройки синхронизации

Поле	Описание
AD/LDAP Сервер	FQDN или IP-адрес сервера корпоративной службы каталогов
AD/LDAP Порт	Номер порта сервера корпоративной службы каталогов для TCP/UDP соединений. **Значение по умолчанию:** *порт 389*.
Логин	Логин пользователя в корпоративной службе каталогов для связи со службой каталогов. Режим ReadOnly. Рекомендуется создать в корпоративной службе каталогов отдельную учетную запись для СУ.
Пароль	Пароль пользователя в корпоративной службе каталогов для связи со службой каталогов

3. Для проверки соединения с корпоративной службой каталогов AD/LDAP нажмите **Проверить**.

После проверки соединения появится сообщение «Соединение успешно установлено». Если соединение не установлено, убедитесь, что все параметры заданы корректно.

***Примечание**. Чтобы задать корректные фильтры для синхронизации данных из AD, обратитесь к системному администратору своей компании.*

4. В поле **Корневой элемент (Base DN)** укажите корневую папку со всеми вложенными контейнерами и организационными подразделениями (Organization Units), в которой СУ осуществляет поиск объектов. Формат: distinguished name (DN).

Например, для фильтра внутри домена *getmobit.ru* укажите

```
dc=getmobit,dc=ru
```

5. В поле **Интервал синхронизации (минут)** задайте интервал времени 1 минута[3] между циклами автоматической синхронизации. Сразу после сохранения настроек запустится синхронизация.
6. В поле **Фильтр для получения списка пользователей с ролью: <роль>** для получения списка всех активных пользователей используйте фильтр:

[3] Интервал времени равный 1 минуте указан в качестве примера. Малые интервалы времени рекомендуется использовать на этапе запуска и отладки системы. В режиме промышленной эксплуатации рекомендуется использовать более длительные интервалы (например, 480 минут, что рано 8 часам).

```
(&(objectCategory=person)(objectClass=user)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))
```

***Примечание**. Все фильтры для получения списков пользователей по ролям пишутся на основе стандартного синтаксиса LDAP фильтров.*

7. Поле **Атрибуты** содержит список полей, которые механизм синхронизации читает из профиля пользователя в службе каталогов.
   Введите через запятую следующие обязательные значения:

```
cn,sn,objectClass,sAMAccountName,objectGUID,userPrincipalName,objectSid
```

   где:

sAMAccountName	логин пользователя в AD/LDAP
userPrincipalName	пароль пользователя в AD/LDAP
cn	общее имя
sn	фамилия
objectClass	группировка связанных объектов, например, *user*
objectGUID	идентификатор объекта
objectSid	уникальный идентификатор пользователя AD, на основе которого при синхронизации генерируется значение uidNumber. Необходим для корректной работы авторизации пользователей в системе

   Для синхронизации фото на аватаре добавьте *thumbnailPhoto*.

***Примечание**. Чтобы добавить минимальный список атрибутов из шаблона MS AD, нажмите кнопку Шаблоны значений.*

8. В поле **Соответствие полей** через запятую укажите список названий полей профиля пользователя СУ и корпоративной службы каталогов для одинаковых параметров. Список доступных ключей представлен в подразделе 5.5.
   Необходимо указать в формате *ключ=значение*. Где *ключ* – запись в БД СУ, а *значение* – атрибуты, считанные из службы каталогов. Все поля, указанные в качестве значений, должны быть в списке **Атрибутов** (см. п.5), в противном случае возможны ошибки синхронизации.

   Обязательные значения:

```
password=userPrincipalName,title=cn,username=sAMAccountName
```

Примечания

1. *Чтобы добавить минимальный список соответствия полей из шаблона MS AD, нажмите кнопку **Шаблоны значений**.*
2. *Чтобы в профиле пользователя добавлялся логин из AD в поле **VDI Пользователь**, необходимо добавить значение: **configuration.vdi.user=sAMAccountName***

9. Нажмите кнопку **Сохранить изменения**. После нажатия кнопки запускается сессия синхронизации. Во время этого в AD выполняется поиск записей пользователей, удовлетворяющих условиям ролевых фильтров, эти записи также должны удовлетворять условиям, заданным в корневом элементе. У пользователей, которые удовлетворяют условиям фильтров, извлекаются атрибуты службы каталогов и на их основе формируется профиль пользователя. Этот профиль отображается в разделе **Пользователи**.

Дополнительная информация по настройке синхронизации с корпоративной службой каталогов приведена в п. 5.16.2.

Результат

Выполнена синхронизация полей корпоративной службы каталогов AD/LDAP и полей внутренней службы каталогов СУ. Пользователи из службы каталогов отображаются в разделе **Пользователи** веб-консоли СУ.

Если через 30-40 секунд после нажатия кнопки не появилось сообщения на зеленом фоне «Синхронизация запущена» (Рисунок *14*) - перезапустите СУ. Если после перезапуска сообщение так и не появилось, обратитесь в в Service Desk GETMOBIT.

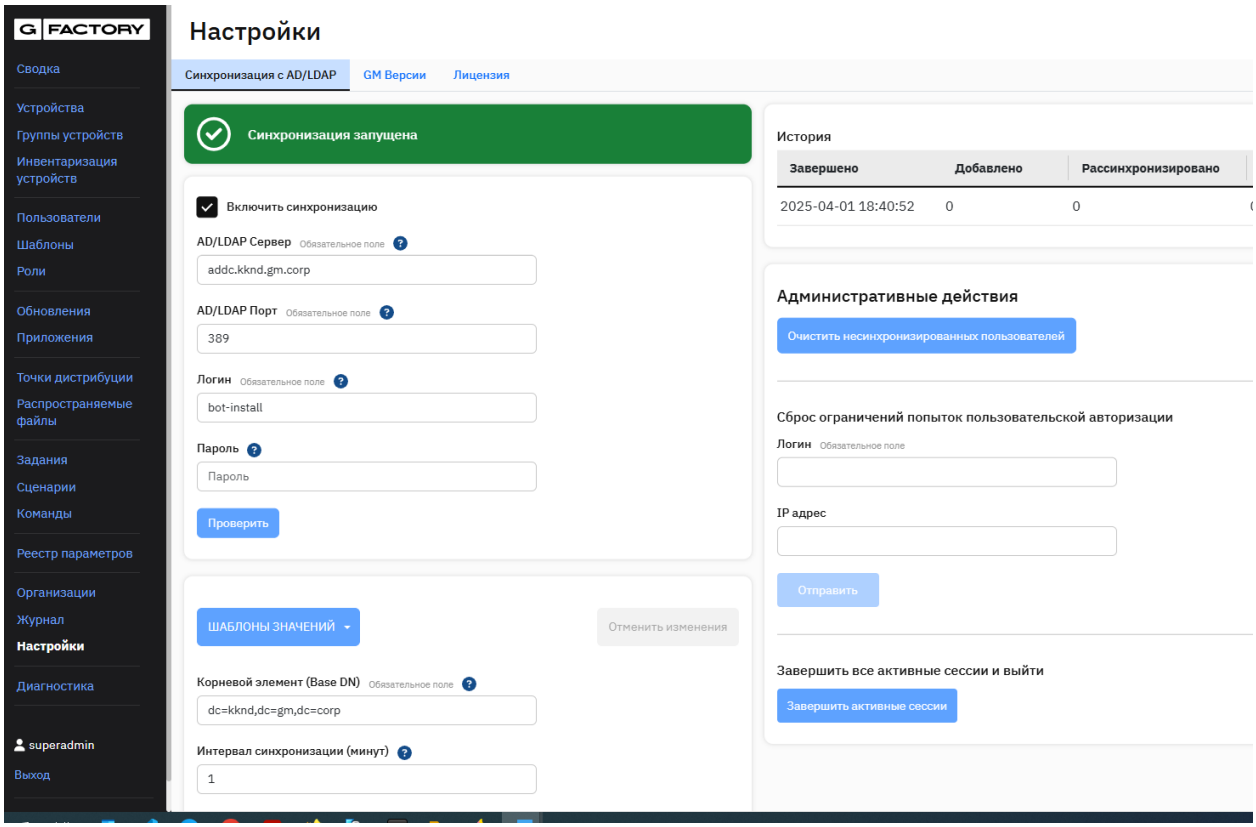


Рисунок 14 – Настройка синхронизации данных

Если появилось сообщение «Синхронизация запущена», но список пользователей в разделе Пользователи пуст, проверьте правильность заданных значений в полях **Корневой элемент (BASE DN)**, **Атрибуты** и **Соответствие полей**.

4.6 Базовые рекомендации по обеспечению информационной безопасности

Внимание! *Полный перечень рекомендаций по обеспечению информационной безопасности представлен в отдельном документе «Рекомендации по обеспечению информационной безопасности», предоставляемом по запросу.*

Для обеспечения информационной безопасности измените значения по умолчанию и выполните следующие рекомендации:

1) в файле конфигурации **/usr/local/etc/GETMOBIT/docker/config.env** измените параметр JWT_SECRET_KEY=<Произвольная строка>;
2) в файле **/usr/local/etc/GETMOBIT/docker/config.env** смените пароли у пользователей с ролью ADMIN и SUPERADMIN, используемые по умолчанию (см. разделы Редактирование учетной записи пользователя с системной ролью SUPER_ADMIN);

3) после изменения паролей администраторов перезапустите СУ;
4) настройте HTTPS протокол;
5) отключите HTTP протокол;
6) запретите доступ к серверу по протоколу SSH или ограничьте доступ к СУ по протоколу SSH с определенных ресурсов;
7) не задавайте пароли с использованием поля «**Значения по умолчанию**». Используйте для задания паролей соответствующие поля в **Шаблонах**.

4.6.1 Настройка протокола HTTPS (TLS)

Внимание! *Настройка протокола HTTPS (TLS) выполняется при необходимости. Настройка HTTPS требует настройки LDAPS на СУ. Выполните настройку LDAPS после настройки протокола HTTPS (TLS).*
Убедитесь, что имя файла сертификата состоит из цифр и латинских букв и не содержит пробелы.

1. Сгенерируйте закрытый ключ в формате PEM (Base64) для СУ и выпустите сертификат открытого ключа в формате PEM (Base64) в УЦ вашей компании (см. пример ниже).
2. Скопируйте открытый и закрытый ключи на СУ:

```
cp <путь к сертификату> /usr/local/etc/GETMOBIT/docker/ssl/
```

3. Установите права:

```
chmod 644 /usr/local/etc/GETMOBIT/docker/ssl/*
```

4. Добавьте строки в файл **/usr/local/etc/GETMOBIT/docker/config.env**

```
USE_SSL=true
SSL_CERT=<ssl.crt>
SSL_CERT_KEY=<ssl.key>
LDAP_CERT_FILE=<ssl.crt>
LDAP_KEY_FILE=<ssl.key>
USE_LDAPS=true
```

5. В значениях <**ssl.crt**> и <**ssl.key**> укажите имена подготовленных в п. 1 файлов открытого сертификата и закрытого ключа.
6. Перезапустите СУ управления командой:

```
systemctl restart gmserver
```

Для загрузки сертификата УЦ компании на подключенные устройства в веб-консоли создайте задание (п. 5.11.1) на выполнение команды **Patch config CA 2 (*.crt)**[4] (для устройств с GM OS версии ниже 2.0 используйте команду **Patch config CA (*.crt)**). Подключение устройств описано в п. **4.5.5**.
Для использования защищенного TLS-соединения от устройства GM-Box до LDAP-каталога в веб-консоли создайте задание (п. 5.11.1) на выполнение команды **Force LDAP SSL**.

4.6.1.1 Пример генерации сертификатов и их загрузки на СУ и устройство

Внимание! *Настройка HTTPS требует настройки LDAPS на СУ. Выполните настройку LDAPS после настройки протокола HTTPS (TLS).*
Убедитесь, что имя файла сертификата состоит из цифр и латинских букв и не содержит пробелы.

Примечания

1. *Приведенный пример неприменим для случаев, когда в полях Common Name (server FQDN или YOUR name) содержится IP адрес.*
2. *Для получения информации о значении ключей используйте **man openssl** или документацию проекта openssl (https://www.openssl.org/)*

1. Создайте самоподписанный сертификат openssl и закрытый ключ для CA:

```
openssl req -newkey rsa:2048 -nodes -keyout ca.key -x509 -out ca.crt -days 100
```

2. Создайте закрытый ключ и запрос на подпись открытого ключа (обязательно к заполнению поле "Common Name (e.g. server FQDN or YOUR name):

```
openssl req -newkey rsa:2048 -nodes -keyout domain.key -out domain.csr
```

3. С помощью CA подпишите сертификат, из созданного запроса:

```
openssl x509 -req -in domain.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out domain.crt -days 50
```

4. Загрузите ***ca.crt***, ***domain.key***, ***domain.crt*** на GM-Server в папку ***/usr/local/etc/getmobit/docker/ssl/***
5. Отредактируйте ***/usr/local/etc/getmobit/docker/config.env***:

```
# включает SSL для подключения GM-Box к GM-Server и доступа к web-странице управления GM-Server
USE_SSL=true
SSL_CERT=domain.crt
SSL_CERT_KEY=domain.key
```

[4] См. 5.13.1, 5.13.2

```
# включает SSL для подключения GM-Box к проксирующему LDAP серверу,
встроенному в GM-Server
USE_LDAPS=true
LDAP_CERT_FILE=ca.crt
LDAP_KEY_FILE=domain.key
LDAP_CERT_FILE=domain.crt
```

6. Загрузите корневой сертификат **ca.crt** на управляемое устройство для доверия к сертификату сервера **domain.crt**, используя команду **Patch config CA 2** или воспользуйтесь функцией загрузки сертификатов на GM-Box через GDS архив (инструкция предоставляется по запросу).

4.6.1.2 Проверка сертификатов

Для проверки сертификатов можно использовать следующие команды:

1) проверка подписи:

```
openssl verify -verbose -CAfile ca.crt domain.crt
```

2) проверка целостности закрытого ключа:

```
openssl rsa -in [key-file.key] -check -noout
```

4.6.2 Отключение протокола HTTP (режим «только HTTPS»)

Внимание! *Доступ по протоколу HTTPS (TLS) должен быть предварительно настроен и протестирован.*

Примечание. *Для корректной работы требуется либо использование актуальной версии прошивки с включенной опцией tls verify, либо предварительная загрузка сертификатов непосредственно на устройство*

Для отключения использования протокола HTTP и настройки доступа к СУ исключительно по HTTPS (порт 443) выполните действия, описанные ниже.

1. Установите CA сертификаты СУ на все управляемые устройства.
2. Выполните следующие настройки:
   a) Отредактируйте/добавьте в файле конфигурации **/usr/local/etc/GETMOBIT/monitoring/config.env** следующие переменные:

```
PROM_TARGETS=https://<адрес СУ>
```

   b) Перезапустите docker-compose для применения настроек:

```
sudo systemctl restart gmserver-monitoring
```

3. Выполните следующие настройки на СУ:
   a) Отредактируйте/добавьте в файле конфигурации **/usr/local/etc/getmobit/docker/config.env** следующие переменные:

```
GATEWAY_HTTP_ENABLED=false
```

   b) Перезапустите сервис СУ:

```
sudo systemctl restart gmserver
```

5 Настройка и администрирование СУ

Настройка и администрирование СУ осуществляется с помощью веб-консоли. Для входа в веб-консоль:

1) откройте браузер и адрес СУ, например, ***http://getmobit.example.org***.
2) в открывшейся форме введите логин и пароль администратора СУ.

Значения по умолчанию:

Login: superadmin;
Password: superadmin.

Поддерживаемые браузеры для работы с консолью:

- Google Chrome версии 85.0 и выше;
- Chromium версии 85.0 и выше.

В веб-консоли доступны разделы, которые позволяют администратору:

- Сводка – Просматривать сводную информацию и журнал операций;
- Устройства – Управлять устройствами;
- Группы устройств – Управлять группами устройств;
- Инвентаризация устройств – Создавать шаблоны отчетов по инвентаризации
- Пользователи – Управлять учетными записями пользователей;
- Шаблоны – Управлять шаблонами;
- Роли – Управлять ролями;
- Обновления – Управлять базовым ПО;
- Приложения – Управлять SD App-приложениями;
- Точки дистрибуции – Настраивать точки дистрибуции;
- Распространяемые файлы – Управлять распространяемыми файлами;
- Задания – Управлять заданиями;
- Сценарии – Управлять сценариями;
- Команды – Управлять разрешенными командами;
- Организации – Настраивать Discovery адрес для Сервера управления;
- Журнал – Просматривать журнал событий;
- Настройки – Настраивать синхронизацию с корпоративной службой каталогов, добавлять и обновлять лицензионные файлы;
- Диагностика – Настраивать и запускать диагностические команды.

Внимание! *Выше приведен полный список разделов. Доступ к отдельным разделам определяется редакцией сервера и/или наличием необходимой лицензии.*

5.1 Сводка

В разделе **Сводка** (Рисунок 15) отображается информация о количестве включенных и выключенных устройств, о доступных и установленных обновлениях, а также информация о текущих событиях на сервере.

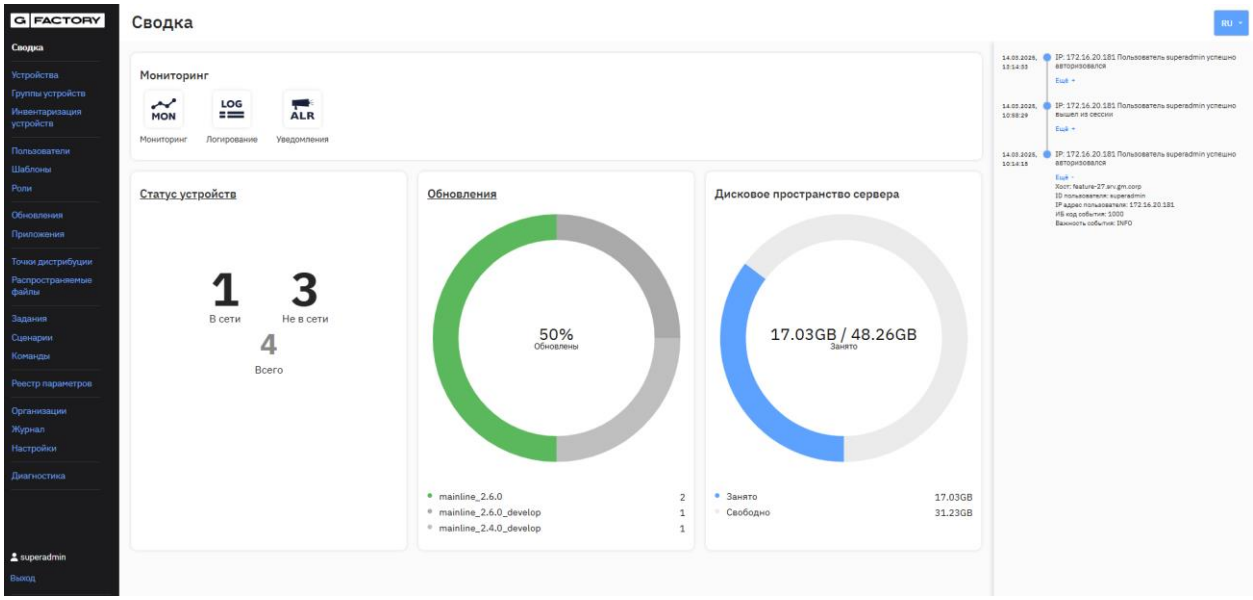


Рисунок 15 – Вид окна раздела **Сводка**

5.2 Устройства.

В разделе **Устройства,** администратору доступны следующие функции:.

- поиск по зарегистрированным на СУ устройствам;
- сортировка устройств в списке;
- просмотр настроек устройства;
- создание заданий для выбранных устройств;
- удаление устройств.

5.2.1 Добавление устройства

Добавление управляемых устройств в список, подключенных к СУ, выполняется автоматически после его включения и получения сетевых настроек.

5.2.1.1 Импорт данных по устройствам

Для автоматического заполнения серийных номеров устройств необходимо загрузить файл с данными, в формате csv. Для этого выполните действия, описанные ниже.

Примечание. *Для получения файла с данными в формате csv обратитесь в отдел техподдержки ООО «ГЕТМОБИТ».*

1. В разделе **Устройства** нажмите Импорт данных по устройствам (Рисунок 16).

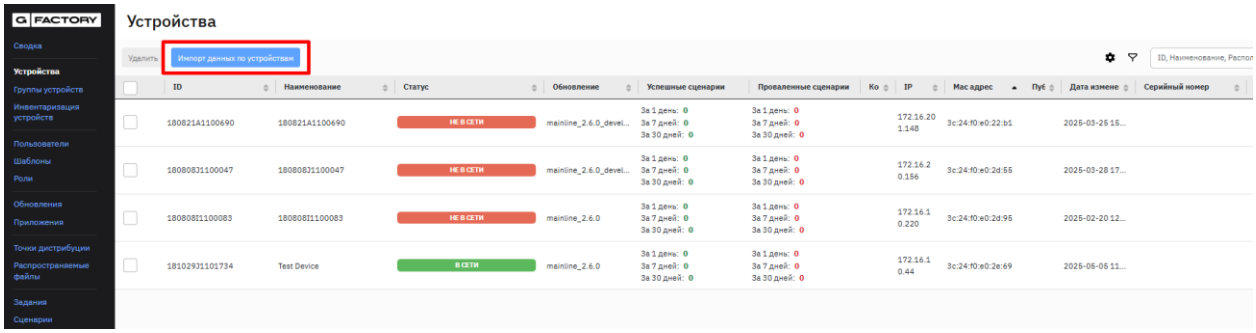


Рисунок 16 – Импорт данных по устройствам

2. Перетащите файл с данными по устройствам, в открывшееся окно или нажмите «Выберите через проводник».
3. Нажмите **Импорт** (Рисунок 17).

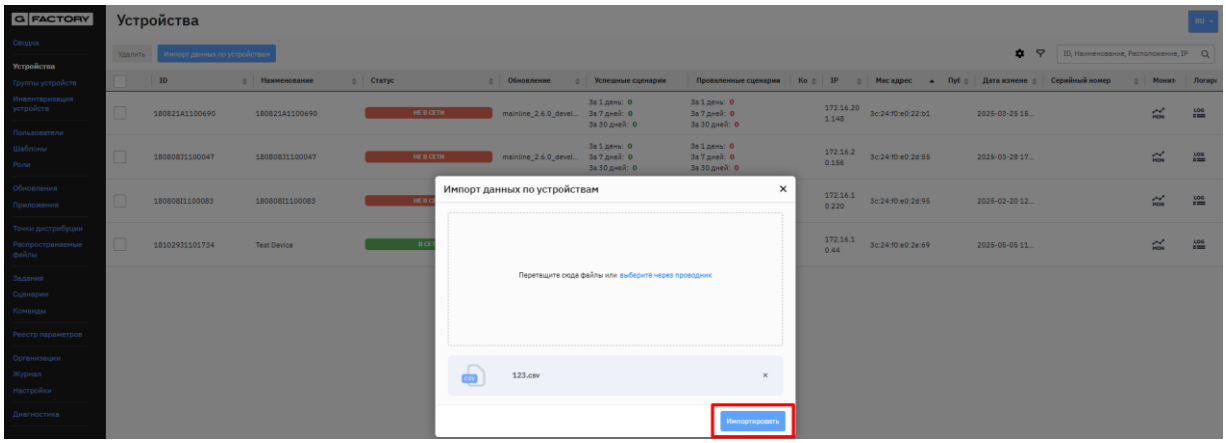


Рисунок 17 – Загрузка файла с данными

5.2.2 Редактирование карточки устройства

Чтобы отредактировать информацию об устройстве, выберите его в списке. В открывшемся окне отобразиться общая информация о данном устройстве.

В правой части окна отображается карточка устройства, в которой содержится информация о следующих статусах устройства:

- В СЕТИ/НЕ В СЕТИ – подключено/не подключено устройство к СУ;
- В карантине/не в карантине – ограничен/не ограничен функционал устройства.

Так же в карточке устройства отображаются следующие поля:

- **ID** – идентификатор устройства, поле заполняется автоматически;
- **Наименование** – название устройства. Первоначально заполняется автоматически, может быть изменено администратором;
- **Обновление** – текущая версия ПО, установленного на устройстве, поле заполняется автоматически;
- **IP-адрес устройства**;
- **Часовой пояс** – соответствует географическому местоположению устройства;
- **Расположение** – местонахождение устройства;
- **Комментарий**.

Для применения отредактированных настроек нажмите **Сохранить изменения**.

Поля, подсвеченные серым цветом, недоступны для редактирования.

Чтобы выйти из режима редактирования без сохранения, закройте карточку.

5.2.3 Создание и выполнение заданий на устройствах

Чтобы создавать задания, например, на перезагрузку и выключение устройства, на обновление ПО устройства и т.д., выполните действия, описанные ниже.

1. При необходимости отфильтруйте устройства с помощью строки поиска и отсортируйте список по одному из полей.
2. Отметьте галочкой необходимые устройства.
3. В верхней части раздела нажмите **Еще→Создать задание** (Рисунок 18). В правой части откроется карточка задачи.

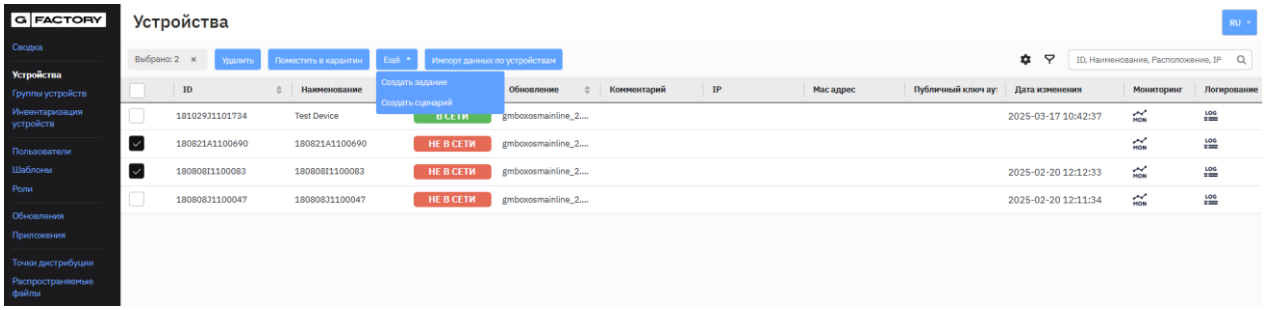


Рисунок 18 – Создание задания

4. Укажите название задачи. В поле **Назначить на** автоматически подставится ID устройств, отмеченных галочкой.
5. Укажите периодичность выполнения задачи.
6. Выберите из выпадающего списка команду, которую необходимо выполнить.
7. Нажмите **Создать**.

5.2.4 Удаление устройства из списка управляемых устройств

Чтобы удалить устройство из списка управляемых, отметьте его галочкой и в верхней части раздела нажмите →**Удалить**.

При удалении устройства из списка происходит сброс адреса СУ на управляемом устройстве. Повторное подключение устройства к СУ может потребовать наличие физического доступа к устройству. Для последующего подключения убедитесь, что в настройках устройства включена опция автоматического подключения к СУ или введите адрес СУ вручную.

5.3 Группы устройств

5.3.1 Создание группы устройств

Администратор может назначить задание на выполнение команды, например, на перезагрузку и выключение устройства, на обновление ПО устройства и т.д., нескольким устройствам одновременно. Для этого необходимо объединить устройства в группы.

1. В веб-консоли выберите раздел **Группы устройств**. В открывшемся окне для создания группы в корне выберите папку **Устройства**, а для создания подгруппы устройств – выберите папку **Новая группа** (Рисунок 19).

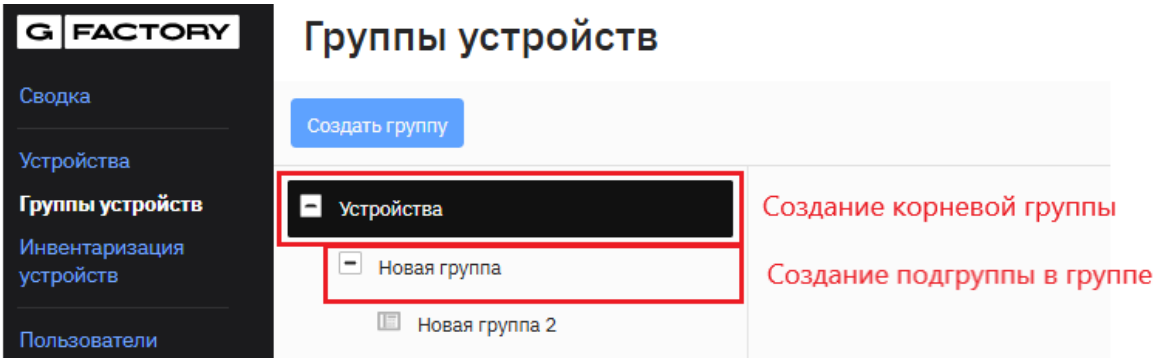


Рисунок 19 – Создание групп и подгрупп устройств

2. В верхней части раздела нажмите **Создать группу**.
3. Заполните поля: Название и Комментарии с описанием создаваемой группы.
4. Нажмите **Создать группу**.

5.3.1.1 Добавление устройств в группу

1. Выберите в списке созданную группу или подгруппу.
2. В верхней части раздела нажмите **Действие для группы** → **Показать все устройства** (Рисунок 20). Отобразится список доступных устройств.

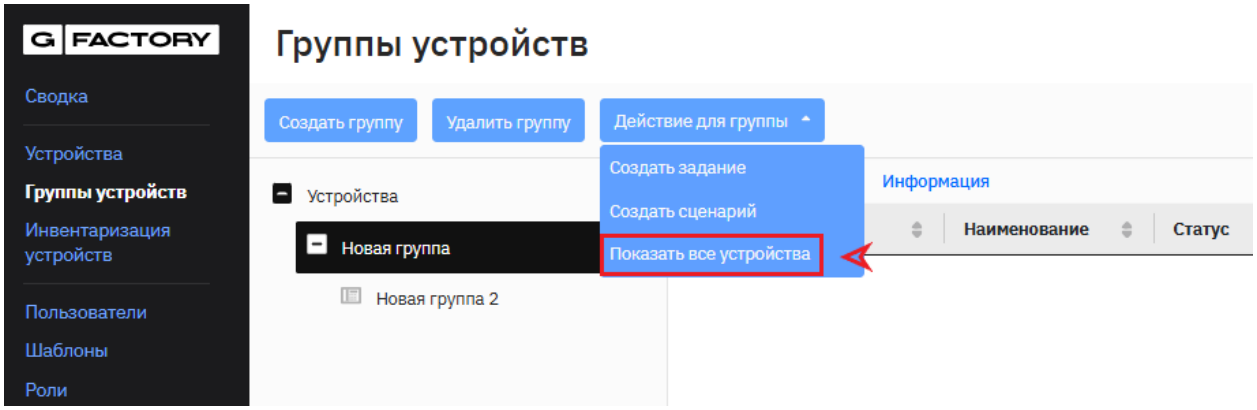


Рисунок 20 – Отображение доступных устройств

3. Отметьте флажками устройства, которые необходимо добавить в группу/подгруппу.
4. Нажмите **Действие для устройств** → **Добавить в группу** (Рисунок 21). Отобразится список устройств, добавленных в группу.

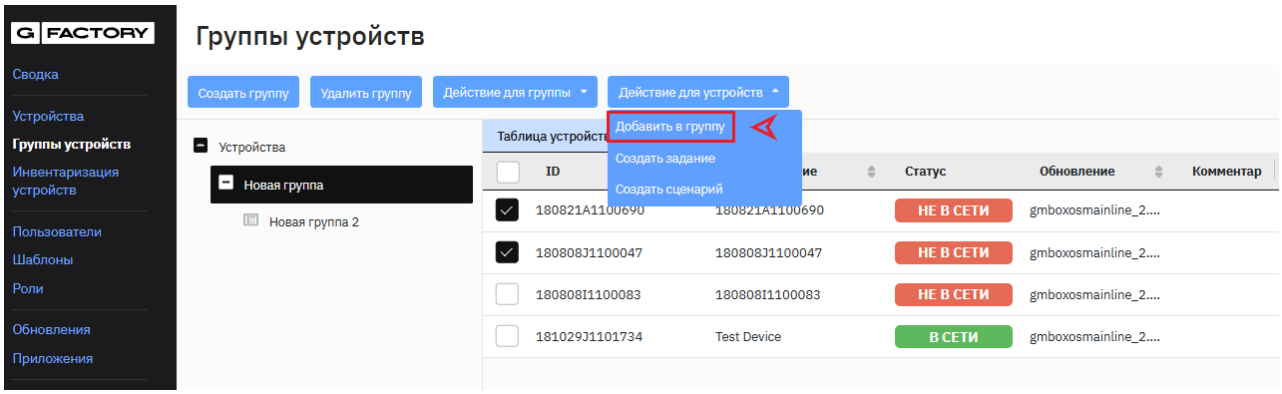


Рисунок 21 – Добавление устройств в группу или подгруппу

Как назначить выполнение задания на группу устройств см. п. 5.11.1.

5.3.2 Удаление устройства из группы

1. Выберите группу, из которой необходимо удалить устройство.
2. Перейдите на вкладку **Таблица устройств** и отметьте флажками устройства, которые необходимо удалить из группы.
3. Нажмите **Действие для устройств** → **Удалить из группы** (Рисунок 22).

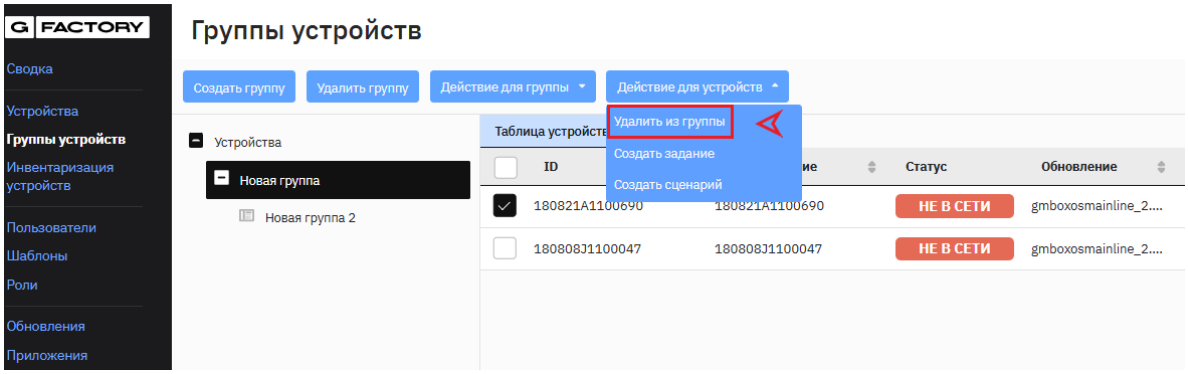


Рисунок 22 – Удаление устройств из группы

5.3.3 Удаление группы устройств

1. Удалите все устройства из группы.
2. Выберите удаляемую группу, нажмите **Удалить группу** (Рисунок 23).

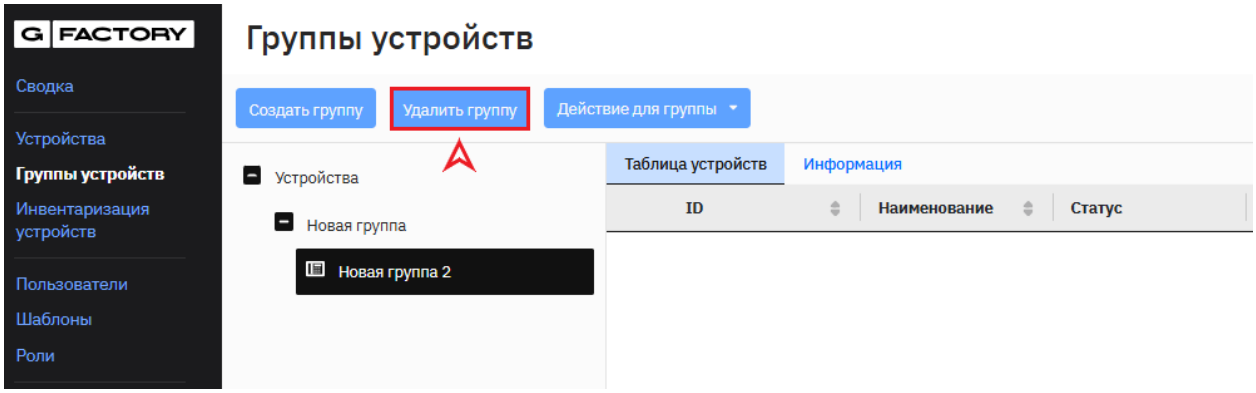


Рисунок 23 – Удаление группы устройств

3. Нажмите **Удалить**.

5.4 Инвентаризация устройств

***Примечание**. Раздел **Инвентаризация устройств** является лицензируемой опцией, доступной не во всех редакциях СУ. За подробной информацией обратитесь в GETMOBIT или к официальному дистрибутору.*

В данном разделе администратор может формировать шаблоны отчетов инвентаризации по устройствам, к СУ, с целью систематизации данных об их характеристиках, состоянии и использовании.

Основной функционал инвентаризации:

- выгрузка отчетов в форматах: json, csv, xml;
- группировка устройств по типу, версии ПО, материнской плате и другим атрибутам;
- выбор отображаемых колонок (серийные номера, IP-адреса, устройств установленные приложения и т.д.);
- фильтрация по атрибутам (например, версии BIOS или установленным приложениям).

5.4.1 Создание шаблонов отчетов инвентаризации

Для создания шаблона отчета инвентаризации выполните действия, описанные ниже.

1. В веб-консоли выберите раздел **Инвентаризация устройств**. В открывшемся окне Шаблоны отчетов инвентаризации нажмите **Добавить** (Рисунок 24)

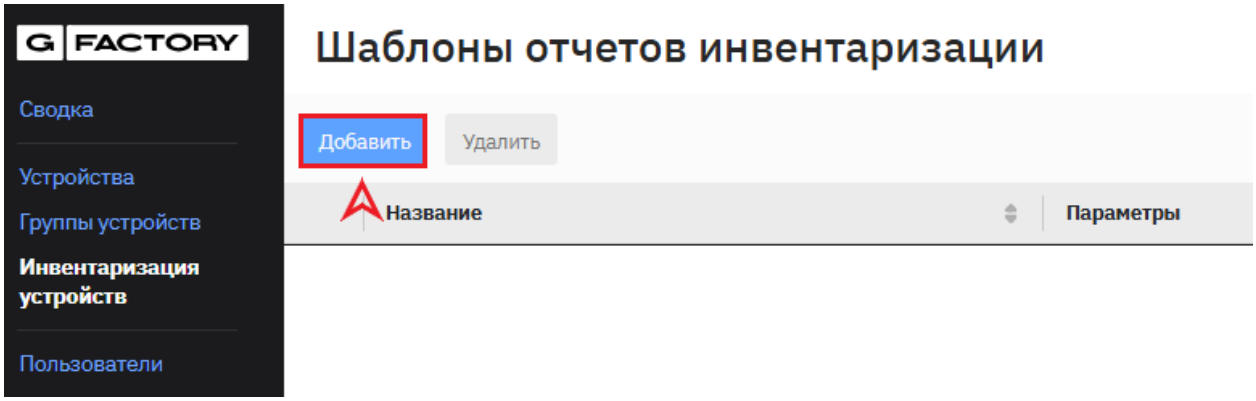


Рисунок 24 – Добавление шаблонов отчетов инвентаризации

2. Откроется окно **Создание шаблона отчета** (Рисунок 28). В левой части окна располагаются редактируемые поля, которые необходимо заполнить:

   - **Наименование** – название шаблона отчета;

   - **Группировать по**– группировка имеющихся устройств по выбранному атрибуту. Для сброса группировки, в списке атрибутов необходимо выбрать "Не задано";

   - **Фильтрация** – позволяет отображать только те устройства, чей атрибут содержит указанное в параметрах фильтра значение. Для добавления условия фильтрации нажмите на иконку . В открывшемся окне (Рисунок 25) выберите атрибут, по которому нужно фильтровать устройства. Если атрибутов несколько нажмите «Добавить условие», затем нажмите «Применить»

   Для сброса выбранного фильтра необходимо нажать на соответствующую иконку или нажать «Сбросить все».

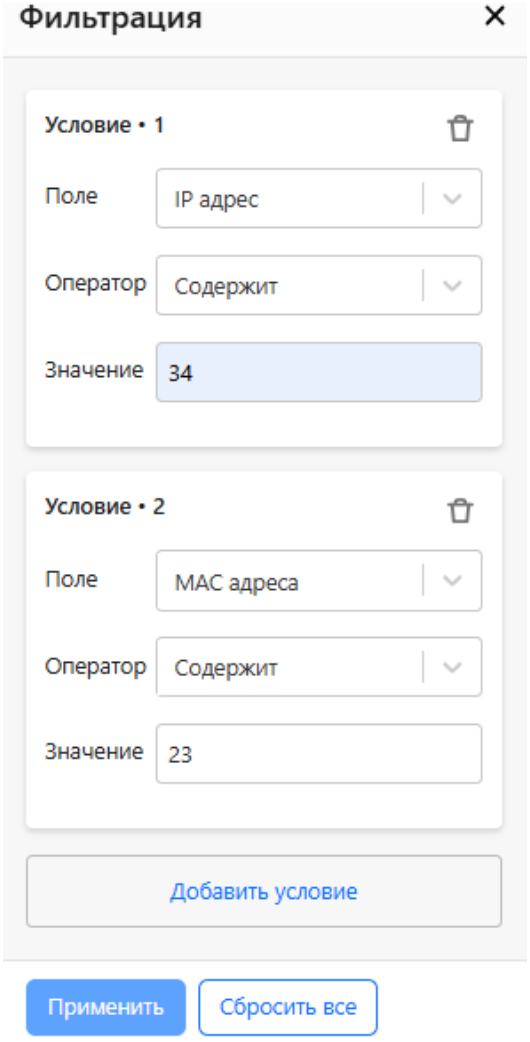


Рисунок 25 – Вид поля **Фильтрация**

- **Атрибуты** – настройка отображаемой информации в шаблоне отчета зависит от выбранных атрибутов. Для добавления атрибута выберите из раскрывающегося списка необходимые. Удаление атрибутов возможно двумя способами, указанными на Рисунок 26

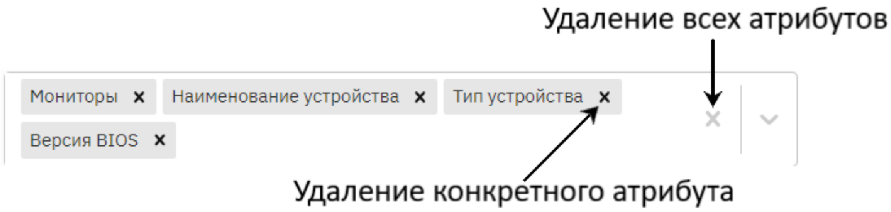


Рисунок 26 – Вид поля **Атрибуты**

- **Сортировать по** – позволяет отсортировать данные, добавленные в отчет, по определенному атрибуту как по убыванию, так и по возрастанию. Для сброса параметров сортировки необходимо в списке доступных параметров выбрать "Не задано".

***Примечание**. Количество параметров для сортировки зависит от количества добавленных ранее атрибутов в шаблон отчета*

- **Комментарий** – позволяет оставить дополнительную информацию для выбранного шаблона.

3. Заполните поля и в левом нижнему углу окна нажмите **Создать** (Рисунок 27).

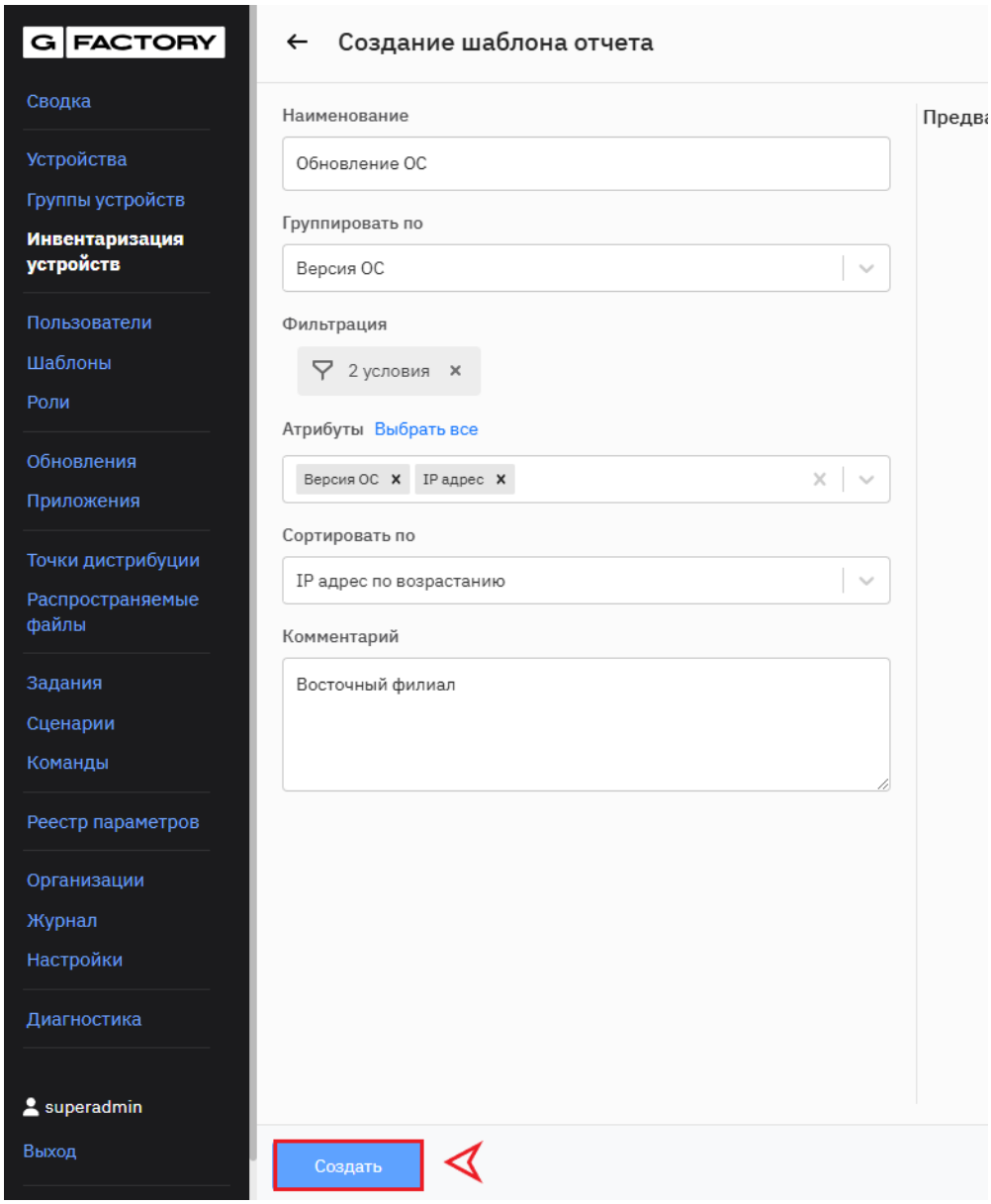


Рисунок 27 – Создание шаблона отчета

В правой части окна отобразится окно предварительного просмотра создаваемого шаблона отчета (Рисунок 28).

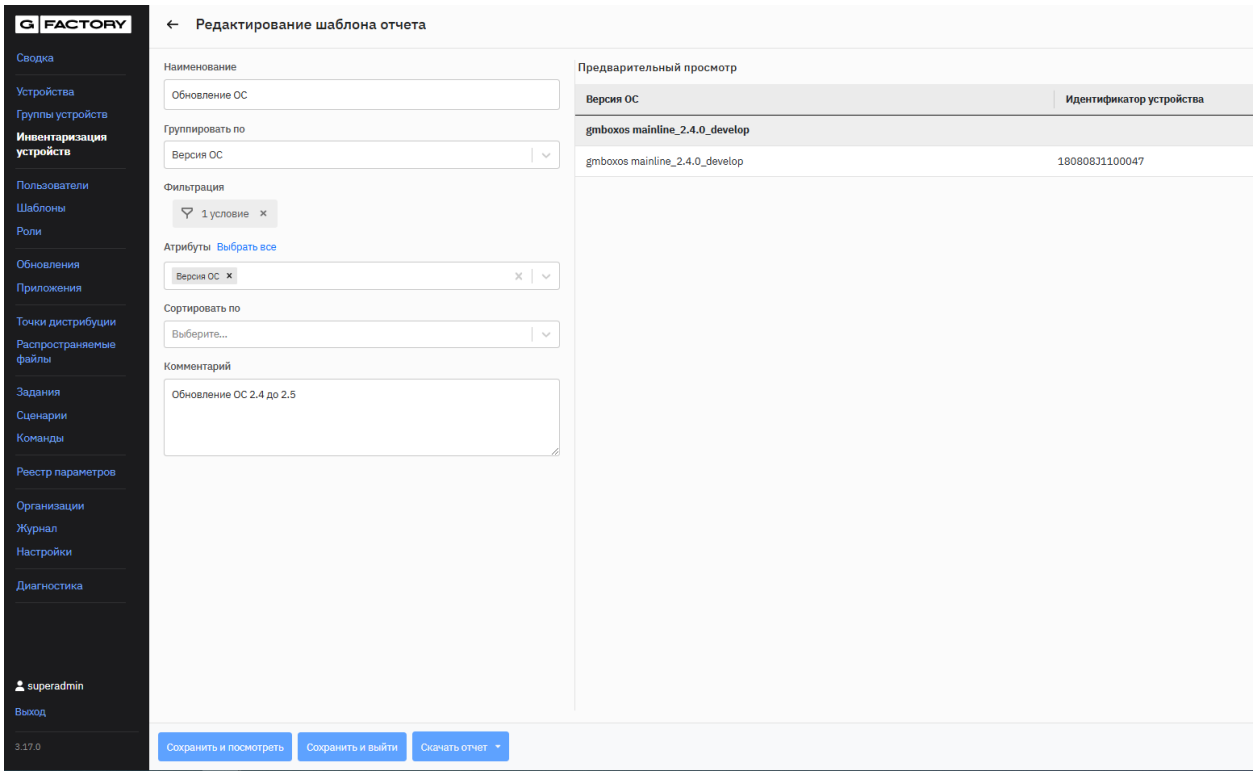


Рисунок 28 – Вид окна Редактирование шаблона отчета

4. Для завершения работы и сохранения отчетов на СУ в левом нижнем углу окна нажмите **Сохранить и выйти** или **Сохранить и посмотреть** (Рисунок 28).

5.4.2 Выгрузка и удаление шаблонов отчетов

Все созданные и сохраненные шаблоны отчетов будут отображаться в разделе **Шаблоны отчетов инвентаризации** и будут доступны для редактирования. Для того, чтобы отредактировать отчет выберите его и нажмите ЛКМ. Откроется окно «Редактирование шаблона отчета». Внесите необходимые изменения.

Для отображения внесенных изменений и обновления предварительного просмотра отредактированного отчета в левом нижнем углу окна нажмите **Сохранить и посмотреть**. (Рисунок 28).

Экспортировать отчет из СУ можно двумя способами.

1. На странице редактирования шаблона отчета, в нижней части окна, необходимо нажать **Скачать отчет** (Рисунок 28) и в выпадающем списке выбрать формат файла, в котором необходимо экспортировать отчет.
2. В разделе **Инвентаризация устройств** выбрать шаблон из общего списка и нажать **Скачать отчет** и в выпадающем списке выбрать формат файла, в котором необходимо экспортировать отчет.

Для удаления шаблона отчета необходимо в общем списке шаблонов выбрать интересующий и нажать **Удалить** (Рисунок 29).

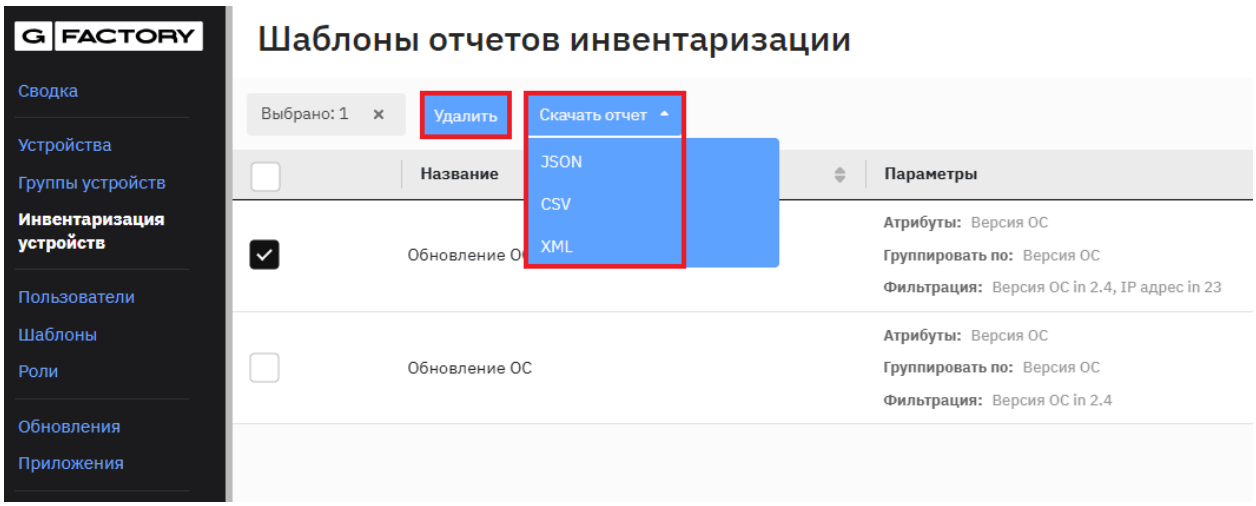


Рисунок 29 – Удаление шаблонов отчетов инвентаризации

5.5 Пользователи.

Управление профилями пользователей выполняется в разделе **Пользователи**.

Информация о типах учетных записей пользователей указана в п. 2.2.2.

В разделе отображается список учетных записей пользователей: локальные учетные записи пользователей, созданные через веб-консоль (обозначены значком), и AD/LDAP учетные записи пользователей, синхронизированных с корпоративной службой каталогов.

Синхронизация учетных записей пользователей со службами каталогов позволяет получать список пользователей, работающих в системе, из AD/LDAP-каталога. Подробнее о настройке синхронизации и схеме ее работы в п. 5.16.2.

Создавать, редактировать или удалять учетные записи пользователей может администратор, у которого есть соответствующие права.

5.5.1 Создание локальной учетной записи пользователя

Внимание! *При создании локального пользователя убедитесь, что в AD/LDAP организации отсутствует пользователь с аналогичным логином.*

1. Для создания локальной учетной записи пользователя в веб-консоли выберите раздел **Пользователи**.
2. В верхней части раздела нажмите **Добавить** (Рисунок 30). Откроется карточка нового пользователя (Рисунок 31)

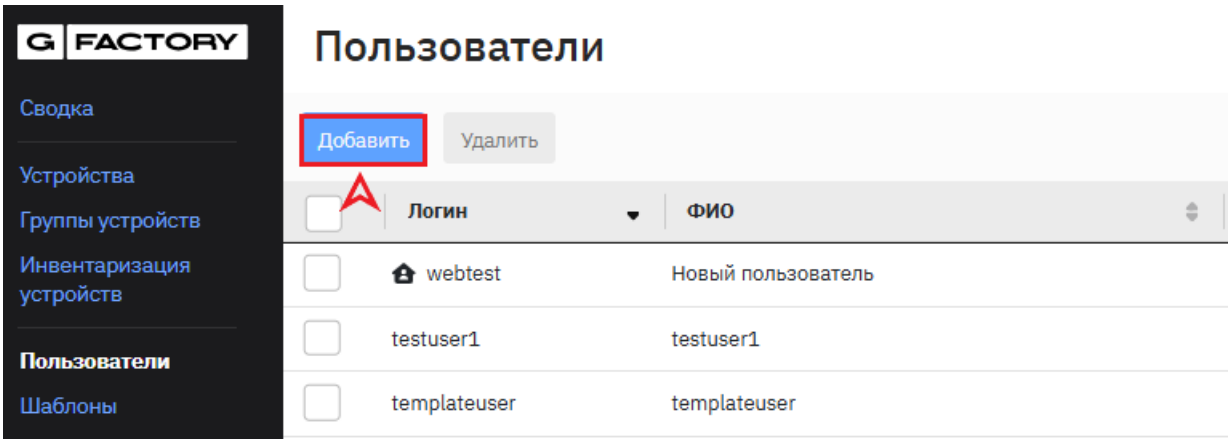


Рисунок 30 – Вид окна карточки нового пользователя

3. Во вкладке **Профиль**, для успешного создания учетной записи необходимо заполнить обязательные поля:
    a. Логин;
    b. Пароль;
    c. ФИО.

Примечание. *Если не ввести данные в обязательные поля, то учетная запись не будет создана*

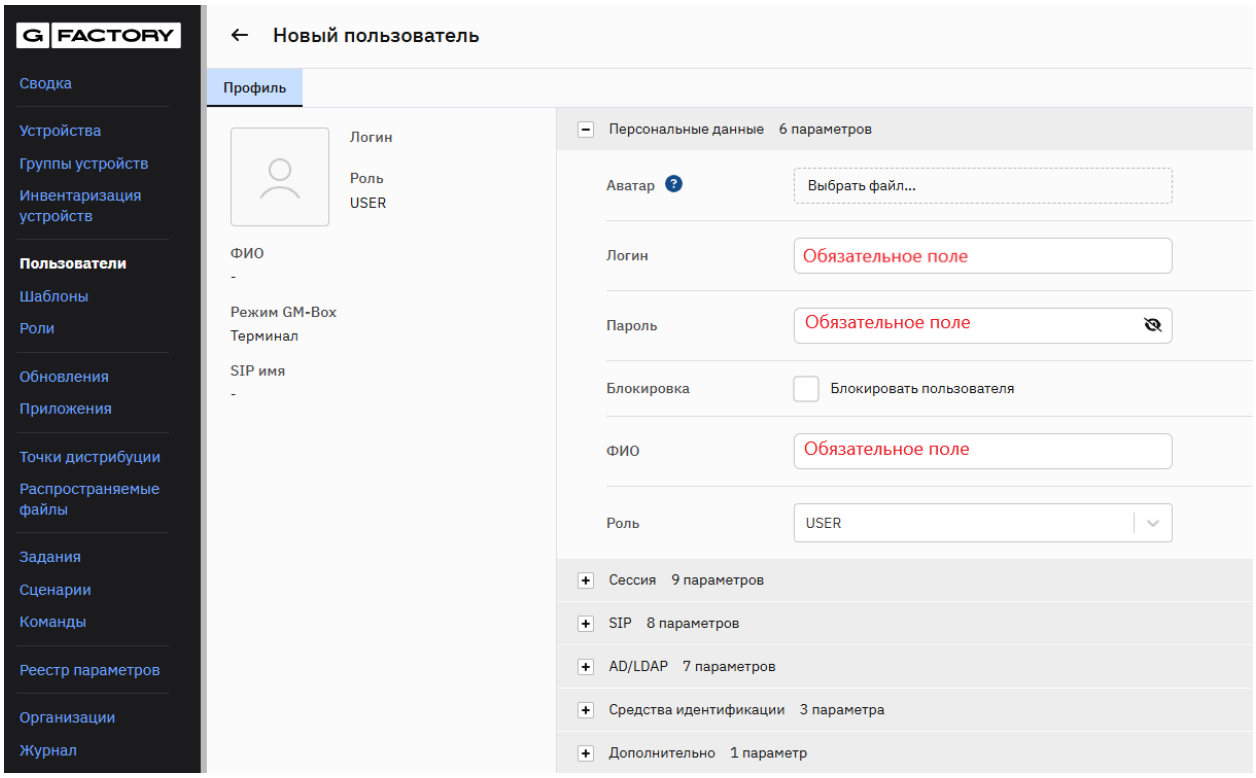


Рисунок 31 – Вид окна карточки «Новый пользователь»

5.5.2 Вкладка «Профиль»

Профиль **Новый пользователь** (Рисунок 32) представляет собой страницу с основными разделами:

- **Персональные данные** параметры, отвечающие непосредственно за основную информацию о пользователе;
- **Сессия:** параметры профиля пользователя, отвечающие за настройку доступа к инфраструктурным сервисам предприятия;
- **SIP:** параметры настройки SIP-телефонии;[5]
- **AD/LDAP:** параметры AD/LDAP;
- **Средства идентификации:** параметры настройки NFC, RFID, токенов;
- **Дополнительно:** поле, позволяющее добавлять различные дополнительные параметры для профиля пользователя.

Описание основных разделов профиля пользователя представлено в следующих подпунктах.

[5] Настройки IP телефонии применимы для устройств GM-Box G1

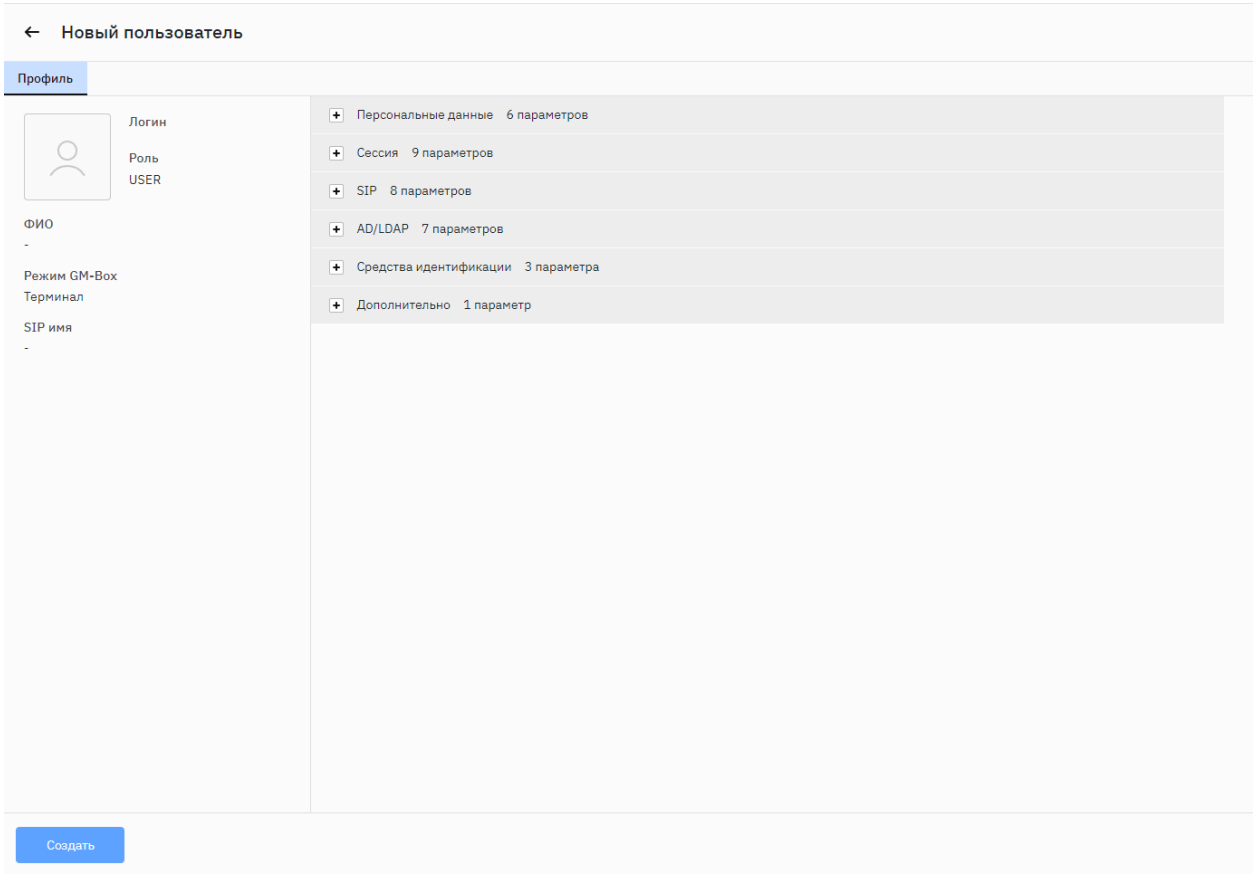


Рисунок 32 – Вид окна вкладки «Профиль»

5.5.2.1 «Персональные данные»

Данный раздел (Рисунок 33) предназначен для редактирования пользовательских данных.

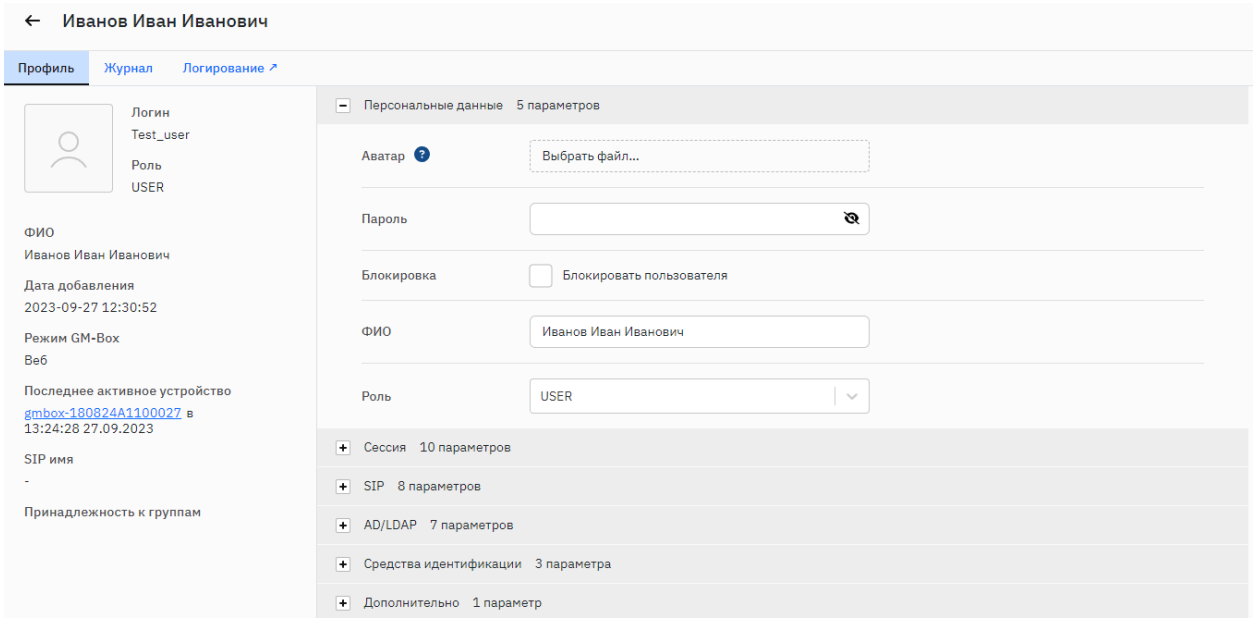


Рисунок 33 – Вид окна «Персональные данные»

5.5.2.1.1 Редактируемые поля

Перечень редактируемых полей раздела «Персональные данные» и их описание приведены в Таблица 3.

Таблица 3 – Редактируемые поля раздела «Персональные данные» и их описание

Параметр	Ключ*	Описание
Аватар	avatar	Изображение пользователя. Отображается при входе пользователя в систему и используется в адресной книге. По умолчанию синхронизируется из корпоративной службы каталогов. Для синхронизации изображения из LDAP, необходимо в Атрибутах синхронизации указать *thumbnailPhoto* и добавить в Соответствие полей запись *avatar=thumbnailPhoto* ***Внимание!*** *Импортируемое изображение должно быть в форматах JPEG, PNG, размер не более 2 Мб.*
Блокировка	archived	Флаг, который используется для блокировки и снятия блокировки учетной записи пользователя.
Логин	username	Логин пользователя, по умолчанию синхронизируется из корпоративной службы каталогов.
Пароль	password	Стандартная политика паролей подразумевает, что пароль должен включать в себя минимум 8 символов, среди которых обязательно должны быть: буквы верхнего регистра, цифры, специальные символы. ***Внимание!*** *Политика паролей может быть изменена администратором. При создании/смене пароля необходимо повторить введенный пароль.*
Роль	roles	Роль пользователя. Выбирается из выпадающего списка.
ФИО	title	Полное имя пользователя. ФИО может быть заполнено вручную (в случае если пользователь является локальным). Если пользователь является доменным, то данное поле уже является заполненным теми данными, которые указаны в службе каталогов.
**Ключ можно задавать значением по умолчанию при синхронизации пользователей с корпоративной службой каталогов AD/LDAP.*		

5.5.2.1.2 Информационные поля

Информационные поля (Рисунок 34) предназначены для отображения основной информации о пользователе.

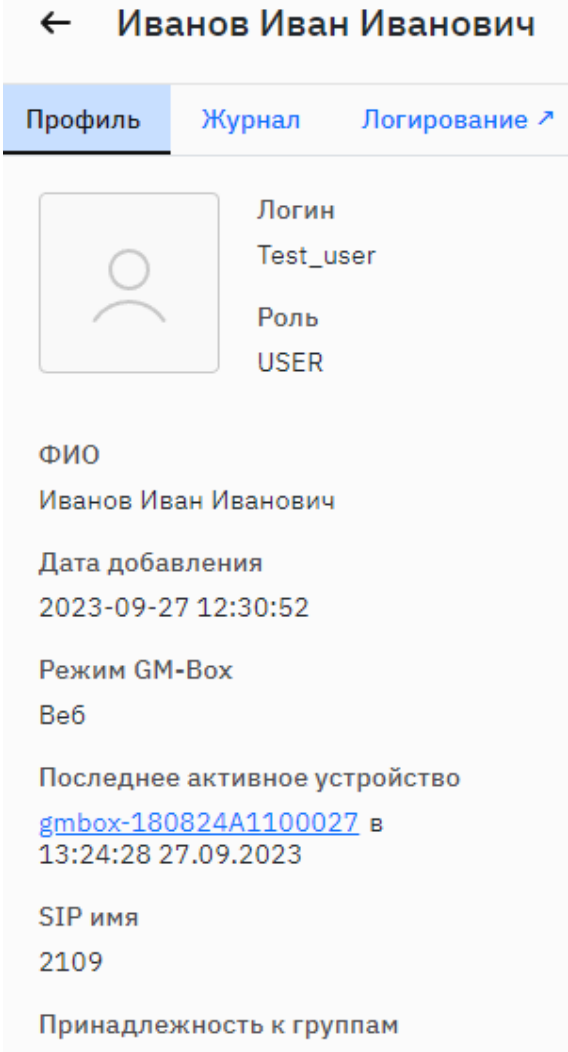


Рисунок 34 – Информационные поля

Поле – см. пункт «Редактируемые поля».

Логин – роль пользователя, которая была назначена ему администратором.

Роль – ФИО пользователя.

ФИО – дата добавления пользователя на сервер управления GMSS NG Factory.

Формат отображения даты добавления: гггг-мм-дд чч:мм:сс.

Дата добавления – режим работы устройства, который был выбран администратором.

Режим GM-Box – данное поле предназначено для отображения даты, времени и ID последнего устройства, за которым работал пользователь. ID устройство отображается в виде ссылки, переходя по которой администратор попадает на страницу карточки устройства, чей ID указан в поле "Последнее устройство".

Последнее активное устройство – имя пользователя SIP-сервера.

SIP имя – данное поле отображает к какой группе AD принадлежит пользователь.

Принадлежность к группам – см. пункт «Редактируемые поля».

5.5.2.2 «Сессия»

Данный раздел (Рисунок 35) предназначен для настройки параметров подключения пользователя к устройству и VDI-инфраструктуре предприятия. Перечень редактируемых полей раздела «Сессия» и их описание приведены в Таблица 4

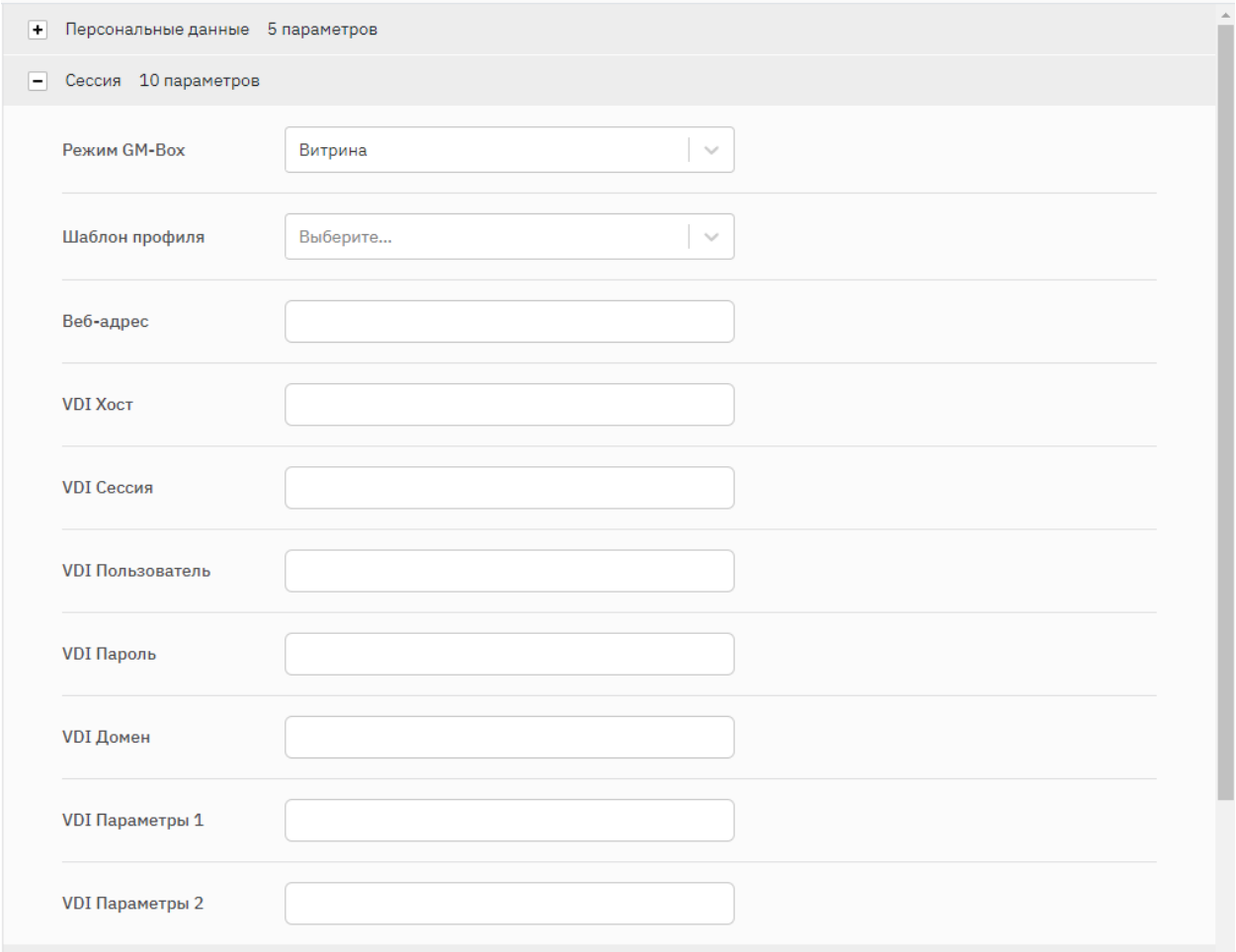


Рисунок 35 – Вид окна «Сессия»

Таблица 4 – Редактируемые поля раздела «Сессия» и их описание

<table>
<tr><th>Параметр</th><th>Ключ</th><th colspan="3">Описание</th></tr>
<tr><td rowspan="5">Режим GM-Box</td><td rowspan="5">configuration.gm_mode</td><td colspan="3">Режим работы пользователя. Ниже приведены возможные режимы (список доступных режимов может измениться):</td></tr>
<tr><td>Режим</td><td>Ключ</td><td>Описание</td></tr>
<tr><td>Терминал</td><td>configuration.gm_mode=terminal</td><td>Режим тонкого клиента RDP. При работе в нем будет использоваться клиент RDP для подключения к терминальному серверу Microsoft.</td></tr>
<tr><td>Веб</td><td>configuration.gm_mode=web</td><td>Режим веб-клиента. В этом режиме пользователь может работать с веб-системой, используя встроенный в GM OS веб-браузер.</td></tr>
<tr><td>Киоск</td><td>configuration.gm_mode=kiosk</td><td>Режим веб-клиента без элементов управления веб-браузером, в том числе использования адресной строки.</td></tr>
<tr><td></td><td></td><td>VMware</td><td>configuration.gm_mode=vmware</td><td>Режим клиента VDI VMware Horizon для подключения к ВМ по совместимым с VMware Horizon протоколам.</td></tr>
</table>

<table>
<tr><th>Параметр</th><th>Ключ</th><th colspan="3">Описание</th></tr>
<tr><td rowspan="5"></td><td rowspan="5"></td><th>Режим</th><th>Ключ</th><th>Описание</th></tr>
<tr><td>Citrix</td><td>configuration.gm_mode=mwccitrix</td><td>Режим клиента Citrix. При работе в нем будет использоваться агент Citrix Receiver для подключения.</td></tr>
<tr><td>Баррикады</td><td>configuration.gm_mode=barricada</td><td>Режим клиента Barricada. При работе в нем будет происходить подключение GM-Box к серверам VDI Barricada.</td></tr>
<tr><td>Huawei</td><td>configuration.gm_mode=huawei</td><td>Режим клиента Huawei. При работе в нем будет происходить подключение GM-Box к серверам VDI Huawei Fusion.</td></tr>
<tr><td colspan="3">Примечание. Доступные пользователю режимы / SD App-приложения добавляются динамически при добавлении администратором SWU файла в реестр приложений на СУ.</td></tr>
<tr><td>Шаблон профиля</td><td>profile_template</td><td colspan="3">Администратор из выпадающего списка может выбрать нужный шаблон подключения профиля пользователя к сервисам предприятия: Citrix, VMware, Vitrina, Web</td></tr>
<tr><td>Веб-адрес</td><td>configuration.web_url</td><td colspan="3">Адрес веб-страницы. Поле отображается только при выборе режимов «Веб», «Киоск» или «Киоск в режиме Инкогнито».</td></tr>
<tr><td>VDI хост</td><td>configuration.vdi.host</td><td colspan="3">IP-адрес или DNS-имя сервера VDI или терминального сервера.</td></tr>
<tr><td>VDI сессия</td><td>configuration.vdi.session</td><td colspan="3">Пул/машина/десктоп или пустое значение для задания значения по умолчанию.</td></tr>
<tr><td>VDI пользователь</td><td>configuration.vdi.user</td><td colspan="3">Доменное имя пользователя.</td></tr>
</table>

Параметр	Ключ	Описание
VDI пароль	configuration.vdi.password	Пароль пользователя. Поле может потребоваться в случае, если пользователь выполняет вход в систему не под доменной учетной записью, а под локальной учетной записью пользователя на СУ, но при этом в VDI-системе используется другой пароль.
VDI домен	configuration.vdi.domain	Домен VDI. Может не указываться, если в поле VDI пользователь значение задано с указанием домена (domain\username, username@domain).
VDI параметры 1	configuration.vdi.param1	Используется для интеграции с различными VDI-решениями: 1) gfx - использование прогрессивного JPEG, подходит для слабых каналов и внешних сотрудников за VPN; 2) h264 - использование видеокодека h264 позволяет смотреть видео в ВМ; 3) lddqd - режим полного определения (отладочный режим) администратором параметров подключения клиентом xfreerdp. При пустом поле будут использоваться параметры по умолчанию, которые можно дополнить параметрами из поля.
VDI параметры 2	configuration.vdi.param2	Используется для интеграции с различными VDI-решениями. Данный параметр определяется режимом работы пользователя (используемым VDI клиентом) и может содержать стандартный для данного клиента набор ключей, передаваемых в командной строке. 1) Примеры значений для MS RDP: /gfx +gfx-progressive +window-drag /sec:tls /smartcard *Дополнительные параметры см. CommandLineInterface FreeRDP/FreeRDP Wiki (github.com)* 2) Примеры значений для VMware: --protocol="PCOIP" Изменяет протокол подключения к ВМ См. документацию VMware *Horizon Client Configuration Settings and Command-Line Options* (*https://docs.omnissa.com/ruRU/bundle/HorizonClientLinuxGuideV2303/page/HorizonClientConfigurationSettingsandCommandLineOptions.html*)

5.5.2.3 Раздел «SIP»

В данном разделе администратор может настраивать параметры SIP для пользователя (Рисунок 36)

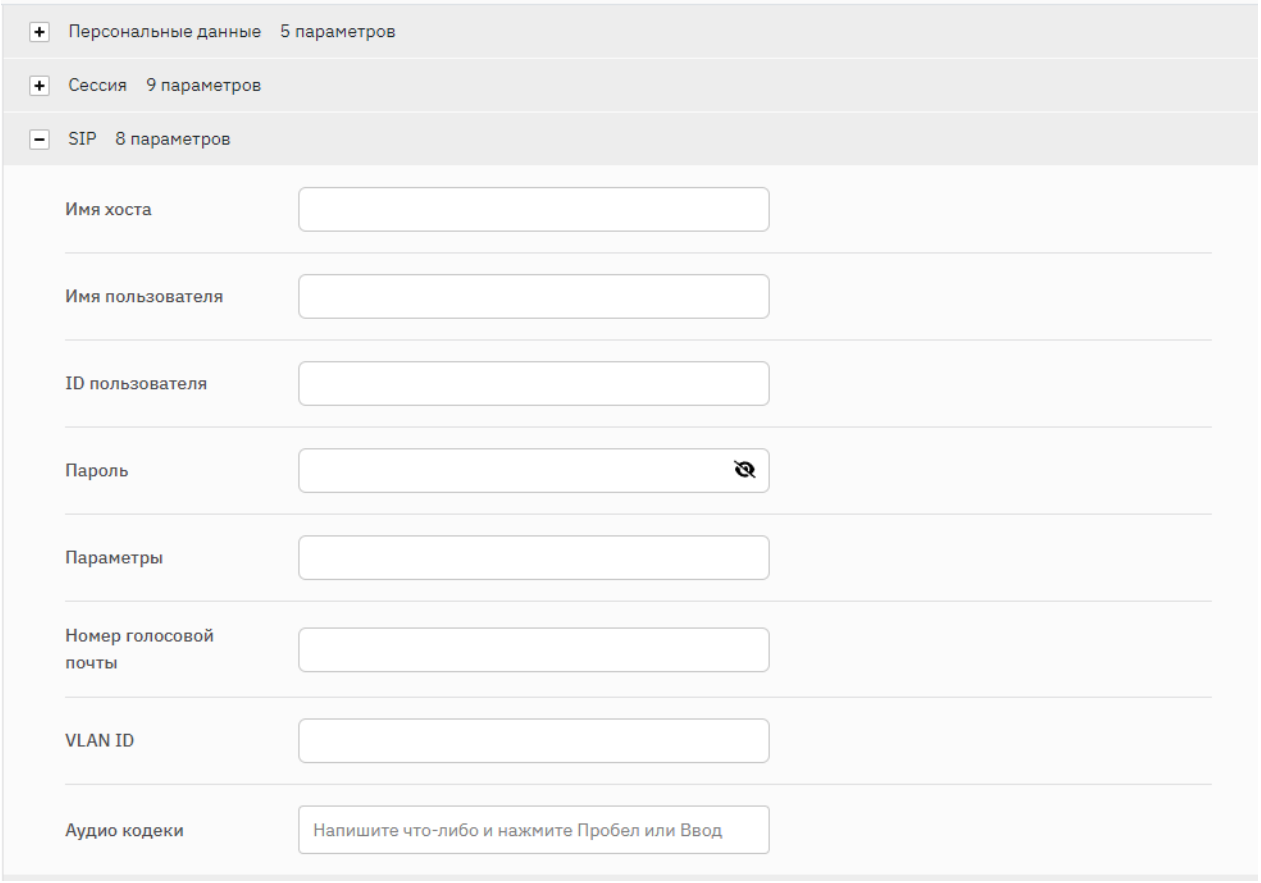


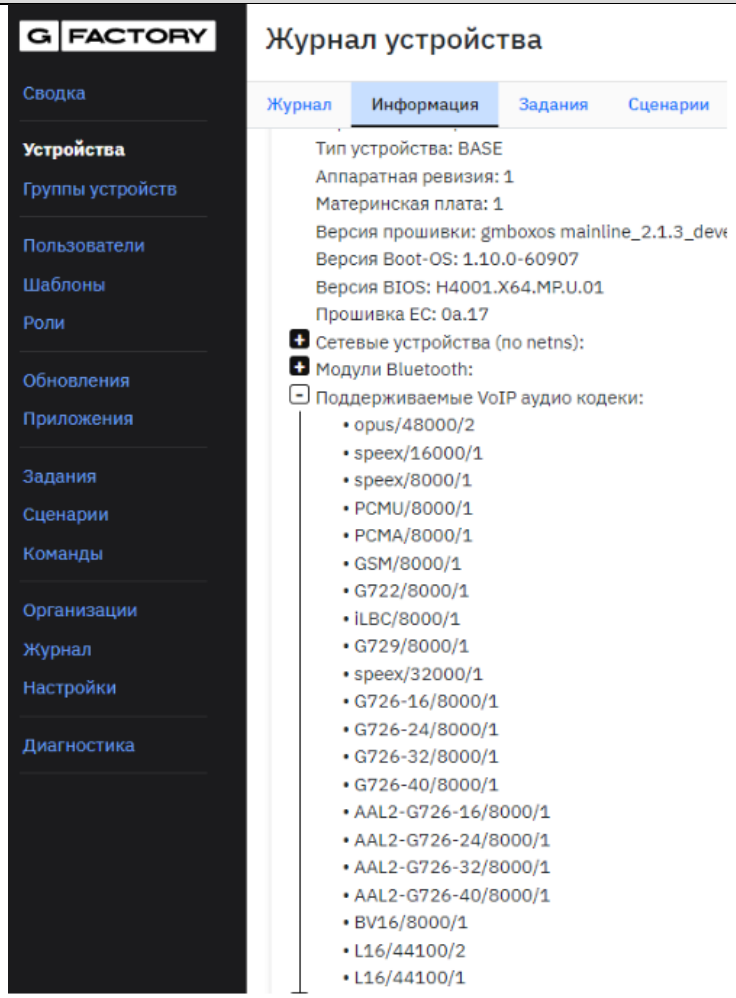
Рисунок 36 – Вид окна раздела «SIP»

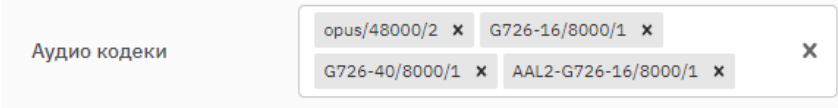
Перечень параметров «SIP» и их описание приведены в Таблица 5.

Таблица 5 – Перечень параметров «SIP» и их описание

Параметр	Ключ	Описание	Пример
Имя хоста	configuration.sip.hostname	IP-адрес или DNS-имя сервера IP-телефонии (SIP-сервера).	172.16.4.172
Имя пользователя	configuration.sip.username	Имя пользователя SIP-сервера.	2197
ID пользователя	configuration.sip.userid	При подключении к Cisco Unified Communications Manager (далее – CUCM) указывается значение «Digest Credentials». При этом значение является чувствительным к регистру и должно быть указано строго в соответствии с параметром, заданным на CUCM.	
Пароль	configuration.sip.password	Пароль пользователя SIP-сервера.	1234
Параметры	configuration.sip.phone	Дополнительные параметры SIP-клиента.	
VLAN ID	configuration.sip.vlanid	VLAN-индентификатор для SIP-телефонии. Используется в случаях, когда для работы IP-телефонии применяется отдельный VLAN. ***Внимание!*** *В случае выделения сервиса IP-телефонии в отдельный VLAN (voice VLAN), необходимо обеспечить функционирование сервиса DHCP и трансляцию DNS в voice VLAN.*	

Параметр	Ключ	Описание	Пример
		пустое значение - VLAN не присваивается, VLAN интерфейс не создается. **AUTO** - VLAN присваивается автоматически с использованием протокола LLDP. **Фиксированный номер VLAN** (например, 314) - для SIP трафика будет использован VLAN с указанным номером.	
Аудио кодеки	configuration.sip.audio_codecs	Поле предназначено для выбора аудиокодека, который будет использован в АТС. Чтобы посмотреть список поддерживаемых аудиокодеков, необходимо открыть карточку устройства и зайти во вкладку "Информация".	opus/48000/2 speex/16000/1 speex/8000/1 PCMU/8000/1 PCMA/8000/1 GSM/8000/1 G722/8000/1 iLBC/8000/1 G729/8000/1 speex/32000/1 G726-16/8000/1 G726-24/8000/1 G726-32/8000/1 G726-40/8000/1

Параметр	Ключ	Описание	Пример
			AAL2-G726-16/8000/1 AAL2-G726-24/8000/1 AAL2-G726-32/8000/1 AAL2-G726-40/8000/1 BV16/8000/1 L16/44100/2 L16/44100/1

Параметр	Ключ	Описание	Пример
		Для добавления в профиль пользователя интересующего аудио кодека необходимо: - скопировать название интересующего аудио кодека$ - зайти в профиль пользователя и открыть раздел "SIP". - вставить скопированное название в поле и нажать ENTER. После выполненных действий, добавленные аудиокодеки будут отображаться следующим образом:  ***Внимание!*** *Если поле "Аудио кодеки" оставить пустым, то GM-Box автоматически будет поддерживать только стандартные аудиокодеки. При ручном добавлении аудио кодеков, в сессии пользователя будут поддерживаться только те кодеки, которые отображаются в поле "Аудио кодеки" (напр. если указали только opus/48000/2, значит в сессии будет поддерживаться только этот кодек).*	

5.5.2.4 «AD/LDAP»

Данный раздел (Рисунок *37*) позволяет администратору редактировать параметры службы каталогов для синхронизации контактов и адресной книги. Учетная запись пользователя работает только в режиме чтения.

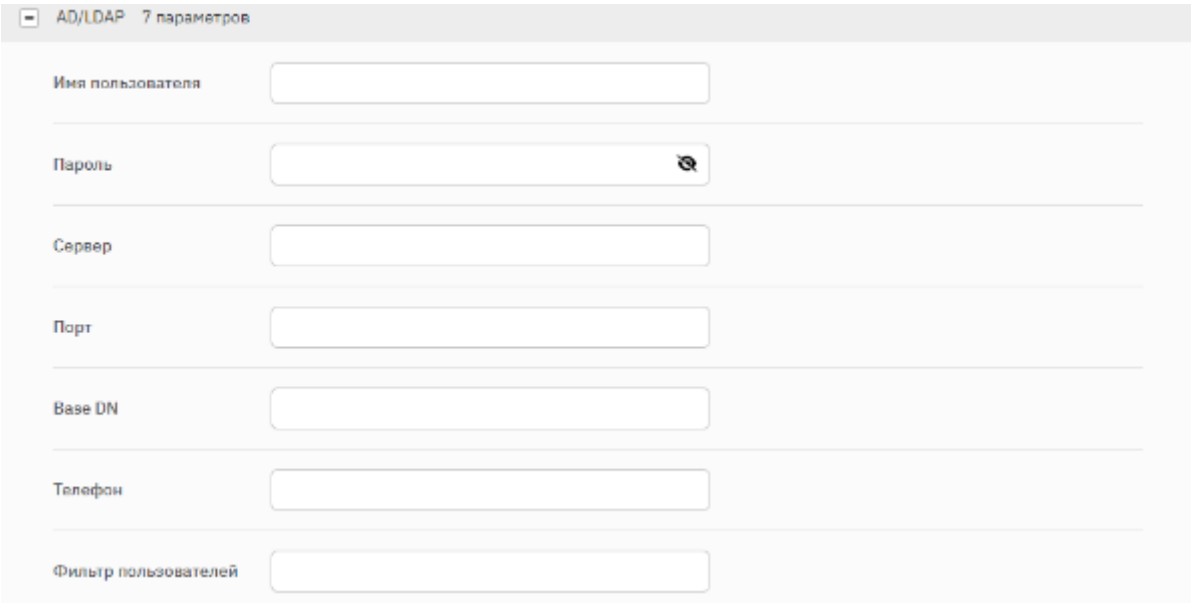


Рисунок 37 – Вид окна раздела «AD/LDAP»

Перечень редактируемых параметров «AD/LDAP» и их описание приведены в Таблица 6.

Таблица 6 –Перечень редактируемых параметров «AD/LDAP» и их описание

Параметр	Ключ	Описание	Пример
Имя пользователя	configuration.ad.username	Логин специальной учетной записи для получения информации для адресной книги из корпоративной службы каталогов	uid=gm-user,o=1, ou=USER_ OU,dc=USER_DC,dc=RU"
Пароль	configuration.ad.password	Пароль специальной учетной записи	Password
Сервер	configuration.ad.server	IP-адрес или DNS-имя корпоративной службы каталогов	Ad.example.org
Порт	configuration.ad.port	Номер порта на сервере корпоративной службы каталогов для TCP/UDP соединений.	389
Base DN	configuration.ad.base	Корневая папка поиска. СУ будет осуществлять поиск объектов в данной папке и во всех вложенных контейнерах и Organization Units.	Для корневого контейнера домена example.org:dc=example,dc=org

Параметр	Ключ	Описание	Пример
Телефон	configuration.ad.telephone	Название поля учетных записей корпоративной службы каталогов, в котором хранится информация о телефонном номере сотрудника.	telephoneNumber
Фильтр пользователей	configuration.ad.filter	Фильтр поиска. Позволяет задавать точные параметры поиска объектов для их добавления в адресную книгу. Указывается в формате LDAP search filter.	(&(objectClass=person)(!(objectClass=computer)))

5.5.2.5 Раздел «Средства идентификации»

Данный раздел (Рисунок *38*) позволяет администратору добавлять пользователю различные средства идентификации. На данный момент система поддерживает следующие средства идентификации:

- контактные смарткарты;
- бесконтактные смарткарты.

Перечень редактируемых параметров раздела «Средства идентификации» и их описание приведены в тТаблица *7*.

***Примечание**. Поддерживаемые стандарты для контактных смарткарт: ISO 7816, USB; Поддерживаемые стандарты для бесконтактных смарткарт: NFC, RFID. Режим идентификации пользователя по картам и токенам поддерживается на устройствах GM-Box.*

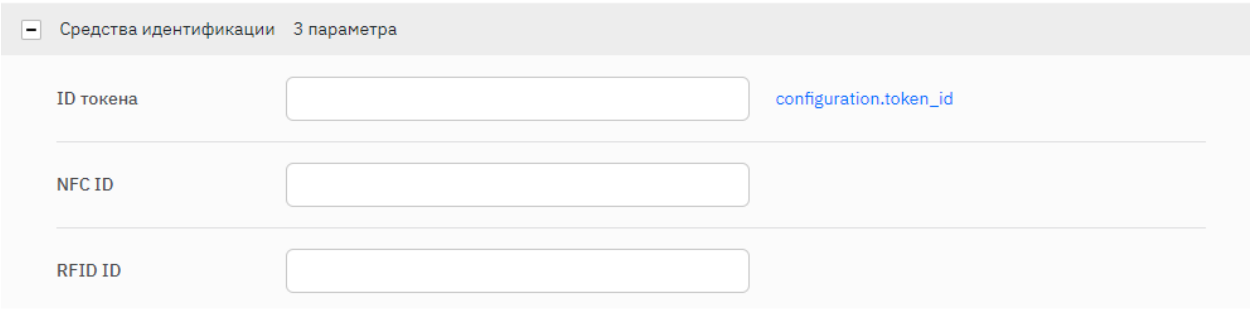


Рисунок 38 – Вид окна раздела «Средства идентификации»

Таблица 7 – Перечень редактируемых параметров раздела «Средства идентификации» и их описание

Параметр	Ключ	Описание	Пример
Контактная смарткарта/Токен	configuration.token_id	Идентификатор USB или другого токена пользователя. Используется при идентификации пользователя при помощи токена.	356e4c7d

Параметр	Ключ	Описание	Пример
Бесконтактная NFC-смарткарта	configuration.nfc_id	Идентификатор NFC-устройства пользователя. Используется при идентификации пользователя с помощью NFC-карты.	044e664a6e4d80
Бесконтактная RFID-смарткарта	configuration.rfid_id	Идентификатор RFID-карты пользователя. Используется при идентификации пользователя с помощью RFID-карты.	737efe49

5.5.2.5.1 Подключение NFC-карты к учетной записи пользователя

При идентификации пользователей с помощью NFC-карт необходимо у каждого пользователя заполнить поле NFC ID.

Для автоматического заполнения этих полей выполните действия, описанные ниже.

1. Убедитесь, что в конфигурационном файле *greeter.conf* в параметре **NFC** указаны следующие значения:

```
{
    "pluginName": "NFC",
    "isEnabled": true,
    "isUsable": true
}
```

   При необходимости отредактируйте конфигурационный файл *greeter.conf*. Для применения обновленного конфигурационного файла на устройствах пользователей в веб-консоли создайте задание на выполнение команды **Patch config Greeter (greeter.conf)**.

2. В веб-консоли выберите раздел **Пользователи** и создайте учетную запись администратора для работы в веб-режиме, заполните следующие поля:

   - Учетная запись – AdminWeb;

- Пароль и повторный ввод пароля;
- ФИО;
- Роль – User;
- Режим GM-Box – Веб;
- Веб-адрес – адрес СУ, например, ***getmobit.example.org***;
- Дополнительное поле – для включения возможности использования NFC после входа в сессию добавьте строку:

```
ENABLE_NFC=true
```

3. Выполните вход в веб-сессию на GM-Box под учетной записью администратора.
4. В веб-консоли выберите раздел **Пользователи,** найдите учетную запись пользователя, которому необходимо подключить NFC-карту, и откройте карточку пользователя на редактирование.
5. Поднесите NFC-карту к GM-Box. Поле NFC ID будет заполнено автоматически.

5.5.2.5.2 Подключение RFID-карты к учетной записи пользователя

При идентификации пользователей с помощью RFID-карт необходимо у каждого пользователя заполнить поле RFID ID.

Для автоматического заполнения этого поля выполните действия, описанные ниже.

1. Убедитесь, что в конфигурационном файле *greeter.conf* в параметре **RFID** указаны следующие значения:

```
{
  "pluginName": "RFID",
  "isEnabled": true,
  "isUsable": true
},
```

   При необходимости отредактируйте конфигурационный файл *greeter.conf*. Для применения обновленного конфигурационного файла на устройствах пользователей в веб-консоли создайте задание на выполнение команды **Patch config Greeter (greeter.conf)**.
2. В веб-консоли выберите раздел **Пользователи** и создайте учетную запись администратора для работы в веб-режиме, заполните следующие поля:

- Учетная запись – AdminWeb;
- Пароль и повторный ввод пароля;
- ФИО;
- Роль – User;
- Режим GM-Box – Веб;
- Веб-адрес – адрес СУ, например, ***getmobit.example.org***.

3. Выполните вход в веб-сессию на GM-Box под учетной записью администратора.
4. В веб-консоли в разделе **Пользователи** найдите учетную запись пользователя, которому необходимо подключить RFID-карту, и откройте карточку пользователя на редактирование.
8. Поднесите RFID-карту к GM-Box. Поле RFID ID будет заполнено автоматически.

5.5.2.5.3 Подключение токена к учетной записи пользователя

При идентификации пользователей с помощью токена необходимо у каждого пользователя заполнить поле TOKEN ID.

Для автоматического заполнения этого поля выполните действия, описанные ниже.

1. Убедитесь, что в конфигурационном файле *greeter.conf* в параметре **Token** указаны следующие значения:

```
{
  "pluginName": "Token",
  "isEnabled": true,
  "isUsable": true
},
```

   При необходимости отредактируйте конфигурационный файл *greeter.conf*. Для применения обновленного конфигурационного файла на устройствах пользователей в веб-консоли создайте задание на выполнение команды **Patch config Greeter (greeter.conf)**.
2. В веб-консоли выберите раздел **Пользователи** и создайте учетную запись администратора для работы в веб-режиме, заполните следующие поля:

   - Учетная запись – AdminWeb;
   - Пароль и повторный ввод пароля;
   - ФИО;
   - Роль – User;
   - Режим GM-Box – Веб;
   - Веб-адрес – адрес СУ, например, ***getmobit.example.org***.

3. Выполните вход в веб-сессию на GM-Box под созданной учетной записью администратора.
4. В веб-консоли в разделе **Пользователи** найдите учетную запись пользователя, которому необходимо подключить токен, и щелчком мыши откройте карточку пользователя на редактирование.
9. Подключите токены Rutoken и Jacarta к GM-Box. Поле TOKEN ID будет заполнено автоматически.

5.5.2.6 Раздел «Дополнительно»

Дополнительное поле (Рисунок *39*) предназначено для ручного ввода дополнительных настроек пользователя.



Рисунок 39 – Вид окна раздела «Дополнительное поле»

Дополнительное поле.

1) Описание параметров приведено в п. 5.16.2 С помощью регулярного выражения можно удалить из записи телефонного номера лишние символы – скобки, пробелы и дефисы.

SIP_NUMBER_EXCLUDE_REGEXP="[()-]"

2) Как настроить доменную аутентификацию пользователей по протоколу Kerberos в VDI Citrix см. подраздел 12.6

5.5.3 Вкладка «Журнал»

Данная вкладка (Рисунок *40*) доступна только при корректно настроенном сервисе мониторинга и необходима для просмотра администратором на СУ следующих событий:

- Идентификация;
- Аутентификация;
- Изменение статуса сессии пользователя (напр. вход выполнен успешно, сессия завершена).

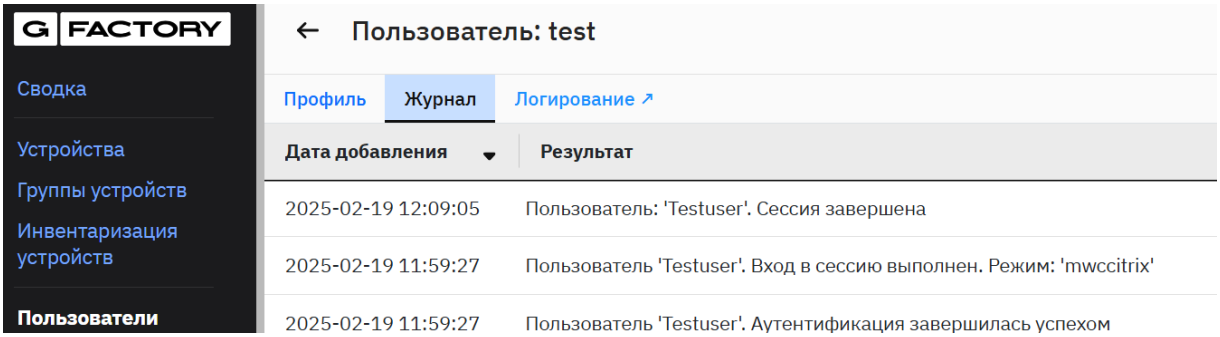


Рисунок 40 – Вид окна вкладки «Журнал»

Данные выводятся в виде таблицы, которая имеет следующие поля:

- Дата добавления события – в формате гггг-мм-дд чч:мм:сс. По умолчанию сортировка событий происходит от новых к старым;
- Результат – описание результата события;
- Процесс – компонент системы, который отправил сообщение в поле "Результат";
- ID устройства – ID материнской платы устройства, с которым взаимодействовал пользователь.

5.5.4 Вкладка «Логирование»

Данная вкладка (Рисунок *41*) доступна только при корректно настроенном сервисе мониторинга и позволяет перейти в сервис логирования Kibana для просмотра логов пользователя. Для перехода на сервис логирования необходимо нажать на вкладку.

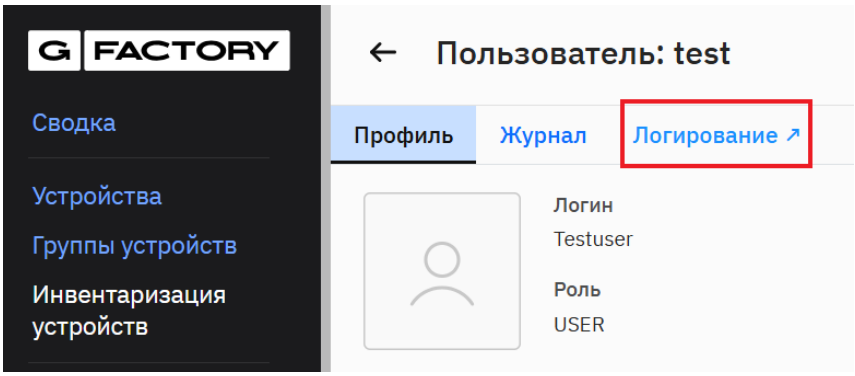


Рисунок 41 – Вкладка «Логирование»

5.5.5 Редактирование учетной записи пользователя

Редактирование учетной записи осуществляется для существующего пользователя.

Чтобы внести изменения в профиль пользователя, необходимо войти в профиль, внести необходимые изменения и нажать **Сохранить** (Рисунок *42*).

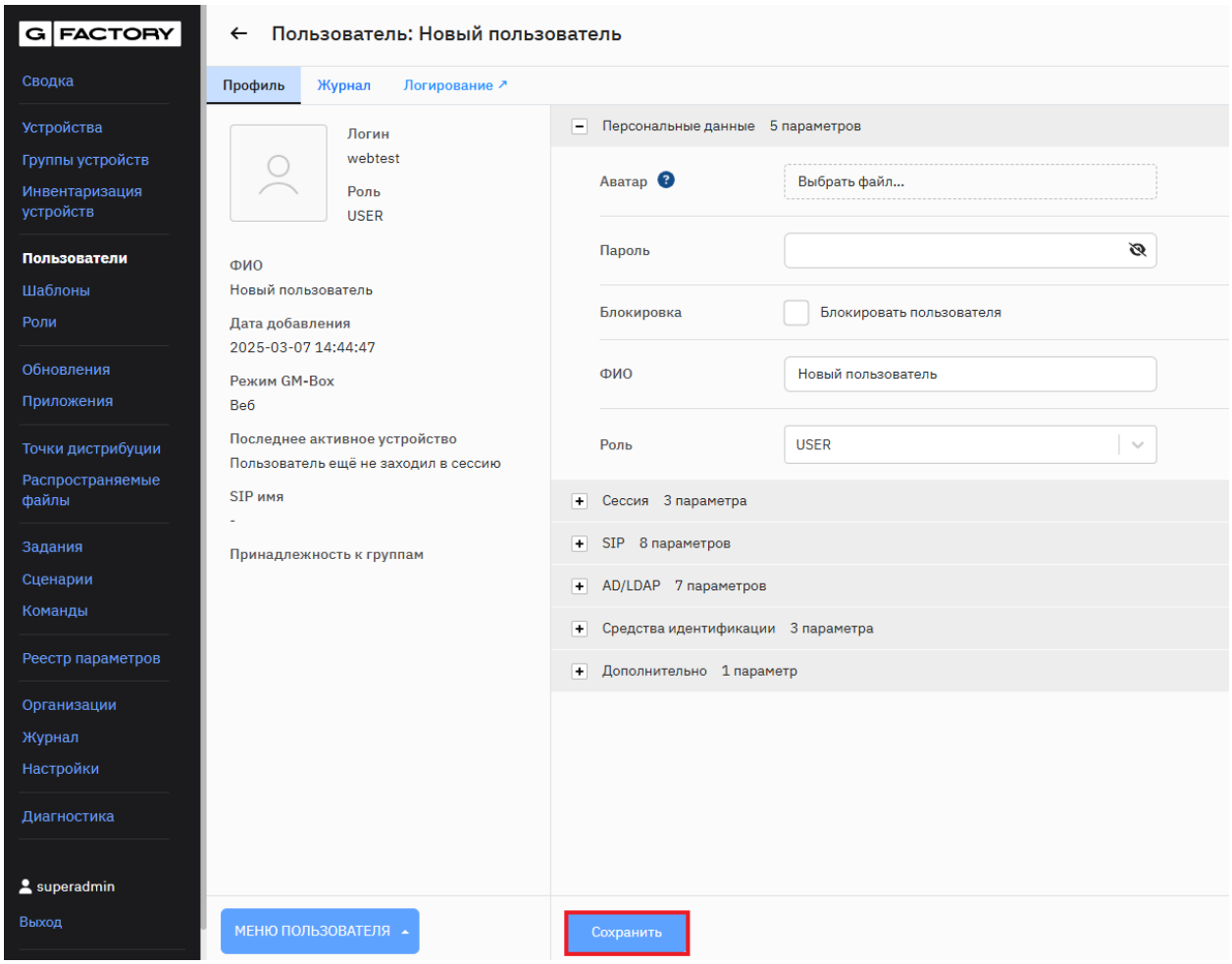


Рисунок 42 – Редактирование учетной записи пользователя

Внимание!!!*При изменении пароля, роли или блокировки в профиле пользователя, все его активные браузерные сессии (в других вкладках, браузерах, на других устройствах) будут сброшены.*

5.5.6 Удаление учетной записи пользователя

Для удаления учетной записи пользователя с СУ необходимо отметить флажком нужную учетную запись и нажать **Удалить** (Рисунок *43*)

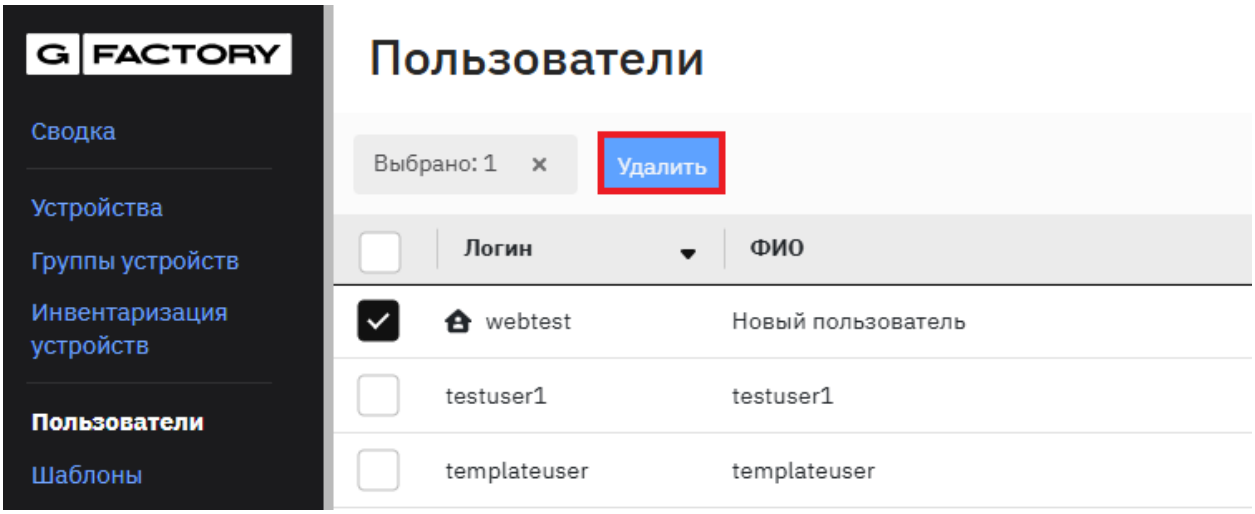


Рисунок 43 – Удаление учетной записи пользователя

5.6 Шаблоны

При помощи шаблонов, администратор может формировать профили пользователей или групп пользователей.

Шаблон задает группе / категории пользователей единые параметры подключения к SIP АТС, режимы и параметры запуска VDI клиентов и клиентов терминального доступа, список доступных приложений и сервисов и т.д.

Создавать, редактировать или удалять шаблоны может администратор, у которого есть соответствующие права.

В разделе **Шаблоны** отображается список шаблонов, созданных через веб-консоль и доступных на СУ.

5.6.1 Создание шаблона

Перед созданием шаблона необходимо выполнить действия, описанные ниже.

1. В службе каталогов пользователей определить атрибуты для деления на группы и добавить пользователей в эти группы.
2. Определить требования к корневым шаблонам настроек пользователей и групп пользователей, таким как: параметры подключения к SIP АТС, режимы и параметры запуска VDI клиентов и клиентов терминального доступа и т.д.

3. Для создания шаблона в веб-консоли выберите раздел **Шаблоны** и в верхней части раздела нажмите **Добавить** (Рисунок *44*).

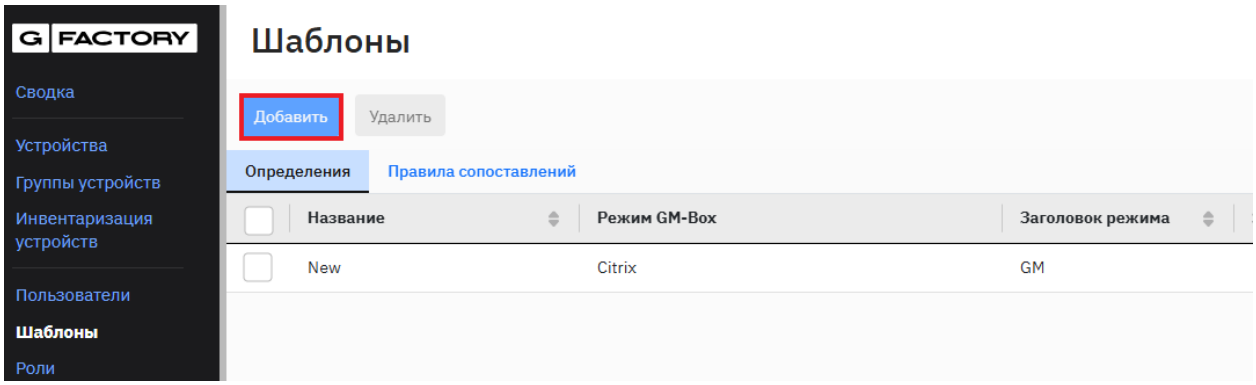


Рисунок 44 – Вид окна раздела Шаблоны

Откроется карточка нового шаблона (Рисунок *45*)

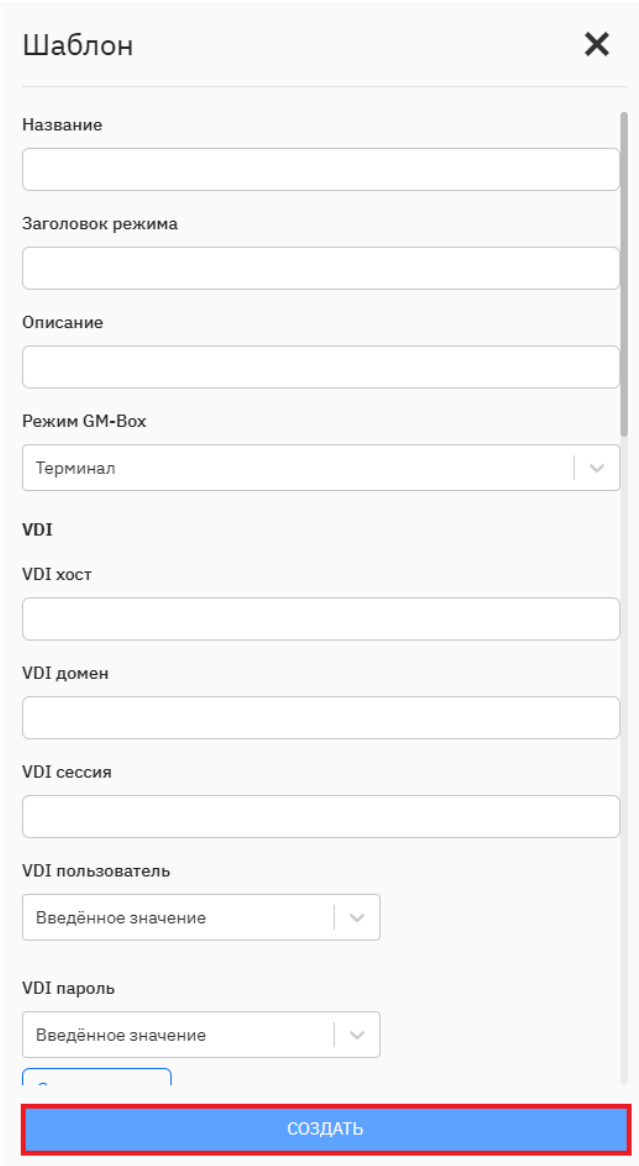


Рисунок 45 – Вид окна карточки нового шаблона

4. Заполните поля :
   1) **Название** шаблона;
   2) **Описание** шаблона;
   3) **Режим GM-Box** – режим работы пользователя. Список возможных режимов приведен в Таблица 4.
   4) **Раздел VDI** – задайте параметры подключения VDI клиентов;
   5) **Раздел SIP** – задайте параметры SIP-телефонии;
   6) Параметры корпоративной службы каталогов для синхронизации контактов и корпоративной адресной книги.
5. Нажмите **Создать**.

5.6.2 Редактирование шаблона

Для редактирования выберите шаблон в списке.

Внесите необходимые изменения и нажмите **Сохранить изменения**.

5.6.3 Создание шаблона «Витрина»

Для настройки шаблона «Витрина» выполните следующие действия:

1. При создании шаблона выберите в поле **Режим GM-Box** значение Витрина.
2. Свяжите шаблон «Витрина» с пользователем с помощью правил сопоставлений или выберите шаблон в профиле пользователя в поле **Шаблон профиля**.
3. Создайте шаблоны для всех необходимых SD App-приложений.
4. Свяжите шаблоны для SD App-приложений с шаблоном «Витрина», для этого выберите в поле **Связанные шаблоны** все необходимые шаблоны SD App-приложений.

При входе в сессию пользователь на рабочем столе витрины увидит доступные ему SD App-приложения.

5.6.4 Правила сопоставлений

Администратор может определить правила сопоставления, на основе которых пользователям шаблоны назначаются динамически.

Чтобы задать правило сопоставления, в веб-консоли выберите раздел **Шаблоны,** вкладку **Правила сопоставлений** и в верхней части раздела нажмите **Добавить**. Откроется карточка нового правила.

Заполните поля:

1) **Тип** – задает условие, при выполнении которого шаблон назначается пользователю:
   - Атрибут (поле и значение) – если указанное поле в учетной записи пользователя имеет одно из указанных значений;
   - Группа AD/LDAP (значение) – если пользователь принадлежит к одной из указанных групп. Сейчас проверка происходит по CN групп AD/LDAP;
   - По умолчанию – если никакие другие правила сопоставления не подошли. Можно задать только одно правило по умолчанию, оно будет последним в списке правил.
2) **Шаблон** – выберите один из заданных ранее шаблонов.
3) **Описание** – укажите краткое описание правила.

При входе пользователя в сессию выполняется проверка учетной записи для назначения шаблона:

1) если шаблон был задан администратором в учетной записи пользователя - назначается указанный шаблон;
2) в противном случае по порядку (сверху вниз) проверяется соответствие правил и учетной записи пользователя, назначается первый шаблон, удовлетворяющий правилам;
3) если совпадений не найдено, то пользователю назначается шаблон по умолчанию;
4) если совпадений не найдено и шаблон по умолчанию не создан, ни один шаблон не назначается.

Чтобы проверить какое правило было сопоставлено пользователю, в веб-консоли выберите раздел **Пользователи** и откройте учетную запись пользователя для редактирования. В поле **Шаблон профиля** указано название шаблона, если он был назначен динамически.

Дополнительно информация о приоритетах правил сопоставления указана в п.п. 2.2.2.3.

5.6.5 Удаление шаблона

Для удаления шаблона отметьте его флажком в левой части списка и нажмите **Удалить.**

5.7 Роли

Роль позволяет ограничивать права доступа пользователей к разделам веб-консоли, например, можно просматривать список устройств, но отключена возможность отправлять задания на GM-Box.

Создавать, редактировать или удалять роли может администратор с соответствующими правами.

Чтобы выполнять действия с ролями, выберите раздел **Роли**. В разделе отображается список ролей, доступных в вашей компании. СУ поддерживает два типа ролей: системные, заданные по умолчанию, и роли, созданные в веб-консоли. По умолчанию заданы следующие системные роли:

1) **USER** – учетная запись с ограниченными правами, используется для аутентификации пользователей на устройствах;
2) **ADMIN** – учетная запись, которая используется для администрирования СУ, позволяет управлять профилями пользователей и устройств;
3) **SECURITY** – учетная запись, позволяет управлять профилями сотрудников отдела безопасности и создавать задания с командами, разрешенными SUPER_ADMIN;
4) **SUPER_ADMIN** – учетная запись с максимальными правами, имеет доступ ко всей функциональности СУ, включая возможность создания и редактирования команд.

5.7.1 Создание роли

Для создания роли в веб-консоли:

1. Выберите раздел **Роли** и в верхней части раздела нажмите **Добавить** (Рисунок 46). Откроется карточка новой роли.

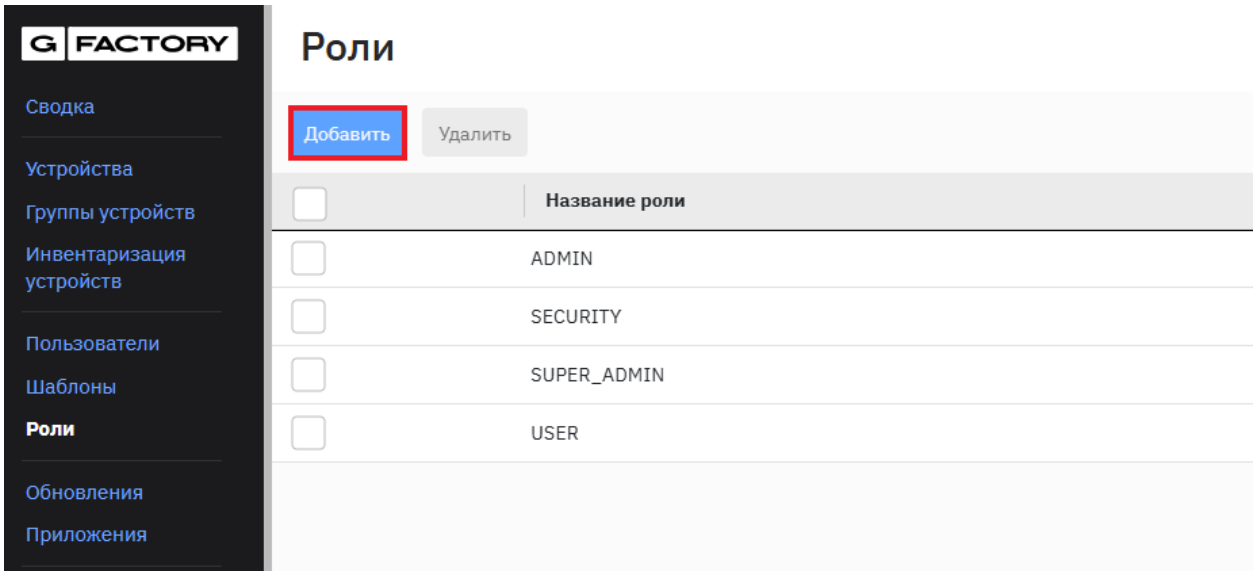


Рисунок 46 – Вид окна «Роли»

2. Заполните поля (Рисунок *47*):

1) **Название роли** – укажите название роли на английском языке, также допустимы символы -(дефис и нижнее подчеркивание);
2) **Описание роли** – в произвольной форме укажите особенности прав доступа этой роли;
3) **Шаблон** – выберите из выпадающего списка.

3. В правой части окна задайте галочками права доступа к разделам веб-консоли:

1) Чтение – возможность просматривать данные в разделе;
2) Обновление – возможность редактировать данные в разделе;
3) Исполнение – возможность исполнения сценариев и выполнения диагностики.

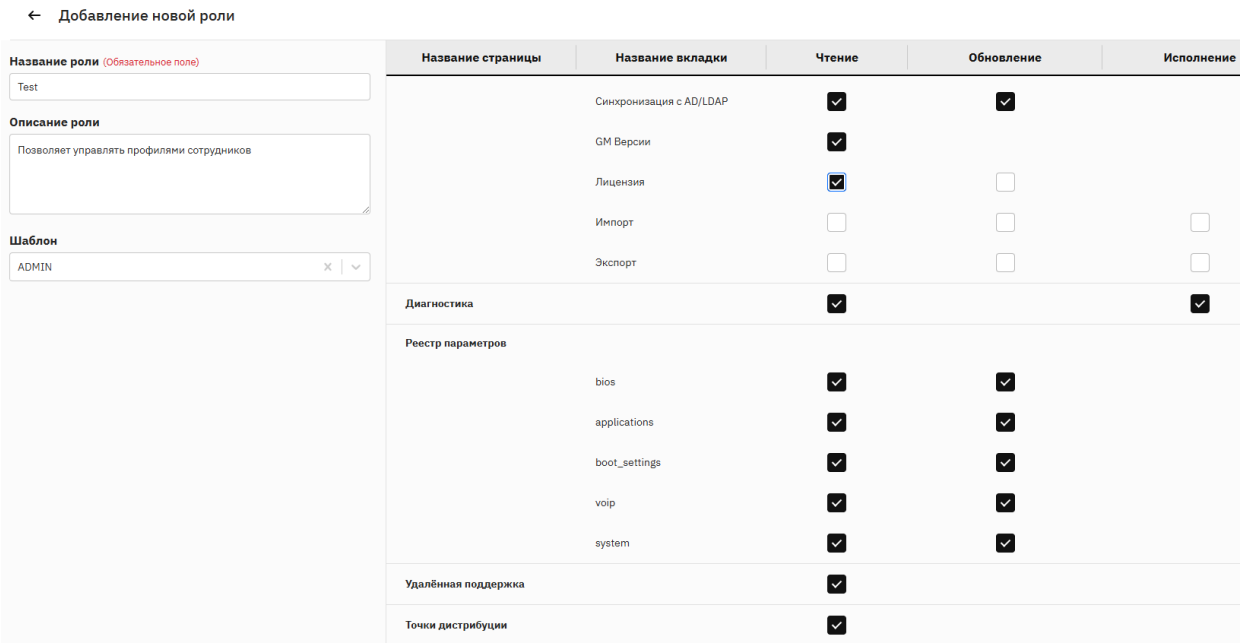


Рисунок 47 – Вид окна «Добавление новой роли»

4. Нажмите **Добавить**.

Созданная роль отобразится в списке и будет доступна для назначения пользователям.

5.8 Обновления

СУ позволяет выполнять централизованное обновление базового встроенного ПО (GM CORE KIT) устройств GM-Box, а также дополнительно устанавливать SD App-приложения, например, VDI-клиенты и VoIP реализации.

Для этого на СУ предусмотрены два реестра:

- реестр обновлений для хранения и управления файлами обновлений базового встроенного ПО (GM CORE KIT);
- реестр приложений для хранения и управления файлами SD App–приложений.

Управление файлами обновлений выполняется в разделе **Обновления**, а управления файлами приложений – в разделе **Приложения**. Администратор может выполнять следующие действия с обновлениями/приложениями:

1) добавить обновление/приложение в реестр на СУ;
2) редактировать карточку обновления/приложения;
3) удалять обновление/приложение из реестра с СУ.

5.8.1 Добавление файла обновлений

Примечание. *После загрузки обновления необходимо создать задание на его распространение по устройствам*

Файлы обновлений («прошивки») имеют расширение .**swu** и размещаются в Личном кабинете.

Для добавления файла обновления на СУ выполните действия, описанные ниже.

1. Загрузите файл с расширением **.swu**.
2. Выберите в веб-консоли раздел **Обновления** и нажмите **Добавить** (Рисунок *48*). В правой части раздела откроется карточка нового файла обновления.

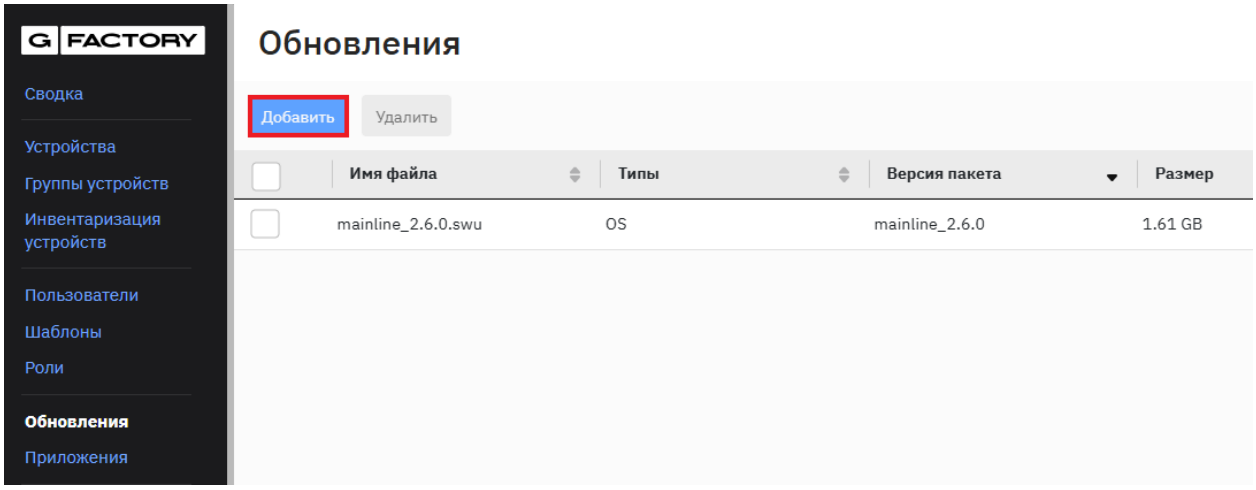


Рисунок 48 – Вид окна раздела Обновления

3. Перетащите файл обновления в карточку, в область, отмеченную пунктирными границами, или щелкните по этой области и выберите файл в открывшемся окне проводника.
4. Нажмите **Загрузить** (Рисунок *49*). Процесс загрузки файла можно приостанавливать и возобновлять. Если в процессе загрузки возникла сетевая ошибка, загрузка файла продолжается после восстановления сетевого соединения.

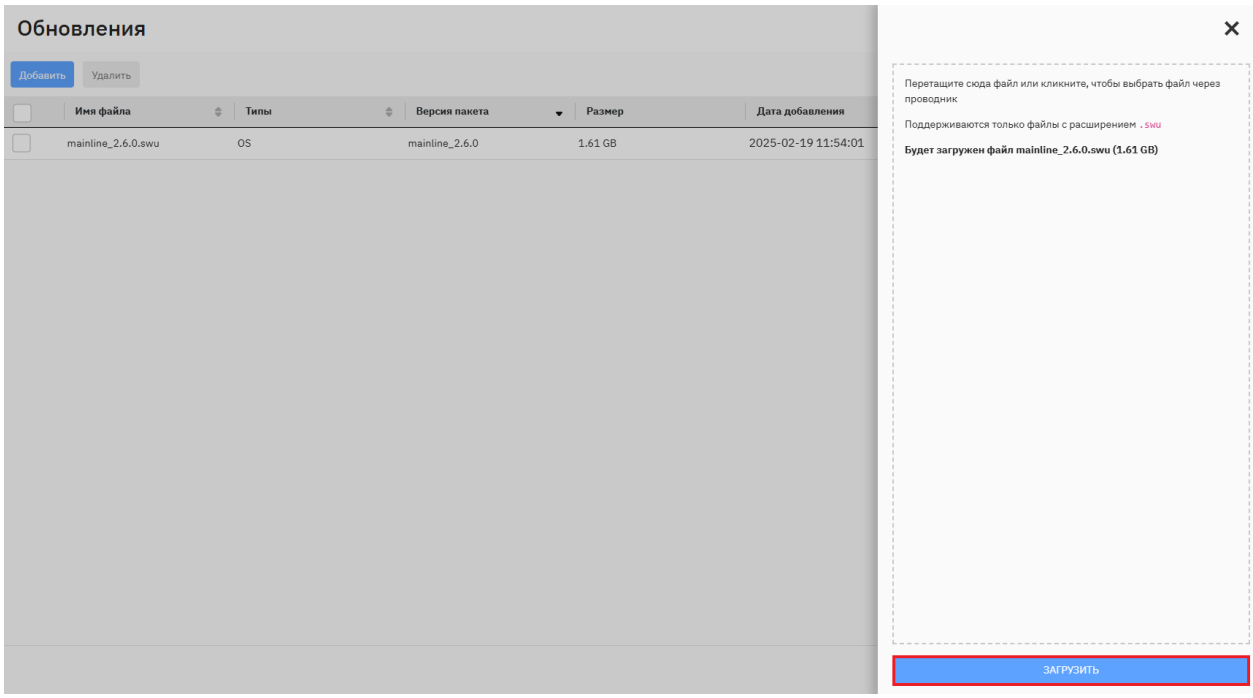


Рисунок 49 – Добавление и загрузка файла обновления

После загрузки файла карточка автоматически закроется, и новый файл обновления появится в списке.

5.8.2 Удаление файла обновлений

Для удаления файла обновления/приложения отметьте его флажком в левой части списка и нажмите **Удалить**.

5.9 Приложения

Внимание! *Начиная с версии GM OS 2.0.0-RC, на управляемые устройства может потребоваться установка SD App-приложений. Полный список доступных SD App-приложений, реализуемых ими режимов, а также режимов, доступных без установки SD App-приложений приводится в бюллетене о выпуске соответствующей версии ПО (Release notes).*

Порядок установки SD App-приложений также приводится в соответствующих им Release notes.

SD App-приложения хранятся в энергонезависимой памяти устройства и запускаются в момент вызова приложения, если их запуск предусмотрен для пользователя, вошедшего в сессию на устройстве.

При установке приложения администратор должен убедиться, что:

1) версия СУ не ниже 3.3.1;
2) версия ПО на GM-Box не ниже 2.0.0;
3) на СУ есть лицензия на приложение;
4) в личном кабинете есть установочный файл SD App-приложения в формате swu.

Внимание! *Если на СУ нет лицензии на SD App-приложение, то установочный файл не загрузится, а если лицензия закончилась, то приложение не запустится на GM-Box.*

5.9.1 Загрузка приложения на СУ

Для загрузки файла с расширением .swu на СУ, выполните действия, описанные ниже.

1. Скачайте установочный файл SD App-приложения из личного кабинета (cp.getmobit.ru, раздел Файлы).
2. Выберите в веб-консоли раздел **Приложения** и нажмите **Добавить** (Рисунок *50*). В правой части раздела откроется карточка нового файла приложения. После успешной загрузки файл отобразится в списке.

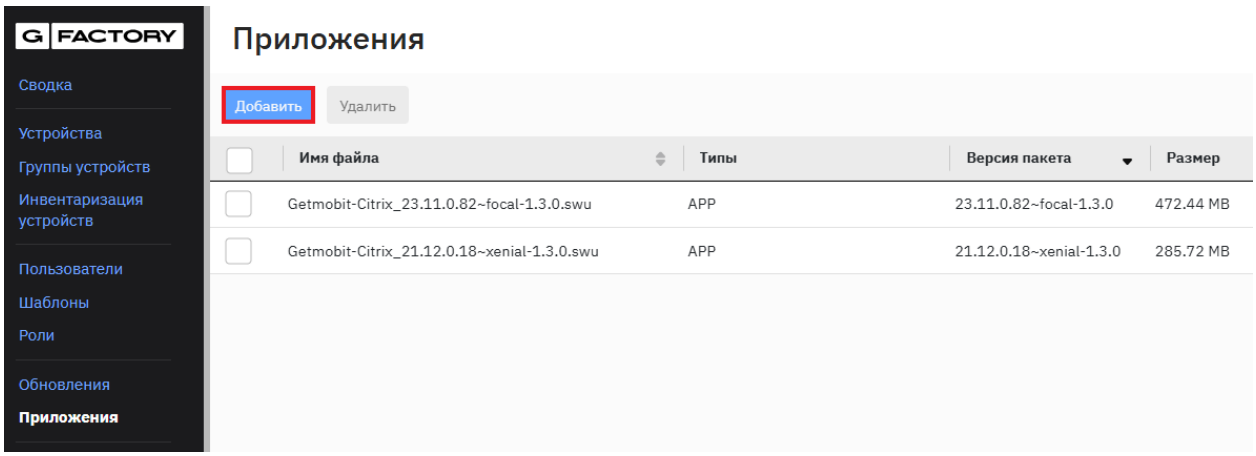


Рисунок 50 – Вид окна раздела «Приложения»

3. Перетащите файл приложения в карточку, в область, отмеченную пунктирными границами, или щелкните по этой области и выберите файл в открывшемся окне проводника.
4. Нажмите **Загрузить** (Рисунок *51*). Процесс загрузки файла можно приостанавливать и возобновлять. Если в процессе загрузки возникла сетевая ошибка, загрузка файла продолжается после восстановления сетевого соединения.

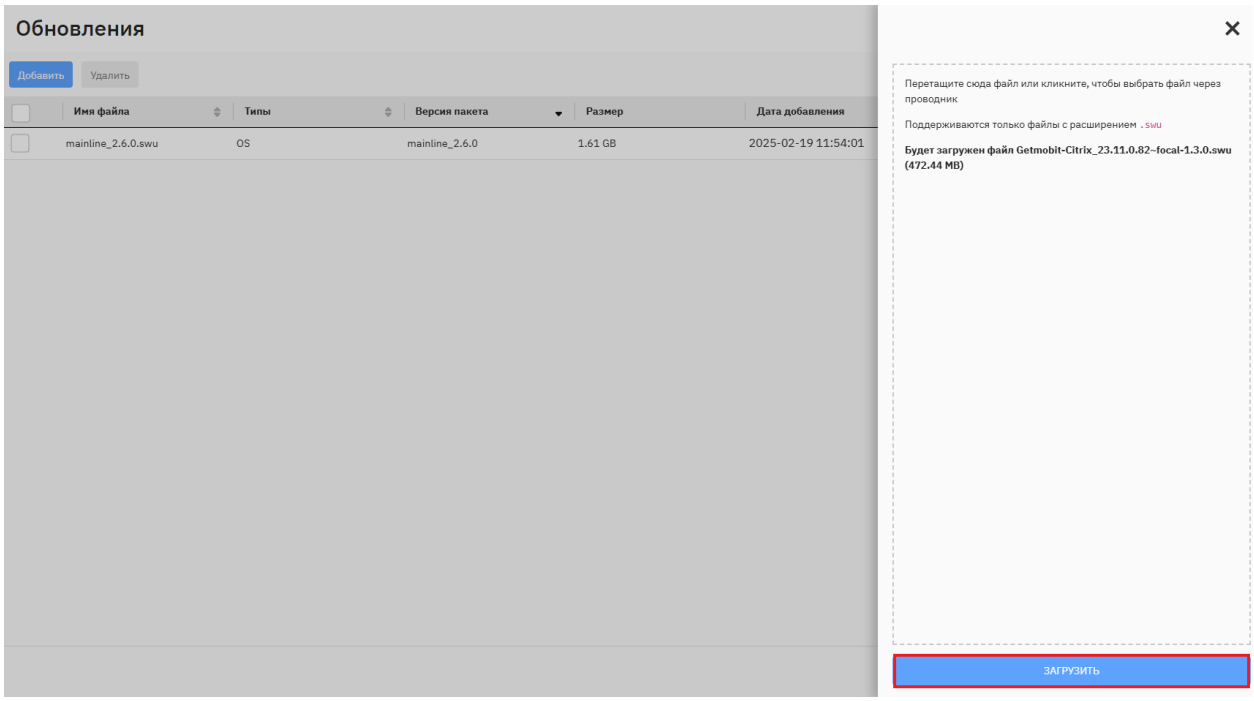


Рисунок 51 – Добавление и загрузка файла приложения

После загрузки файла карточка автоматически закроется, и новый файл приложения появится в списке.

5.9.2 Установка приложения

Для установки SD App-приложения, в общем случае, выполните действия, описанные ниже.

1. Загрузите из личного кабинета (cp.getmobit.ru раздел Файлы) необходимую версию SD App-приложения.
2. В веб-консоли в разделе **Приложения** загрузите файле (файл с расширением swu).
3. В веб-консоли создайте задание на очистку логов с устройств (команда Clear Logs).

Примечание: *Если команда **Clear logs** отсутствует в списке доступных команд на вашем СУ, создайте ее (см. п. 5.13.2)*

4. В открывшемся диалоговом окне введите:
   1) **Наименование**: Clear logs;
   2) **Тип**: SYSTEM;
   3) **Данные**: (cmd "/opt/getmobit/bin/gmbox-clean-varlogs mail.* *.log* debug messages watchdog/* syslog*")
5. Нажмите кнопку **Создать**.

Дождитесь выполнения задания на очистку логов.

6. В веб-консоли создайте задание на выполнение команды установки приложения (команда Install Application & Reboot). Дождитесь выполнения задания.
7. Убедитесь, что в информации (Рисунок *52*) об устройстве отображается установленное приложение (**Устройства – Информация – Smart Desktop – installed_apps**):

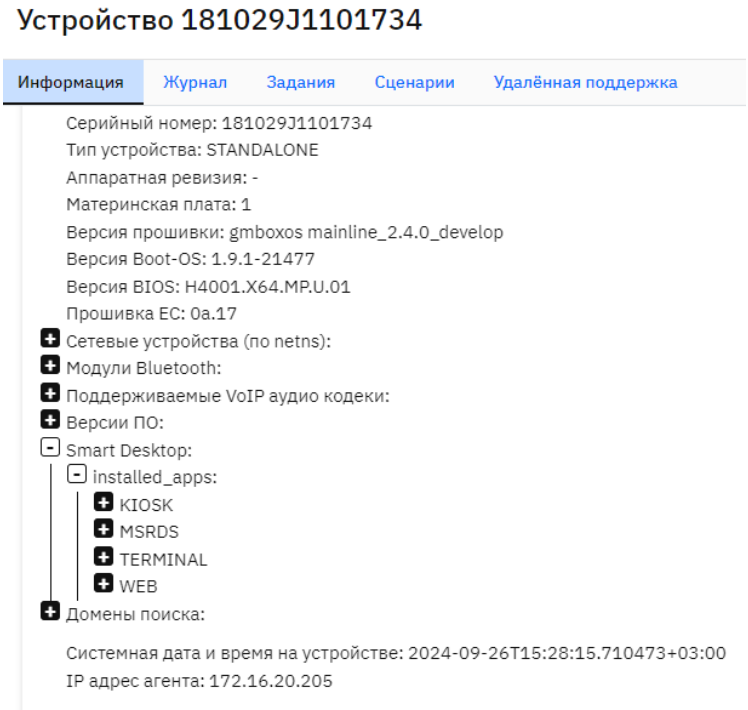


Рисунок 52 – Отображение установленных приложений

8. Выполните тестовый вход в сессию пользователем, для которого настроен режим работы с использованием установленного SD App-приложения.

Примечание. *Режимы (SD App-приложения), доступные пользователю, добавляются динамически при добавлении SWU-файла в реестр приложений*

5.9.3 Проверка установленных приложений и их версий на управляемых устройствах

1. В веб-консоли выберите раздел **Устройства**.
2. Выберите необходимое устройство (в т.ч. GM-Box).
3. Перейдите во вкладку **Информация**.
4. Далее в дереве выберите **Smart Desktop→installed_apps.** Выберите необходимое приложение. В пункте Ver указана версия приложения.
5. Чтобы посмотреть версию установленного пакета, выберите раздел **Packages**.

5.9.4 Удаление приложений с управляемых устройств

Чтобы удалить установленные приложения необходимо создать задание.

1) В веб-консоли выберите раздел **Задания**;
2) Нажмите **Добавить**;
3) Введите в поле **Назначить на** идентификатор GM-Box;
4) В выпадающем списке выберите команду **Remove Installed Applications & Reboot**;
5) Нажмите кнопку **Создать**.

Дождитесь завершения задания и перезагрузки GM-Box.

***Примечание**. В текущей версии СУ не поддерживается удаление отдельных приложений. После выполнения команды **Remove Installed Applications & Reboot** потребуется повторная установка необходимых Smart Desktop приложений.*

5.9.5 Переустановка приложения

Чтобы переустановить приложение, выполните следующие действия:

1. Удалите приложения (см. п. 5.9.4).
2. Затем установите приложение (см. п. 5.9.2).

5.10 Точки дистрибуции и распространяемые файлы

***Примечание.** Информация по установке, настройке и администрированию модуля GM Smart System New Generation. Distribution Point приводится в документе «**Руководство администратора. Модуль GM SMART SYSTEM NEW GENERATION. DISTRIBUTION POINT**»*

Точки дистрибуции (далее – ТД) предназначены для обеспечения эффективного распространения файлов, необходимых для работы устройств, а также для поддержки процессов установки и конвертации устройств (процесс преобразования сторонних устройств для взаимодействия с СУ).

Основная цель ТД – оптимизация доставки данных за счет использования локальных серверов, что снижает нагрузку на СУ и ускоряет доступ к файлам.

Основной функционал ТД:

- распространение файлов;

- администрирование через веб-консоль;
- автоматическая и ручная синхронизация файлов;
- мониторинг и управление файлами;
- просмотр загруженных файлов на ТД.

5.11 Задания

СУ позволяет осуществлять централизованное управление устройствами GETMOBIT (см. подраздел 5.2) методом удаленного выполнения команд. Это могут быть команды на перезагрузку и выключение устройства, принудительное завершение сессии пользователя и обновление ПО устройства т.д.

Задания позволяют указать, какие команды должны быть выполнены на устройствах, и расписание их выполнения.

Задание можно назначить на одно устройство или группу устройств, однократно или с регулярным повторением для выполнения в определенные дни недели или месяца (см. п. 5.11.1).

Для автоматического выполнения заданий на впервые подключенных (в т.ч. сброшенных на настройки по умолчанию) необходимо в качестве устройств выбрать вариант **Впервые подключенные**.

Задание, назначенное на впервые подключенные устройства, будет выполнено после первого подключения устройства к СУ и проведения его первичной настройки (см. п. 4.5.5). Чтобы это задание снова выполнилось, можно удалить устройство из списка и заново подключить его к СУ.

Задание, назначенное на вновь настроенные устройства, будет выполняться каждый раз после первичной настройки устройства – то есть, после первого подключения устройства к СУ, переподключения устройства с другого СУ к данному, а также по факту подключения устройства к СУ после проведенного сброса к заводским настройкам.

Управление заданиями осуществляется в веб-консоли в разделе **Задания**.

Администратор может:

- создать новое задание;
- редактировать карточку задания;
- удалить задание.

5.11.1 Создание задания

Для создания нового задания выполните действия, описанные ниже.

1. В консоли выберите раздел **Задания** (Рисунок 53).
2. Нажмите **Добавить**. В правой части откроется карточка нового задания. Укажите название задания.
3. В поле **Назначить на** выберите из выпадающего списка устройства или введите название устройства/группы устройств, на которых необходимо выполнить задание.
4. Укажите периодичность выполнения задания.
5. Выберите из выпадающего списка команду, которую необходимо выполнить.
6. Нажмите **Создать**.

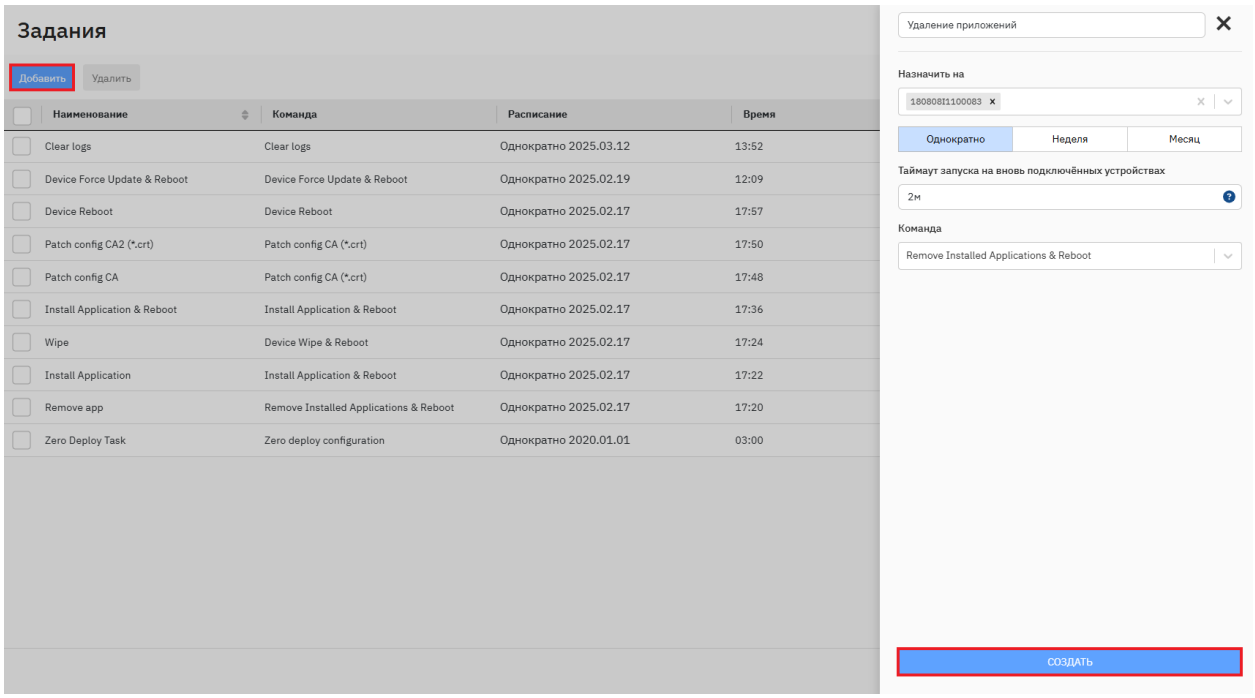


Рисунок 53 – Создание задания

5.11.2 Редактирование карточки задания

Чтобы отредактировать карточку задания откройте раздел **Задания** и выберите задание в списке.

На открывшейся странице отображаются:

- в центре – история выполнения задания, которая обновляется в режиме реального времени;
- справа – поля карточки задания.

В Истории отображается список устройств, на которые было назначено выполнение этого задания. Справа от наименования устройства отображается статус выполнения задания:

- Initial (Инициализация) - здание принято к выполнению;
- Pending (В работе) - задание отправлено на устройство;
- Process (Выполняется) - задание выполняется на устройстве;
- Finished (Завершено) - задание успешно выполнено;
- Error (Ошибка) - задание завершено с ошибкой (см. поле Результат для уточнения подробностей);
- Unknown (Неизвестно) - результат выполнения задания неизвестен (характерно для заданий, включающих перезагрузку устройства)

5.11.3 Удаление задания

Для удаления задания установите флажок в левой части списка и нажмите **Удалить**.

5.12 Сценарии

Внимание!!! *Функционал сценариев доступен для устройств GM-Box с ПО Core Kit 2.3.0+ и СУ GM Workspace Factory 3.12.3+.*

СУ позволяет формировать цепочки последовательно выполняемых команд (шагов) на выбранных устройствах и группах устройств. Такими цепочками могут быть:

- установка сертификатов, конфигурации VPN и настройка персонализации при подключении нового устройства к СУ;
- регулярная очистка логов и временных файлов на устройствах;
- иные административные сценарии.

Сценарии могут выполняться:

- по запросу администратора (единоразово в момент запуска сценария);
- по расписанию – ежедневно, по дням недели, по дням месяца;
- по событию, при наступлении предопределенного события, в том числе:
    a. для впервые подключенных устройств;
    b. для вновь настроенных устройств.

При работе со сценариями администратор также может:

- выполнить тестовый запуск сценария по расписанию;

- контролировать выполнение команд: изменять их последовательность и добавлять команды, при неуспешном выполнении которых не происходит досрочное завершение сценария;
- учитывать часовой пояс устройства в сценариях по расписанию;
- просматривать истории запусков сценария, статусы и результаты выполнения отдельных команд.

5.12.1 Создание нового сценария

Для создания нового сценария выполните следующие действия:

1. В веб-консоли выберите раздел **Сценарии**.
2. Нажмите → **Добавить**.

Откроется окно нового сценария (Рисунок *54*).

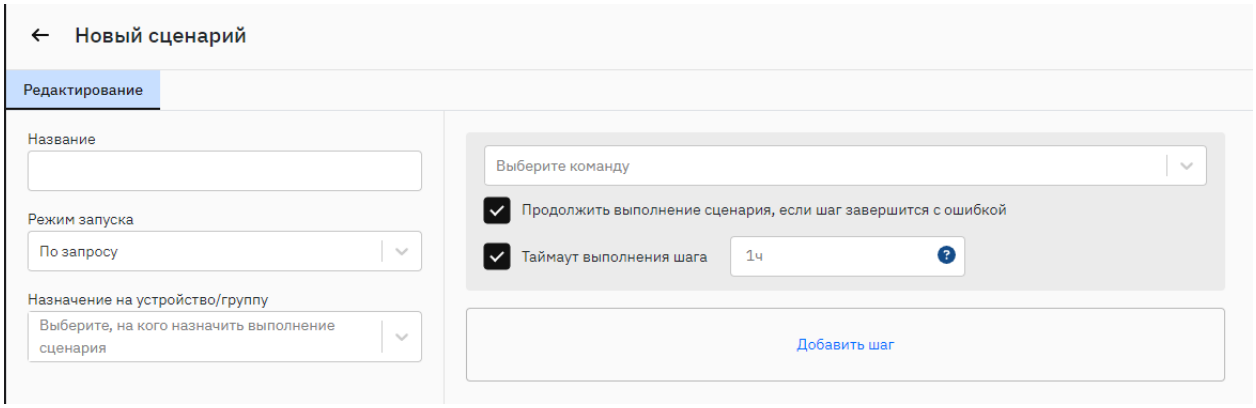


Рисунок 54 – Вид окна Новый сценарий

3. Выберите последовательность команд, которые необходимо выполнить. При необходимости установите галочку **Продолжить выполнение, если команда завершится с ошибкой** (Рисунок *55*).

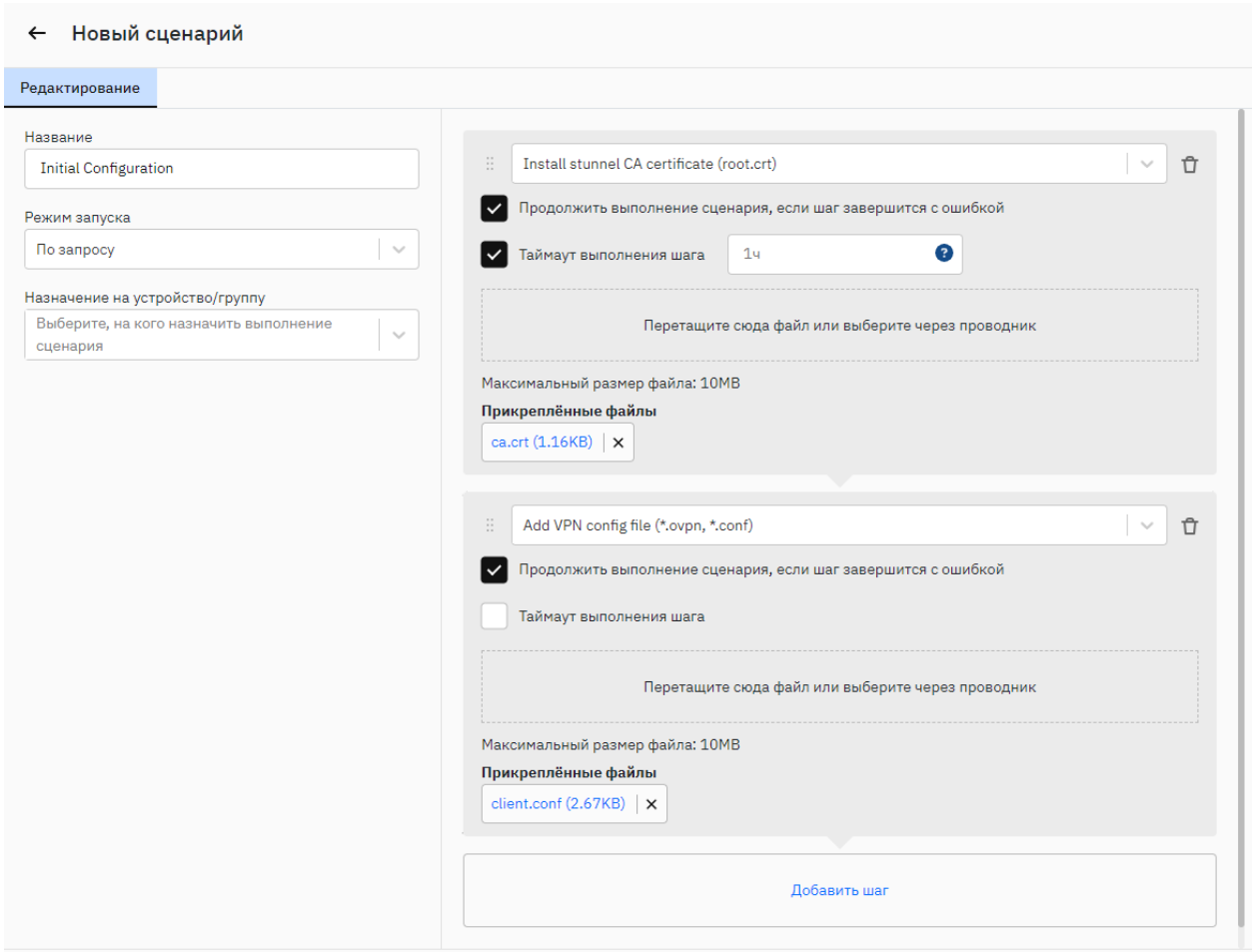


Рисунок 55 – Выбор последовательности команд

4. Введите название сценария, которое описывает спектр выполняемых команд.
5. Выберите режим запуска сценария (Рисунок *56*):

- по запросу: выберите устройства и группы, на которых необходимо выполнить сценарий;
- по событию: выберите доступные события из списка, по наступлению которых необходимо выполнить сценарий на устройствах;
- по расписанию:
    a. выберите периодичность выполнения;
    b. выберите дни недели или месяца, по каким необходимо выполнять сценарий;
    c. выберите время (часы:минуты), когда необходимо выполнять сценарий;
    d. выберите устройства и группы, на которых необходимо выполнять сценарий при наступлении заданной даты и времени;

e. укажите, учитывать ли часовой пояс устройства при расчете времени запуска сценария. При включении данной опции, задание выполняется на устройстве по местному времени.

Примечание. *Например, если СУ расположен во временной зоне Москвы (Europe/Moscow, UTC +3), то сценарий, назначенный на 00:00 в понедельник будет выполнен:*

- в 00:00 по Московскому времени на устройствах, находящихся в часовом поясе UTC+3
- в 16:00 в воскресенье по Московскому времени на устройствах, находящихся на Сахалине (UTC+11), что соответствует 00:00 понедельника на Сахалине.

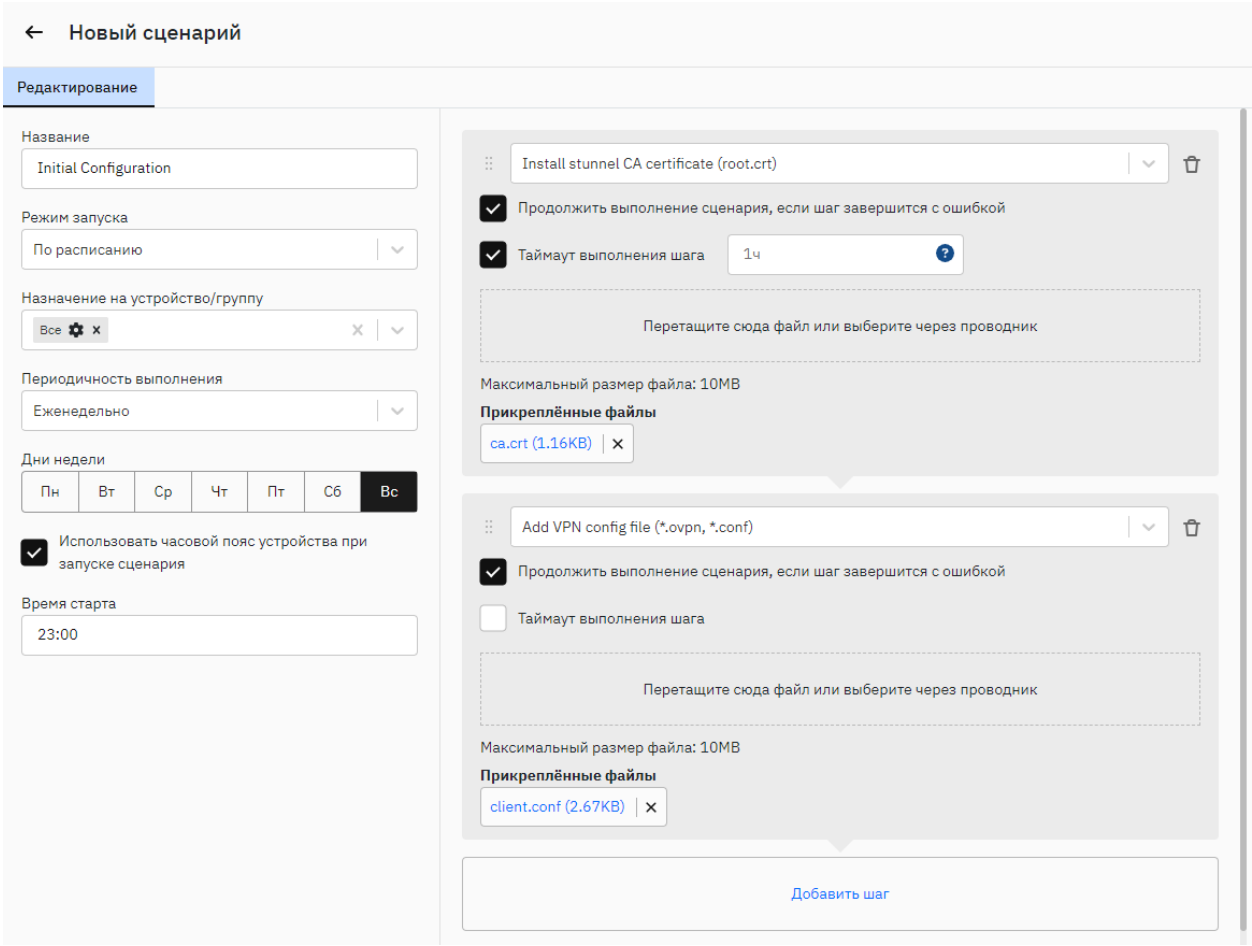


Рисунок 56 – Настройка нового сценария

6. Нажмите **Сохранить**.

5.12.2 Редактирование сценария

Чтобы отредактировать созданный ранее сценарий выполните действия, описанные ниже.

1. В веб-консоли выберите раздел **Сценарии**.

При необходимости отсортируйте список, нажав на заголовок столбца таблицы.

2. Выберите необходимый сценарий в списке.
3. На открывшейся странице редактирования сценария измените необходимые данные.
4. Нажмите кнопку **Сохранить**.

5.12.3 Удаление сценария

Чтобы удалить один или несколько сценариев:

1. В веб-консоли выберите раздел **Сценарии**.
2. Установите флажки в левом столбце таблицы на строках сценариев, требующих удаления.
3. Нажмите **Удалить**.

5.12.4 Запуск сценария

1. В веб-консоли выберите раздел **Сценарии.**
2. Выберите в списке сценарий с периодичностью выполнения *По запросу* или по расписанию (*Ежедневно*, *Еженедельно*, *Ежемесячно* и т.д.).
3. Проверьте содержимое сценария.
4. Нажмите кнопку **Сохранить и Запустить** (или **Запустить сейчас** для сценариев по расписанию).

5.12.5 Быстрые сценарии

Функционал быстрых сценариев является дополнением к уже имеющемуся функционалу сценариев.

Быстрые сценарии позволяют запускать созданные сценарии напрямую из карточки конкретного устройства, без необходимости переключения между разделами **Устройства** и **Сценарии**.

5.12.5.1 Создание быстрого сценария

Для создания быстрого сценария необходимо выполнить следующие действия:

1) веб-консоли GM-Factory выберите раздел **Сценарии**;
2) нажмите **Добавить**.

Далее будут рассмотрены имеющиеся способы создания быстрого сценария.

5.12.5.1.1 Создание быстрого сценария «с нуля»

После добавления сценария появится следующее окно (Рисунок *57*):

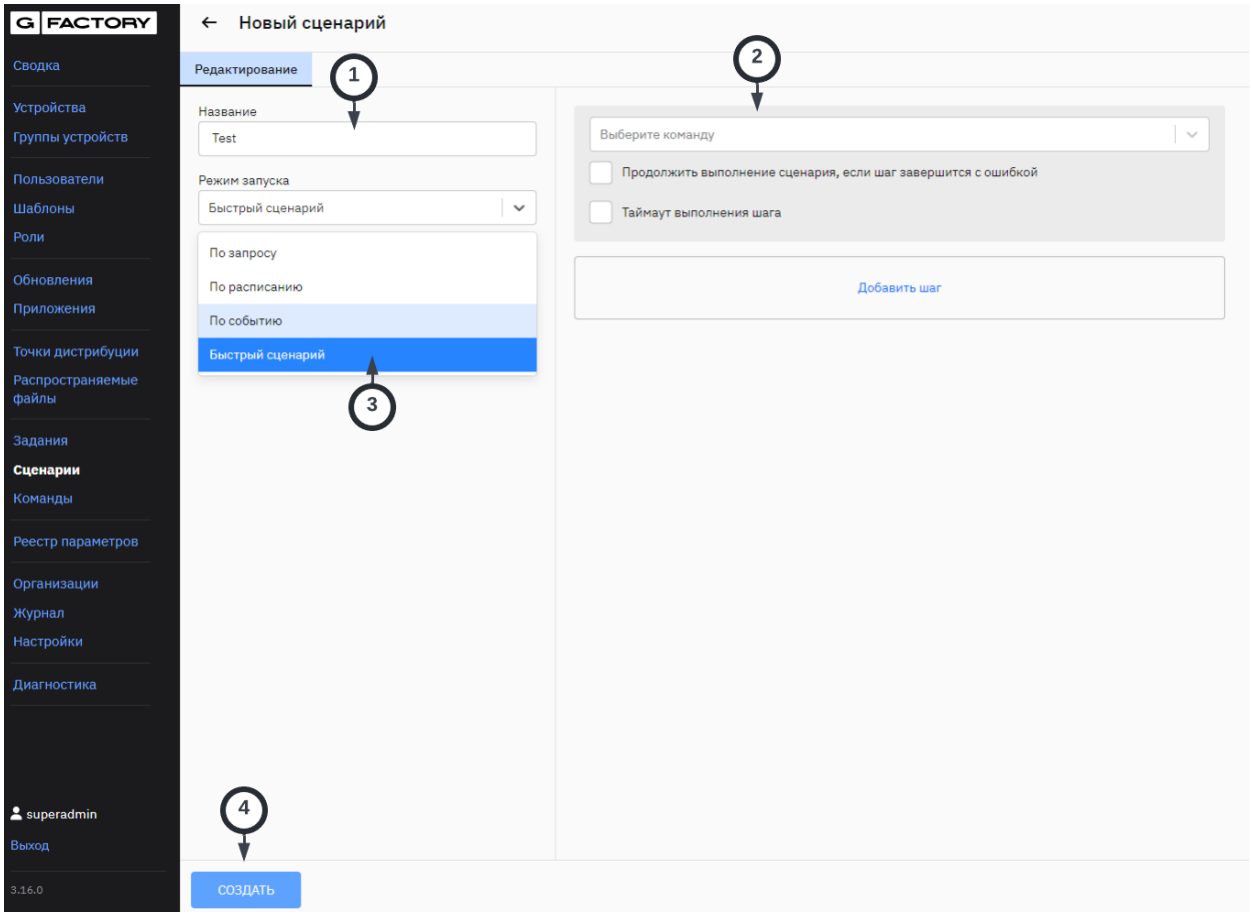


Рисунок 57 – Настройка быстрого сценария

После появления окна сценария необходимо выполнить следующие шаги, указанные на Рисунок *57* :

1) дать название сценарию, так как поле **Название** не может быть пустым при сохранении;
2) выбрать команды, которые будут выполняться в сценарии;
3) выбрать режим **Быстрый сценарий** выпадающего списка;
4) нажать **Создать**.

Внимание!!! *Сценарий добавляется в карточку устройства только в том случае, если режим его запуска выбран как "Быстрый сценарий".*

Если сценарий имеет режим запуска "Быстрый сценарий", то он будет добавлен в карточку ***КАЖДОГО УСТРОЙСТВА****, подключенного к СУ GM-Factory.*

5.12.5.1.2 Изменение режима запуска уже имеющегося сценария

В случае, если у администратора уже есть заранее подготовленные сценарии, ему достаточно будет изменить режим запуска этого сценария.

Это сделано для удобства, чтобы у администратора была возможность более гибко настраивать уже существующие сценарии.

Для изменения режима запуска сценария на **Быстрый сценарий** необходимо выполнить следующие шаги (Рисунок 58):

1) в веб-консоли GM-Factory выбрать раздел **Сценарии**;
2) выбрать интересующий сценарий среди списка существующих сценариев;
3) в появившемся окне сценарий необходимо изменить режим запуска сценария следующим образом:
    a. выбрать режим запуска **Быстрый сценарий**.
    b. сохранить изменения и выйти.

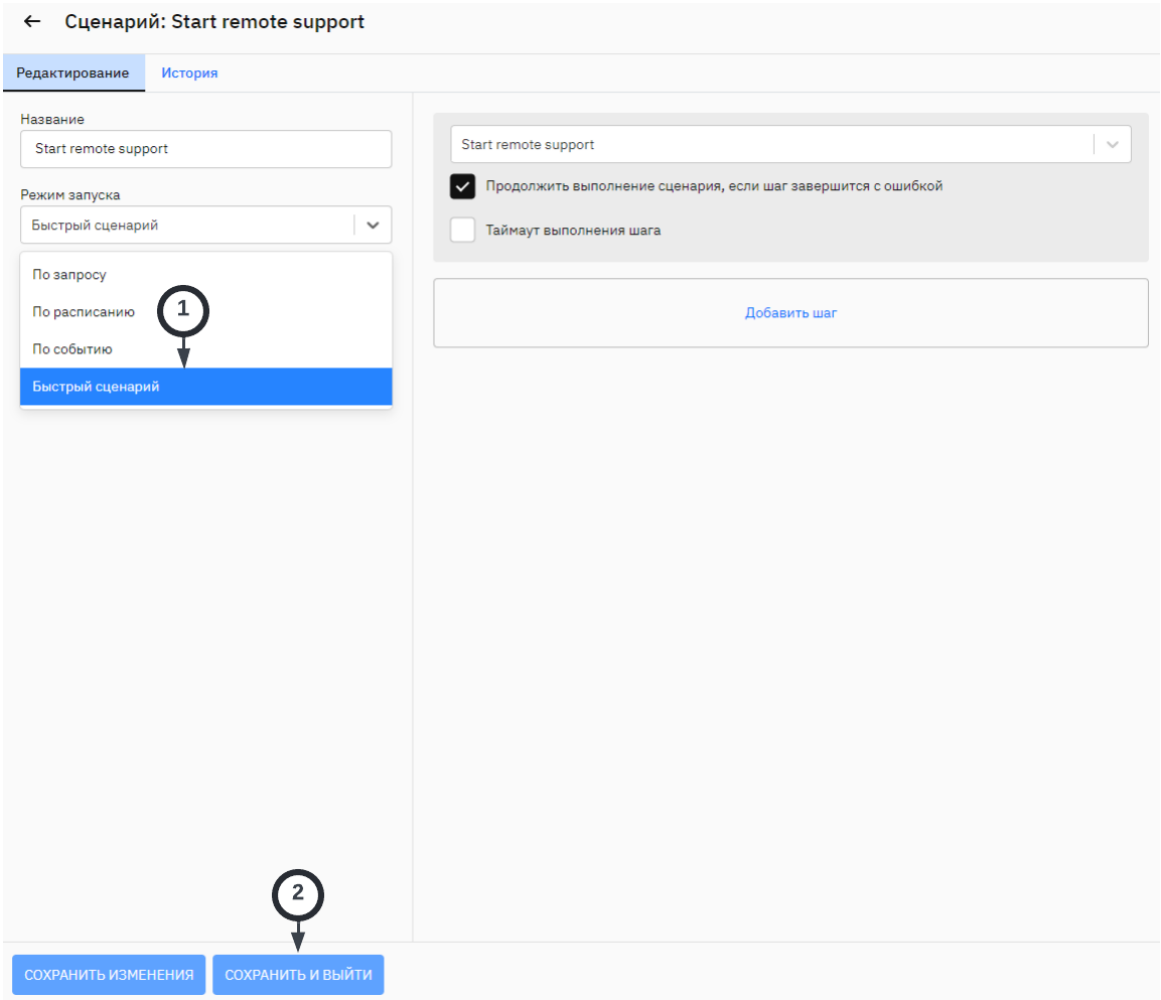


Рисунок 58 – Изменение режима запуска сценария

5.12.5.2 Запуск быстрого сценария

Для запуска быстрого сценария необходимо выполнить следующие шаги:

1) открыть карточку любого устройства (Рисунок *59*);
2) перейти на вкладку **Сценарии** (Рисунок *60*);
3) нажать на кнопку выпадающего списка **Запустить сценарий** (Рисунок 61);
4) выбрать нужный быстрый сценарий.

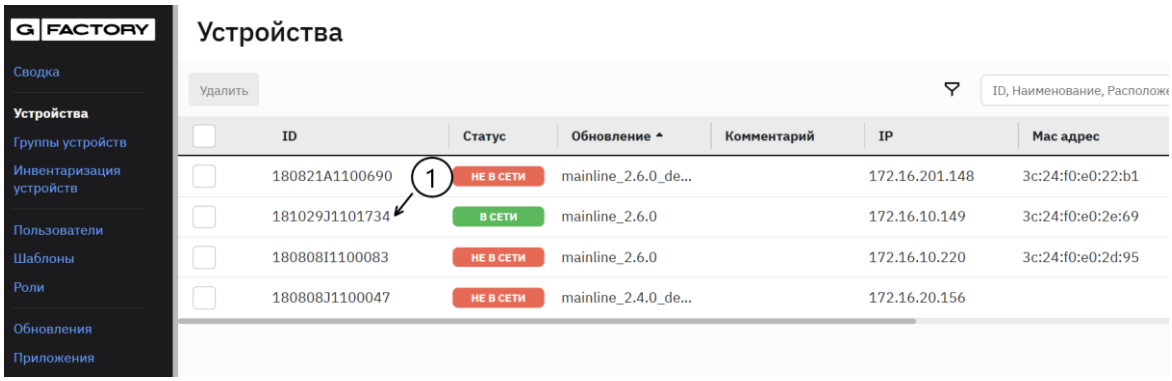


Рисунок 59 – Выбор карточки устройства

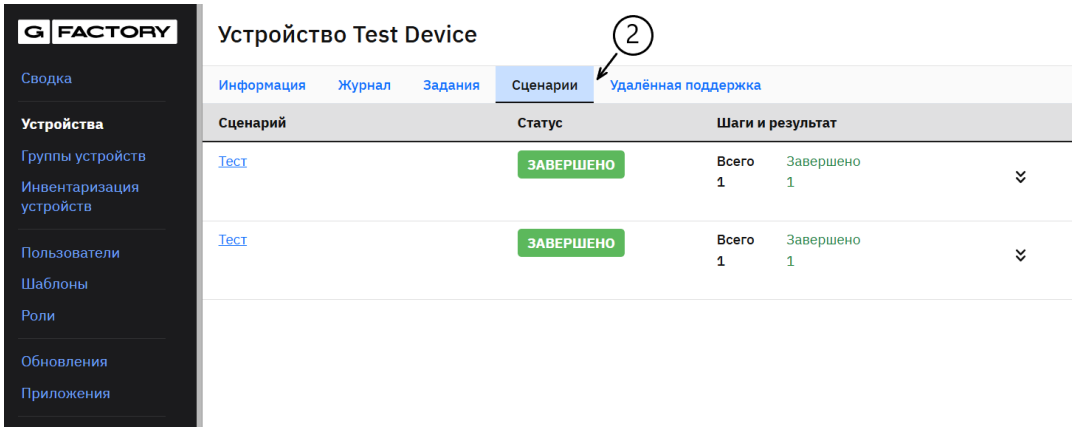


Рисунок 60 – Вкладка «Сценарии»

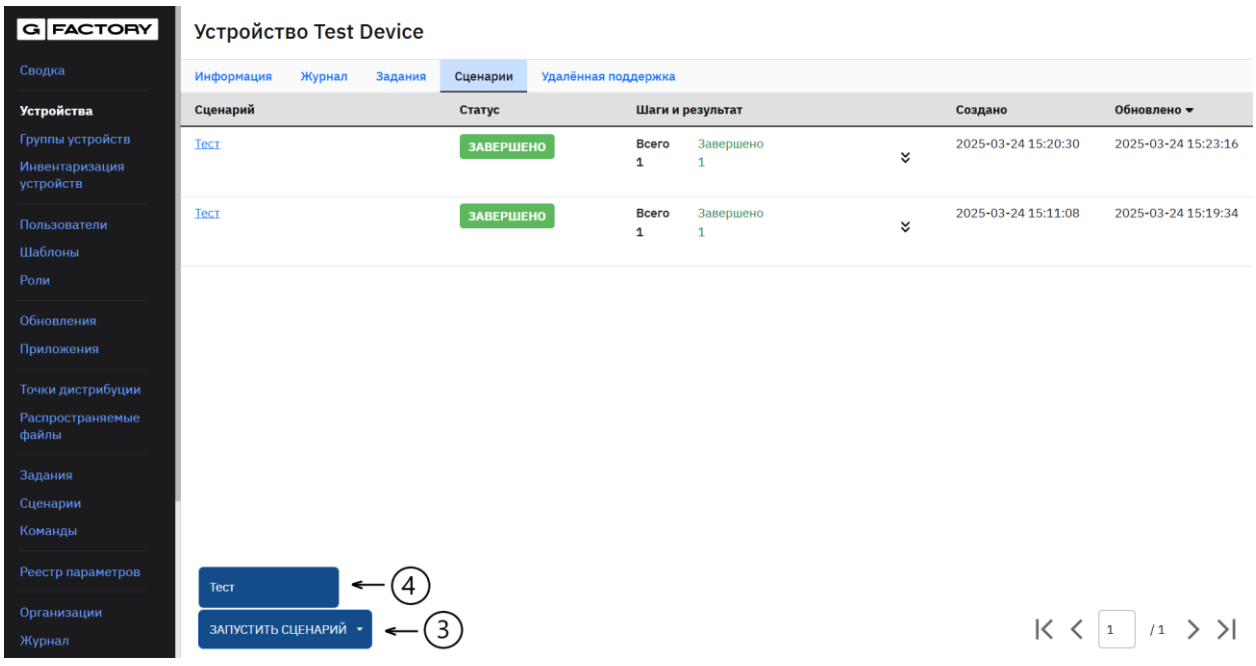


Рисунок 61 – Выбор сценария

5.12.6 Просмотр истории выполнения сценария

Для сценариев сохраняется история их выполнения на устройствах, включая статусы и результаты выполнения отдельных шагов.

Для просмотра истории выполнения отдельного сценария выполните следующие действия:

1. В веб-консоли выберите раздел **Сценарии.**
2. Выберите необходимый сценарий в списке.
3. Нажмите на вкладку **История.**

   Откроется история со статусами выполнения шагов по отдельным запускам сценария. По умолчанию сценарии отсортированы от последних завершенных запусков (Рисунок *62*).

   По отдельным запускам сценариев можно посмотреть детальную информацию о процессе и результатах выполнения отдельных шагов, нажав .

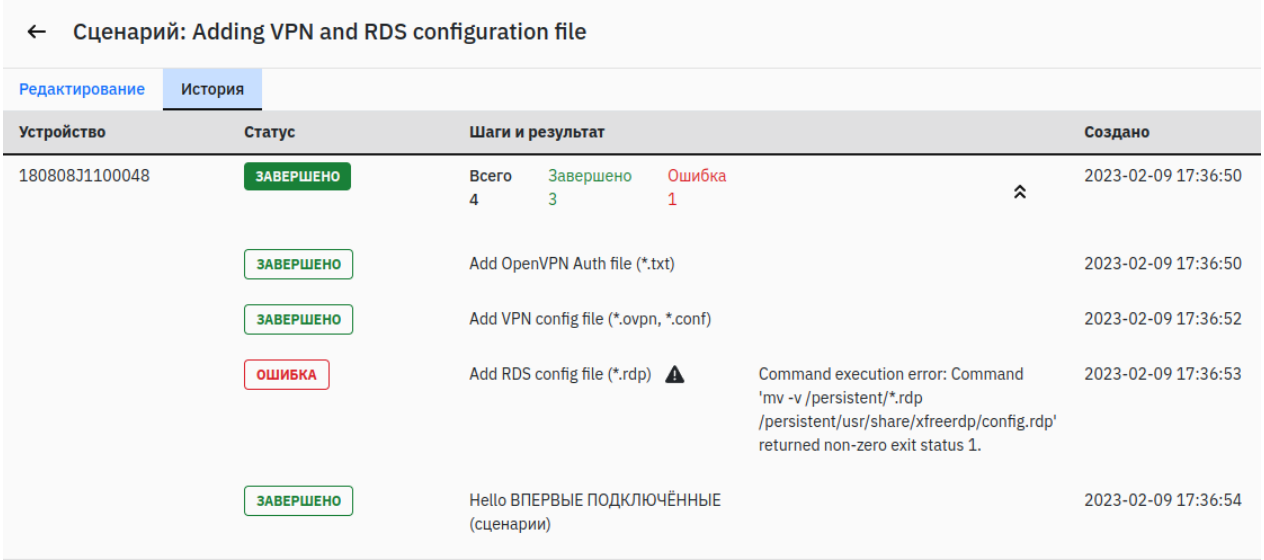


Рисунок 62 – Вид окна просмотра истории выполнения сценариев

Возможные статусы выполнения сценария:

1) INITIAL (ОЖИДАЕТ) – сценарий проходит процедуру запуска;
2) PROCESS (В РАБОТЕ) – сценарий в процессе выполнения;
3) FINISHED (ЗАВЕРШЕНО) – сценарий успешно завершен (Каждый шаг либо завершился успешно, либо был настроен как необязательный);
4) ERROR (ОШИБКА) – сценарий завершился с ошибкой (Сценарий был прерван в связи с ошибочным завершением выполнения обязательного шага). В поле **Команды и результат** на строке выполнения сценария отразится причина ошибки.

Возможные статусы выполнения отдельных шагов:

1) INITIAL (ОЖИДАЕТ) – шаг подготовлен к запуску и ожидает своей очереди;
2) PREPARED (ПОДГОТОВЛЕН) – шаг подготовлен, но не может быть отправлен на устройство, убедитесь, что устройство подключено к СУ;
3) SKIPPED (ПРОПУЩЕН) – шаг не будет выполнен в связи с ошибочным завершением предыдущего;
4) PROCESS (В РАБОТЕ) – команда принята к выполнению на устройстве;
5) FINISHED (ЗАВЕРШЕНО) – шаг сценария успешно выполнен;
6) ERROR (ОШИБКА) – выполнение команды завершилось неудачно. В поле **Команды и результат** на строке выполнения шага отразится причина ошибки.

5.13 Команды

Управление командами осуществляется пользователем, которому выданы соответствующие права (см. подраздел 5.7).

Все команды делятся на следующие типы:

1. SYSTEM – тип команды по умолчанию. Дополнительные поля в карточку задания не выводятся;
2. CONFIGURATION – команды, связанные с передачей файлов конфигурации. В карточку задания будет выводиться поле для загрузки конфигурационных файлов;
3. APPLICATION – команды, связанные с установкой приложений;
4. FIRMWARE – команды, связанные с обновлением базового встроенного ПО.

5.13.1 Набор команд по умолчанию

СУ поставляется с предустановленным набором команд. Перечень предустановленных на СУ команд приведен в Таблица 8.

Таблица 8 – Перечень предустановленных на СУ команд

Команда	Описание
Add monitor config (displays.json)	Загрузить конфигурационный файл с настройками мониторов: разрешение экрана, выбор основного монитора

Команда	Описание
Add OpenVPN Auth file (*.txt)	Добавить на устройство конфигурационный файл с настройками для подключения по OpenVPN с авторизацией по имени пользователя и паролю. Вид файла: **login** **password**
Add RDS config file (*.rdp)	Добавить на устройство конфигурационный файл config-onestring.rdp, который запускает сессию с минимальным набором настроек
Add VMware camera config (config.yml)	Добавить на устройство конфигурационный файл, который в режиме VMware включает камеру
Add VPN Config file (*.ovpn, *.conf)	Добавить на устройство конфигурационный файл с настройками VPN-подключения. ***Внимание!*** *Конфигурационный файл не должен содержать пробелов в имени файла.*
BLE Certification (certificate.cer, certificate-key.pem)	Установить на устройстве сертификат, позволяющий использовать безопасное Bluetooth-соединение для аутентификации пользователя с помощью смартфона.
Change Greeter background image (background.png)	Установить изображение в качестве заставки на экране приветствия. ***Внимание!*** *Название и формат файла изображения – **background.png**.* *Размер файла не должен превышать 10 Мб.*
Change small screen background image (small_background.png)	Установить изображение в качестве заставки на дисплее GM-Box ***Внимание!*** *Название и формат файла изображения – **small_background.png**.* *Размер файла не должен превышать 10 Мб.*
Debug mode OFF	Отключить получение дополнительных логов
Debug mode ON	Включить получение дополнительных логов с GM-Box
Device Force Update	Принудительно обновить устройство, даже если на устройстве установлено ПО более поздней версии

Команда	Описание
Device Update & Reboot	Выполнить обновление прошивки устройства и сразу перезапустить его.
Device Reboot	Перезапустить устройство.
Device Shutdown	Выключить устройство.
Device Update	Выполнить обновление прошивки устройства.
Device Wipe	Выполнить обновление прошивки устройства до первоначальных настроек
Device Wipe & Reboot	Выполнить обновление прошивки устройства до первоначальных настроек и сразу перезапустить его
Force LDAP SSL	Использовать защищенный канал связи от устройства до LDAP-каталога
Force LDAP SSL OFF	Отключить использование защищенного канала связи от устройства до LDAP-каталога
Force SSL	Использовать защищенный канал связи с СУ на устройстве, если на СУ установлен действующий (валидный) сертификат
Force SSL OFF	Отключить использование защищенного канала связи на устройстве.
Force VMware use external camera	Использовать внешнюю USB-камеру в VDI VMware
Force VMware use internal camera	Использовать в VDI VMware камеру, встроенную в GM-Box
Install Application	Установить приложение
Install Application & Reboot	Установить приложение и перезагрузить GM-Box
Install stunnel CA certificate (root.crt)	Установить на устройстве сертификат УЦ, позволяющий использовать клиент stunnel. ***Внимание!*** *Название файла сертификата должно быть* ***root.crt***

Команда	Описание
Patch config CA (*.crt)	Загрузить сертификат. Файл должен быть в формате PEM и закодирован в Base64, с расширением .CRT. Имя файла должно состоять из цифр и латинских букв и не должно содержать пробелов. ***Внимание!*** *После выполнения команды перезагрузите GM-Box с помощью команды **Device reboot** или после выхода из сессии нажмите на мониторе кнопку  и выберите в меню **Перезагрузить**.* *При использовании VDI VMware или Citrix обязательно загрузить root CA (центр сертификации).* *Данная команда применяется только для GM-Box с версией GM OS ниже 2.0.0.*

Команда	Описание
Patch config CA 2 (*.crt)	Загрузить сертификат. Файл должен быть в формате PEM и закодирован в Base64, с расширением .CRT. Имя файла должно состоять из цифр и латинских букв и не должно содержать пробелов. ***Внимание!*** *Данная команда должна быть создана администратором для серверов версий 3.7.1 и ниже:* *Наименование: Patch config CA 2 (*.crt)* *Тип: CONFIGURATION* *Данные:* *((patch-config <filename>)(cmd "cp -v /persistent/*.crt /usr/local/share/ca-certificates/")(cmd "c_rehash /usr/local/share/ca-certificates/")(cmd "update-ca-certificates")(cmd "mkdir -p /persistent/certs")(cmd "mv /persistent/*.crt /persistent/certs")(cmd "/gm-bin/install_chromium_certificates.sh"))* *После выполнения команды перезагрузите GM-Box с помощью команды **Device reboot** или после выхода из сессии нажмите на мониторе кнопку*  *и выберите в меню **Перезагрузить**.* *При использовании VDI VMware или Citrix обязательно загрузить root CA (центр сертификации).*
Patch config Citrix	Загрузить конфигурационные файлы при использовании VDI Citrix.
Patch config Greeter (greter.conf)	Загрузить конфигурационный файл *greeter.conf*. Файл содержит конфигурации загружаемых плагинов, которые обеспечивают процедуры идентификации и аутентификации пользователя, настройку сетевых интерфейсов.
Patch config TLS (additional.ini)	Конфигурационный файл для установки уровня проверки сертификатов.
Patch config VMWare	Загрузить конфигурационные файлы при использовании VDI VMware

Команда	Описание
Remove Installed Applications	Удалить установленные приложения
Remove Installed Applications & Reboot	Удалить установленные приложения и перезагрузить GM-Box
Usbguard default allow	Разрешить подключение USB-устройств к GM-Box
Usbguard default block	Запретить подключение USB-устройств к GM-Box
Upload upload rules (rules.conf)	Загрузить файл с правилами, разрешающими/ запрещающими подключение USB-устройств к GM-Box
User's kickoff	Завершить сессию пользователя.
Zero deploy	Задать первоначальные настройки для вновь подключенных устройств или применить на устройствах новые инфраструктурные изменения.

5.13.2 Добавление команды

Для добавления новой команды выполните следующие действия:

1. В консоли выберите раздел **Команды**.
2. Нажмите кнопку **Добавить**. В правой части откроется карточка новой команды. Заполните поля:

   a) Наименование команды;
   b) Тип команды выберите из выпадающего списка;
   c) Данные – указываются команды на встроенном скриптовом языке.

3. Установите флажки напротив тех ролей, которым разрешено создавать задания на выполнение этой команды.
4. Нажмите **Создать**.

5.13.3 Редактирование карточки команды

Для редактирования карточки нажмите левой кнопкой мыши на наименовании команды в списке.

Внесите необходимые изменения и нажмите **Сохранить изменения**.

5.13.4 Удаление команды

Для удаления команды установите флажок в левой части списка и нажмите **Удалить**.

5.14 Организации

Настройка первичного Discovery адреса для СУ осуществляется в веб-консоли в разделе **Организация**. Настройка является обязательной, без первичного Discovery адреса устройство не сможет найти СУ.

Для настройки в веб-консоли выберите раздел **Организации**. В поле **Первичный discovery адрес** задайте корректный Discovery адрес (IP или FQDN) СУ (поддерживаются также кириллические домены и адреса, заданные с помощью протоколов IPv4 и IPv46).

Например, ***getmobit***.example.org
Где *getmobit.examlple.org* - DNS имя СУ.

Примечание. *DHCP-сервер должен транслировать зону* ***example.org***.

Внимание! *При отсутствии DNS-записи и настройки DHCP-сервера (включая DHCP option 119 - 'Domain Search List') устройство GM-Box не сможет обнаружить и подключиться к СУ автоматически.*

5.15 Журнал

События, произошедшие на GM-Box или на СУ, отображаются в разделе **Журнал.**

На вкладке **GM-Box** (Рисунок *63*) отображаются сообщения, полученные с устройств, при выполнении аутентификации, выходе из сессии, изменении настроек, перезагрузке устройства и т.д.

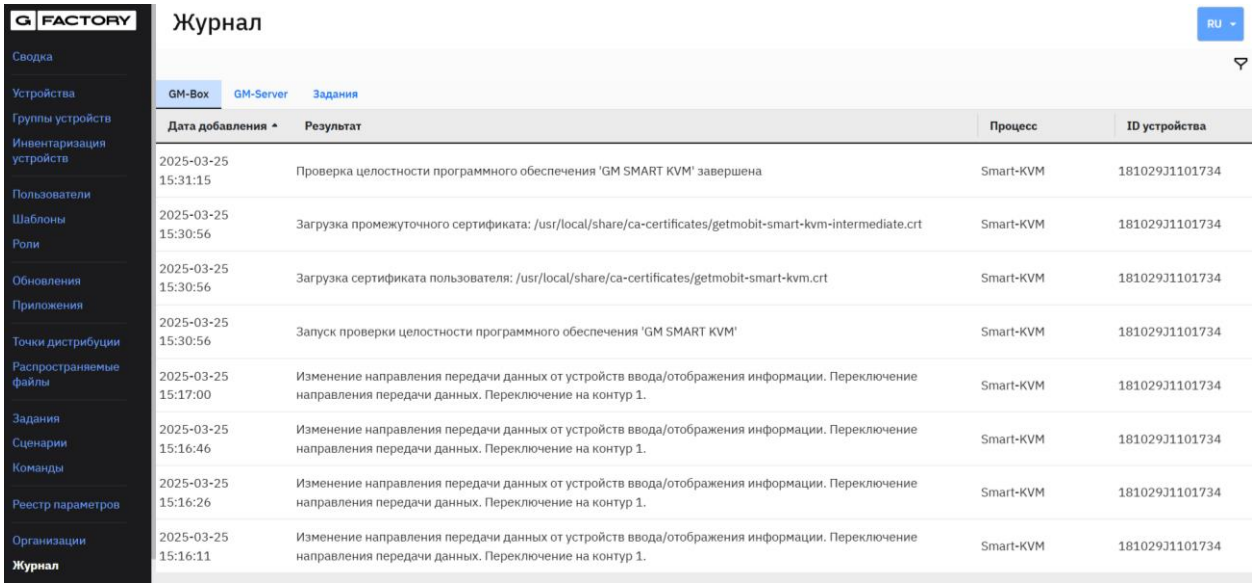


Рисунок 63 – Вкладка GM-Box

На вкладке **GM-Server** (Рисунок 64) отображаются сообщения о действиях, выполненных на СУ:

- аутентификация в веб-консоли СУ;
- операции с пользователями, устройствами или организациями;
- создание, редактирование или удаление команд, заданий и сценариев;
- изменение настроек, например, включение/отключение синхронизации с корпоративной службой каталогов.

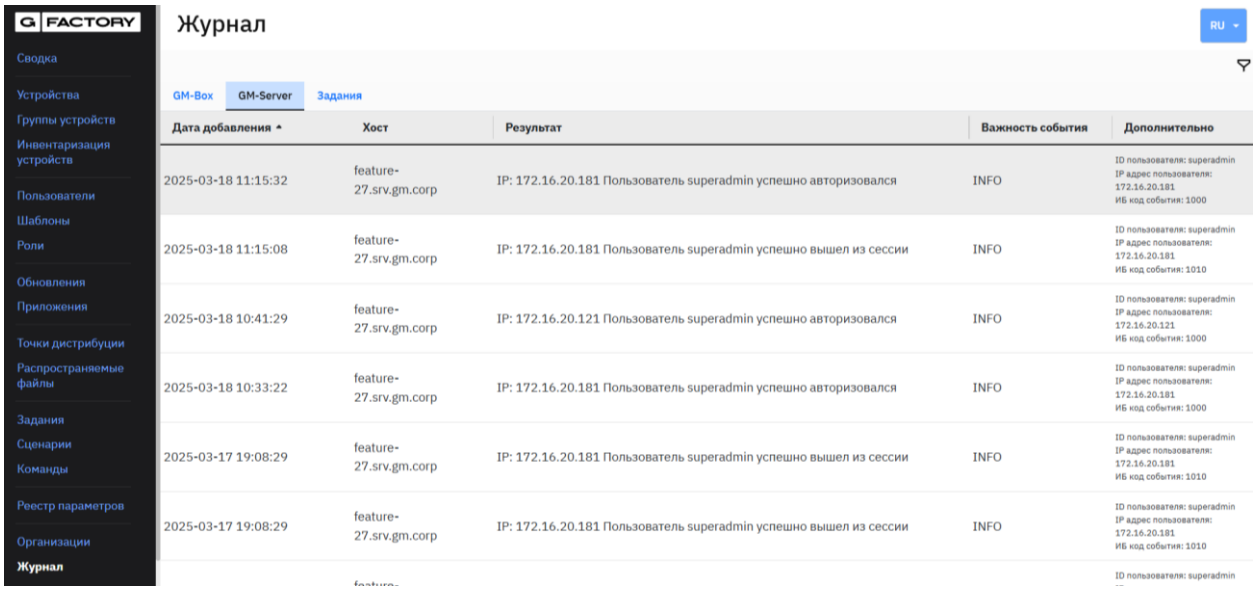


Рисунок 64 – Вкладка GM-Server

Результат выполнения заданий на GM-Box отображается на вкладке **Задания** (Рисунок *65*).

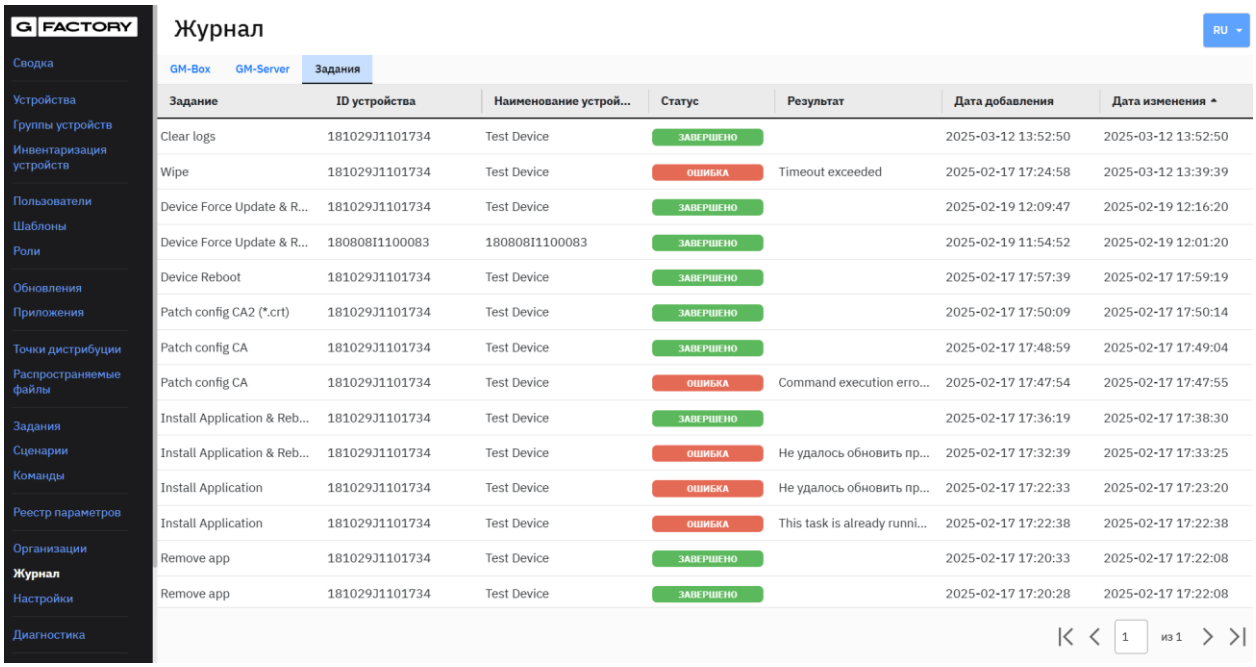


Рисунок 65 – Вкладка Задания

5.16 Настройки

5.16.1 Добавление и обновление лицензионного файла

Для использования СУ необходимо активировать лицензию. Лицензия определяет набор разрешенных к использованию функций, допустимое количество GM-Box, подключаемых к СУ и список доступных приложений.

Лицензионный файл состоит из нескольких типов лицензий:

- **Устройства** – данный тип лицензии определяет отдельно права на количество подключений устройств GETMOBIT и сторонних устройств.
- **Приложения** – данный тип лицензии определяет права на использование режимов / SD App-приложений у пользователя на конечных устройствах.

Лицензионный файл доступен из личного кабинета по адресу: **http://cp.getmobit.ru** (логин и пароль для доступа в личный кабинет запросите в отделе технической поддержки ООО «ГЕТМОБИТ») или по запросу у дистрибутора.

Для загрузки лицензионного файла в веб-консоли выберите раздел **Настройки,** перейдите на вкладку **Лицензия** и загрузите лицензионный файл.

Примечание. *Если в лицензионном файле будет отсутствовать тип лицензии Приложение для необходимого режима, то использовать данный режим будет невозможно*

5.16.2 Настройка синхронизации с корпоративной службой каталогов/LDAP

Настройка синхронизации данных с корпоративной службой каталогов необходима для того, чтобы пользователи могли выполнять аутентификацию на GM-Box с использованием доменных учетных записей и автоматически назначать настройки VDI, SIP-телефонии и др.

Синхронизация данных выполняется в одностороннем порядке (технологической учетной записи должны быть предоставлены права доступа на чтение каталога AD/LDAP). В момент синхронизации СУ подключается к корпоративной службе каталогов и получает перечень новых, измененных и удаленных объектов. Все изменения СУ вносит в свою внутреннюю базу данных (локальная служба каталогов). В корпоративной службе каталогов со стороны СУ никакие изменения не вносятся.

Внимание!
*Пароль пользователя не синхронизируется, используется механизм **SASL** для делегирования аутентификации пользователя в корпоративной службе каталогов*

1. В полях **AD/LDAP Сервер** (host без ldap:// и т.п.), **AD/LDAP Порт**, **Логин**, **Пароль** укажите необходимые значения, приведенные в Таблица 9.

Таблица 9 – Перечень значений полей настройки синхронизации с корпоративной службой каталогов

Поле	Описание
AD/LDAP Сервер	FQDN или IP-адрес сервера корпоративной службы каталогов
AD/LDAP Порт	Номер порта сервера корпоративной службы каталогов для TCP/UDP соединений. **Значение по умолчанию:** *порт 389*.

Поле	Описание
Логин	Логин пользователя в корпоративной службе каталогов для связи со службой каталогов. Режим ReadOnly. Рекомендуется создать в корпоративной службе каталогов отдельную учетную запись для СУ.
Пароль	Пароль пользователя в корпоративной службе каталогов для связи со службой каталогов

2. Для проверки соединения с корпоративной службой каталогов AD/LDAP нажмите **Проверить**.

Если ваши данные не позволяют подключиться к AD/LDAP, отобразится ошибка (Рисунок *66*).

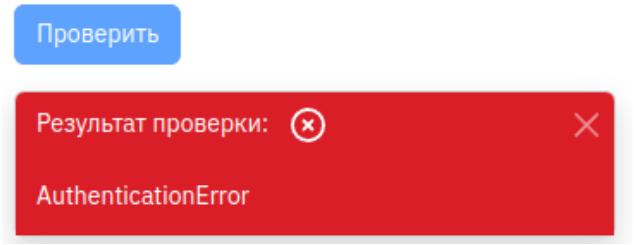


Рисунок 66 – Результат проверки с ошибкой

При возникновении ошибки, убедитесь в корректности введеных значений, выполнении требований к инфраструктуре.

Если проверка завершена успешно (Рисунок *67*), переходите к следующим полям настройки синхронизации.

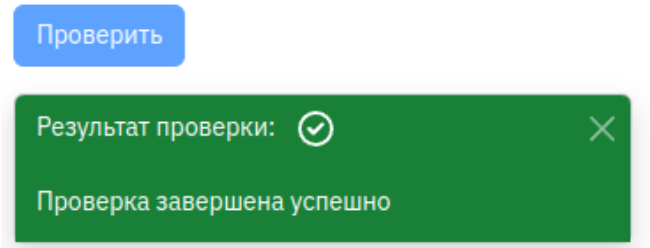


Рисунок 67 – Результат успешной проверки

***Примечание**. Чтобы задать корректные фильтры для синхронизации данных из AD, обратитесь к системному администратору своей компании.*

3. В поле **Корневой элемент (Base DN)** укажите корневую папку со всеми вложенными контейнерами и организационными подразделениями (Organization Units), в которой СУ осуществляет поиск объектов. Формат: distinguished name (DN).

Для корневого контейнера домена корпоративной службы каталогов company.local:

```
dc=company,dc=local
```

Например, для фильтра внутри домена *getmobit.ru* укажите

```
dc=getmobit,dc=ru
```

4. В поле **Интервал синхронизации (минут)** задайте интервал времени между циклами автоматической синхронизации. Сразу после сохранения настроек запустится синхронизация.

Каждый интервал происходит синхронизация тех пользователей, которые были изменены после последней синхронизации.

Примечание**. Для уменьшения сетевого трафика после первой синхронизации рекомендуется установить значение не меньше **30 минут

5. В поле Фильтр для получения списка пользователей с ролью: <роль> по умолчанию укажите:

***Примечание**. Количество полей зависит от количества ролей, настроенных на СУ*

```
(&(objectClass=person)(!(objectClass=computer)))
```

Возможные значения:

Фильтры по конкретным пользователям:

```
(&(objectClass=person)(!(objectClass=computer))(|(sAMAccountName=Petrov.Peter)(sAMAccountName=Ivanov.Ivan)))
```

Фильтры по группе пользователей, которые будут использовать GM-Box:

```
(&(objectClass=person)(!(objectClass=computer))(memberOf=CN=getmobit-users,OU=getmobit,DC=local))
```

Фильтры всех сотрудников филиала branch.local:

```
(&(objectClass=person)(!(objectClass=computer))(memberOf=all_worker,CN=Users,DC=branch,DC=local))
```

Например, для получения списка всех активных пользователей используйте фильтр:

```
(&(objectCategory=person)(objectClass=user)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))
```

***Примечание**. Список доступных фильтров определяется ролью авторизованного пользователя (см. Роли). Все фильтры для получения списков пользователей по ролям пишутся на основе стандартного синтаксиса LDAP фильтров.*

Внимание!
Для проверки созданных фильтров рекомендуется использовать приложение ApacheDirectoryStudio или аналогичное.
Создаваемые фильтры не должны пересекаться. Если пользователь входит в несколько групп, возникнут ошибки при синхронизации.
После изменения фильтра настройки, заданные вручную в профиле пользователя, удалятся при следующей синхронизации.

Поле **Атрибуты** содержит список полей, которые механизм синхронизации читает из профиля пользователя в службе каталогов.

6. Нажмите кнопку Шаблоны значений и укажите через запятую из шаблона MS AD следующие обязательные значения:

```
cn,sn,objectClass,sAMAccountName,objectGUID,userPrincipalName,objectSid
```

где:

sAMAccountName –	логин пользователя в AD/LDAP
userPrincipalName –	пароль пользователя в AD/LDAP
cn –	общее имя
sn –	фамилия
objectClass –	группировка связанных объектов, например, *user*
objectGUID –	идентификатор объекта
objectSid –	уникальный идентификатор пользователя AD, на основе которого при синхронизации генерируется значение uidNumber. Необходим для корректной работы авторизации пользователей в системе

Для синхронизации фото на аватаре добавьте *thumbnailPhoto*.

7. В поле **Соответствие полей** через запятую укажите список названий полей профиля пользователя СУ и корпоративной службы каталогов для одинаковых параметров. Список доступных ключей представлен в таблице ниже.

8. Нажмите кнопку Шаблоны значений и укажите из шаблона MS AD обязательные значения в формате *ключ=значение*. Где *ключ* – запись в БД СУ, а *значение* – атрибуты, считанные из службы каталогов. Все поля, указанные в качестве значений, должны быть в списке **Атрибутов**, в противном случае возможны ошибки синхронизации.

Обязательные значения:

```
configuration.ad.member_of=memberOf,password=userPrincipalName,title=cn,username=sAMAccountName
```

Для синхронизации фото на аватаре добавьте *thumbnailPhoto*.

9. Нажмите кнопку **Сохранить изменения**.
   После нажатия кнопки запускается сессия синхронизации. Во время этого в AD выполняется поиск записей пользователей, удовлетворяющих условиям ролевых фильтров, эти записи также должны удовлетворять условиям, заданным в корневом элементе. У пользователей учетные записи которых удовлетворяют условиям фильтров, извлекаются атрибуты из службы каталогов и на их основе формируется профиль пользователя. Этот профиль отображается в разделе **Пользователи**.

   Статус синхронизации может иметь следующие значения:

   1) синхронизация запущена, статус обозначает, что предыдущая синхронизация с AD/LDAP завершилась успешно;
   2) синхронизация выполняется;
   3) неизвестное. Статус выполнения синхронизации в настоящий момент неизвестен;
   4) синхронизация не запущена. Статус обозначает, что синхронизация не настроена, либо перестали работать сохраненные настройки.

10. В поле **Значения по умолчанию** можно указать дополнительные атрибуты в формате *ключ=значение,* где:

    1) *ключ* – название поля учетной записи пользователя,
    2) *значение* – подставляемое значение, допускается использование названий полей СУ, заключенных в фигурные скобки. Эти атрибуты будут автоматически установлены для всех пользователей при синхронизации из корпоративной службы каталогов. Список доступных ключей представлен в Таблица 10. Каждая пара указывается с новой строки.

Внимание! *Типовые значения, а также значения для профилей пользователей используемые по умолчанию, рекомендуется задавать через Шаблоны. Поле «Значения по умолчанию» будет исключено в следующих версиях СУ.*

Пароли, указываемые в поле «Значения по умолчанию», не маскируются. Для соответствующих значений используйте функционал Шаблонов.

Настройки, отличающиеся у пользователей, необходимо задавать в ***Дополнительное поле*** *у каждого пользователя.*

Для применения настроек нажмите **Сохранить изменения**

5.16.2.1 Доступные ключи

Таблица 10 – Перечень ключей, используемых в полях **Соответствие полей** и **Значения по умолчанию**

Ключ	Описание	Примеры значений
username	Имя пользователя в системе (логин)	ipetrov
title	ФИО пользователя	Petrov
password	Пароль пользователя	*******
avatar	Изображение пользователя	Фото пользователя в формате .jpg или .png размером до 10MB
roles	Роль пользователя	USER
archived	Флаг заблокированного пользователя	

Ключ	Описание	Примеры значений
configuration.gm_mode	Режим работы пользователя	Терминал
configuration.token_id	ID USB-токена	
configuration.nfc_id	ID бесконтактной NFC карты	
configuration.rfid_id	ID бесконтактной карты 125кГц	
configuration.web_url	URL для режимов работы пользователя, связанных с браузером	
configuration.sip.hostname	SIP имя хоста	172.16.4.172
configuration.sip.username	SIP логин пользователя	2055
configuration.sip.userid	SIP ID пользователя	
configuration.sip.password	SIP пароль	
configuration.sip.phone	Дополнительные параметры SIP-клиента	
configuration.sip.voicemail	Номер голосовой почты SIP	
configuration.sip.vlanid	VLAN ID для приложения VOIP	
configuration.ad.username	AD/LDAP имя пользователя	Helen
configuration.ad.password	AD/LDAP пароль	********

Ключ	Описание	Примеры значений
configuration.ad.server	AD/LDAP сервер	
configuration.ad.port	Порт для подключения к серверу AD/LDAP	389
configuration.ad.base	Корневой элемент для поиска по каталогу AD/LDAP	
configuration.ad.telephone	Название поля в AD/LDAP, в котором хранится телефонный номер сотрудника	
configuration.ad.filter	Фильтр поиска объектов для добавления в телефонную книгу	
configuration.ad.member_of	Атрибут принадлежности пользователя к организационным группам AD/LDAP	
configuration.extra	Поле дополнительных настроек (см. пп. 5.16.2.2, 5.16.2.3)	
configuration.vdi.domain	Домен VDI	horizon.vdi.getmobit.ru
configuration.vdi.password	VDI пароль	**********
configuration.vdi.session	Пул/машина/десктоп	Windows-10
configuration.vdi.host	Адрес VDI или терминального сервера	10.78.192.250
configuration.vdi.user	Имя пользователя VDI	Uesss1

Ключ	Описание	Примеры значений
configuration.vdi.param1	Дополнительно, используется для интеграции с различными VDI решениями	**h264** - для использования кодека H.264 для RDP **gfx** – для использования кодека JPEG для RDP
configuration.vdi.param2	Дополнительные параметры для VDI клиента	/dvc:urbdrc,dev:058f:5608

5.16.2.2 Использование регулярных выражений

В поле **Значения по умолчанию** можно задать значения с помощью регулярных выражений. Рекомендуем пользоваться этим способом в исключительных ситуациях, вместо значений по умолчанию использовать **Шаблоны** (см. раздел 5.6).

В регулярных выражениях используются следующие методы:

1) **Sub** – выполняет поиск шаблона в строке и заменяет его на указанную подстроку. Если шаблон не найден, строка остается неизменной;
2) **Findall** - возвращает список всех найденных совпадений. У метода нет ограничений на поиск в начале или конце строки.

Синтаксис регулярных выражений:

```
{ключ значения из корпоративной службы каталогов|sub(r'-', '')}
```

После вертикальной черты для метода:

1) **sub(r'-', '')**
   первый аргумент - регулярное выражение,
   второй – подстрока, на которую нужно заменить (подробнее см. https://docs.python.org/3/library/re.html#re.sub)
2) **{cn|findall(r'\w+', 0)}**
   первый аргумент - регулярное выражение,
   второй - индекс вхождения. Если вхождение не обнаружено, значение останется без изменений.

Например:

1. Удалить тире из телефонного номера TelephoneNumber=251-23-54

   ```
   configuration.sip.phone={TelephoneNumber|sub(r'-', '')}
   ```

   Результат 2512354
2. Объединить телефонный номер и фамилию для полей TelephoneNumber=251-23-54, cn=Ivan Ivanov

   ```
   configuration.sip.username={TelephoneNumber|sub(r'-', '')} - {cn|findall(r'\w+', 1)}
   ```

   Результат: 2512354 - (Ivanov)
3. Удалить из поля с телефонным номером буквы и спецсимволы: TelephoneNumber=+7-666-666.66.66-мой-тел-$#@-

   ```
   configuration.sip.username={telephoneNumber|sub(r'[^\d]+', '')}
   ```

   Результат: 76666666666

5.16.2.3 Настройка и использование поля configuration.extra

Таблица 11 – Перечень ключей для настройки поля configuration.extra

Ключ	Описание	Значение
AUTOMOUNT	Монтирование USB-носителей в RDP сессии.	true/false
SIP_FAVORITES	Избранные контакты VoIP	"347812,347813,347815"
SIP_LABEL	"Отображаемое имя после регистрации VoIP"	
SIP_HOSTS	Адреса SIP-серверов	IP1,FQDN2
DISABLE_SIDEBAR	Отключение sidebar	false/true
SIP_REGISTER_EXPIRES	Интервал перерегистрации на SIP-сервере. Время в секундах	целое число
VOIP_DIAL_INTERVAL	Время начало автонабора в миллисекундах	целое число
VOIP_MASTER_CONFIG	Настройки VoIP: звук/камера/громкость, общая для всех пользователей или индивидуальная	true/false
ENABLE_NFC	Включение модуля NFC в сессии пользователя	true/false
SIP_NUMBER_EXCLUDE_REGEXP	Удаление нежелательных символов из телефонных номеров, синхронизированных из AD/LDAP	"[()-]"
KRB_DEFAULT_DOMAIN	Используется для получения Kerberos тикета от имени вошедшего пользователя в сессию GM-Box	"Имя домена"
KRB_KDC	Используется при доменной авторизации в Citrix	”<IP_address/DNS_name сервера со службой Kerberos KDC>”

5.16.2.4 Рассинхронизация пользователей

Так как фильтры для получения списков пользователей применяются на каждом цикле синхронизации, возможна ситуация, при которой ранее синхронизированные пользователи более не попадают под текущие фильтры.

Это может произойти по ряду причин, включая: удаление пользователя из AD, изменения данных пользователя и его групповой принадлежности, а также изменение состава фильтров администратором.

В таком случае все пользователи, не удовлетворяющие текущим фильтрам синхронизации, будут отмечены как «несинхронизированные», о чем свидетельствует иконка  на списке пользователей.

Внимание! *«Несинхронизированные» пользователи не будут удалены автоматически из списка пользователей в разделе* ***Пользователи****.*

Так как аутентификация доменных пользователей осуществляется службой каталогов, то при удалении пользователя из службы каталогов, такие пользователи больше не смогут войти в сессию на GM-Box, несмотря на отображение в СУ как «несинхронизированные».

Администратор, имеющий права на настройку синхронизации, может произвести массовое удаление профилей «несинхронизированных пользователей», нажав кнопку **Очистить несинхронизированных пользователей** (Рисунок *68*) в разделе **Настройки -> Синхронизация с AD/LDAP -> Блок Административные действия.**

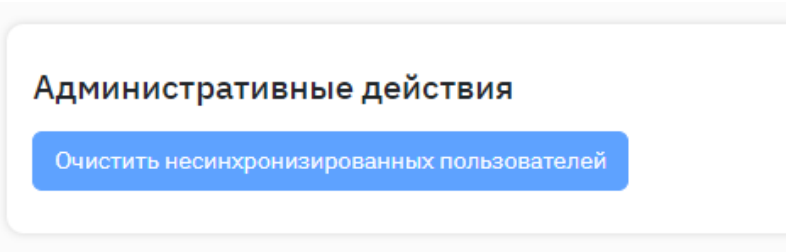


Рисунок 68 – Удаление профилей «несинхронизированных пользователей»

5.16.3 Проверка корректности фильтров LDAP

Для корректной синхронизации сервера управления со службой каталогов (см. п. 4.5.6) необходимо корректно настроить фильтры получения пользователей.

При составлении фильтров используется стандартный синтаксис LDAP запросов:

1) в качестве логического оператора **И** используется символ **&**
2) в качестве логического оператора **ИЛИ** используется символ **|**

3) в качестве логического оператора **НЕ** используется знак **!**.

Использование операторов осуществляется в префиксной нотации.

Соответствие единичному атрибуту, например:

```
(objectClass=person)
```

Соответствие двум атрибутам, например:

```
(&(objectClass=person)(objectClass=user))
```

Соответствие трем атрибутам, например:

```
(&(objectClass=user)(objectClass=top)(objectClass=person))
```

Соответствие одному из атрибутов, например:

```
(|(objectClass=person)(objectClass=user))
```

Если администратор службы каталогов затрудняется составить фильтр, можно воспользоваться бесплатной утилитой **Apache Directory Studio**, имеющей графический интерфейс пользователя, либо встроенной в сервер управления утилитой **ldapsearch** для проверки предполагаемых фильтров:

Запустите утилиту **ldapsearch** на сервере управления из контейнера **Docker gmnode_slapd_1:**

```
docker exec -it gmnode_slapd_1 bash
```

Запустите **ldapsearch** с вашим фильтром, например:

```
ldapsearch -D CN=username -w password H ldap://FQDN/ -v -x -b
“dc=vdi,dc=getmobit,dc=ru” -LLL
‘(&(objectCategory=person)(objectClass=user)(memberOf=CN=MSK,DC=vdi,DC=GETMOBIT,
DC=ru))’ cn
```

где:

1) **D** – указывает **DN** пользователя;
2) **CN** – на имя учетной записи **username**;
3) **w** – на пароль **password** учетной записи с правом чтения каталога;
4) **FQDN** – доменное имя сервера службы каталогов.

Внимание! *Синтаксис имени пользователя может зависеть от используемой службы каталогов.*

Альтернативный вариант поиска:

```
ldapsearch -LLL -H ldap://172.16.10.53 -x -D 'domain\username' -w 'password' -b
'dc=example,dc=com'
```

```
'(&(objectCategory=person)(objectClass=user)(memberOf=CN=groupname,DC=example,DC=com))' cn
```

5.16.4 Экспорт/импорт объектов

Примечание. *Функционал экспорта/импорта объектов является лицензируемой опцией, доступной не во всех редакциях СУ. За подробной информацией обратитесь в GETMOBIT или к официальному дистрибутору.*

Функционал экспорта/импорта объектов предназначен для быстрого переноса конфигурации (настроек) СУ с тестового на основной (рабочий).

Экспорт – процесс выгрузки объектов с СУ в файл (архив), содержащий файлы с редактируемыми параметрами СУ.

Импорт – процесс загрузки объектов на СУ из файла (архива) для восстановления данных или их применения.

Для экспорта/импорта доступны редактируемые параметры из следующих разделов:

- Шаблоны;
- Задания;
- Сценарии;
- Команды;
- Роли;
- Параметры реестра (ключ + значение);
- Настройки синхронизации с AD/LDAP;
- Устройства;
- Группы устройств.

Основные цели использования экспорта/импорта объектов

1. Быстро и безопасно перенести все настроенные параметры с тестового сервера управления на рабочий.
2. Обеспечение возможности восстановления данных всей конфигурации системы в случае сбоев, потери данных или других непредвиденных ситуаций.
3. Создание резервной копии (Backup) текущей конфигурации системы
4. Редактирование параметров объектов с помощью сторонних текстовых редакторов

5.16.4.1 Экспорт объектов

Для экспорта объектов выполните действия, описанные ниже.

1. В веб-консоли выберите раздел **Настройки.** Перейдите во вкладку **Экспорт** (Рисунок 69).

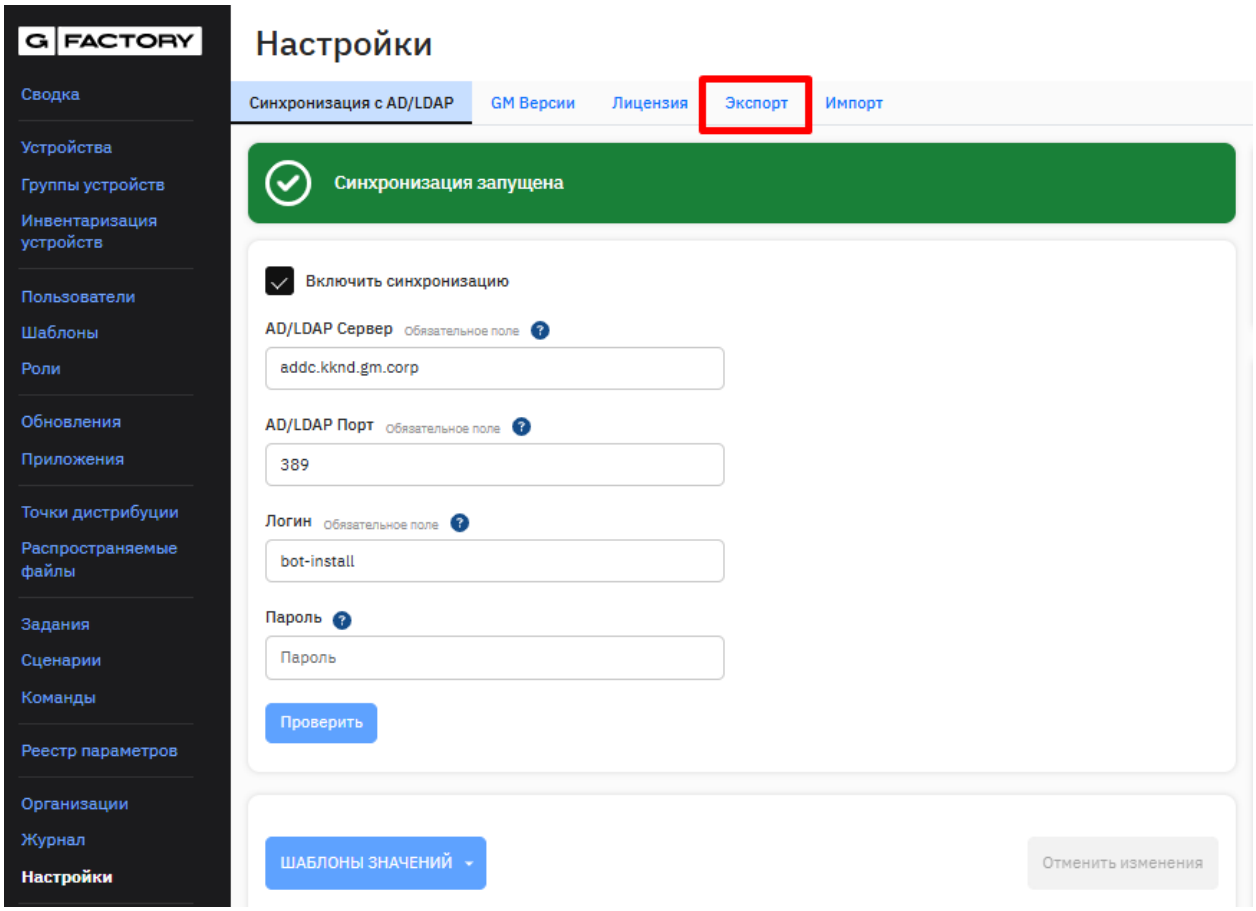


Рисунок 69 – Экспорт объектов

2. В открывшейся вкладке Экспорт, в левой части экрана выберите, установив флажки, объекты экспорта, которые необходимо скопировать (Рисунок *70*).

Примечание. *Некоторые объекты экспортируются только в сочетании с другими объектами, поскольку их функциональность зависит от определенных правил и взаимосвязей. Это обеспечивает корректность конфигурации при импорте и предотвращает потерю зависимостей между элементами СУ.*

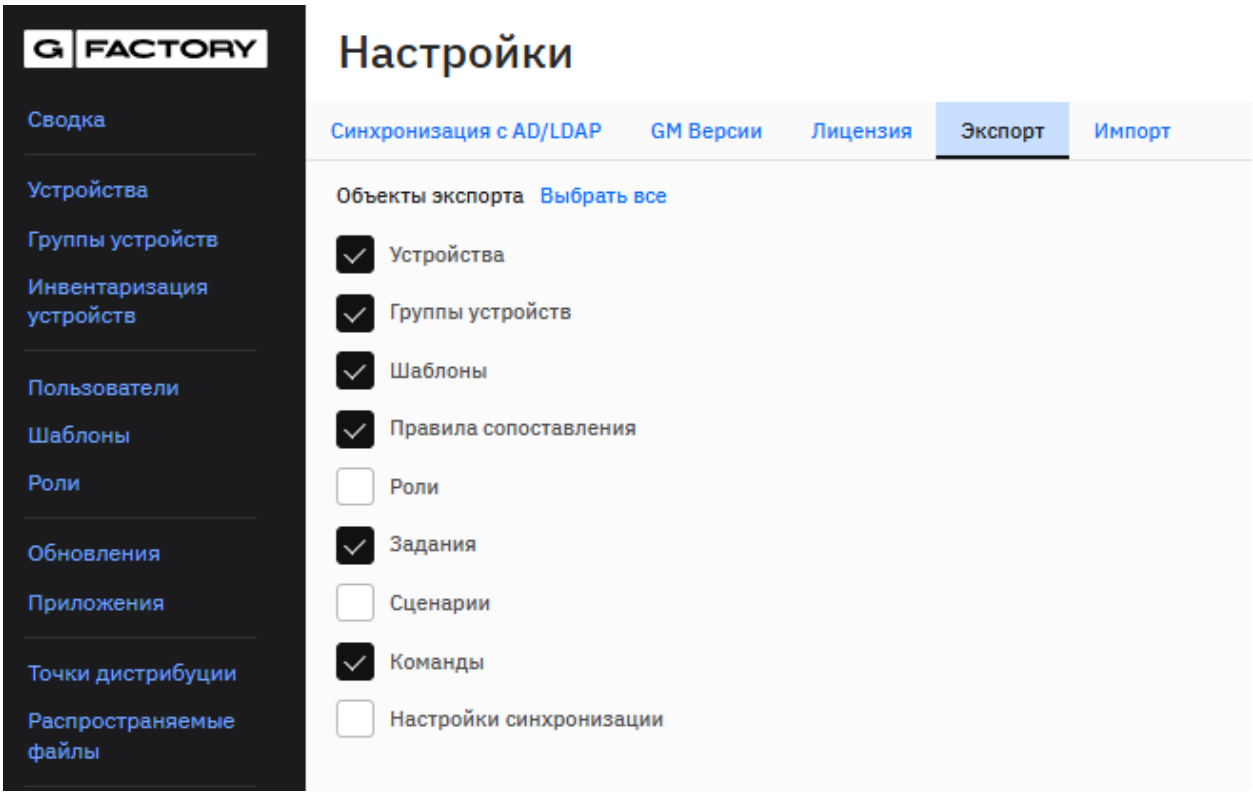


Рисунок 70 – Выбор объектов для экспорта

3. В правой части окна, задайте пароль или сгенерируйте его, нажав соответствующую кнопку (Рисунок *71*).

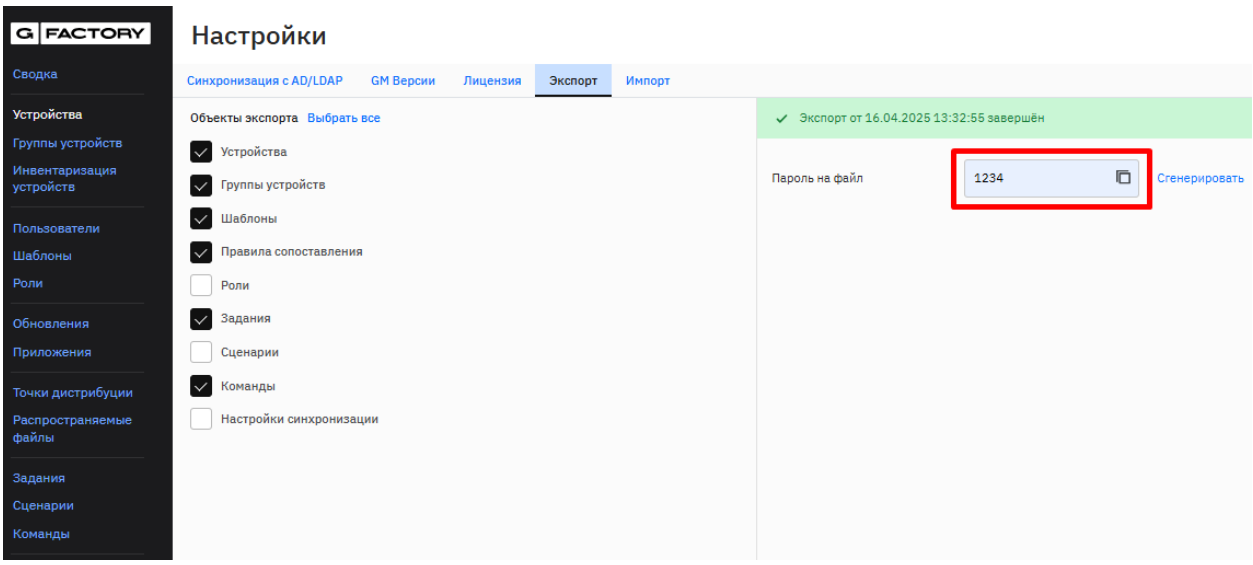


Рисунок 71 – Задание пароля на файл экспорта

4. В левом нижнем углу экрана нажмите **Экспортировать** (Рисунок *72*)

5. В правом верхнем углу сформируется файл (архив) для скачивания. Нажмите на иконку  (Рисунок *72*) и файл с данными будет сохранен в папку «Загрузки» по умолчанию.

Внутри архива экспортированные объекты представлены отдельными папками, названными по имени разделов. В каждой такой папке находится файл, соответствующий объекту данного раздела в формате JSON.

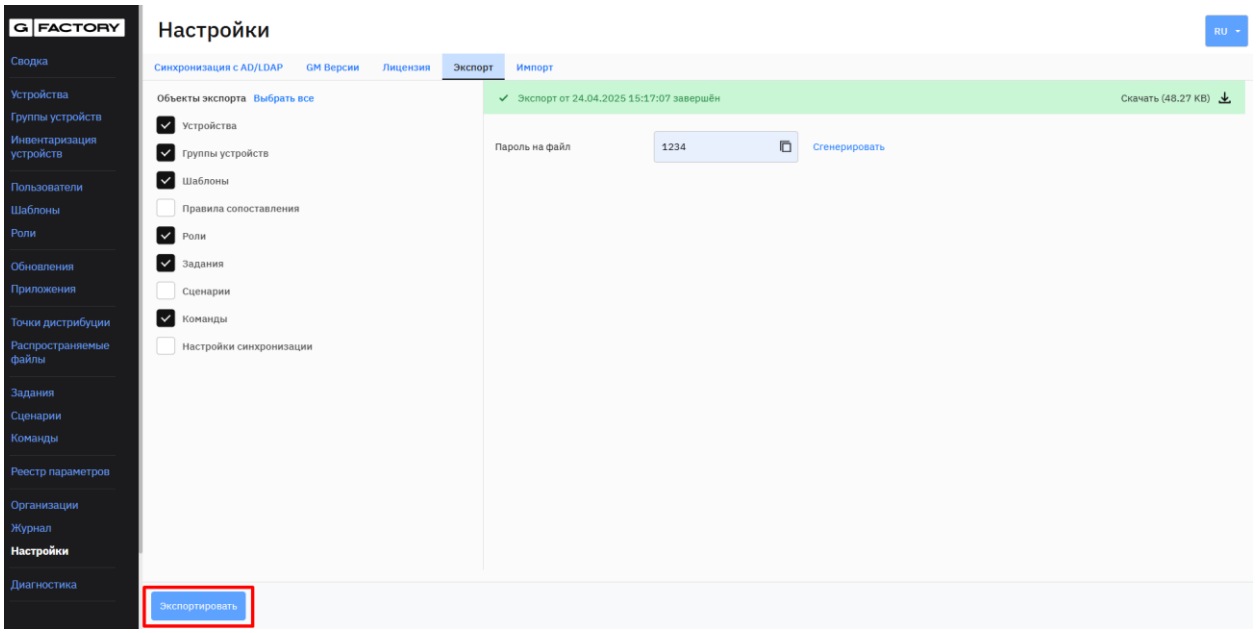


Рисунок 72 – Экспорт объектов с СУ

5.16.4.2 Импорт объектов

Для импорта выгруженных объектов, выполните действия, описанные ниже.

1. В веб-консоли выберите раздел **Настройки.** Перейдите во вкладку **Импорт** (Рисунок 73).

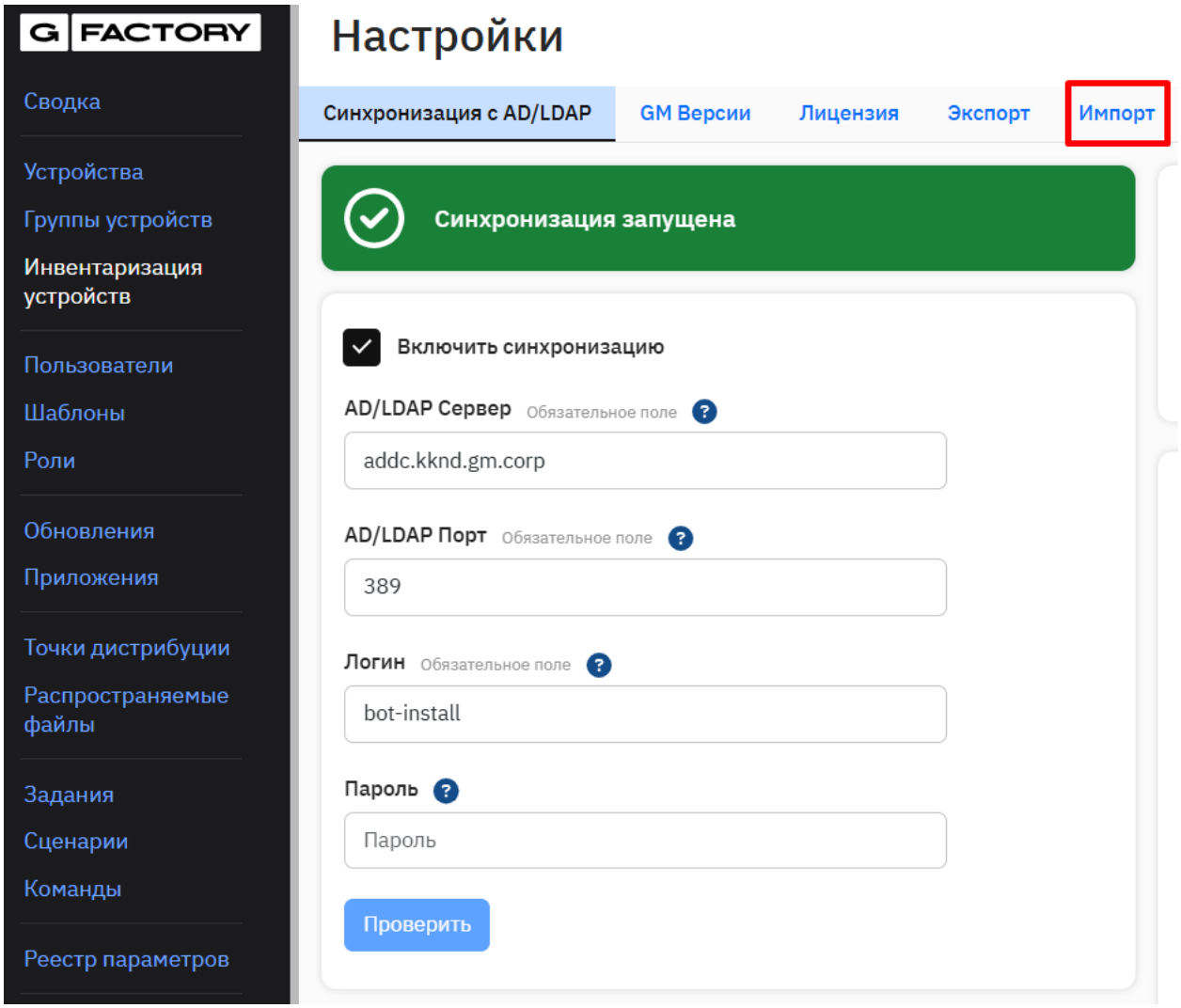


Рисунок 73 – Импорт объектов

2. В открывшейся вкладке **Импорт,** необходимо перенести файл (архив) с данными, выгруженный ранее с СУ. Для этого переместите файл в центральную часть экрана или нажмите «Выберите через проводник» (Рисунок *74*).

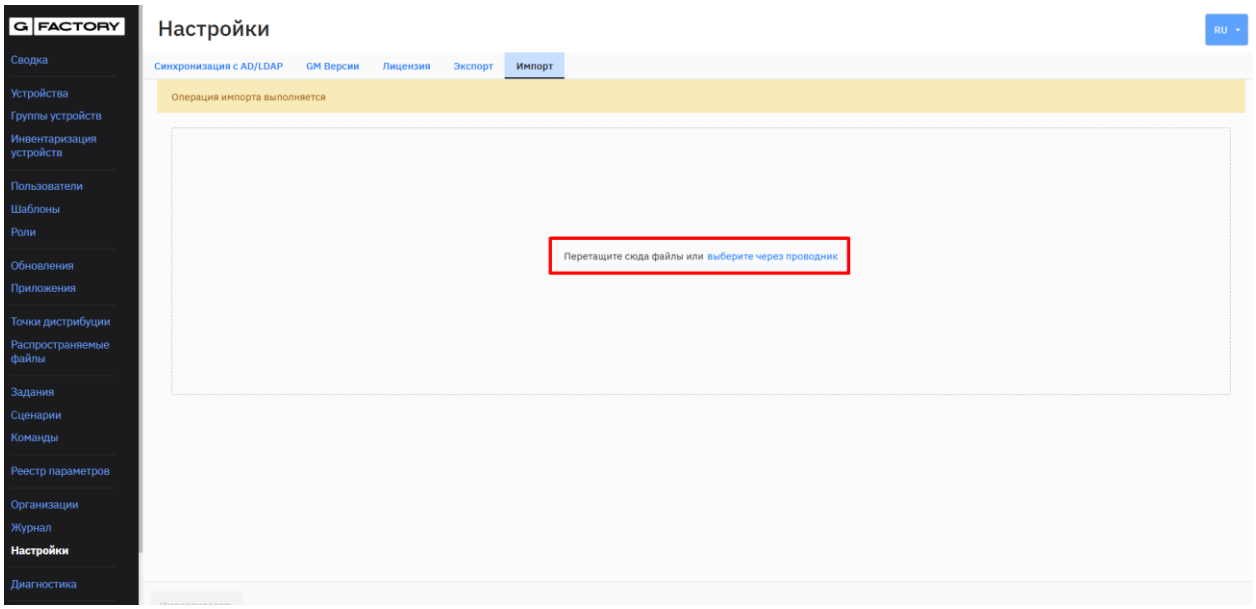


Рисунок 74 – Загрузка файла на СУ

3. После успешной загрузки файла на СУ, в левой части экрана отобразится список «Объекты импорта», в правой – загруженный файл. Нажмите «Выбрать все», а затем – **Импортировать** (Рисунок *75*).

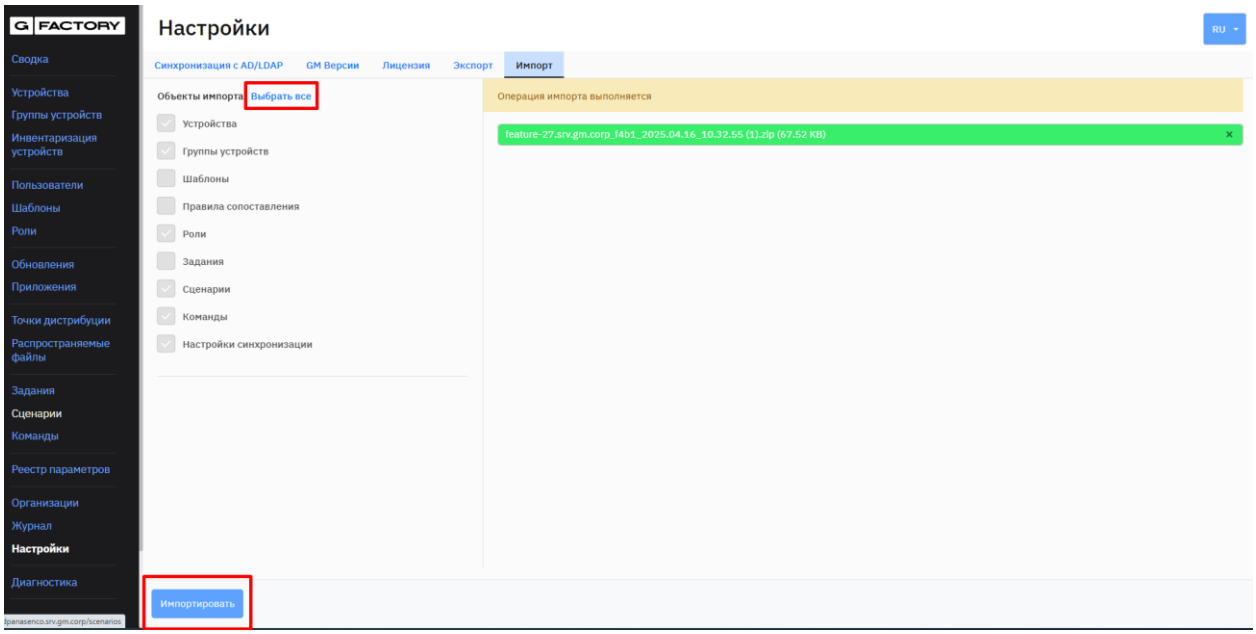


Рисунок 75 – Импорт объектов на СУ

После успешного импорта объектов на СУ в строке отображения статуса Импортирования появится обновленная дата и время.

5.16.5 Версия СУ

Для просмотра версии СУ и отдельных компонентов в веб-консоли выберите раздел **Настройки,** перейдите на вкладку **GM Версии**. Версия СУ приведена в поле **GMSERVER** (**GMFACTORY**), в других полях отображаются версии отдельных компонентов СУ.

Примечание. *При обращении в Service Desk обязательно предоставляйте информацию о версии СУ с этой вкладки.*

5.17 Удаленная поддержка пользователей

Примечание. *Информация по настройке удаленной поддержки пользователей в веб-интерфейсе администратора СУ приводится в отдельном документе «**GMSS. Удаленная поддержка**». Для получения документа обратитесь в отдел технической поддержки GETMOBIT.*

Для удаленного контроля интерфейсов ввода-вывода пользователя под управлением GM CORE KIT или GMSS NG Client, рекомендуется использовать функциональность удаленной поддержки из веб-интерфейса администратора СУ.

Удаленная поддержка обеспечивает:

- безопасное подключение с аутентификацией и TLS-шифрованием;
- гибкую настройку через конфигурационные файлы и параметры портов;
- управление сессиями (просмотр, контроль, перезагрузка устройств);
- автоматическое отключение для минимизации рисков;
- интеграцию с ролевой моделью СУ для контроля доступа.

5.18 Работа с таблицами

Во всех разделах веб-консоли, с табличным отображением информации, доступна функция настройки отображения столбцов. Для того, чтобы скрыть или отобразить нужный столбец, выполните действия, описанные ниже.

1. Выберите и откройте раздел в веб-консоли, в котором требуется настроить отображение таблицы.
2. Нажмите на иконку ⚙, расположенную в правом верхнем углу экрана (Рисунок 76).

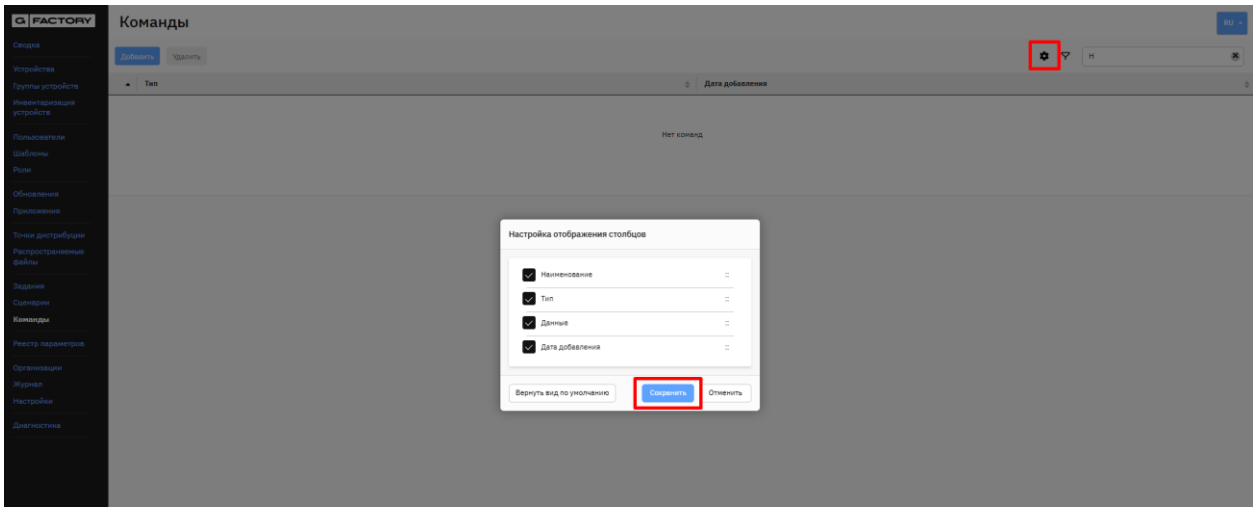


Рисунок 76 – Настройка отображения столбцов

Откроется окно Настройка отображения столбцов.

3. Выберите галочками из списка необходимые для отображения/скрытия столбцы и нажмите **Сохранить**.

6 Настройка сервиса мониторинга

6.1 Настройка ротации логов

Для управления файлами логов – ограничения их размера, архивирования и автоматического удаления неактуальных файлов логов - используется особый сервис journald, отвечающий за ротацию логов. Если необходимо настроить логирование и ротацию логов сервисов gmserver, gmserver-monitoring или других сервисов, потребуется выполнить следующие шаги.

1. Создать директорию для модульных конфигураций journald, если не создана:

```
sudo mkdir -p /etc/systemd/journald.conf.d
```

2. Создать и заполнить дополнительный файл конфигурации journald:

```
cat << EOF | sudo tee > /etc/systemd/journald.conf.d/10-gmms.conf
[Journal]
Storage=persistent
SystemMaxUse=5G
EOF
```

3. Перезагрузить сервис journald:

```
sudo systemctl restart systemd-journald
```

4. Убедиться, что настройки применены:

```
sudo systemd-analyze cat-config systemd/journald.conf
```

6.1.1 Дополнительная информация о настройках логирования GMMS

Логи контейнеров GMMS используют стандартный драйвер "json-file" и следующие настройки ротации, реализованные средствами docker-compose:

```
options:
    max-size: "100m"
    max-file: "3"
```

Примечание. *Максимальный размер лог-файлов для каждого из контейнеров равен 300 мб. Для 24-х сервисов, включенных в поставку GM-Server максимальный размер лог-файлов всех контейнеров не превысит 7200 mb.*

Следует иметь ввиду, что конфигурация логирования в /etc/docker/daemon.json не имеет приоритета над переопределенной конфигурацией каждого из контейнеров в случае с GMMS.

6.1.2 Общие рекомендации по настройке логирования

Общие рекомендации по настройке логирования в случае, если в системе есть другие сервисы, использующие Docker, описаны ниже.

1. Сконфигурируйте ротацию логов docker контейнеров по умолчанию, например:

/etc/docker/daemon.json

```
{
 "log-driver": "json-file",
 "log-opts": {
  "max-size": "10m",
  "max-file": "3"
 }
}
```

2. Убедитесь в том, что сервис journald настроен на ротацию журналов:

```
sudo systemd-analyze cat-config systemd/journald.conf
```

Примечание. *Обратите внимание на следующие директивы:*
SystemMaxUse : Максимальный объем дискового пространства для логов.
SystemKeepFree : Минимальное свободное место, которое должно оставаться на диске.
SystemMaxFileSize : Максимальный размер одного файла журнала.
SystemMaxFiles : Максимальное количество файлов журналов.
Если значения не установлены, systemd-journald использует значения по умолчанию

Не используйте директиву **ForwardToSyslog=yes**, выставленную по умолчанию в большинстве дистрибутивов, а также другую конфигурацию, приводящую к дублированию лог-файлов на локальной машине.

3. Убедитесь, что сервис logrotate настроен на ограничение файлов в директории /var/log по размеру, например:

cat /etc/logrotate.d/syslog

```
/var/log/syslog
{
    rotate 7
    daily
    missingok
```

```
    size 1G
    notifempty
    delaycompress
    compress
    postrotate
        invoke-rc.d syslog-ng reload > /dev/null
    endscript
}
```

6.2 Настройка ротации индексов Elasticsearch

Для обеспечения ротации событий, генерируемых устройствами и СУ, необходимо задать следующие настройки в файле **/etc/getmobit/monitoring/config.env**:

1) **ELASTIC_ROLLOVER_MAX_AGE** - максимальное время, после прохождения которого лог будет архивирован. Формат: time units (https://www.elastic.co/guide/en/elasticsearch/reference/current/api-conventions.html#time-units). По умолчанию - '7d' (7 дней)
2) **ELASTIC_ROLLOVER_MAX**_SIZE - максимальный размер блока логов, после достижения которого блок будет архивирован. Формат - byte units (https://www.elastic.co/guide/en/elasticsearch/reference/current/api-conventions.html#byte-units). По умолчанию - '5gb' (5 Гб).
3) **ELASTIC_DELETE_MIN**_AGE - время, после которого лог будет удален. Формат - time units (https://www.elastic.co/guide/en/elasticsearch/reference/current/api-conventions.html#time-units). По умолчанию - '30d' (30 дней)

***Примечание**. Логи будут архивированы после достижения хотя бы одной из отсечек ELASTIC_ROLLOVER_MAX_AGE, ELASTIC_ROLLOVER_MAX_SIZE.*

Логи не могут быть удалены до архивации, поэтому ELASTIC_ROLLOVER_MAX_AGE должен быть меньше ELASTIC_DELETE_MIN_AGE

6.3 Настраиваемые отсечки свободного места (watermarks) в Elasticsearch

Отсечки свободного места настраиваются в следующих параметрах *GM-Monitoring config.env*:

1) ELASTIC_WATERMARK_LOW
2) ELASTIC_WATERMARK_HIGH

3) ELASTIC_WATERMARK_FLOOD_STAGE

Формат данных:

4) Относительное значение от общего объема раздела (например, 0.85);
5) Значение в процентах от общего объема раздела (например, 85%);
6) Абсолютное значение (например, 500mb) в формате byte units.

При снижении свободного места на разделе ниже отсечки ELASTIC_WATERMARK_FLOOD_STAGE логи не сохраняются, предупреждающий баннер появится в консоли СУ. Разблокировка индексов происходит автоматически при освобождении места на разделе выше отсечки ELASTIC_WATERMARK_HIGH.

7 Настройка и управление устройствами с установленным GMSS NG Client

7.1 Установка GMSS NG Client

Установка GMSS NG Client осуществляется в соответствии с актуальной версией «Инструкции по установке GMSS NG Client».
Для установки GMSS NG Client должно быть подготовлено устройство, удовлетворяющее следующим минимальным требованиям:

1. Процессор архитектуры x86-64, 2 ядра от 1,1ГГц.
2. Чипсет выпуска 2013г или позднее.
3. 4 ГБ ОЗУ.
4. 16 ГБ ПЗУ.
5. ОС Ubuntu Linux 20.04LTS (серверная редакция, установленная в соответствии с актуальной версией «Инструкция по установке GMSS NG Client»).

Примечание. *Полный перечень протестированных аппаратных платформ предоставляется по запросу. Поддержка (оценка возможности поддержки) дополнительных аппаратных платформ осуществляется по запросу.*

7.2 Подключение и настройка RFID-карты к учетной записи пользователя

Настройка аутентификации пользователя через RFID-карты зависит от модели считывателя, типа используемых карт и алгоритма кодирования ID-карты. Для получения точной информации об алгоритме кодирования, применяемом производителем карт, необходимо обратиться непосредственно к производителю или его официальному представителю.

Для корректного отображения идентификационного номера RFID-карты, необходимо задать алгоритм чтения данных с учетом особенностей битового представления.

7.3 Настройка использования USB flash drive в VDI

Примечание. *Использование USB носителей в VDI и способ их подключения зависит от конкретной среды VDI. Для VDI Space, Basis, Termidesk, Горизонт-ВС, пожалуйста, ознакомьтесь с актуальной инструкцией для соответствующего клиента.*

Для использования USB Flash Drive в **Citrix** или **VMware** не требуется дополнительных настроек.

Примечание. *Убедитесь, что политика VDI позволяет использовать USB накопители и устройства на тонких клиентах.*

Для использования USB Flash Drive в **RDP-сессии** в качестве сетевого накопителя выполните дополнительные настройки одним из следующих способов, описанных ниже.

1. При синхронизации пользователей из корпоративной службы каталогов.

В веб-консоли на странице **Настройки** в поле **Значения по умолчанию** добавьте строки:

```
configuration.extra=AUTOMOUNT=true
```

Настройки будут заданы для всех пользователей.

2. При редактировании пользователя.

Внимание! *Перед указанием настроек пользователя убедитесь, что аналогичные настройки не заданы в настройках синхронизации.*

Если использование USB Flash Drive надо разрешить только отдельным пользователям, то в веб-консоли на странице Пользователи найдите учетную запись пользователя и откройте карточку пользователя на редактирование. При этом в разделе **Настройки** в поле **Значения по умолчанию** не нужно указывать configuration.extra=AUTOMOUNT=true

Добавьте в **Дополнительное поле** строку:

```
AUTOMOUNT=true
```

8 Настройка и управление GM-Box

8.1 Загрузка обновления на GM-Box

Встроенное ПО (прошивка) хранится в энергонезависимой памяти устройства и загружается при включении устройства. Для обновления встроенного ПО выполните следующие действия:

1) на экране приветствия GM-Box в разделе **Информация** узнайте (Рисунок *77*);
2) загрузите из личного кабинета (cp.getmobit.ru, раздел **Файлы**) новую версию прошивки GM-Box;
3) в веб-консоли в разделе **Обновления** добавьте файл обновления (файл с расширением SWU) (п. 5.8.1).
4) в веб-консоли создайте задание (п. 5.11.1) на выполнение команды **Device Update** или **Device Force Update** на устройствах, которые необходимо обновить, если не требуется перезагрузка устройства непосредственно после обновления (если перезагрузка допустима сразу после обновления – воспользуйтесь командой **Device Update and Reboot**) и дождитесь выполнения задания на обновление, прежде чем назначать новое задание на устройство;
5) в веб-консоли создайте задание (п. 5.11.1) на выполнение команды **Device Reboot** на устройствах, которые обновились и дождитесь выполнения задания, прежде чем назначать новое задание на устройство;
6) убедитесь, что на экране приветствия GM-Box в разделе **Информация** обновилась версия прошивки (Рисунок *77*).

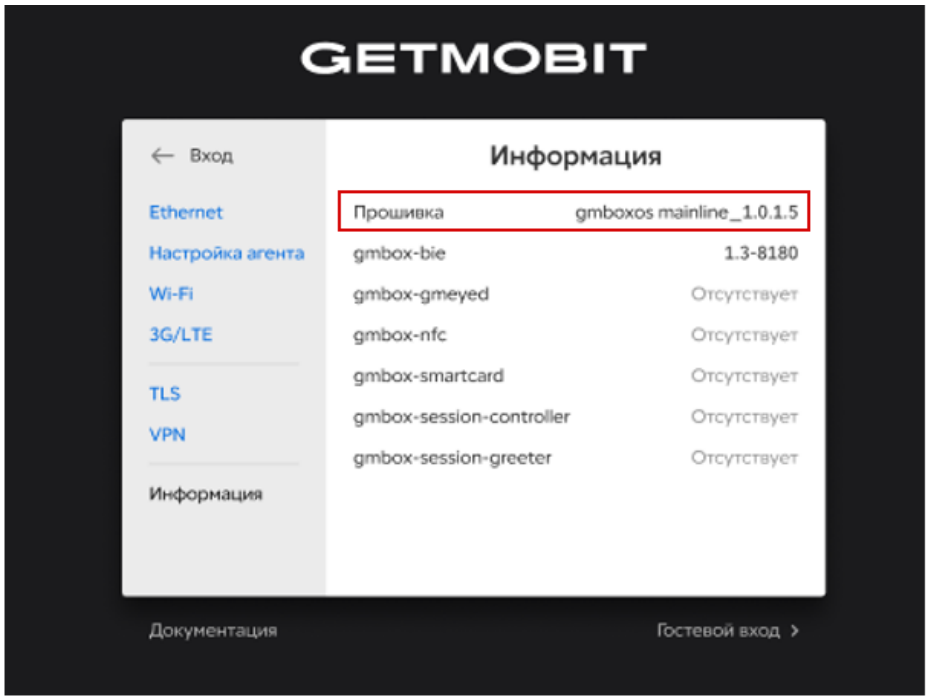


Рисунок 77 – Вид экрана приветствия GM-Box

8.2 Настройка гостевой учетной записи

Гостевой вход позволяет выполнить вход в систему без авторизации.

В веб-консоли в разделе **Пользователи** создайте учетную запись пользователя для гостевого входа (п. 5.5.1). Чтобы разрешить использование GM-Box в качестве VoIP-телефона, заполните следующие поля:

1. учетная запись;
2. пароль;
3. роль;
4. режим GM-Box;
5. SIP имя хоста;
6. SIP имя пользователя.

В конфигурационном файле greeter.conf задайте значения для следующих параметров:

```
"canUseGuestLogin": true,
"guestLogin": "учетная запись пользователя для гостевого входа",
"guestPassword": "пароль пользователя для гостевого входа"
```

Обновленный конфигурационный файл *greeter.conf* необходимо применить на устройстве. Для этого в веб-консоли создайте задание (п. 5.11.1) на выполнение команды **Patch config Greeter (greeter.conf)**.

В результате на экране приветствия GM-Box появится ссылка **Гостевой вход**, и на GM-Box будет доступна кнопка **Гостевой вход** (Рисунок 78).

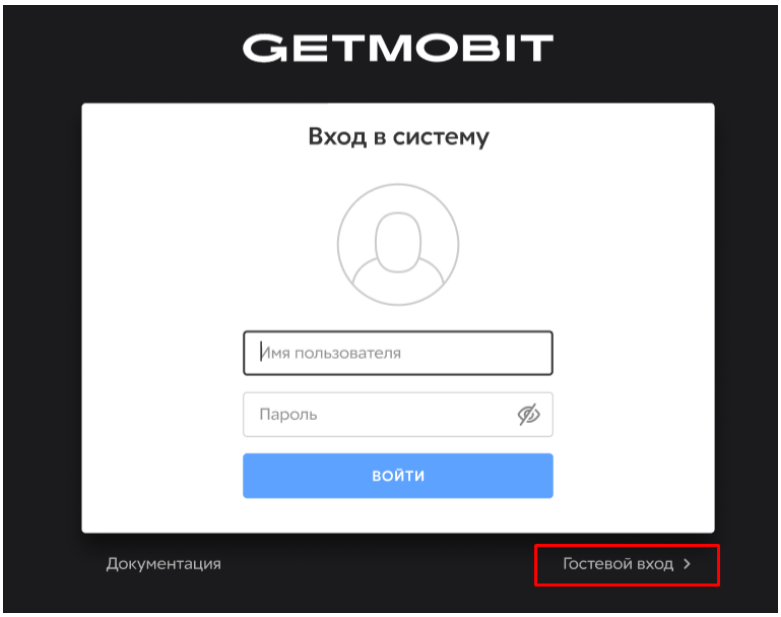


Рисунок 78 – Отображение кнопки «Гостевой вход»

8.3 Блокировка / разрешение подключения USB - устройств к GM-Box

По умолчанию пользователь может подключать любые USB-устройства к GM-Box. Настроить возможность подключения USB-устройств можно одним из следующих способов.

1 способ

- Сформируйте файл правил *rules.conf*, определяющий действия при подключении к GM-Box определенных USB-устройств.
- Для загрузки файла правил на устройство в веб-консоли создайте задание (п. 5.11.1) на выполнение команды **Usbguard upload rules (rules.conf)** и выберите созданный файл *rules.conf*.

2 способ

4. Сформируйте файл правил *rules.conf*, разрешающих подключение к GM-Box определенных USB-устройств, в том числе и внутренних USB-устройств.
5. Для загрузки файла правил на устройство в веб-консоли создайте задание на выполнение команды **Usbguard upload rules (rules.conf)** и выберите созданный файл *rules.conf*.
6. В веб-консоли создайте задание на выполнение команды **Usbguard default block**. После ее выполнения будут заблокированы все внутренние и внешние USB-устройства, не входящие в список разрешающих правил *rules.conf*.

8.3.1 Описание файла rules.conf

Описание синтаксиса правил, разрешающих или запрещающих подключение USB-устройств, см. **https://usbguard.github.io/documentation/rule-language.html**

Классы подключаемых USB-устройств приведены на сайте: **https://microchipdeveloper.com/usb:device-classes**

Пример файла правил, запрещающих все USB носители информации, кроме одного с заданными ID и Serial:

```
allow id 0781:5591 serial "4C530000100504108333" with-interface 08:*:*
block with-interface one-of { 08:*:* }
```

Пример файла правил, разрешающих использование только внутренних USB-устройств GM-Box, клавиатуры, мыши (использование других USB-устройств заблокировано командой **Usbguard default block**):

```
allow with-interface one-of { 03:*:* 03:*:* }
allow id 1d6b:0002 with-interface 09:00:00
allow id 1d6b:0003 with-interface 09:00:00
allow id 0424:2514 with-interface { 09:00:01 09:00:02 }
allow id 0424:2514 with-interface { 09:00:01 09:00:02 }
allow id 8087:0a2a with-interface { e0:01:01 e0:01:01 e0:01:01 e0:01:01 e0:01:01 e0:01:01
e0:01:01 }
allow id 058f:5608 with-interface { 0e:01:00 0e:02:00 0e:02:00 0e:02:00 0e:02:00 }
allow id 10c4:ea60 with-interface ff:00:00
allow id 12d1:15c3 with-interface { ff:06:10 ff:06:13 ff:06:12 ff:06:16 ff:06:16 ff:06:14
ff:06:1b 02:06:00 0a:06:00 ff:06:10 ff:06:13 ff:06:12 ff:06:14 ff:06:1b 02:0e:00 0a:00:02
0a:00:02 ff:06:14 }
```

8.4 Настройка использования принтеров

Печать на сетевые и локальные принтеры выполняется с использованием подсистемы печати Common UNIX Printing System (далее – CUPS). Вы можете настраивать CUPS и отслеживать его состояние, управлять принтерами через web-интерфейс, который по умолчанию доступен по адресу: **http://<IP-адрес пользователя GM-Box>:631**.

На GM-Box по умолчанию установлены драйверы для большинства используемых принтеров (полный список поддерживаемых принтеров приведен на сайте **https://cp.getmobit.ru** на вкладке **Документы**). Если вашего принтера нет в списке, вы можете дополнительно загрузить драйвер принтера (файл в формате PPD).

Перенаправление принтеров в RDP-сессию выполняется автоматически, а для режима *iddqd* необходимо в списке параметров пользователя в поле **VDI параметры 2** указать значение */printer*.

Принтеры перенаправляются в VMware-сессию как подключаемое локальное устройство или как сетевой принтер.

Перенаправление принтеров в Citrix-сессию выполняется автоматически.

8.4.1 Настройка сетевого принтера

Для добавления в VDI сетевого принтера выполните действия, описанные ниже.

1. В браузере в строке адреса введите **<IP-адрес пользователя>:631** Откроется web-интерфейс подсистемы печати CUPS.
2. Перейдите на вкладку **Администрирование** и нажмите **Добавить принтер** (Рисунок *79*).

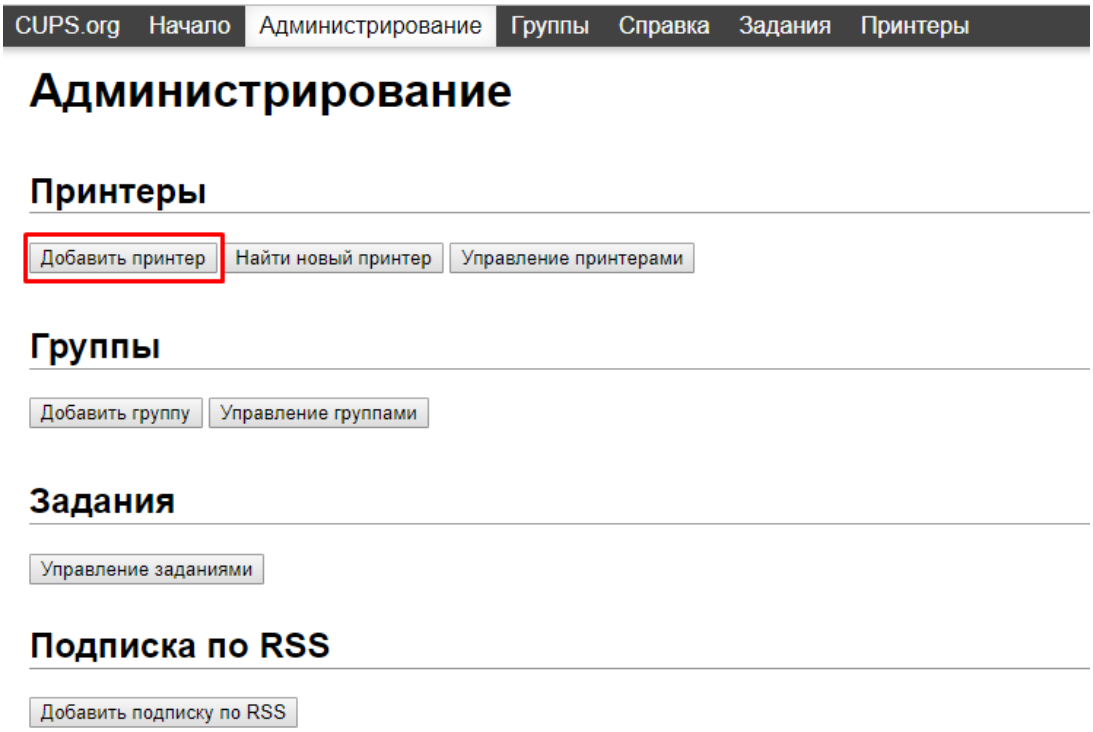


Рисунок 79 – Добавление принтера

3. Выберите протокол интернет-печати (например, ipps) и нажмите **Продолжить** (Рисунок *80*).

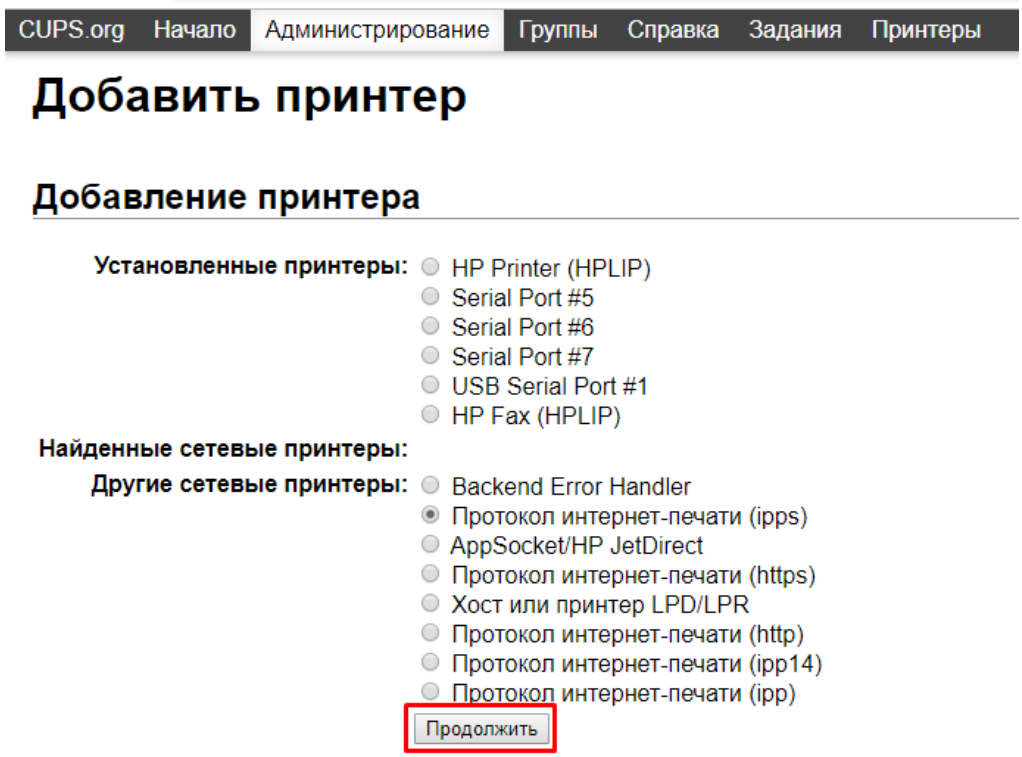


Рисунок 80 – Выбор протокола интернет-печати

4. В поле **Подключение** укажите IP-адрес или DNS-имя сетевого принтера и нажмите **Продолжить** (Рисунок *81*).

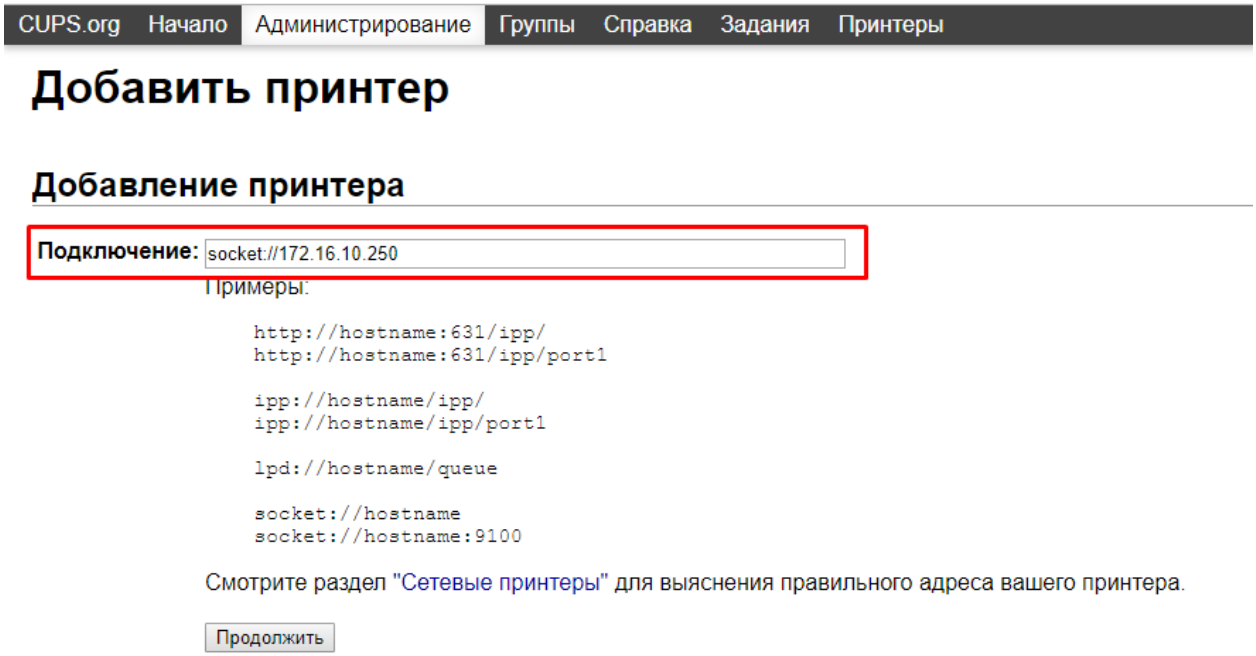


Рисунок 81 – Подключение принтера по IP-адресу

5. В обязательном поле **Название** (Рисунок *82*) введите название принтера, остальные поля и чек-бокс на этой странице заполните при необходимости.
6. Нажмите **Продолжить**.

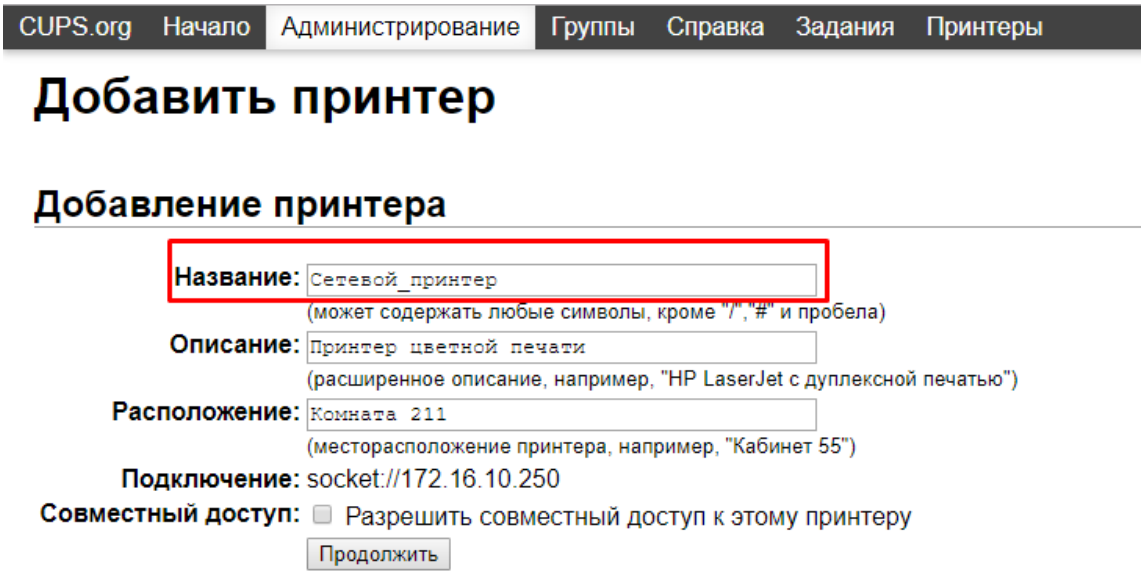


Рисунок 82 – Добавление названия принтера

7. Выберите производителя принтера и нажмите **Продолжить** (Рисунок *83*).

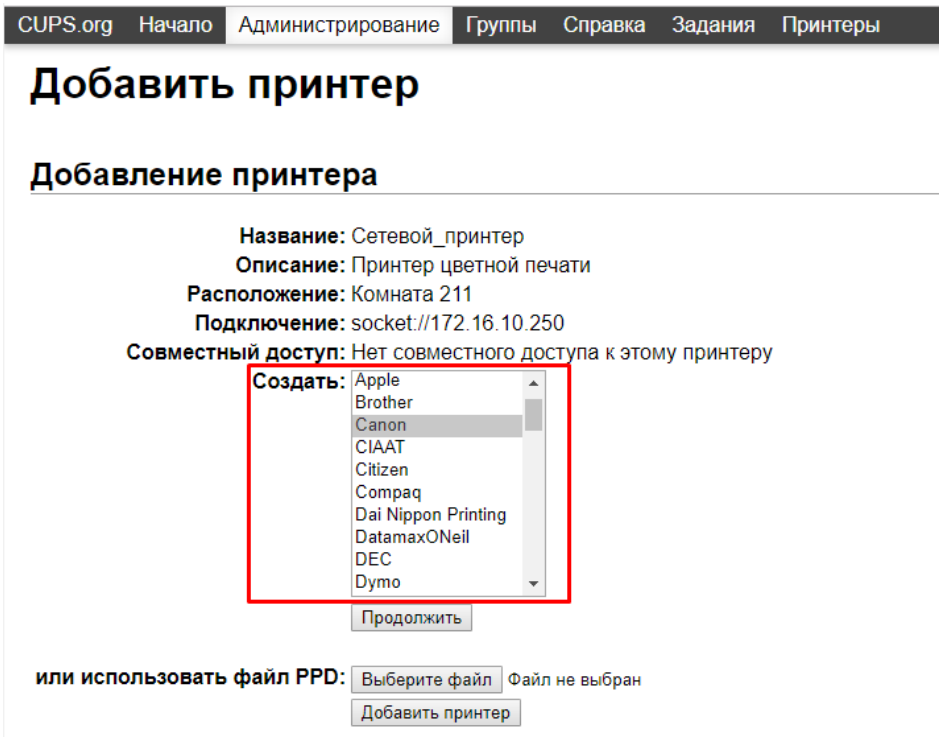


Рисунок 83 – Выбор производителя принтера

8. В открывшемся списке доступных моделей выберите необходимый принтер и нажмите **Добавить принтер** (Рисунок *84*). Если ваш принтер не найден в списке, нажмите **Выберите файл** и загрузите драйвер принтера (файл в формате PPD).

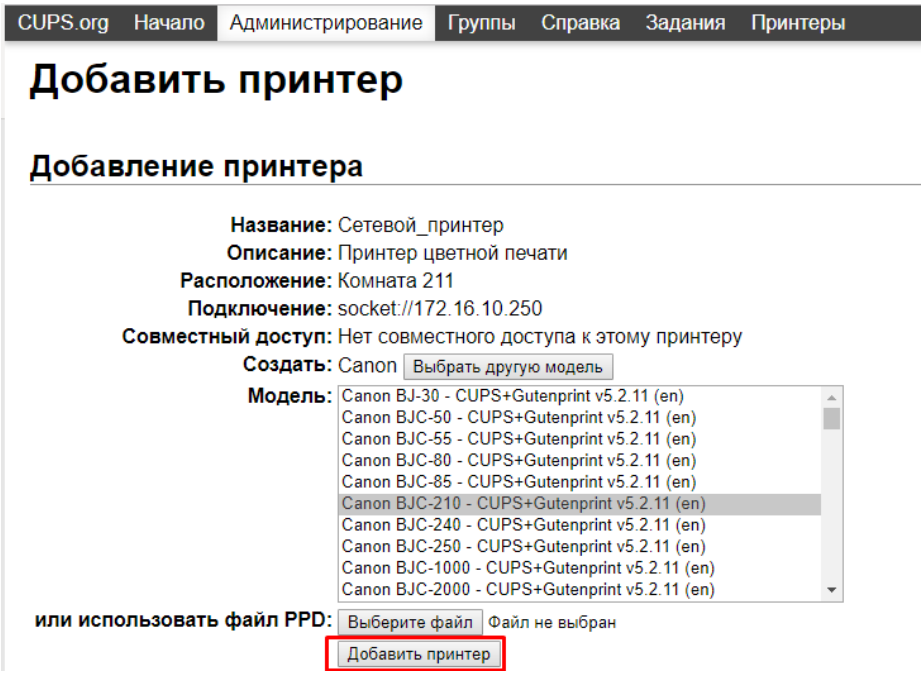


Рисунок 84 – Выбор модели принтера

9. Настройте параметры принтера или оставьте их по умолчанию и нажмите **Сохранить параметры** (Рисунок *85*).

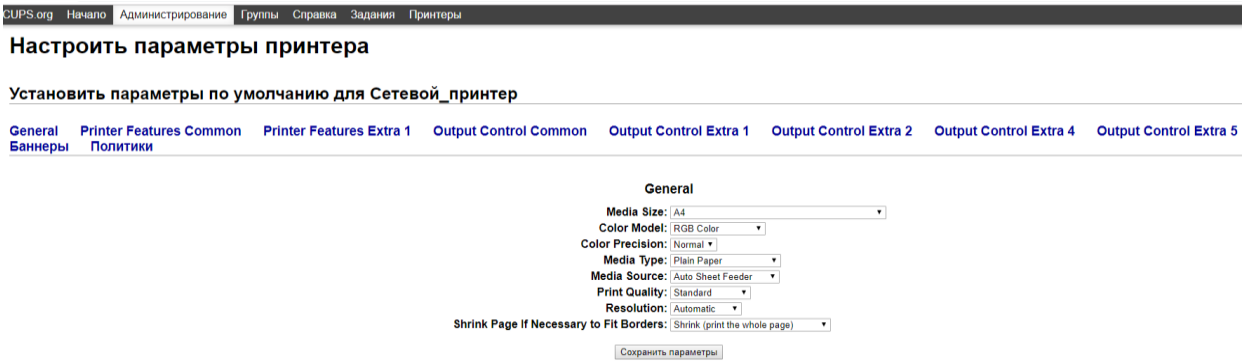


Рисунок 85 – Настройки параметров принтера

10. Для того чтобы убедиться, что принтер корректно добавлен, распечатайте пробную страницу. Перейдите на вкладку **Принтеры**, выберите добавленный сетевой принтер и на открывшейся странице выберите из выпадающего списка **Печать пробной страницы** (Рисунок 86).

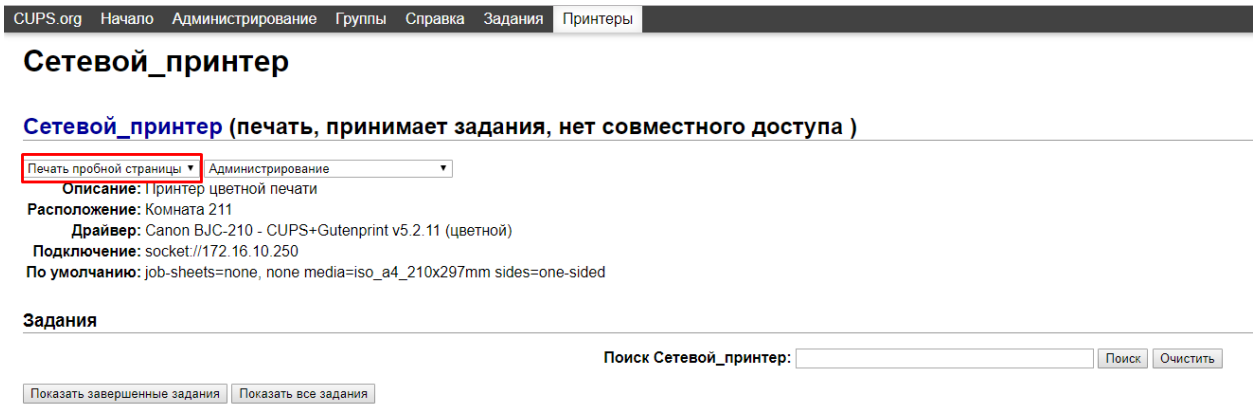


Рисунок 86 – Проверка работоспособности принтера

8.4.2 Как настроить использование локального принтера

Для настройки локального принтера выполните следующие действия:

1. Подключите локальный принтер к GM-Box через USB-порт.
2. В браузере в строке адреса введите **<IP-адрес пользователя GM-Box>:631** Откроется web-интерфейс подсистемы печати CUPS.
3. Перейдите на вкладку **Администрирование** и нажмите **Добавить принтер** (Рисунок *87*).

Выберите установленный принтер и нажмите **Продолжить**.

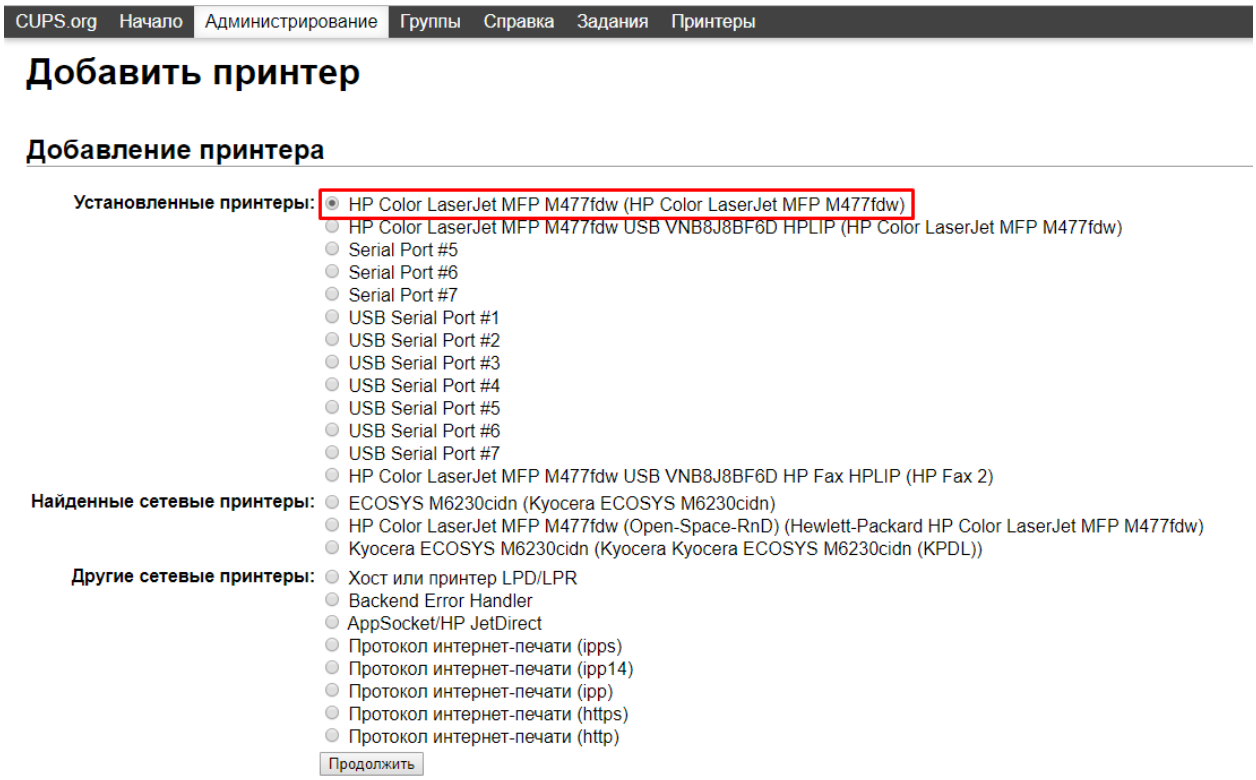


Рисунок 87 – Добавление локального принтера

4. Отредактируйте поля **Название** и **Описание** и нажмите **Продолжить** (Рисунок *88*).

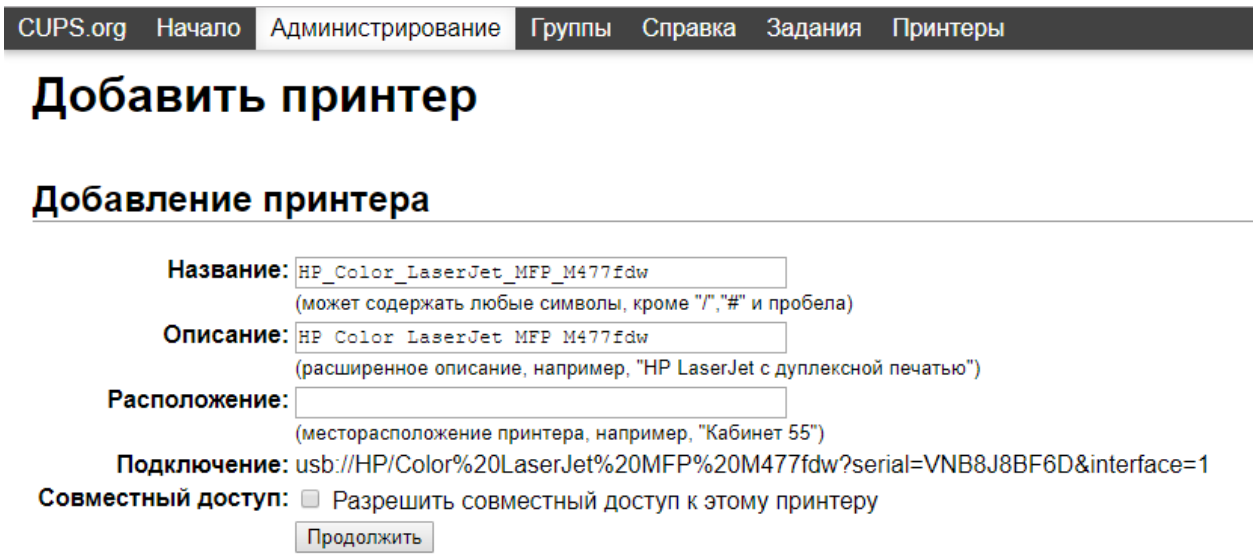


Рисунок 88 – Редактирование полей

5. В открывшемся списке доступных моделей выберите необходимый принтер и нажмите **Добавить принтер**. Если ваш принтер не найден в списке, нажмите **Выбрать файл** и загрузите драйвер принтера (файл в формате PPD).

6. Настройте параметры принтера или оставьте их по умолчанию и нажмите кнопку **Сохранить параметры** (Рисунок *89*).

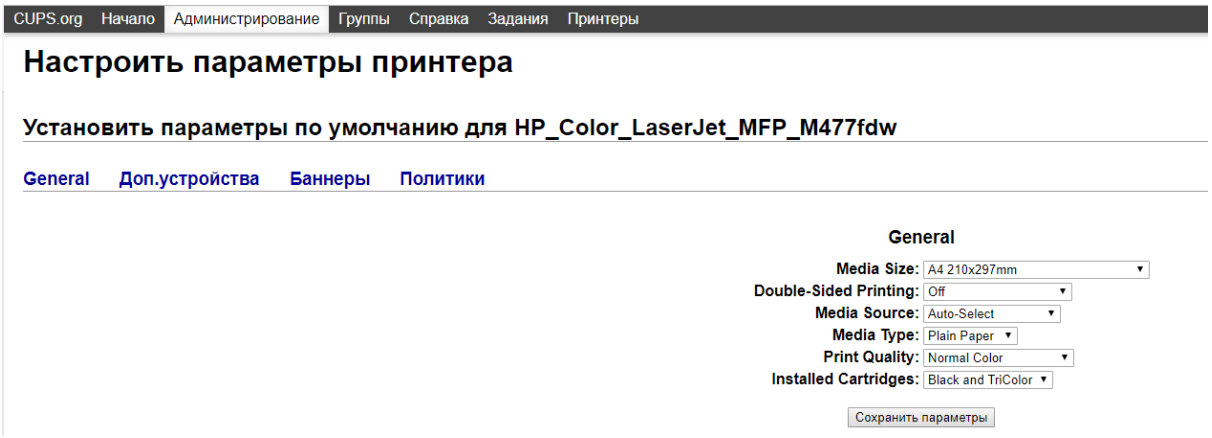


Рисунок 89 – Настройки параметров локального принтера

7. Для того чтобы убедиться, что принтер корректно добавлен, распечатайте пробную страницу. Перейдите на вкладку **Принтеры**, выберите добавленный локальный принтер и на открывшейся странице выберите из выпадающего списка **Печать пробной страницы**.

8.5 Настройка использования USB flash drive в VDI

Примечание. *Использование USB носителей в VDI и способ их подключения зависит от конкретной среды VDI. Для VDI Space, Basis, Termidesk, Горизонт-ВС, пожалуйста, ознакомьтесь с актуальной инструкцией для соответствующего клиента.*

Для использования USB Flash Drive в **Citrix** или **VMware** не требуется дополнительных настроек.

Примечание. *Убедитесь, что политика VDI позволяет использовать USB накопители и устройства на тонких клиентах.*

Для использования USB Flash Drive в **RDP**-сессии в качестве сетевого накопителя выполните дополнительные настройки одним из двух способов, описанных ниже.

1. При синхронизации пользователей из корпоративной службы каталогов.

   В веб-консоли на странице **Настройки** в поле **Значения по умолчанию** добавьте строки:

```
configuration.extra=AUTOMOUNT=true
```

Настройки будут заданы для всех пользователей.

2. При редактировании пользователя.

Внимание! *Перед указанием настроек пользователя убедитесь, что аналогичные настройки не заданы в настройках синхронизации.*

Если использование USB Flash Drive надо разрешить только отдельным пользователям, то в веб-консоли на странице Пользователи найдите учетную запись пользователя и откройте карточку пользователя на редактирование. При этом в разделе **Настройки** в поле **Значения по умолчанию** не нужно указывать configuration.extra=AUTOMOUNT=true

Добавьте в **Дополнительное поле** строку:

```
AUTOMOUNT=true
```

9 Настройка интеграции с сервисами IP-телефонии

9.1 Настройка телефонной книги

Телефонная книга содержит имена и номера телефонов пользователей из службы каталогов. Для доступа к телефонной книге нажмите кнопку **Контакты** на GM-Box.

9.1.1 Как настроить телефонную книгу

Для отображения телефонной книги необходимо заполнить соответствующие поля в профиле пользователя или шаблоне.

1. В веб-консоли выберите раздел **Пользователи** или **Шаблоны** и откройте профиль пользователя или шаблон.
2. В нижней части карточки пользователя или шаблона заполните поля (Рисунок *90*):

    - **AD/LDAP Имя пользователя** – логин специальной учетной записи для получения информации для телефонной книги из корпоративной службы каталогов;
    - **AD/LDAP Пароль** - пароль специальной учетной записи;
    - **AD/LDAP Сервер** - IP-адрес или DNS-имя корпоративной службы каталогов;
    - **AD/LDAP Порт** - номер порта на сервере корпоративной службы каталогов для TCP/UDP соединений;
    - **AD/LDAP Base DN** – укажите корневую папка поиска;
    - **AD/LDAP Телефонное поле** - название поля учетных записей корпоративной службы каталогов, в котором хранится информация о телефонном номере сотрудника;
    - **AD/LDAP Фильтр пользователей** - позволяет задавать точные параметры поиска объектов для их добавления в телефонную книгу.



Рисунок 90 – Заполнение полей в разделе **Пользователи**

3. Нажмите **Сохранить изменения**.
4. Войдите в сессию, нажмите **Контакты** на GM-Box и убедитесь, что пользователи из службы каталогов и номера телефонов появились (Рисунок *91*).

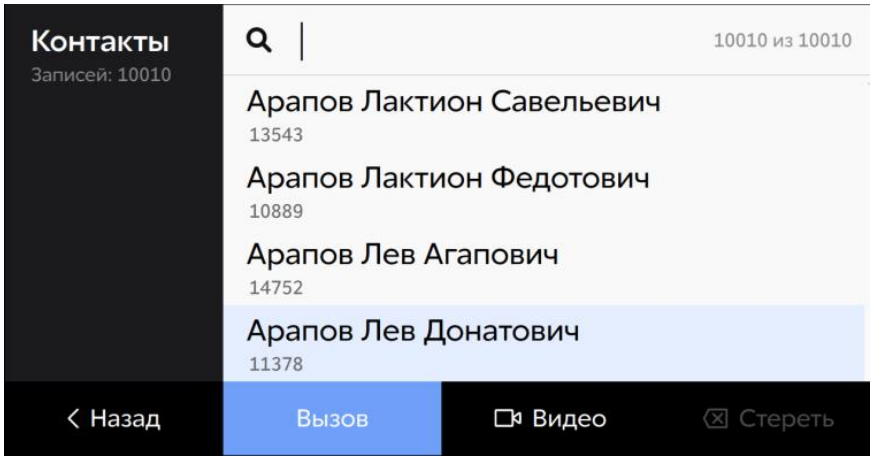


Рисунок 91 – Вид окна Контакты

9.2 Настройка поддержки аудиокодеков

Список аудиокодеков, поддерживаемых устройством, можно посмотреть в разделе **Устройства** на вкладке **Информация** (Рисунок *92*).

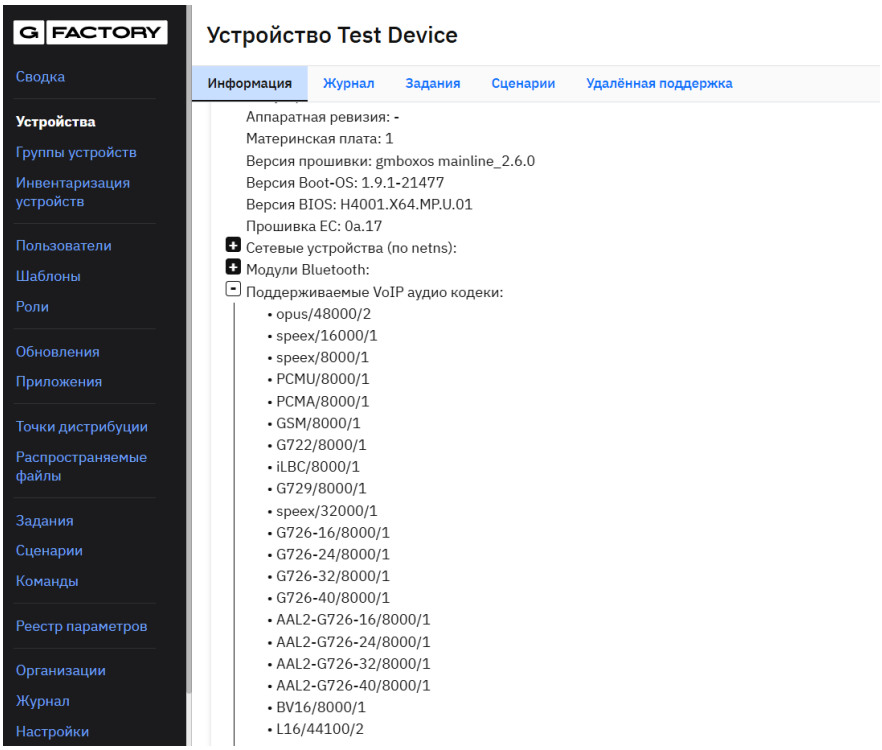


Рисунок 92 – Список поддерживаемых кодеков

Для поддержки аудиокодеков у пользователя в веб-консоли выберите раздел **Пользователи**, откройте карточку пользователя и в поле **SIP аудиокодеки** (Рисунок *93*) добавьте одно или несколько необходимых значений:

opus/48000/2
speex/16000/1
speex/8000/1
PCMU/8000/1
PCMA/8000/1
GSM/8000/1
G722/8000/1
iLBC/8000/1
G729/8000/1
speex/32000/1
G726-16/8000/1
G726-24/8000/1
G726-32/8000/1
G726-40/8000/1
AAL2-G726-16/8000/1
AAL2-G726-24/8000/1
AAL2-G726-32/8000/1
AAL2-G726-40/8000/1
BV16/8000/1
L16/44100/2
L16/44100/1

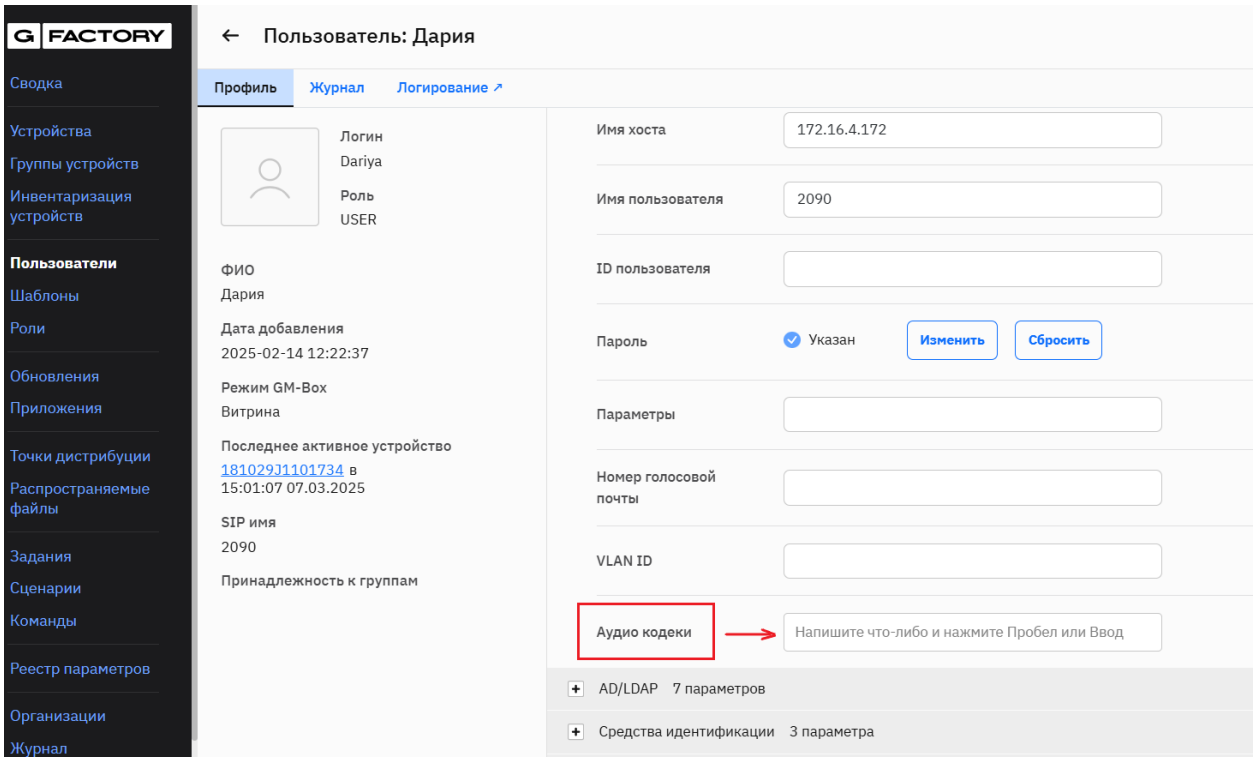


Рисунок 93 – Настройка аудио кодеков

9.3 Настройка отображения избранных контактов

Чтобы добавить в список контактов пользователя избранные контакты, выполните действия, описанные ниже.

В веб-консоли в разделе **Пользователи** при редактировании или создании пользователя в **Дополнительном поле** задайте параметр:

```
SIP_FAVORITES=”<phone number 1>, <phone number 2>, <phone number n>”
```

Где phone number – значение поля с телефонным номером абонента, импортированным из корпоративной службе каталогов (поле **AD телефонное поле** у пользователя).

У пользователя контакты будут отображаться в том порядке, как записано в параметре SIP_FAVORITES.

Если в перечне SIP_FAVORITES указан номер, который не содержится ни у одного пользователя в корпоративной службе каталогов, то контакт с этим номером отображается в списке с именем *Неизвестный*.

9.4 Режим проверки и повторной регистрации VoIP клиента

В системном ПО GM-Box реализована поддержка высокой доступности IP-телефонии и повторной регистрации. Данная функция включена по умолчанию независимо от количества установленных в инфраструктуре АТС и позволяет обеспечивать актуальную информацию о состоянии регистрации VoIP клиента.

Администратор может принудительно выключить данную функцию, задав параметр VOIP_LEGACY_REGISTER_MODE. Параметр VOIP_LEGACY_REGISTER_MODE задается в **Профиле пользователя** или **Шаблоне** в поле **Дополнительное поле** в следующем формате:

```
VOIP_LEGACY_REGISTER_MODE=”true”
Или
VOIP_LEGACY_REGISTER_MODE=”yes”
```

9.5 Настройка высокой доступности IP телефонии

В системном ПО GM-Box реализована поддержка высокой доступности IP телефонии. Для ее включения, необходимо в профиле пользователя указать список узлов (регистраторов) АТС.

Список АТС задается в **Профиле пользователя** или **Шаблоне** в поле **Дополнительное поле** в следующем формате:

```
SIP_HOSTS=”HOST1,HOST”
```

Например:

```
SIP_HOSTS=” 172.16.4.172, 172.16.4.173
```

Адреса АТС задаются без пробелов, количество указываемых адресов не ограничено.

Принцип работы механизма обеспечения высокой доступности:

1) при запуске VoIP клиент поочередно перебирает список АТС в том же порядке, который указан в параметре SIP_HOSTS;
2) если VoIP клиент не может установить соединение с АТС, то АТС считается недоступно»;
3) если соединение с АТС установлено, VoIP клиент отсылает запрос на регистрацию пользователя;

4) если попытка регистрации завершилась с ошибкой, то АТС считается недоступной;
5) если текущая АТС из списка недоступна, то VoIP клиент переходит к следующей АТС по списку;
6) если список АТС закончился, перерегистрация замораживается на некоторый промежуток времени (по умолчанию 30 секунд, задается через параметр SIP_REGISTER_DROP в Дополнительном поле. Пример: SIP_REGISTER_DROP="60"). После пробуждения VoIP клиент сбрасывает список недоступных АТС и начинает цикл опроса по АТС заново;
7) если VoIP клиент успешно подключился к АТС и зарегистрировался, то процесс перерегистрация замораживается. Зарегистрированная АТС назначается текущей АТС. После чего VoIP клиент периодически проверяет доступ к АТС, пытаясь установить соединение к АТС по порту 5060 и/или ожидая сообщение об ошибке регистрации от АТС (по умолчанию 300 секунд, задается через параметр SIP_REGISTER_EXPIRES в Дополнительном поле. Пример: SIP_REGISTER_EXPIRES="600");
8) если повторно установить соединение не удалось или была получена ошибка регистрации, то текущая АТС считается "недоступной". VoIP клиент сбрасывает текущую АТС и размораживает перерегистрацию, переходя на следующую АТС по списку.

9.6 Описание сообщений VoIP клиента

В процессе работы VoIP клиент может выводить сообщения в строке состояния на встроенном в GM-Box экране. Перечень сообщений, выводимых в строке состояния приведен в Таблица 12.

Таблица 12 – Перечень сообщений, выводимых в строке состояния

Текст	Описание
имя_пользователя или номер	Регистрация пользователя успешно проведена
Не задан прокси-сервер	В настройках пользователя не указана АТС
Не задано имя пользователя	В настройках пользователя не указано поле "SIP Имя пользователя"

Текст	Описание
Не заданы настройки телефонии	В настройках пользователя не указаны ни АТС, ни поле "SIP Имя пользователя"
Ошибка аутентификации	Ошибка аутентификации пользователя, неверные пароль пользователя и/или имя пользователя
Ошибка регистрации	Общая ошибка регистрация, точная причина неизвестна
Пользователь не найден	**Поддерживается не на всех АТС** Ошибка аутентификации пользователя, неверное имя пользователя

9.7 Диагностика голосового VLAN

Если в профиле пользователя настроено применение голосового (voice) VLAN, администратор может убедиться в корректности применения параметров голосового VLAN. Для этого:

1. В веб-консоли в разделе **Устройства** найдите устройство, на котором работает пользователь и перейдите на вкладку **Информация** (Рисунок *94*).



Рисунок 94 – Вкладка Информация

2. Находясь на вкладке **Информация**, раскройте раздел **Сетевые устройства (по netns)** (Рисунок 95):

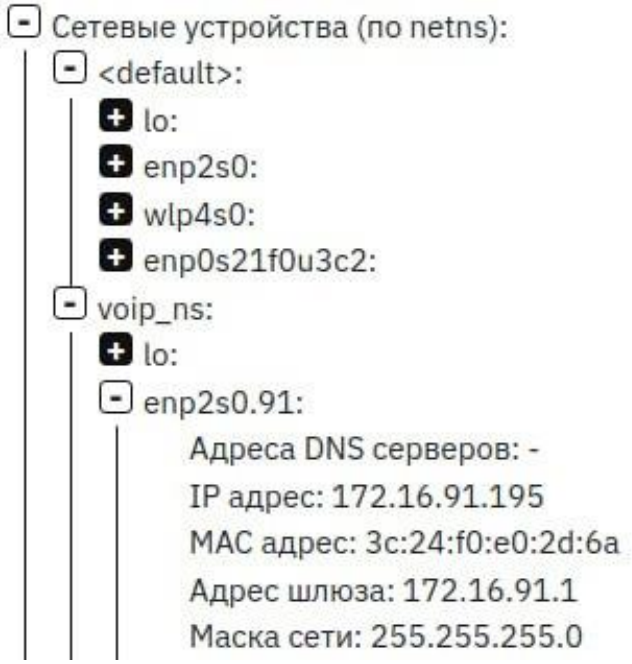


Рисунок 95 – Раздел Сетевые устройства (по nets)

3. Убедитесь, что VLAN интерфейс присутствует и имеет заполненные параметры:
   - VLAN интерфейс располагается в подразделе **voip_ns**;
   - Получены IP-адрес, адрес шлюза, маска сети и DNS сервер

Отсутствие указанных в п. 3 параметров может свидетельствовать об отсутствии корректно настроенного DHCP сервера в голосовом VLAN, некорректно указанном номере VLAN или получении некорректных параметров по протоколу LLDP.

Внимание! *MAC адрес голосового VLAN интерфейса совпадает с MAC адресом интерфейса Ethernet.*

9.8 Регистрация GM-Box в Cisco Unified Communications Manager

Для подключения GM-Box как стороннего SIP терминала с CUCM необходимо выполнить действия, описанные ниже.

1. Создать пользователя и настроить учетные данные.
2. Создать устройство, присвоить номер и связать с пользователем.

Внимание! *В случае выделения сервиса IP-телефонии в отдельный VLAN (voice VLAN), необходимо обеспечить функционирование сервиса DHCP и трансляцию DNS в voice VLAN.*

9.8.1 Создание пользователя

1. В главном окне CUCM перейдите на вкладку **User Management >End User** и нажмите кнопку **Add new**.
2. В открывшемся окне **End User Configuration**:
3. В разделе **User Information** заполните следующие поля (Рисунок *96*):
   - **User ID** - введите идентификатор пользователя (любые символы)
   - **Password**
   - **Confirm Password**
   - **Last Name**
   - **User Locale** выберите *English, United States*
   - **Digest Credentials** - SIP пароль для устройства
   - **Confirm Digest Credentials**

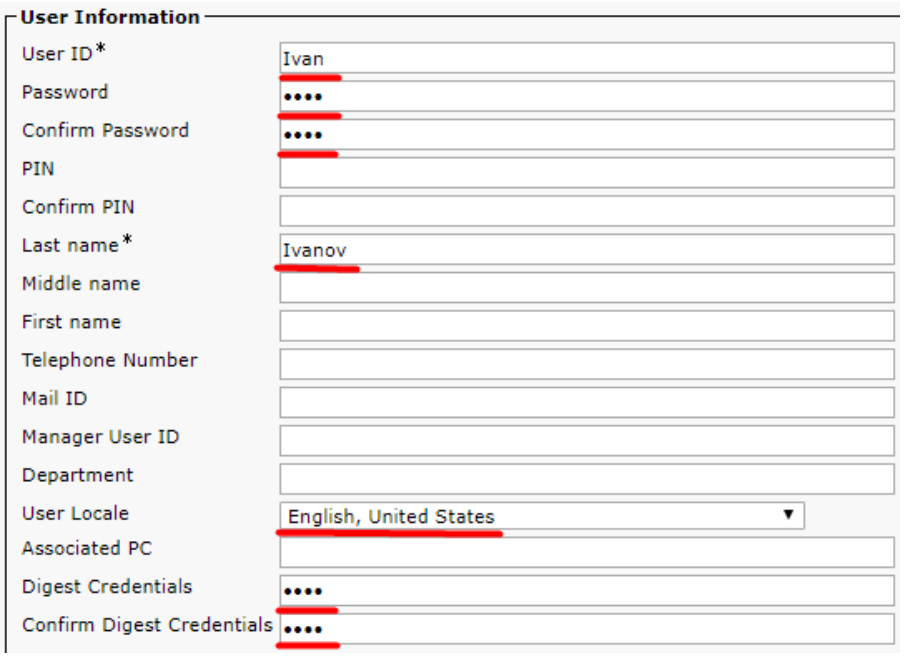


Рисунок 96 – Раздел User information

4. В разделе **Extension Mobility** (Рисунок *97*) в поле **SUBSCRIBE Calling Search Space** – выберите *CSS1*.

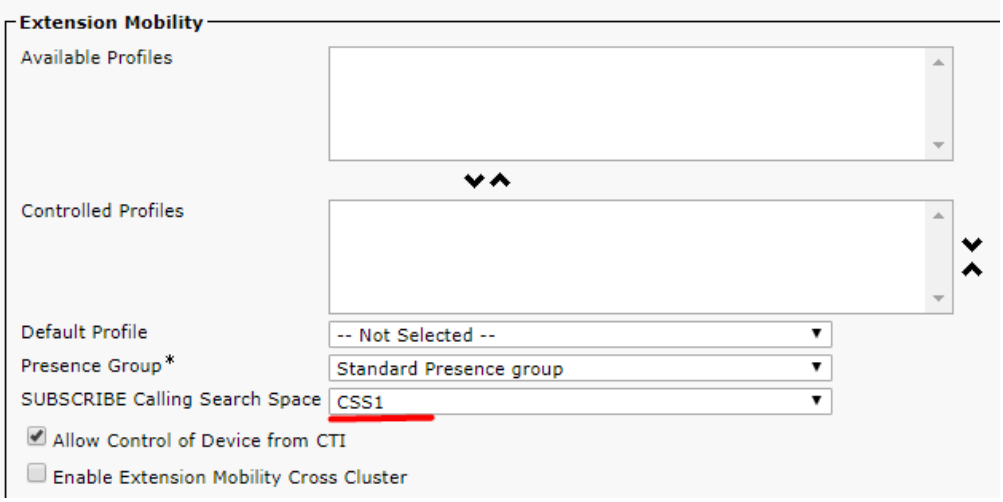


Рисунок 97 – Раздел Extension Mobility

5. Нажмите кнопку **Save**.
6. В разделе **Permissions Information** нажмите кнопку **Add to User Group**.
7. В открывшемся окне **Finde and List User Groups** (Рисунок *98*)в поле фильтра нажмите клавишу **Enter** для отображения групп, в списке выберите **Standard CCM End Users** и нажмите кнопку **Add Selected.**

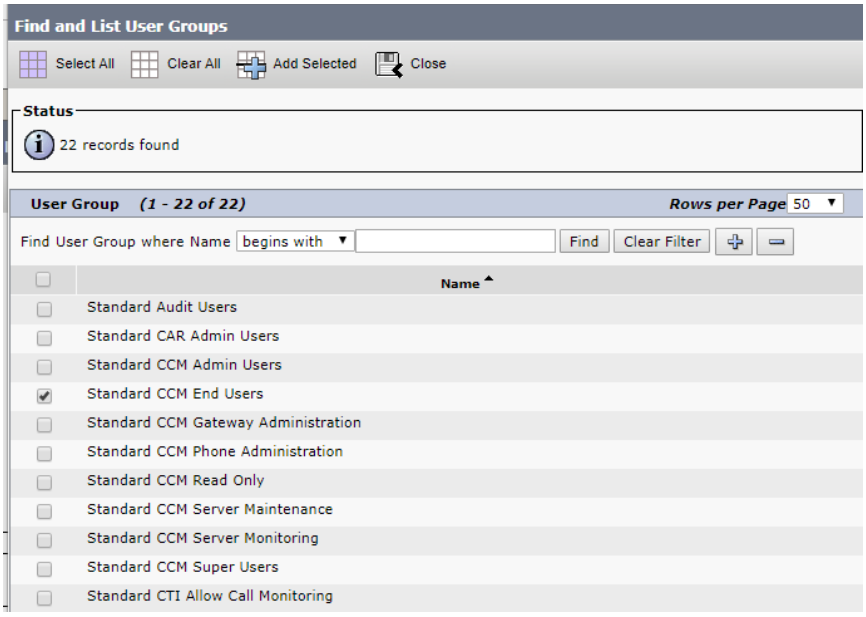


Рисунок 98 – Вид окна **Finde and List User Groups**

8. Нажмите кнопку **Save**.

9.8.2 Создание устройства

1. В главном окне CUCM перейдите на вкладку **Device > Phone** и нажмите кнопку **Add new**.
2. В открывшемся окне (Рисунок *99*) в поле **Phone Type** выберите *Third-party SIP Device (Advanced)* и нажмите кнопку **Next**.

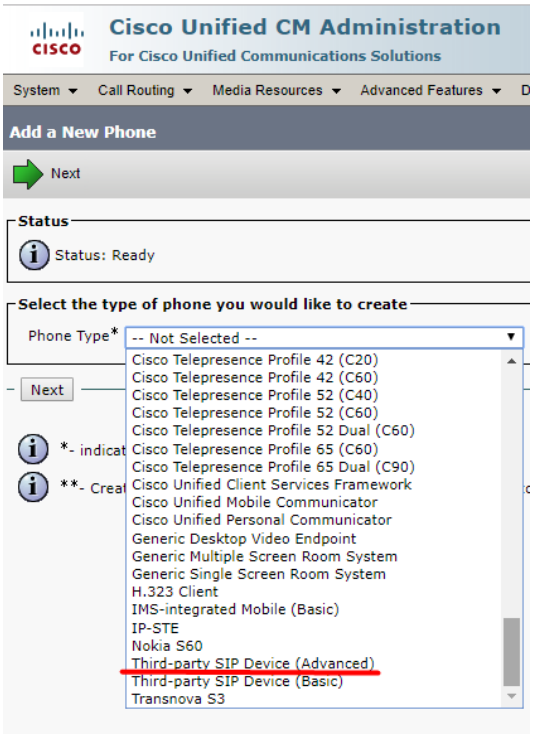


Рисунок 99 – Вид окна Add a new phone

3. В открывшемся окне **Phone Configuration** внесите информацию в разделы, описанные ниже.
4. В разделе **Device Information** заполните следующие поля (рРисунок *100*):

- **MAC Address** – введите MAC-адрес GM-Box, указанный на задней панели устройства (12 символов)
- **Description** - введите краткое описание устройства
- **Device Pool** - выберите *Default*
- **Phone Button Template** – выберите *Third-party SIP Device (advanced)*
- **Calling Search Space** – выберите *CSS1*
- **AAR Calling Search Space** – выберите *CSS1*
- **Owner User ID** - выберите созданного пользователя
- **Calling Party Transformation CSS** – выберите *CSS1*

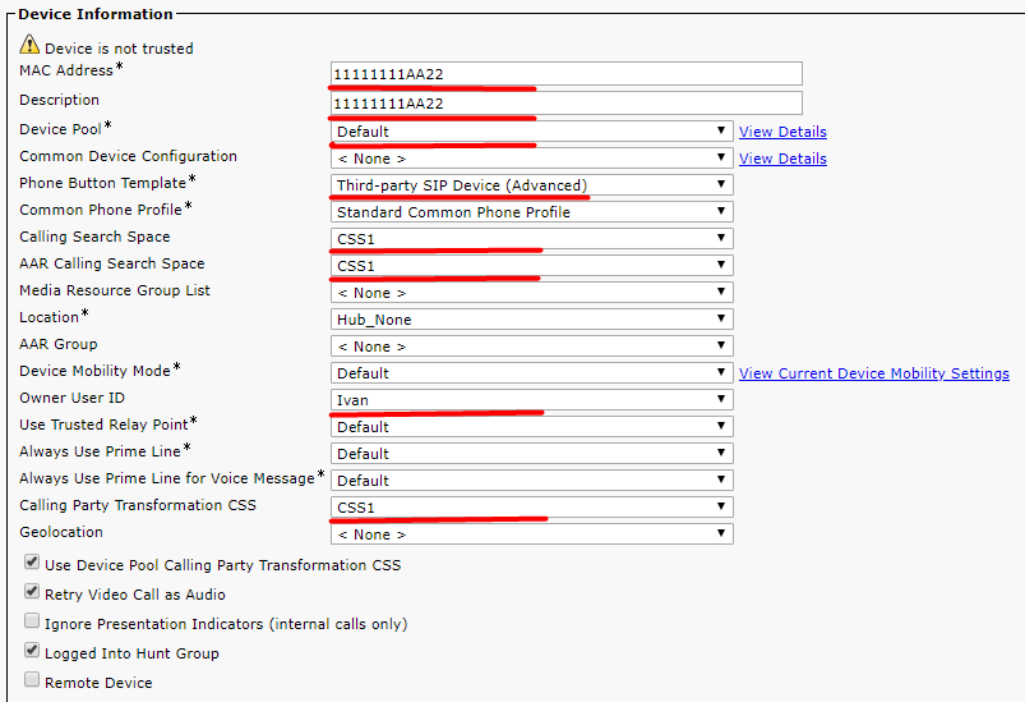


Рисунок 100 – Раздел Device information

5. В разделе **Protocol Specific Information** заполните следующие поля (Рисунок *101*):

- **Device Security Profile** – выберите *Third-party SIP Device Advanced – Standard SIP Non-Secure Profile*
- **SIP Profile** – выберите *Standard SIP Profile*
- **Digest User** – выберите созданного пользователя.

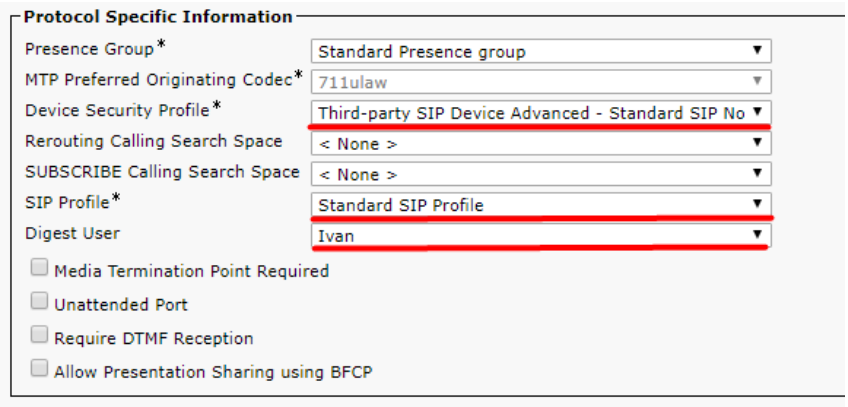


Рисунок 101 – Раздел Protocol Specific Information

6. Нажмите кнопку **Save**. Убедитесь, что следующее окно не содержит сообщений об ошибке. При необходимости исправьте их. Для применения изменений нажмите **OK**.

7. Для присвоения устройству внутреннего номера в разделе **Association Information** нажмите **Line[1] – Add a new DN** (Рисунок *102*).

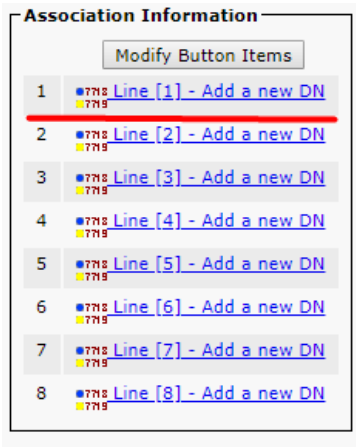


Рисунок 102 – Раздел Association Information

8. В открывшемся окне в разделе **Directory Number Infromation** заполните следующие поля (Рисунок *103*):

- **Directory Number** - введите внутренний номер пользователя
- **Alerting Name -**
- **ASCII Alerting Name**

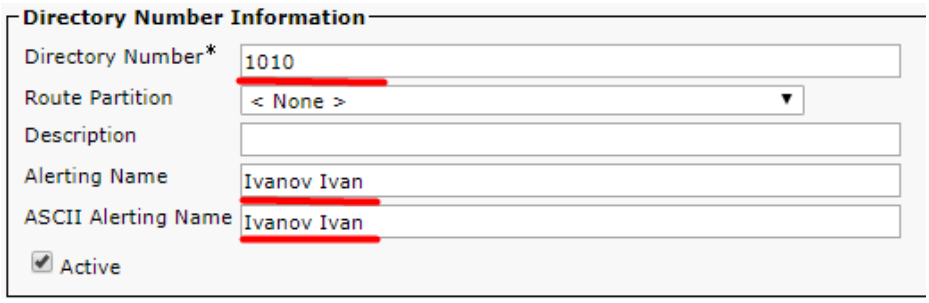


Рисунок 103 – Раздел Directory Number Infromation

9. В разделе **Directory Number Settings** заполните поля (Рисунок *104*):

- **Voice Mail Profile** – выберите *Default*
- **Calling Search Space** – выберите *CSS1*

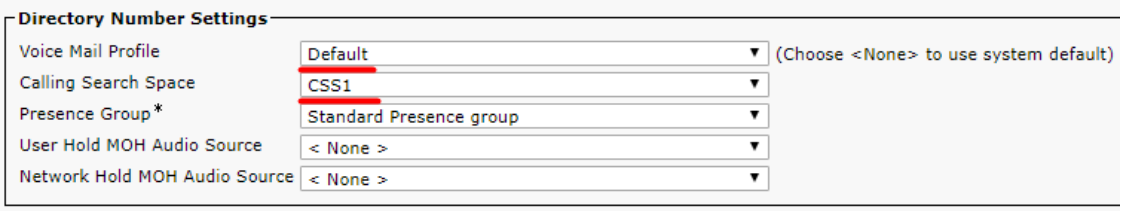


Рисунок 104 – Раздел Directory Number Settings

10. В разделе **Line 1 on Device [Description_Device]** заполните поля (Рисунок *105*):

- **Display (Internal Caller ID)**
- **ASCII Display (Internal Caller ID)** - автоматически добавляется
- **Monitoring Calling Search Space** – выберите *CSS1*

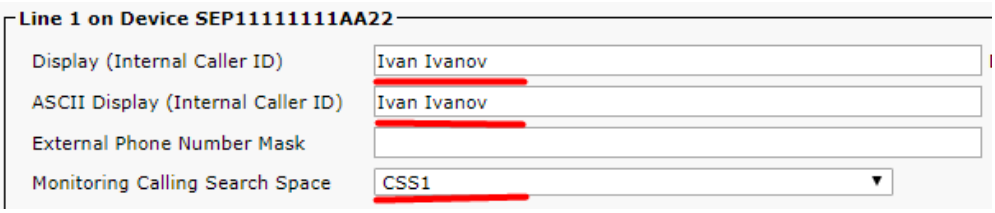


Рисунок 105 – Раздел Line 1 on Device

11. В разделе **Forwarded Call Information Display on Device [Description_Device]** отметьте чек-боксы **Caller Number**, **Redirected Number** (Рисунок 106)

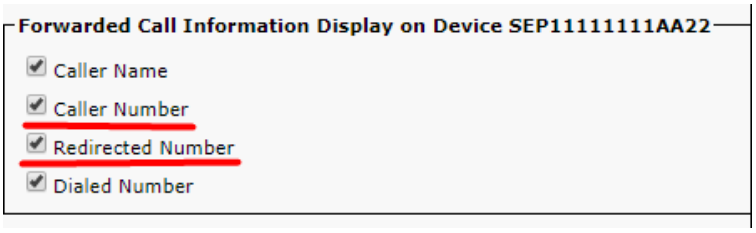


Рисунок 106 – Раздел Forwarded Call Information Display on Device

12. Нажмите кнопку **Save**. После обновления страницы в разделе **User Associated with Line** нажмите кнопку **Associate End Users**
13. В открывшемся окне в поле фильтра нажмите клавишу **Enter** для отображения пользователей, в списке выберите пользователя и нажмите кнопку **Add selected**
14. На странице конфигурирования нажмите кнопки **Save** и **Apply config**
15. В следующем окне для подтверждения изменений нажмите **OK**.

9.9 Регистрация GM-Box в Avaya Aura

Для подключения GM-Box как стороннего SIP терминала с Avaya Aura, в частности с Avaya Aura Session Manager (далее – SM), используется Avaya Aura System Manager.

Внимание! *В случае выделения сервиса IP-телефонии в отдельный VLAN (voice VLAN), необходимо обеспечить функционирование сервиса DHCP и трансляцию DNS в voice VLAN.*

Для подключения выполните следующие действия, описанные ниже.

1. Подключитесь к серверу управления Avaya Aura System Manager (Рисунок *107*) с правами администратора системы по адресу **https://<ip-address>/SMGR**, где <**ip-address**> – это IP-адрес System Manager.

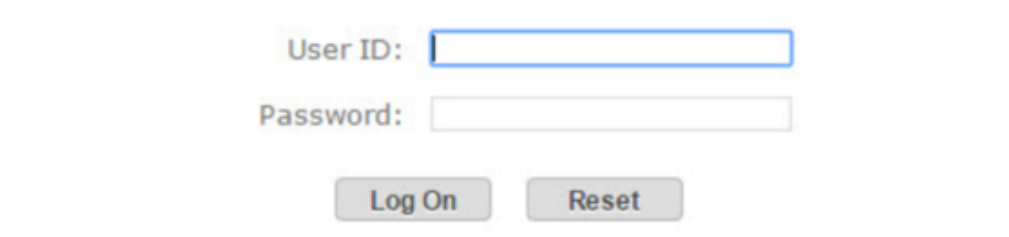


Рисунок 107 – Авторизация в системе Avaya Aura System Manager

После подключения откроется страница, содержащая разделы меню (Рисунок *108*).

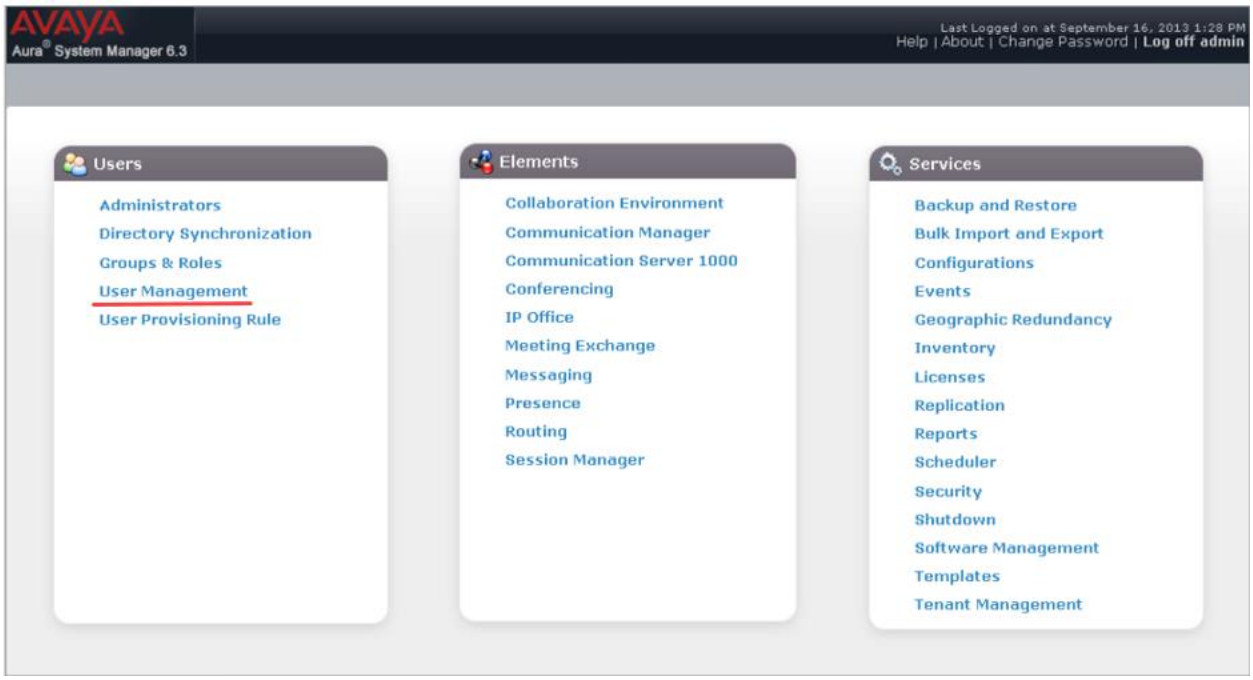


Рисунок 108 – Стартовая страница Avaya Aura System Manager

2. Для добавления нового пользователя в разделе **Users** выберите меню **User management**. На открывшейся странице выберите меню **Manage Users** и нажмите кнопку **New** (Рисунок *109*).

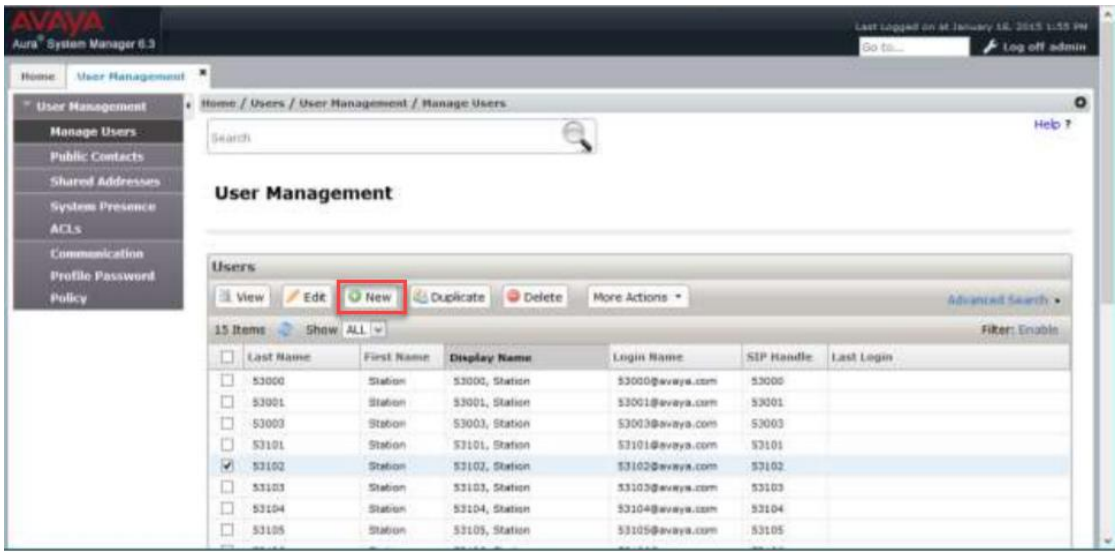


Рисунок 109 – Меню Manage Users

3. На вкладке **Identity** заполните следующие поля учетной записи пользователя (Рисунок *110*):

- **Last Name** - фамилия пользователя;
- **Last Name (Latin Translation)** - фамилия пользователя латинскими буквами;
- **First Name** - имя пользователя;
- **Login Name** - логин пользователя с использованием домена (например, 5555@avaya.ru);
- **Authentication type** – выберите тип аутентификации *Basic*.

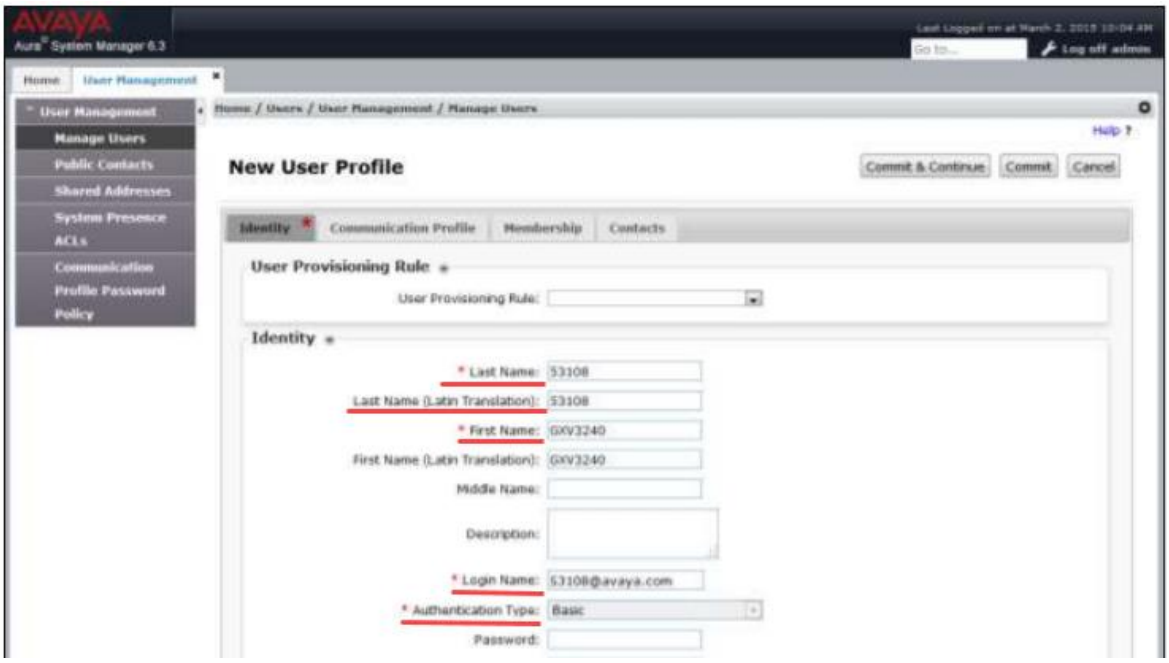


Рисунок 110 – Вкладка **Identity**

4. Перейдите на вкладку **Communication Profile**. Задайте пароль в поле **Communication Profile Password** и подтвердите его (Рисунок 111).

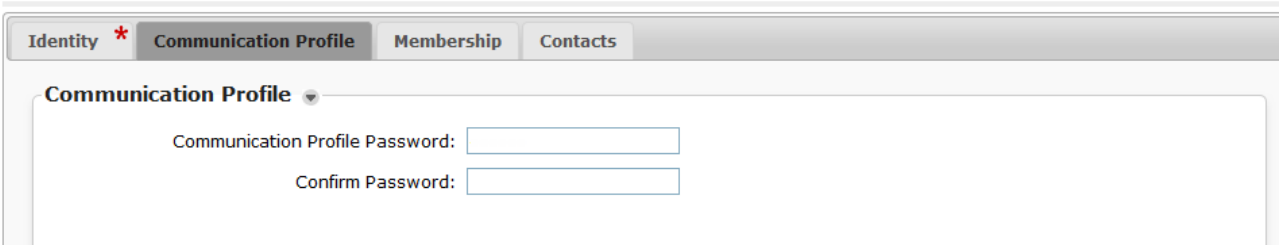


Рисунок 111 – Вкладка *Communication Profile*

5. Во вкладке **Communication Profile** в секции **Communication Address** нажмите кнопку **New** и заполните следующие поля (Рисунок 112):

- **Type** – выберите тип подключения *Avaya SIP;*
- **Fully Qualified Address** – введите логин с указанием домена SIP (аналогичный тому, что был указан на вкладке **Identity**).

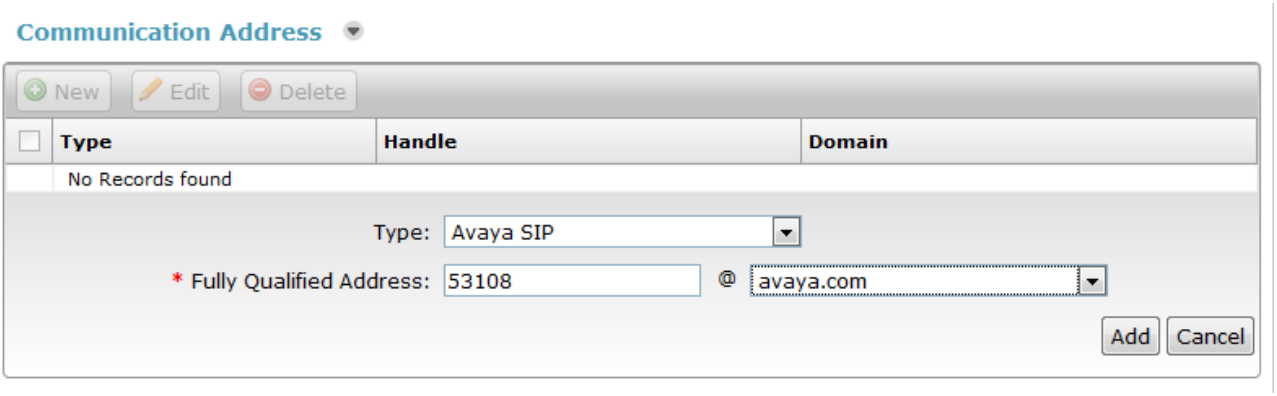


Рисунок 112 – секция *Communication Address*

6. Затем нажмите кнопку **Add**.
7. На вкладке **Communication Profile** установите флажок слева от наименования секции **Session Manager Profile** и заполните следующие поля (Рисунок 113):

- в разделе **SIP Registratration**:
  - **Primary Session Manager** – укажите основной сервер Avaya Aura Session Manager;
  - **Secondary Session Manager** – укажите вторичный сервер Avaya Aura Session Manager;
- в разделе **Application Sequences**:
  - **Origination Sequence** – укажите *Origination Sequence* или оставьте поле пустым;

- **Termination Sequence** - укажите *Termination Sequence* или оставьте поле пустым;

- в разделе **Call Routing Settings**:
  - **Home Location** – укажите домашнее расположение GM-Box.

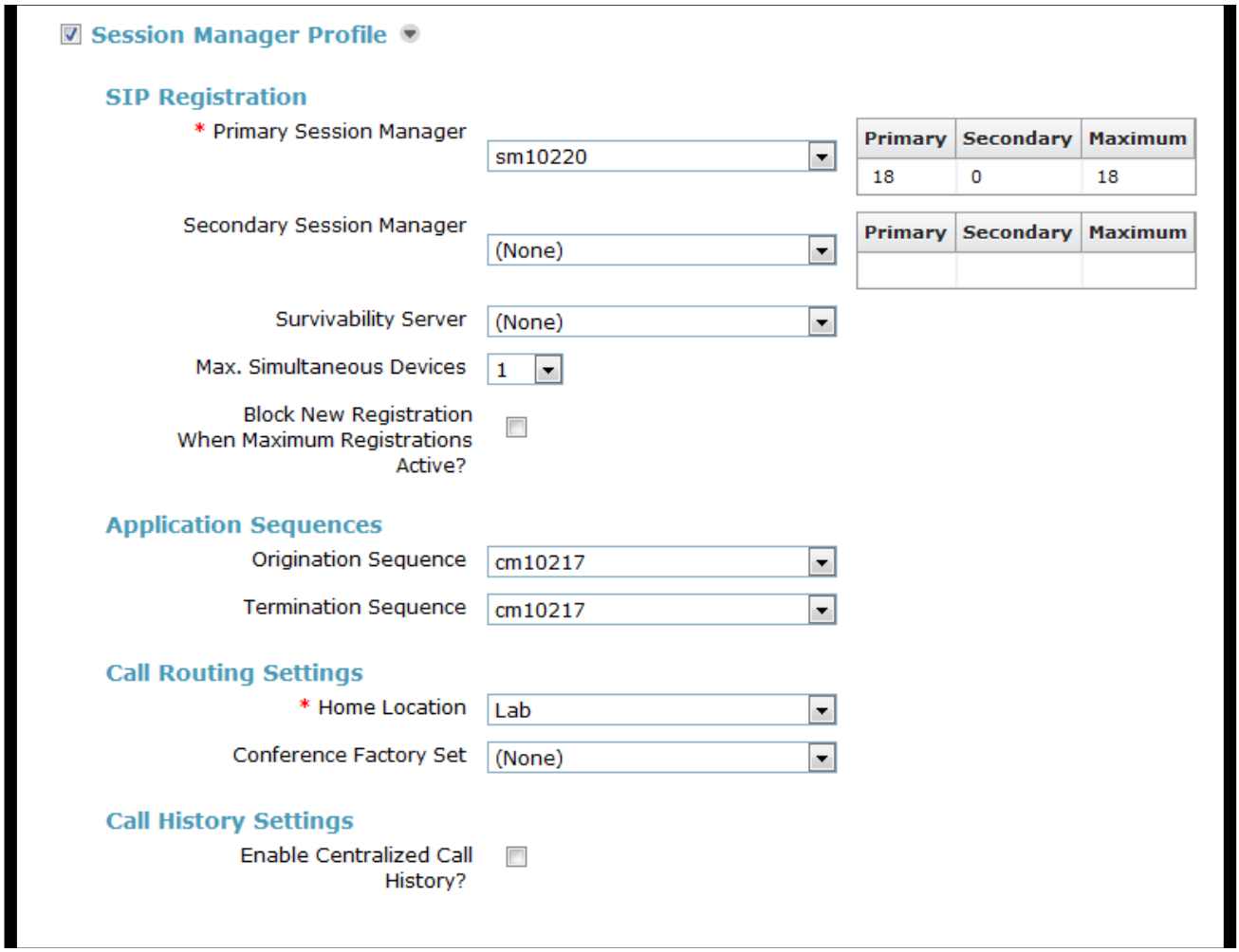


Рисунок 113 – Вкладка Communication Profile

8. На вкладке **Communication Profile** перейдите в секцию **CM Endpoint Profile**. Если между Avaya Aura Communication Manager и Avaya Aura Session Manager настроена маршрутизация, снимите флажок слева от названия секции **CM Endpoint Profile**.
   Если требуется использование маршрутизации Avaya Aura Communication Manager для связи между аппаратами, оставьте флажок слева от названия секции **CM Endpoint Profile** и заполните следующие поля (Рисунок *114*):

   - **System** - укажите *cm10217* или ваш сервер Communication Manager;
   - **Profile Type** - выберите *Endpoint*;
   - **Extension** – введите телефонный номер пользователя GM-Box;

- **Template** – выберите профиль *9641SIP_DEFAULT_CM_6_3* или аналогичный;
- **Security Code** - укажите код безопасности для GM-Box;
- **Voice Main Number** – при наличии укажите номер голосовой почты.

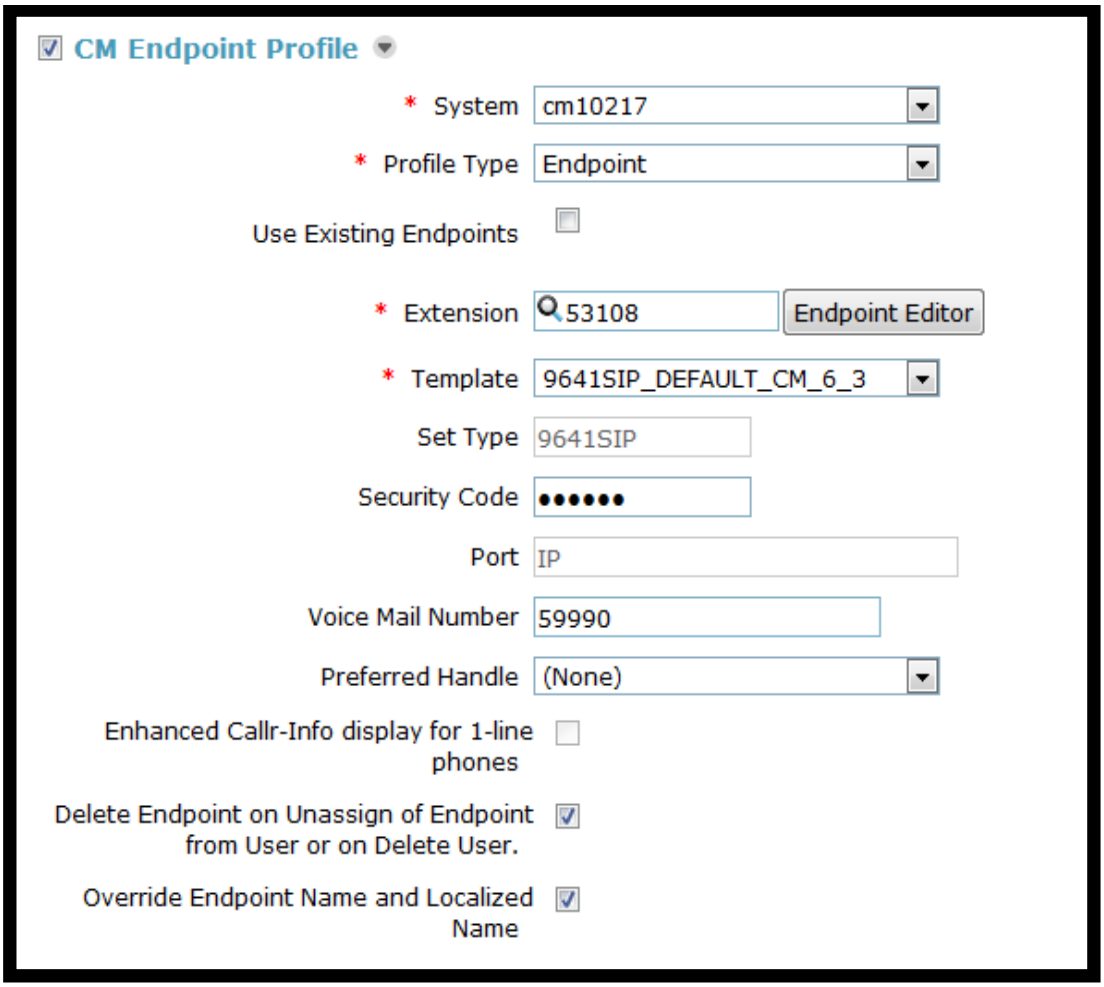


Рисунок 114 – Секция CM Endpoint Profile

9. Для сохранения настроек нажмите кнопку **Commit**.

9.10 Настройка записи голосового трафика

Запись голосового трафика осуществляется посредством настройки доступных сервисов на стороне IP-АТС, что позволяет осуществлять запись и хранение разговоров централизованно, что особенно важно для пользователей, работающих удаленно на устройствах GM-Box.

Проконсультируйтесь с разработчиком IP-АТС для уточнения возможности реализации записи голосового трафика и требуемых настроек.

10 Настройка удаленного подключения

Управляемые устройства могут быть настроены для удаленного подключения несколькими способами:

1) через СУ (требуется первичное подключение устройства к СУ в интранет);
2) удаленно с использованием сервиса GDS;
3) с использованием заранее подготовленного и записанного на USB носитель конфигурационного файла в режиме GDS-USB.

10.1 Настройка удаленного подключения

В состав ПО GM CORE KIT входят предустановленные средства криптозащиты информации (VPN и TLS клиенты). Поддержка VPN подключений для GMSS NG Client будет доступна в следующих релизах ПО.

Настройка управляемого устройства, например GM-Box, для удаленного подключения может быть выполнена двумя основными способами:

1. Установкой конфигурации на управляемое устройство через СУ.
Доставка конфигурации с использованием сервиса GDS (Global Discovery Service, более подробно – см. «Руководства Администратора GM Smart System: GM GDS Config Provider).

Доступные способы настройки удаленного подключения, в зависимости от выбранного средства криптозащиты информации, представлены в Таблица *13*.

Таблица 13 – Способы настройки удаленного подключения

	OpenVPN	**TLS**	**ViPNET**
GMSS NG Factory	✓	✓	x
GDS - Online	✓	✓	Не рекомендуется
GDS – USB	✓	✓	✓

✓ *- способ настройки доступен,* **x** *– способ настройки недоступен*

Установка конфигурации через Сервер управления требует первичного подключения управляемого устройства к инфраструктуре предприятия и Системе управления.

Доставка конфигурации с использованием сервиса GDS может быть выполнена на устройстве удаленно и не требует его предварительной настройки в инфраструктуре предприятия.

Внимание! *Доставка конфигурационного файла ViPNET через публичные сети не допускается.*

Описание настройки подключения с использованием OpenVPN и TLS через Систему управления приведено далее в разделах (10.2) и (10.4).

10.2 Создание защищенного соединения с использованием OpenVPN

Внимание! *Если используется файл с учетными данными, то первой выполняется задание на базе команды Add OpenVPN Auth file, а после ее выполнения – Add VPN config file.*

1. В веб-консоли создайте задание (п. 5.11.1) на выполнение команды Add VPN config file **(*.ovpn, *.conf)** и загрузите файл конфигурации VPN-соединения (файл с расширением .ovpn или .conf).
   Если для подключения к VPN требуется логин/пароль, то:
   - создайте файл с учетными данными, например, *credentials.txt* (имя файла может быть любым). В файле укажите логин и пароль
   - в конфигурационном задайте использование файла с учетными данными: auth-user-pass credentials.txt
   - в веб-консоли создайте задание на выполнение команды **Add OpenVPN Auth file (*.txt)** и загрузите файл с учетными данными credentials.txt.
2. У пользователя GM-Box на экране приветствия GM-Box (Рисунок *115*) для перехода в раздел настроек нажмите пиктограмму  и выберите **VPN**. Включите использование доступных настроек. Дождитесь применения настроек до появления пиктограммы ✓.

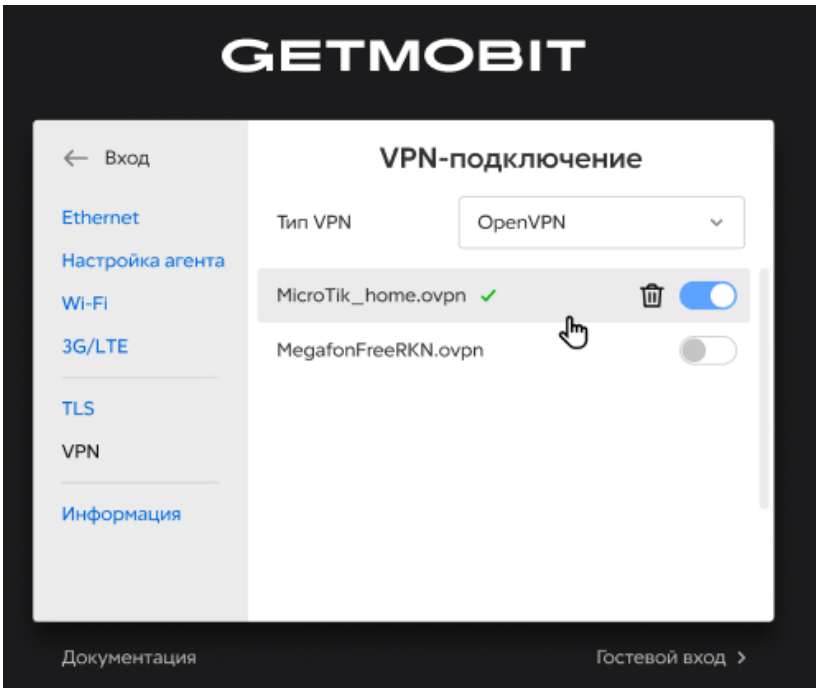


Рисунок 115 – Защищенное соединение с использованием OpenVPN

3. Затем отключите возможность редактирования пользователем настроек VPN-соединения (пользователю будут недоступны для редактирования параметры на вкладке **VPN**). Для этого в конфигурационном файле *greeter.conf* в параметре **VPN** установите следующие значения:

```
{
	"pluginName": "vpn",
	"isEnabled": true,
	"isUsable": false
}
```

4. Обновленный конфигурационный файл *greeter.conf* необходимо применить на устройстве. Для этого в веб-консоли создайте задание (п. 5.11.1) на выполнение команды **Patch config Greeter (greeter.conf)**.

Пример конфигурационного файла сервера OpenVPN:

```
proto tcp
dev tun1
server IP MASK # указать адрес и маску сервера
ca /etc/openvpn/certs/ca.crt #путь к CA
cert /etc/openvpn/certs/server.crt # путь к сертификату сервера
key /etc/openvpn/certs/server.key #путь ко ключу сервера
dh /etc/openvpn/certs/dh2048.pem #путь к файлу сертификата по DH
push "route NETWORK1 MASK1" #анонсируемые через клиент сети
push "route NETWORK2 MASK2"
```

```
push "dhcp-option DNS IP" #анонсируемый через клиент адрес DNS сервера
push "dhcp-option DOMAIN domain.sample" #анонсируемый через клиент домен
push "block-outside-dns" #блокировка использования внешнего DNS при подключении
через VPN
port PORT #порт для подключения к серверу
client-to-client #разрешение трафика между клиентами
keepalive 10 120 #время жизни подключения
verb 4 #уровень логирования
max-clients 10 #указываем максимальное количество подключенных к серверу
клиентов
duplicate-cn #разрешаем подключения с одинаковым общим именем
```

Пример конфигурационного файла клиента OpenVPN:

```
client
remote IP #публичный адрес сервера OpenVPN
port PORT #публичный порт сервера OpenVPN
dev tun
proto tcp #транспортный протокол
verb 3 #уровень отладки
script-security 2 system
up /etc/openvpn/update-resolv-conf #обновление resolv-conf
down /etc/openvpn/update-resolv-conf

<ca>
-----BEGIN CERTIFICATE-----
В ЭТОТ БЛОК НЕОБХОДИМО СКОПИРОВАТЬ СЕРТИФИКАТ
-----END CERTIFICATE-----
</ca>
<cert>
Certificate:
   Data:
      Version: 3 (0x2)
      Serial Number:
         #СЕРИЙНЫЙ НОМЕР
      Signature Algorithm: sha256WithRSAEncryption #указано в качестве примера
      Issuer: CN=sysadmin #указано в качестве примера
      Validity
         Not Before: Sep 32 10:00:00 2020 GMT #указано в качестве примера
         Not After : Sep 32 10:00:00 2023 GMT #указано в качестве примера
      Subject: CN=client1 #указано в качестве примера
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption #указано в качестве примера
            RSA Public-Key: (2048 bit) #указано в качестве примера
            Modulus:
   УКАЗЫВАЕТСЯ СПЕЦИФИЧЕСКОЕ ЗНАЧЕНИЕ ДЛЯ ИНСТАЛЛЯЦИИ
```

```
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE  #указано в качестве примера
            X509v3 Subject Key Identifier:
    УКАЗЫВАЕТСЯ СПЕЦИФИЧЕСКОЕ ЗНАЧЕНИЕ ДЛЯ ИНСТАЛЛЯЦИИ
            X509v3 Authority Key Identifier:
    УКАЗЫВАЕТСЯ СПЕЦИФИЧЕСКОЕ ЗНАЧЕНИЕ ДЛЯ ИНСТАЛЛЯЦИИ
                DirName:/CN=sysadmin
    УКАЗЫВАЕТСЯ СПЕЦИФИЧЕСКОЕ ЗНАЧЕНИЕ ДЛЯ ИНСТАЛЛЯЦИИ
            X509v3 Extended Key Usage:
                TLS Web Client Authentication
            X509v3 Key Usage:
                Digital Signature
    Signature Algorithm: sha256WithRSAEncryption
    УКАЗЫВАЕТСЯ СПЕЦИФИЧЕСКОЕ ЗНАЧЕНИЕ ДЛЯ ИНСТАЛЛЯЦИИ
-----BEGIN CERTIFICATE-----
В ЭТОТ БЛОК НЕОБХОДИМО СКОПИРОВАТЬ СЕРТИФИКАТ
-----END CERTIFICATE-----
</cert>
<key>
-----BEGIN PRIVATE KEY-----
В ЭТОТ БЛОК НЕОБХОДИМО СКОПИРОВАТЬ СЕРТИФИКАТ
-----END PRIVATE KEY-----
</key>
```

10.3 Создание защищенного удаленного соединения с использованием ViPNET

Для создания удаленного подключения с использованием ViPNET, в инфраструктуре должен быть установлен и настроен ViPNET координатор и сгенерирован DST файл для подключаемого устройства.

Загрузка DST файла на устройство и инициализация ViPNET клиента возможна с использованием сервиса GDS. Для этого необходимо подготовить GDS архив.

GDS Archive упаковывается и передается через онлайн сервис GDS или на USB носителе в архиве в формате 7z.

Формат контейнера. Архив в формате 7z, с методом сжатия LZMA2 без использования технологии SFX.

Шифрование данных. Шифрование данных, при необходимости, осуществляется средствами 7z (AES 256), но с ограничением на "шифрование имен файлов" (т.е. заголовка 7z-архива).

Наименование. Имя пакета настроек задается в зависимости от способа доставки GDS архива. Если доставка настроек осуществляется с USB-накопителя, имя файла должно быть строго **gmbox-config.7z**, а в случае получения настроек с сервера GDS, имя формируется из произвольной последовательности чисел, символов латинского алфавита, в нижнем регистре, разделителей '_' и '-' и постфиксом '.7z'.

Расположение при передаче на USB носителе. Пакет настроек должен быть в корне файловой системы. Содержимое GDS архива представлено в Таблица 14.

Таблица 14 – Содержимое GDS архива

Наименование файла	Содержимое файла
gmserver.url	**[http[s]://]<FQDN или IP>[:<Порт>][/]** Указывает URL сервера управления. Если не указан протокол, по умолчанию используется http
*.dst	Конфигурация ViPNet, защищенная паролем
vipnet_secret.txt	**Необязательный файл** Состоит из одной строки, в которой указан пароль от учетной записи VPN ViPNet

Все файлы располагаются в корне архива

10.4 Создание защищенного удаленного соединения TLS VPN между GM-Box и сетевой инфраструктурой.

Для безопасного подключения удаленных устройств через сеть Интернет в информационную систему компании с использованием российских криптографических алгоритмов используется технология TLS-туннелирования сетевого трафика (Рисунок *116*).

Для построения TLS-туннеля используется программа stunnel, входящая в состав сертифицированного СКЗИ «КриптоПро CSP 4.0», предустановленного в GM CORE KIT.

Совместимость TLS-туннеля с другими решениями российских разработчиков средств криптографической защиты информации (см. https://www.cryptopro.ru/) соответствует стандарту ТК26 TLS (https://www.cryptopro.ru/blog/2014/07/07/metodicheskie-rekomendatsii-tk-26-algoritmy-sertifikaty-cms-tls).

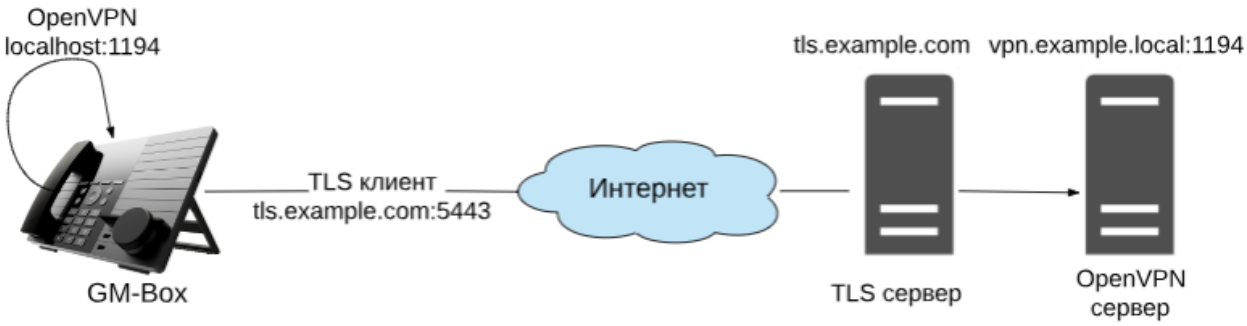


Рисунок 116 – Схема подключения с использованием технологии TLS-туннелирования

Для туннелирования в TLS соединении и дальнейшей маршрутизации сетевого трафика от GM-Box до инфраструктуры информационной системы используется ПО OpenVPN без использования алгоритмов шифрования. Информация об установленном в GM CORE KIT клиенте OpenVPN приведена в документе «Требования к инфраструктуре» и Информационных бюллетенях (Release notes) к выпускаемым версиям ПО. Пример настройки OpenVPN приведен в (п.10.2).

ПО stunnel принимает весь сетевой трафик с OpenVPN клиента на localhost-порт, шифрует и отправляет на удаленный TLS-сервер, где он расшифровывается и перенаправляется на OpenVPN-сервер, где далее маршрутизируется согласно конфигурации.

Рассмотрим настройку TLS-туннеля.

10.4.1 Требования

Для создания TLS-туннеля, выполните действия, описанные ниже.

1. В сетевой инфраструктуре компании должна быть развернута инфраструктура PKI с поддержкой российских криптографических алгоритмов (например, КриптоПро CSP 4.0), или должен использоваться аккредитованный УЦ.
2. Точка распространения списка отзывов сертификатов (CRL или OCSP) должна быть доступна через сеть Интернет.
3. Ссылка на скачивание CRL/ OCSP должна быть в сертификате (необходимо указать российский объектный идентификатор OID).

10.4.2 Настройка сервера TLS

Настройка сервера выполняется в соответствии с документацией производителя (https://www.cryptopro.ru/products/csp/tls).

1. Создайте запрос на сертификат проверки подлинности сервера и заполните все поля. Значение в поле **Имя** (Common Name, CN) должно соответствовать FQDN и совпадать с именем хоста сервера (например, tls.getmobit.ru).
2. Установите на сервере в хранилище CA TLS корневой сертификат УЦ и сертификаты всех подчиненных УЦ.
3. Если требуется двусторонняя аутентификация с проверкой по белому списку (клиент проверяет сервер, сервер проверяет клиента) TLS-сертификат на GM-Box (сертификат клиента) должен быть добавлен в список доверенных пользователей. Например, сертификат на TLS-сервер, работающий под управлением stunnel КриптПро CSP, должен быть добавлен в хранилище TrustedUsers пользователя.

```
root@server:~/# /opt/cprocsp/bin/amd64/certmgr -inst -file user_gm_box_id.crt
-store TrustedUsers
```

***Примечание**. Подробнее смотрите в документации по настройке вашего TLS-сервера.*

10.4.3 Настройка GM-Box

1. Создайте запрос на выпуск сертификата проверки подлинности клиента.
2. Создайте ключевой контейнер с пустым паролем на отчуждаемом носителе USB Flash Drive.
3. Выданный сертификат установите в ключевой контейнер.
4. В веб-консоли создайте задание (п. 5.11.1) на загрузку файла с сертификатом УЦ и сертификатами всех подчиненных УЦ на GM-Box с использованием команды **Install stunnel CA certificate (root.crt)**.

Уровень проверки сертификата TLS-сервера задается в соответствии с документацией на программу stunnel:

- 0 — игнорировать сертификат;
- 1 — проверять наличие сертификата;
- 2 — проверять валидность сертификата;
- 3 — проверять валидность и наличие сертификата в хранилище TrustedUsers.

5. Для задания уровня проверки сертификата создайте конфигурационный файл ***additional.ini*** следующего вида:

```
[Stunnel]
```

```
VerifyLevel=3
```

6. В веб-консоли создайте задание (п. 5.11.1) на выполнение команды Patch config TLS (**additional.ini)** и загрузите созданный конфигурационный файл ***additional.ini***.
7. У пользователя на экране приветствия GM-Box для перехода в раздел настроек нажмите пиктограмму  и выберите **TLS** (Рисунок *117*).
8. Подключите USB Flash Drive с ключевым контейнером КриптоПро к GM-Box. Откроется окно для настроек TLS-соединения.

Внимание!

Во избежание ошибок подключайте USB Flash Drive с ключевым контейнером КриптоПро после появления на мониторе приглашения для входа в систему.

9. Задайте в поле **Адрес сервера** адрес и порт TLS-сервера, в поле **Порт** – локальный порт, который используется ПО stunnel (локальный порт должен совпадать с портом, заданным в файле конфигурации OpenVPN клиента).
10. Для просмотра информации об установленном сертификате нажмите на **Установлен**.

Примечание. *В настоящее время на USB Flash Drive может быть записан только один ключевой контейнер. Ключевой контейнер КриптоПро должен быть в корне USB Flash Drive.*

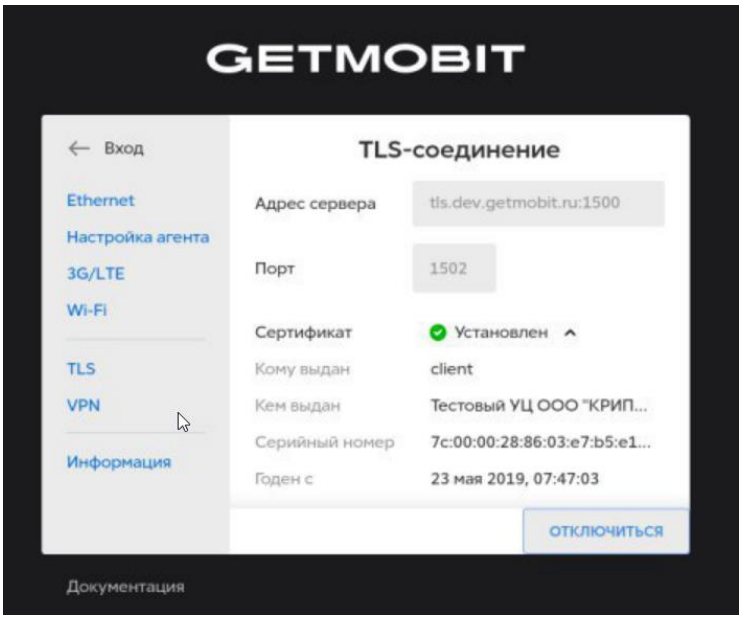


Рисунок 117 – TLS-соединение

11. Нажмите кнопку **Подключиться**
12. Настройте VPN-соединение (подраздел 12.11).

11 Диагностика и устранение неисправностей

GMSS NG предоставляет три основных инструмента для диагностики и устранения неисправностей:

1) сбор и анализ отладочной информации (логов) в сервисе мониторинга;
2) сервисный режим GM-Box;
3) режим диагностики сервера управления GMSS NG Factory.

11.1 Общие рекомендации по диагностике и устранению неисправностей

В большинстве случаев, в сданной в промышленную эксплуатацию системе, неисправности обусловлены вносимыми пользователями или администраторами изменениями в систему.

При возникновении неисправности для ее эффективной диагностики и устранения необходимо выполнить действия, описанные ниже.

1. Убедиться, что неисправность может быть воспроизведена.
2. Проверить воспроизводимость неисправности на тестовом (референсном) профиле пользователя и устройстве.
3. Оценить тип неисправности (индивидуальная – для конкретного пользователя или устройства или общая – наблюдается для группы пользователей или устройств).
4. Уточнить, вносились ли изменения в конфигурации как сервера управления и управляемых устройств, так и интегрируемых компонент.
5. Уточнить, вносились ли изменения в состав и версии ПО как сервера управления и управляемых устройств, так и интегрируемых компонент.
6. Уточнить, изменялись ли правила межсетевого взаимодействия.

Исходя из собранной информации, скорректировать настройки и параметры, вызвавшие неисправность, или провести дополнительную диагностику, в т.ч. собрать отладочную информацию.

11.2 Сбор и анализ отладочной информации (логов) в сервисе мониторинга

Для сбора диагностической информации с управляемых устройств предпочтительным вариантом сбора диагностики является использование сервиса мониторинга с включенным режимом отладки – **Debug Mode On** (Как включить режим **Debug Mode On**).

1. Включите на устройстве, на котором будет воспроизведена неисправность, режим отладки, выполнив задание на базе команды **Debug Mode On**.
2. Воспроизведите проблему.
3. Перейдите в логи устройства в Kibana. Выберите раздел **Устройства** -> найдите устройство, например, по ID или IP-адресу -> нажмите иконку перехода в Kibana (Рисунок 118)



Рисунок 118 – Кнопка перехода в Kibana

4. Добавьте фильтр (Рисунок *119*) на изучаемые процессы (например, Citrix):
   - Нажмите **+Add Filter**.
   - В поле **Field** выберите processName.
   - В поле **Operator** выберите is.
   - В поле **Values** введите значение citrix.
   - Сохраните фильтр.

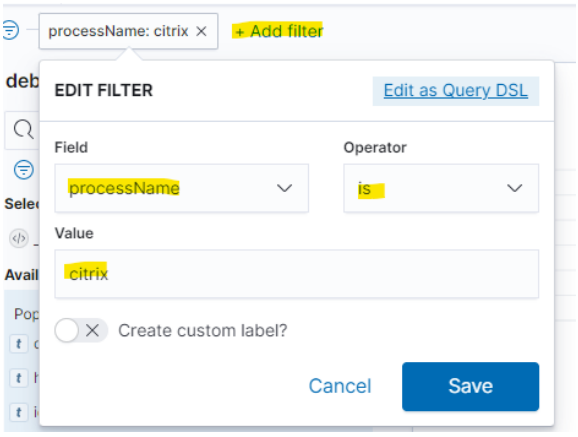


Рисунок 119 – Добавление фильтра

5. Установите временной интервал для отображения логов.

   После задания периода, будет отображен лог событий, связанных с SDApp Citrix (Рисунок *120*). Если логи не отображаются, допущена ошибка в настройках фильтрации или интервале времени. Также, возможна блокировка сетевых портов для передачи данных в сервис журналирования (см. GM Smart System New Generation. Требования к инфраструктуре).

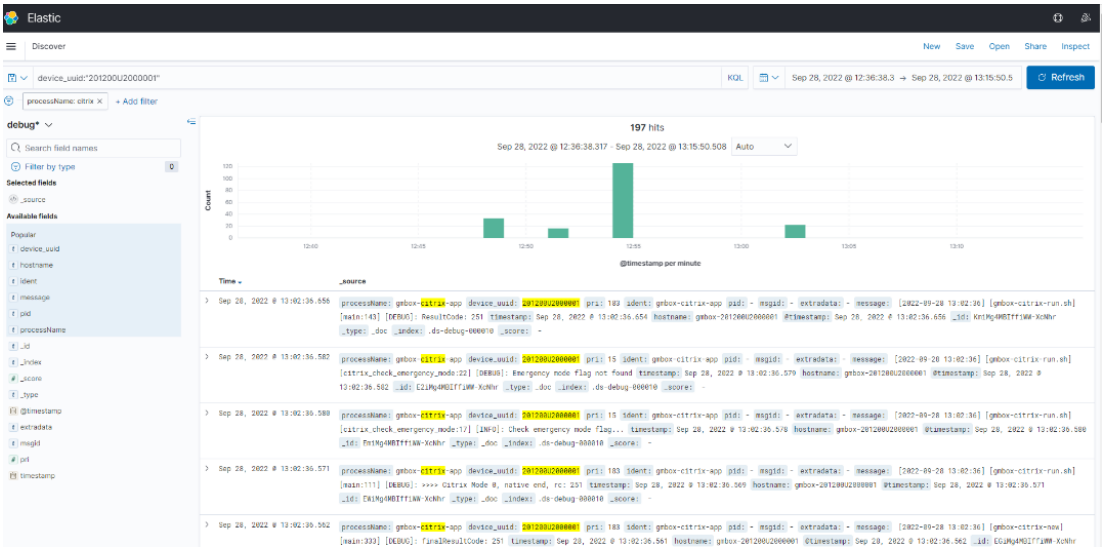


Рисунок 120 – Отображение лога событий с SDApp Citrix

6. После сбора диагностической информации выключите на устройстве режим отладки, выполнив задание на базе команды **Debug Mode Off**.

11.3 Сервисный режим GM-Box

Для выполнения некоторых операций, например, снять дамп траффика с GM-Box, потребуется доступ к консоли устройства. По умолчанию такой доступ отсутствует.

Для получения доступа к консоли устройства выполните действия, описанные ниже.

1. В веб-консоли выберите раздел **Приложения**.
2. Нажмите **Добавить**.
3. Создайте задание (5.11.1) для установки приложения ServiceMode.
4. Проверьте, что приложение установилось (Рисунок *121*).

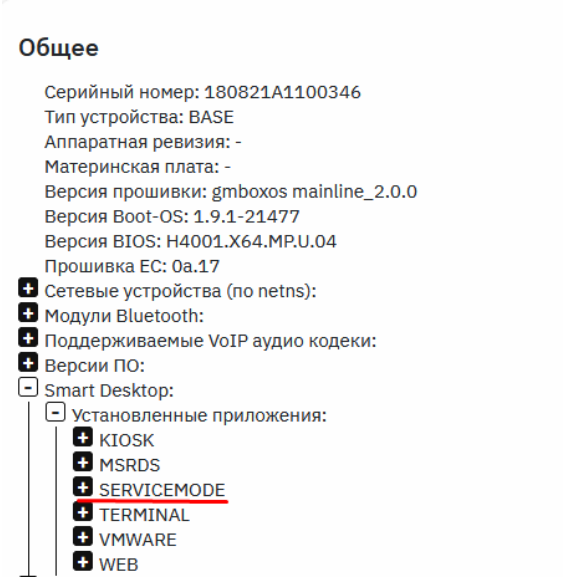


Рисунок 121 – Установка приложения ServiceMode

5. Создайте задание (5.11.1) с командой **ServiceMode**.

Если команды на сервере нет, потребуется создать ее вручную:

```
Наименование: Service Mode Тип: SYSTEM Команда: (cmd "enable-service-mode")
```

Теперь вместо любой сессии запускается **ServiceMode**.

11.3.1 Справка по командам сервисного режима

Для получения справки по доступным командам сервисного режима запустите в терминале команду help <команда>, например:

```
help <net-cat>
```

Примерный результат вывода команды **help net-cat**:

```
help net-cat
"net-cat <address> <port>: command tests the connection, <address> - destination IP-address, <port> - destination port
```

11.3.2 Пример использования команды net-cat для проверки доступности подключения по какому-либо порту

Запустите в терминале команду net-cat. Используйте синтаксис:

```
net-cat <adress> <port>
```

Например, net-cat 172.16.113.35 80.

11.3.3 Пример использования команды dump-tcp и save-logs

1. Запустите в терминале команду tcp-dump. Используйте синтаксис:

```
dump-tcp <time> <file>
```

   Например, dump-tcp 60 tcpdumpvoip, где 60 - время в секундах, tcpdumpvoip - название файла.

2. Перезапустите VoIP командой restart-voip.
3. Подключите USB-накопитель к GM-Box.
4. Запустите в терминале команду save-logs для сохранения файла на USB-накопитель. Используйте синтаксис:

```
save-logs <file>
```

   Например, save-logs tcpdumpvoip.

5. Отключите Service Mode командой disable-service-mode.

   Если команды на сервере нет, потребуется создать ее вручную:

```
Наименование: Service Mode Тип: SYSTEM Команда: (cmd "disable-service-mode")
```

11.4 Режим диагностики СУ GMSS NG Factory

Режим диагностики позволяет:

- автоматизировать процесс сбора базовой информации в случае нештатной работы СУ;
- локализовать неисправность СУ и упростить процесс передачи собранной информации компетентным лицам либо компании GETMOBIT.

Для локализации ошибок нужно запустить в фоновом режиме диагностическую утилиту. Управление утилитой осуществляется в веб-консоли в разделе **Диагностика**.

Для каждой диагностической команды доступны настройки ее выполнения.

Администратор может:

- редактировать диагностические команды: добавлять, удалять шаги диагностики и менять последовательность их выполнения;

- запускать диагностику;
- отслеживать процесс выполнения диагностики;
- скачать результаты диагностики;
- установить пароль на архив с результатами диагностики.

11.4.1 Создание диагностического сценария

11.4.1.1 Добавление шага диагностики

Для добавления шага диагностики выполните следующие действия:

1. В веб-консоли выберите раздел **Диагностика**.
2. В выпадающем списке выберите одну из команд (Рисунок *122*). Команда будет добавлена в **Диагностический запуск**.
3. Укажите настройки команды.

При необходимости добавьте шаг диагностики и повторите перечисления 2, 3.

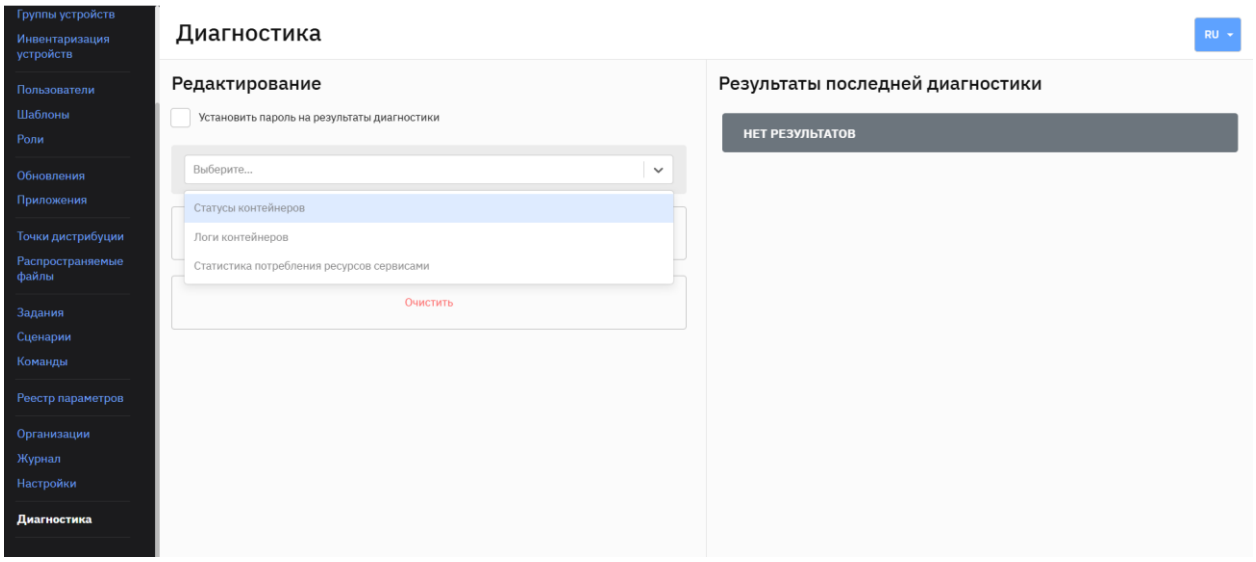


Рисунок 122 – Раздел Диагностика

Администратору доступны диагностические команды:

- **Статусы контейнеров** – отображение статусов контейнеров (запущен, остановлен);

Включение опции **Отображать остановленные контейнеры** отобразит в результатах диагностики остановленные контейнеры (Рисунок *123*).

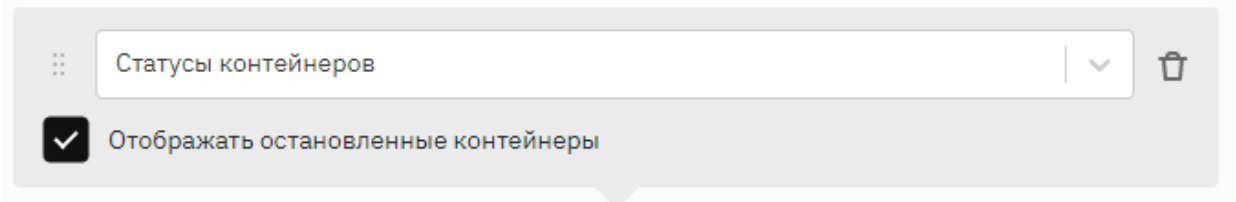


Рисунок 123 – Включение опции Отображать остановленные контейнеры

- **Логи контейнеров** – сбор диагностической информации по контейнерам. По умолчанию, собираются 1000 последних строк лог-файла.
- **Статистика потребления ресурсов сервисами** – отображение статистической информации по потреблению системных ресурсов контейнерами. По умолчанию, статистика собирается со всех контейнеров.

11.4.1.2 Изменение порядка выполнения шагов диагностики

Чтобы изменить порядок выполнения шагов, захватите команду и перетащите в нужное место.

11.4.1.3 Удаление шага диагностики

Чтобы удалить команду из списка диагностики, нажмите значок  или кнопку **Очистить**.

11.4.2 Запуск диагностики

Для запуска созданного сценария диагностики, нажмите **Запустить Диагностику**.

Результаты диагностики будут автоматически заархивированы в файл с расширением ZIP или 7z, который можно получить, нажав на кнопку **Скачать результаты диагностики** (Рисунок *124*). Так же вы можете установить пароль на скачанный архив (см. п. 11.4.4).

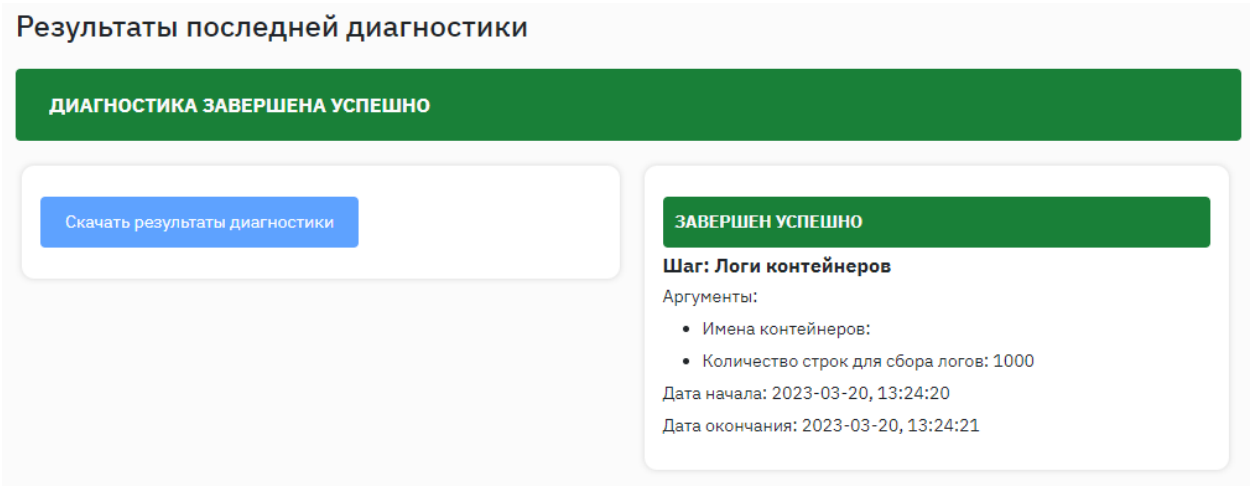


Рисунок 124 – Результат диагностики

11.4.3 Прерывание диагностического запуска

Если вы ошиблись при запуске диагностики, например, некорректно выбрали команду, нажмите кнопку **Прервать** (Рисунок *125*). После остановки будет сгенерирован архив с результатами успешно завершенных шагов, если такие имеются.

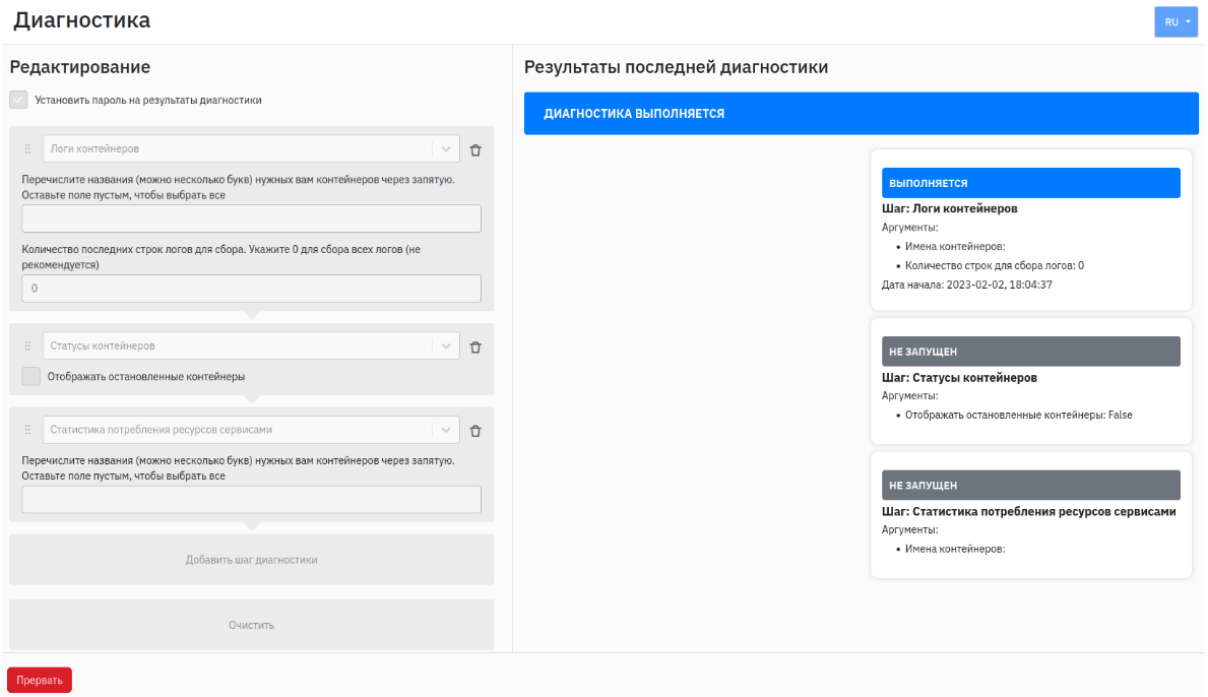


Рисунок 125 – Прерывание диагностического запуска

11.4.4 Как установить пароль на архив с результатами диагностики

Чтобы установить пароль на архив с результатами диагностики, выберите опцию **Установить пароль на результаты диагностики**.

Чтобы посмотреть пароль, после завершения диагностики под кнопкой **Скачать результаты** нажмите .

11.4.5 Отслеживание процесса выполнения диагностики

При выполнении диагностики возможны следующие статусы шагов:

- Не запущен;
- Выполняется;
- Завершен успешно.

11.5 Режим восстановления прошивки GM-Box

Примечание. *В данном подразделе приведены базовые сведения о режиме. Детальная инструкция по режиму предоставляется отдельно.*

Начиная с версии ПО GM CORE KIT 2.4.0, в состав ПО включен режим восстановления. Данный режим позволяет:

- сбросить устройство до заводских настроек;
- восстановить ПО устройства с USB Flash носителя;
- просмотреть журналы (logs) устройства;
- установить системное время;
- перезагрузить устройство.

Вход в режим восстановления осуществляется на этапе загрузки устройства. После появления на экране индикатора загрузки (прогресс-бара), необходимо нажать левую функциональную клавишу GM-Box (Рисунок *126*):



Рисунок 126 – Режим восстановления GM-Box

При успешном запуске режима восстановления, будет запрошен PIN-код для доступа к меню режима (Рисунок *127*):

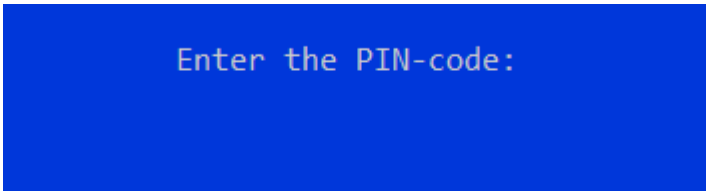


Рисунок 127 – Вид окна запроса PIN-кода

Значение PIN-кода по умолчанию ***0000*** (четыре нуля). После ввода PIN-кода, предоставляется доступ в меню режима восстановления (Рисунок *128*):

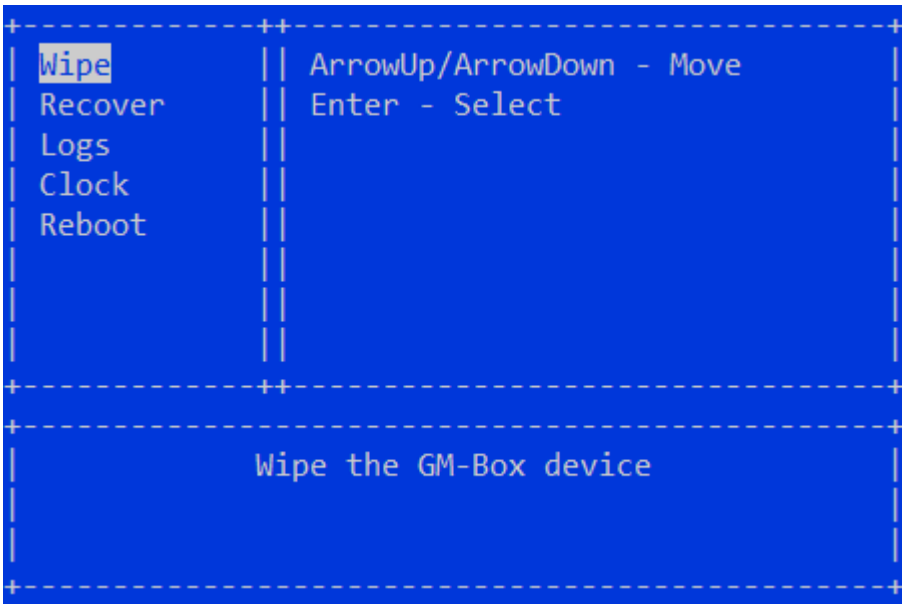


Рисунок 128 – Вид окна меню режима восстановления

11.5.1 Смена PIN-кода режима восстановления

Для смены PIN-кода режима восстановления необходимо на СУ создать команду:

Имя команды: Change recovery mode PIN
Тип команды: Configuration
Содержимое команды: ((patch-config <filename>)(cmd "rm -rf /persistent/configs/gmbox-menu/*.pin")(cmd "mkdir -p /persistent/configs/gmbox-menu/")(cmd "mv /persistent/*.pin /persistent/configs/gmbox-menu/"))

PIN-код задается в текстовом файле с расширением ***.pin***. PIN-код должен состоять из четырех цифр (0-9) в одну строку, без пробелов. Файл должен заканчиваться переводом строки.

12 Часто задаваемые вопросы

12.1 Рекомендации по обновлению ПО

***Примечание**. Обновление ПО рекомендуется осуществлять в случаях, когда:*

- *новая версия ПО содержит необходимые для промышленной эксплуатации исправления ошибок или устранение уязвимостей.*
- *если осуществляется переход на новые версии ПО в связи с окончанием жизненного цикла и поддержки предыдущих версий ПО.*

Обновление ПО в промышленной эксплуатации должно производиться в соответствии с регламентами обслуживания информационных систем, принятых в компании. Как правило, обновление ПО должно производиться поэтапно и с учетом общепринятых рекомендаций, описанных ниже.

1. Для GM CORE KIT:

    a. предварительное тестирование новых версий ПО на ограниченной фокус-группе пользователей;
    b. принятие решения о возможности использования новой версии по результатам тестирования в промышленной эксплуатации;
    c. установка новой версии ПО на все устройства в промышленной эксплуатации.

2. Для GMSS NG FACTORY:

    a. предварительное тестирование новой версии ПО на тестовом сервере и ограниченной фокус-группе пользователей. Для целей такого тестирования вы можете получить ограниченную лицензию;
    b. принятие решения о возможности использования новой версии по результатам тестирования в промышленной эксплуатации;
    c. резервное копирование сервера, находящегося в тестовой эксплуатации;
    d. обновление сервера, находящегося в тестовой эксплуатации.

Все работы по обновлению ПО должны проводиться в согласованные периоды обслуживания с учетом периодов, на которые распространяется запрет на проведение работ.

12.2 Обновление СУ

1. Загрузите из личного кабинета (https://cp.getmobit.ru, раздел **Файлы**) пакеты новой версии СУ.
2. Установите пользователем с правами суперпользователя (root) пакет СУ:

```
sudo dpkg -i gmserver_[VERSION]_amd64.deb
```

3. Дождитесь запуска СУ.
4. Убедитесь, что в веб-консоли в разделе **Настройки**, на вкладке **GM Версии** в поле **GMSERVER** (**GMFACTORY**) отображается новая версия СУ.

12.3 Как вернуть GM-Box к заводским настройкам

Сброс прошивки устройства до заводских настроек можно выполнить с помощью команды **Device Wipe**.

При невозможности подключения GM-Box к СУ пользователь может самостоятельно сбросить прошивку устройства до заводских настроек, выполнив действия, описанные ниже.

1. На мониторе на экране приветствия GM-Box пользователь должен нажать пиктограмму  и выбрать меню **Система**.
2. В открывшемся окне **Системные настройки** нажать кнопку **Выполнить** (Рисунок *129*).

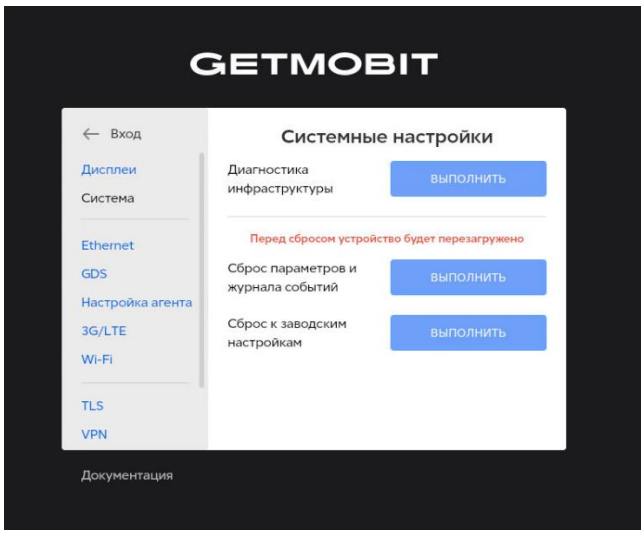


Рисунок 129 – Вид окна Системные настройки

3. Во избежание случайного сброса к заводским настройкам необходимо подтвердить операцию и ввести ПИН-код, написанный над полем (Рисунок *130*).
4. Нажать **Продолжить**.

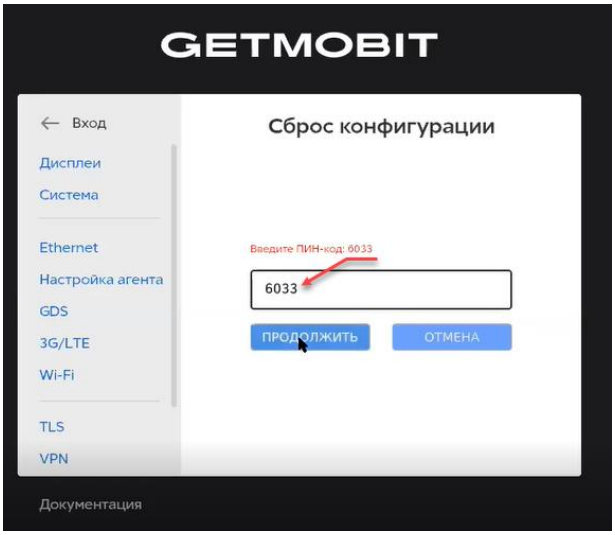


Рисунок 130 – Вид окна сброс конфигурации

5. В открывшемся окне подтверждения нажать (Рисунок *131*):

- **Перезагрузить** для немедленной перезагрузки устройства;
- **Отмена**, сброс настроек произойдет после перезагрузки GM-Box.

В противном случае устройство будет автоматически перезагружено через 30 секунд.

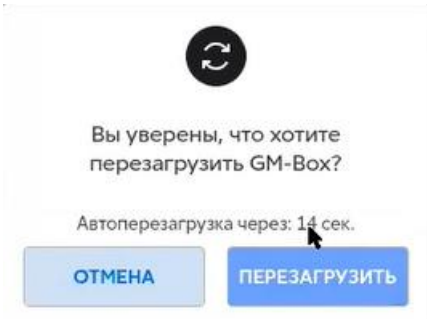


Рисунок 131 – Вид окна подтверждения сброса настроек

12.4 Синхронизация со службой каталогов с использованием SSL

СУ поддерживает возможность синхронизации со службами каталогов с использованием SSL. В примере ниже приведен порядок настройки синхронизации СУ со службой каталогов на базе MS AD 2019.

Подключение к службе каталогов будет осуществляться по одностороннему TLS соединению. Для подключения подготовьте и скопируйте CA сертификат службы каталогов на СУ:

Внимание! *Убедитесь, что имя файла сертификата состоит из цифр и латинских букв и не содержит пробелы.*

1. Скопируйте файл CA сертификата на СУ.

```
sudo cp your_ca.crt /usr/local/etc/getmobit/docker/ssl/ca.crt
```

2. Если имя файла отличается от ca.crt, укажите в конфигурационном файле /usr/local/etc/getmobit/docker/config.env имя сертификата:

```
AD_CA_CERT=ad_ca.crt
```

3. Установите права на чтение CA сертификата:

```
sudo chmod +r /usr/local/etc/getmobit/docker/ssl/ca.crt
```

4. Перезапустите сервер:

```
sudo systemctl restart gmserver
```

Дальнейшие настройки выполните в веб-консоли (Рисунок *132*):

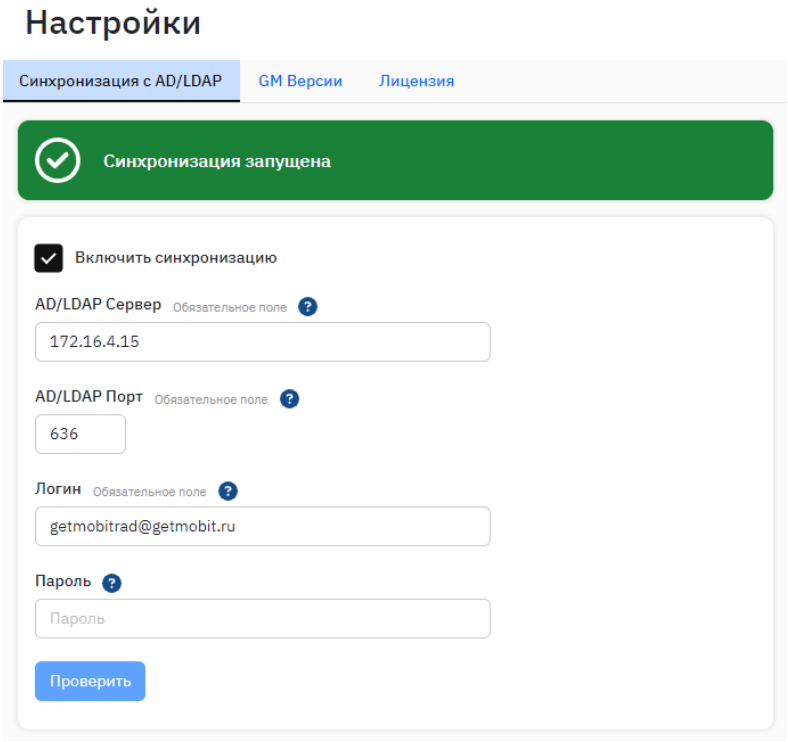


Рисунок 132 – Синхронизация со службой катологов

5. В настройках синхронизации укажите:

- FQDN сервера службы каталогов;
- порт 636.

Если ранее синхронизация была настроена без использования SSL, необходимо провести повторную синхронизацию пользователей (выключить и включить синхронизацию).

12.5 Первичная настройка веб-консоли сервиса мониторинга

Сервис логирования GM-Monitoring использует следующие индексы (коллекции логов):

- agent - основные логи GM-Box;
- backend - основные логи GM-Server;
- debug - дополнительные логи GM-Box.

Для отображения логов в веб-интерфейсе GM-Monitoring (Kibana), необходимо произвести разовую настройку этих индексов.

Для получения дополнительных логов с GM-Box в режиме отладки выполните действия, описанные ниже.

1. Откройте веб-браузер и в строке адреса введите адрес *<сервис мониторинга>/kibana/* например, ***http://getmobit.example.org/kibana/***. Откроется платформа Kibana.

Примечание. *Для перехода к сервису мониторинга также можно воспользоваться кнопкой «Логирование» (Рисунок 133) из веб-консоли СУ в разделах «Сводка», «Устройства» и «Пользователи».*

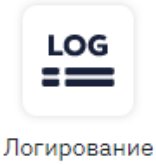


Рисунок 133 – Вид кнопки Логирование

2. Выберите раздел **Management** → **Stack Management** (Рисунок *134*).

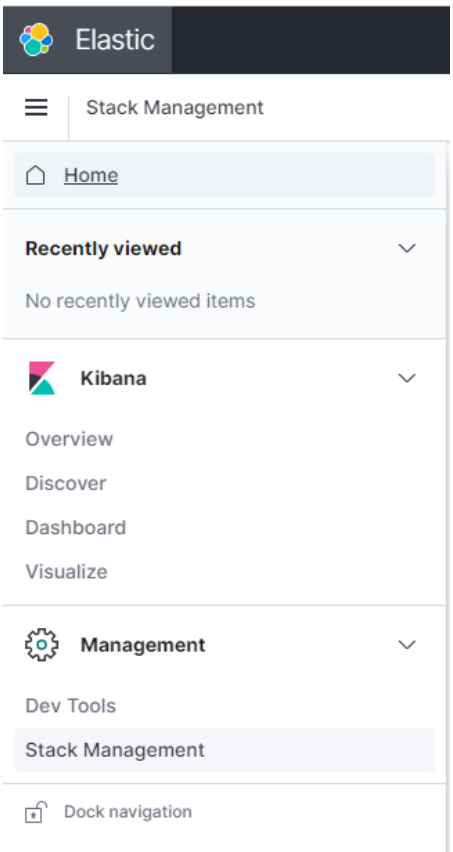


Рисунок 134 – Вид окна меню Management

3. На открывшейся странице, выберите пункт меню **Index Patterns** (Рисунок *135*).

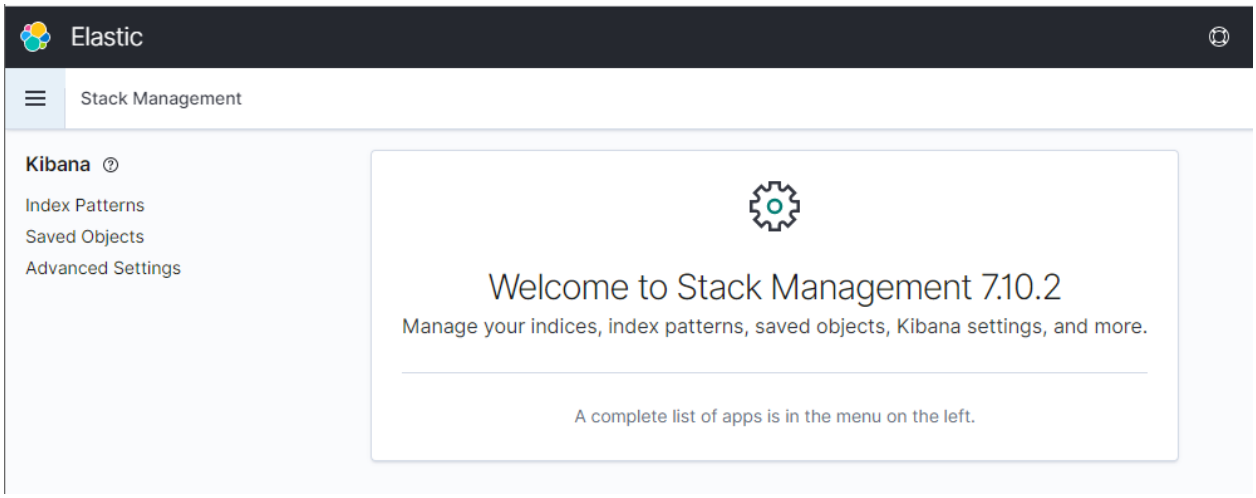


Рисунок 135 – Выбор пункта меню Index Patterns

4. Нажмите кнопку **Create Index Pattern** (Рисунок *136*)

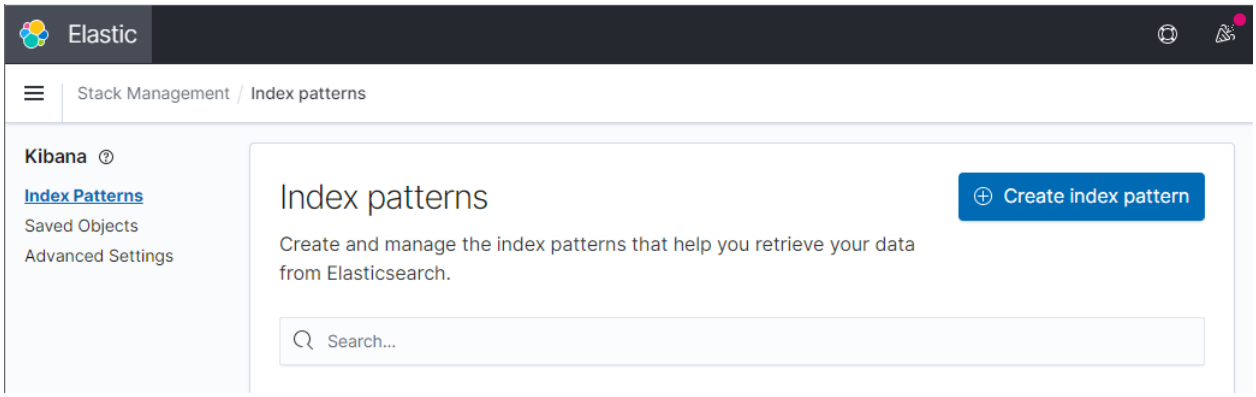


Рисунок 136 – Вид окна меню Index Patterns

5. Создайте индекс *debug** и нажмите **Next step**.

6. В поле **Time Filter field name** выберите *timestamp* и нажмите кнопку **Create Index**.

В результате в платформе Kibana для получения информации по мониторингу будет доступен индекс debug – для получения дополнительной информации с GM-Box в режиме отладки.

7. В поле **Time Filter field name** выберите *timestamp* и нажмите кнопку **Create Index**.

В результате в платформе Kibana для получения информации по мониторингу будет доступен индекс debug – для получения дополнительной информации с GM-Box в режиме отладки.

8. Аналогичным образом, создайте индексы **agent*** и **backend*** (Рисунок *137*)

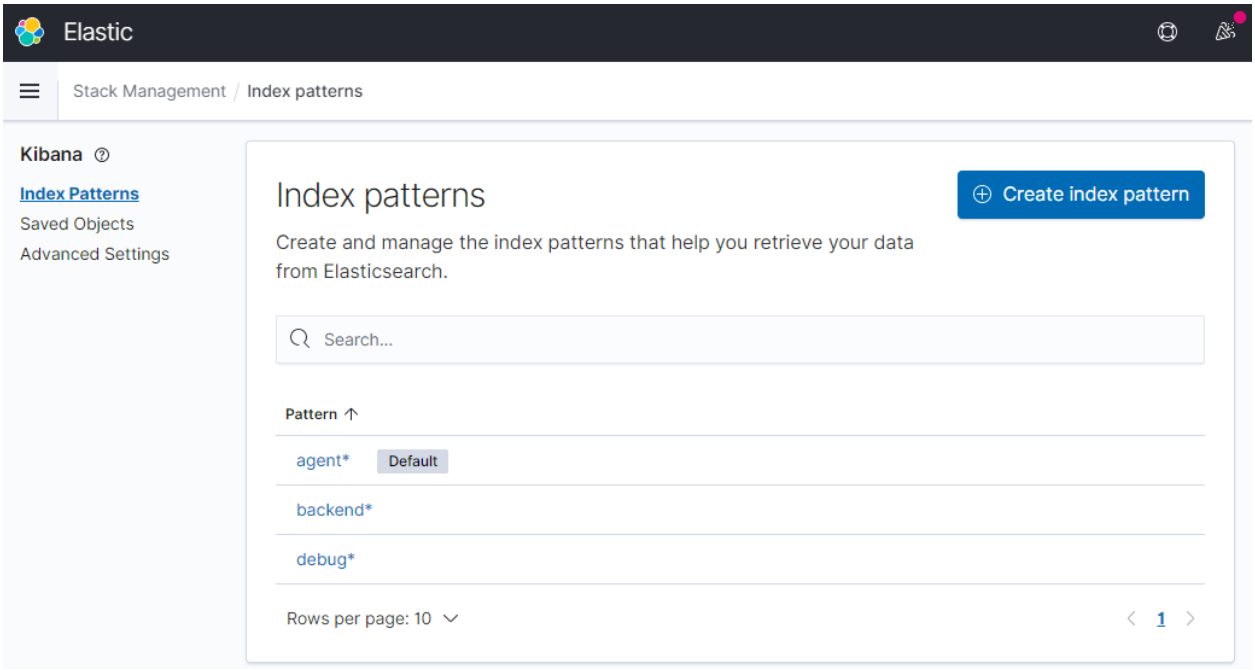


Рисунок 137 – Создание индексов agent* и backend*

9. Для просмотра собранной информации перейдите в платформе Kibana в раздел **Discover** и выберите в выпадающем списке индекс *debug**.

Примечание. *События с индексом debug создаются только при включении режима расширенных логов на GM-Box. Для включения режима расширенных логов на GM-Box в веб-консоли создайте задание на выполнение команды* ***Debug mode ON****. Во избежание переполнения дискового пространства СУ и излишней утилизации канала связи, режим расширенной отладки рекомендуется отключать (команда* ***Debug mode OFF****) после воспроизведения проблемной ситуации и снятия необходимых логов.*

10. Для включения режима расширенных логов на GM-Box в веб-консоли создайте задание на выполнение команды Debug mode ON.

Вся поступающая информация с GM-Box будет отображаться в разделе **Discover** платформы Kibana (Рисунок *138*).

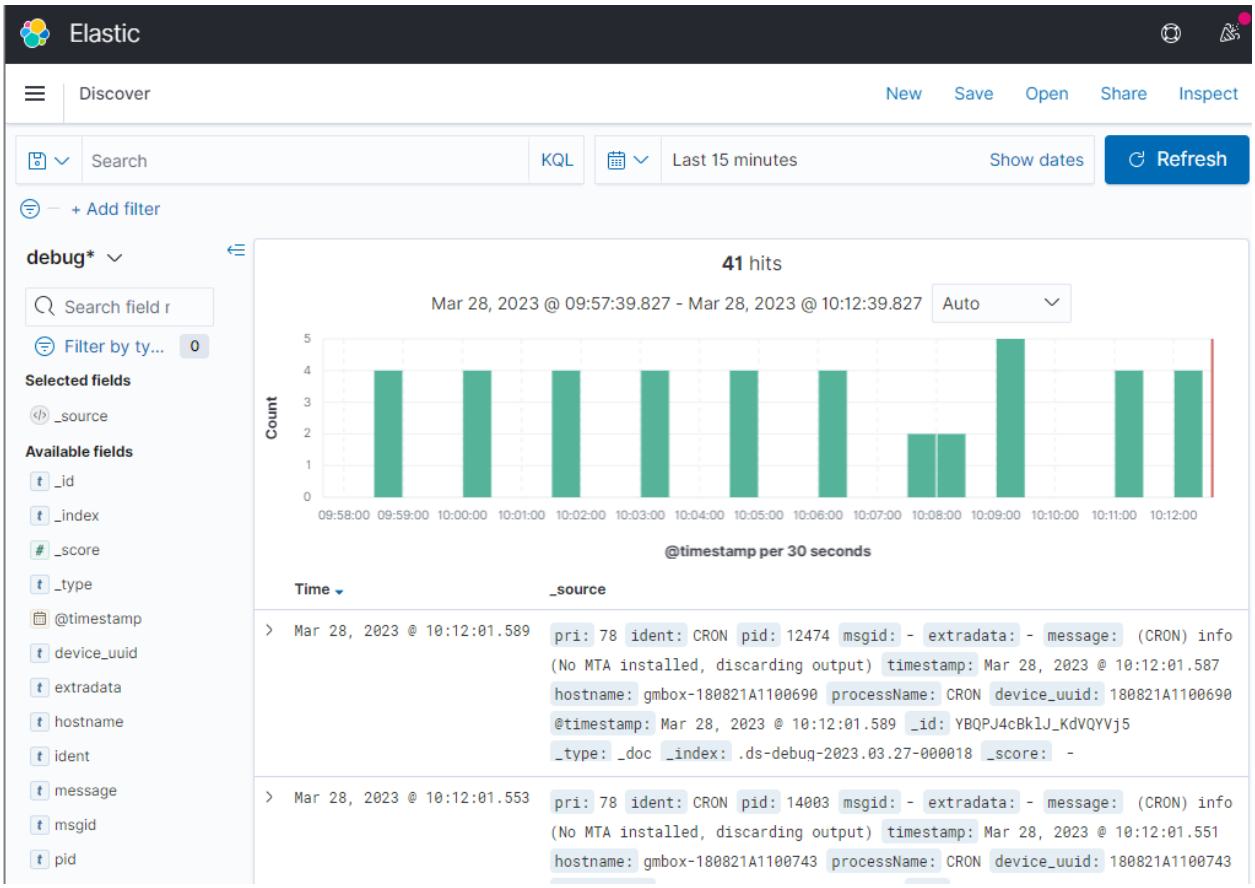


Рисунок 138 – Отображение информации на платформе Kibana

12.6 Настройка аутентификации по протоколу Kerberos в VDI клиенте Citrix

Вы можете настроить аутентификацию по протоколу Kerberos для отдельного пользователя или для пользователей, синхронизированных из корпоративной службы каталогов.

***Примечание**. При настройке отдельного пользователя указывайте доменное имя в кавычках.*

Для настройки аутентификации отдельного пользователя в веб-консоли на странице **Пользователи** при создании или редактировании учетной записи пользователя в **Дополнительном поле** укажите:

```
KRB_DEFAULT_DOMAIN=”<корпоративный домен>”
```

***Внимание!** Значение KRB_DEFAULT_DOMAIN необходимо указывать только заглавными буквами.*

Например, KRB_DEFAULT_DOMAIN=”COMPANY.LOCAL”

```
KRB_KDC=”<IP_address/DNS_name сервера со службой Kerberos KDC>”
```

Например, KRB_KDC=”ad.company.local”

Для настройки аутентификации пользователей, синхронизированных из корпоративной службы каталогов, в веб-консоли на странице **Настройки** в поле **Значения по умолчанию** добавьте строки:

```
configuration.extra=KRB_DEFAULT_DOMAIN=<корпоративный домен>
configuration.extra=KRB_KDC=<IP_address/DNS_name сервера со службой Kerberos KDC>
```

Настройка доменной аутентификации пользователей в консоли Citrix Studio – https://docs.citrix.com/en-us/citrix-workspace-app.html

12.7 Редактирование учетной записи суперпользователя LDAP

Для изменения учетной записи суперпользователя LDAP выполните следующие действия:

1. В конфигурационном файле СУ **/usr/local/etc/getmobit/docker/config.env** добавьте строки и укажите имя пользователя и пароль:

```
LDAP_LOGIN=admin
LDAP_PASSWORD=password
```

2. Перезагрузите СУ:

```
sudo service gmserver restart
```

12.8 Редактирование учетной записи пользователя с системной ролью SUPER_ADMIN / ADMIN

***Примечание**. При каждом перезапуске СУ происходит сброс и создание в системе следующих пользовательских аккаунтов, определенных настройками окружения в конфигурационном файле **config.env**:*

1. *Пользователь с ролью ADMIN:*
   - *логин из переменной LDAP_USER_LOGIN;*
   - *пароль из переменной LDAP_USER_PASSWORD (по умолчанию - admin/admin).*

2. *Пользователь с ролью SUPER_ADMIN:*
   - *логин из переменной LDAP_SUPER_USER_LOGIN;*
   - *пароль из переменной LDAP_SUPER_USER_PASSWORD (по умолчанию - superadmin/superadmin).*

Эти аккаунты можно использовать как "точки восстановления" в случае возникновения проблем с ролевым доступом к консоли администрирования.

Для изменения пользователя с ролью, заданной по умолчанию, выполните действия, описанные ниже.

1. В конфигурационном файле СУ **/usr/local/etc/getmobit/docker/config.env** добавьте строки и укажите имя пользователя и пароль для SUPER_ADMIN:

```
LDAP_SUPER_USER_LOGIN=admin
LDAP_SUPER_USER_PASSWORD=password
```

2. Для ADMIN:

```
LDAP_USER_LOGIN=admin
LDAP_USER_PASSWORD=password
```

3. Перезагрузите СУ:

```
sudo service gmserver restart
```

12.9 Редактирование учетной записи пользователя с правами суперпользователя root в MongoDB

Для изменения пользователя с правами суперпользователя в MongoDB выполните действия, описанные ниже.

1. В конфигурационном файле СУ **/usr/local/etc/getmobit/docker/config.env** добавьте строки и укажите имя пользователя и пароль:

```
MONGO_DB_ROOT_USERNAME=admin
MONGO_DB_ROOT_PASSWORD=password
```

2. Перезагрузите СУ:

```
sudo service gmserver restart
```

12.10 Настройка использования защищенного соединения между СУ и устройством

Для настройки защищенного соединения между управляемым устройством (например, GM-Box) и СУ выполните сдействия, описанные ниже.

1. Загрузите ключи на СУ, указанные в разделе Настройка протокола HTTPS (TLS)
Для загрузки сертификата на устройство в веб-консоли создайте задание на выполнение команды Patch config CA (*.crt).
2. Затем отключите возможность выбора пользователем незащищенного соединения (пользователю будут недоступны для редактирования параметры на вкладке Настройка агента). Для этого в конфигурационном файле greeter.conf в параметре Gmeye установите следующие значения:

```
{
	"pluginName": "Gmeye",
	"isEnabled": true,
	"isUsable": false
}
```

3. Обновленный конфигурационный файл *greeter.conf* необходимо применить на устройстве. Для этого в веб-консоли создайте задание (п. 5.11.1) на выполнение команды **Patch config Greeter (greeter.conf)**.
4. Для использования защищенного канала связи во время работы GM-Box в веб-консоли создайте задание (п. 5.11.1) на выполнение команды **Force SSL** на необходимом устройстве.

12.11 Подключение к корпоративной службе каталогов с ненадежным сертификатом TLS

Можно игнорировать недоверенные сертификаты и сертификаты со слабым шифрованием при настройке синхронизации в файле *GM-Server config.env* с помощью настройки:

```
AD_CERT_POLICY=allow
```

Использование данной настройки допускается только в инфраструктурах со слабыми самоподписанными сертификатами контроллера домена внутри доверенных контуров, где исключена атака man-in-the-middle.

По умолчанию проверяется вся цепочка сертификатов как на валидность, так и на силу шифрования с помощью настройки:

```
AD_CERT_POLICY=demand.
```

12.12 Как установить безопасное соединение между смартфоном и GM-Box

Для установки безопасного соединения между смартфоном и GM-Box выполните действия, описанные ниже.

1. Для загрузки сертификата УЦ компании на устройства в веб-консоли создайте задание на выполнение команды BLE certification для тех GM-Box, на которых необходимо авторизоваться с помощью смартфона.
2. По умолчанию приложение GM MOBILE ASSISTANT содержит сертификаты для смартфона. При необходимости установите на смартфоны с ОС Android сертификат УЦ компании с помощью приложения Certificate Installer.

12.13 В Citrix-сессии не работает переключение раскладки клавиатуры

Для корректного переключения раскладки клавиатуры необходимо подключить клавиатуру к GM-Box обязательно ДО входа в сессию.

12.14 Автоматическая блокировка и отключение сессии пользователя

Автоматическая блокировка и отключение сессии пользователя реализуется посредством применения политик и/или настроек ВМ, терминального сервера или VDI среды, в которой работает пользователь. При наличии соответствующих настроек, заданных администратором VDI среды, терминального сервера или ВМ, возможна автоматическая блокировка сессии после установленного периода неактивности (бездействия) пользователя. Встроенное ПО устройства GM-Box детектирует отключение от терминального сервера или ВМ, и пользовательская

сессия на устройстве автоматически завершается. При блокировке сессии в VDI среде пользовательская сессия не завершается.

Восстановление сессии осуществляется только после повторной аутентификации пользователя.

12.15 Настройка политики требований к сложности паролей локальных пользователей

Администратор может настроить проверку сложности пароля пользователя двумя способами:

- выбрать заготовленный набор правил (preset);
- задать свои правила проверки сложности пароля.

Можно использовать один из следующих наборов правил:

- **none**

  Проверка на сложность пароля не выполняется.

- **standard**
  - проверяется минимальная длина пароля (по умолчанию, 8 символов). Можно изменить с помощью параметра **PASSWORD_POLICY_MIN_LENGTH**;
  - проверяется наличие в пароле цифр, заглавных и прописных букв, спецсимволов. Группы символов задаются с помощью параметра **PASSWORD_POLICY_REQUIRED_SYMBOL_GROUPS**. Укажите через запятую допустимые значения:
    i. digits – цифры;
    ii. lowercase - прописные буквы;
    iii. punctuation – спецсимволы.
- **strict**
  - проверяется минимальная длина пароля (по умолчанию, 8 символов). Можно изменить значение с помощью параметра **PASSWORD_POLICY_MIN_LENGTH**.
  - проверяется наличие в пароле цифр, заглавных и прописных букв, спецсимволов. Группы символов задаются с помощью параметра **PASSWORD_POLICY_REQUIRED_SYMBOL_GROUPS**. Укажите через запятую допустимые значения:
    i. digits – цифры;

ii. uppercase – заглавные буквы;
iii. lowercase – прописные буквы;
iv. punctuation – спецсимволы.

- проверяется отсутствие повторяющихся подряд символов (по умолчанию, больше 3). Можно изменить с помощью параметра **PASSWORD_POLICY_MAX_REPEATING_SYMBOLS**;
- Проверяется отсутствие символов, стоящих рядом на клавиатуре подряд (по умолчанию, запрещено более 3 символов). Можно изменить с помощью параметра **PASSWORD_POLICY_MAX_ADJACENT_SYMBOLS**.

Чтобы применить preset:

1. Добавьте в файле **/usr/local/etc/getmobit/docker/config.env** строку:

```
PASSWORD_POLICY_MODE=<имя пресета>
```

2. Перезапустите СУ командой:

```
systemctl restart gmserver
```

12.15.1 Пользовательская настройка пароля

1. Для произвольной настройки парольной политики в файле **/usr/local/etc/getmobit/docker/config.env** добавьте строку:

```
PASSWORD_POLICY_MODE= custom
```

2. Задайте список проверок в параметре **PASSWORD_POLICY_VALIDATION_METHODS**. Укажите допустимые значения через запятую:

- ***min_length*** - проверка минимальной длины пароля;
- ***required_symbol_groups*** - проверка наличия символов из групп;
- ***blacklist*** - проверяет отсутствие слов из словаря в пароле. (Словарь представляет из себя текстовый файл, где новая строка - новое слово. Путь к файлу задается с помощью параметра **PASSWORD_POLICY_BLACKLIST_PATH**);
- ***max_adjacent_symbols*** - проверяет отсутствие в пароле символов, стоящих рядом на клавиатуре;
- ***max_repeating_symbols*** - проверяет отсутствие в пароле повторяющихся символов.

Пример конфигурации:

```
PASSWORD_POLICY_MODE=custom
PASSWORD_POLICY_VALIDATION_METHODS=min_length,max_adjacent_symbols
```

В этом случае осуществляется проверка максимальной длины и отсутствия идущих подряд 3 и более символов, стоящих рядом на клавиатуре.

Вы можете настроить каждую из проверок, используя параметры, описанные выше.

3. Для применения заданных настроек перезапустите СУ командой:

```
systemctl restart gmserver
```

12.16 Настройка количества попыток неудачного входа в веб-интерфейс администратора

Чтобы защитить СУ от подбора пароля администратора, можно установить максимальное количество попыток входа.

12.16.1 Базовая настройка защиты

1. Добавьте в файл /usr/local/etc/getmobit/docker/config.env строку

```
BRUTEFORCE_REJECT_ENABLED=true
```

2. Чтобы применить настройки, перезапустите СУ командой:

```
systemctl restart gmserver
```

12.16.2 Сложная настройка защиты

1. В файле **/usr/local/etc/getmobit/docker/config.env** добавьте строки:

- BRUTEFORCE_REJECT_MAX_FAILURE_COUNT Количество попыток до блокировки (по умолчанию - 5);
- BRUTEFORCE_REJECT_LOCK_TIMEOUT_SECOND - Количество секунд, на которое пользователю будет заблокирована возможность попыток авторизации. (по умолчанию 60). Если включен параметр BRUTEFORCE_REJECT_INCREASE_TIMEOUT, каждая следующая неудачная попытка удваивает последнее время блокировки;
- BRUTEFORCE_REJECT_MAX_LOCK_TIME_SECONDS - - Максимальное время блокировки авторизации в секундах(по умолчанию – 86400, т.е.1 сутки) . Этот

параметр задает верхний порог времени блокировки доступа к авторизации (применимо при включенном параметре увеличения времени блокировки). Т.е. не смотря на экспоненциальное увеличение времени блокировки, доступ не будет ограничиваться более, чем на время, заданное в этом параметре;

- BRUTEFORCE_REJECT_INCREASE_TIMEOUT (boolean, по умолчанию - true) - Увеличивать время блокировки (формула next=prev*2).

2. Чтобы применить настройки, перезапустите СУ командой:

```
systemctl restart gmserver
```

12.17 Указание прокси-сервера для веб-режима

Чтобы в веб-режиме использовать прокси-сервер, выполните действия, описанные ниже.

1. Откройте карточку пользователя или шаблон с режимом **Веб**.
2. Переключитесь на режим **Терминал**. Станет доступно поле **VDI Параметры 2**.
3. Пропишите в поле **VDI Параметры 2** настройки для прокси сервера: **--proxy-server=[адрес сервера]**. Адрес сервера указывается без кавычек.
4. Нажмите кнопку **Сохранить изменения**.
5. Переключитесь на режим **Веб**.
6. Нажмите кнопку **Сохранить изменения**.

Пример заполнения поля VDI Параметры 2 (Рисунок 139):



Рисунок 139 – Пример заполнения VDI Параметры 2

Приложение А. Экран приветствия GM-Box

На экране приветствия GM-Box отображается следующая информация (Рисунок *140*):

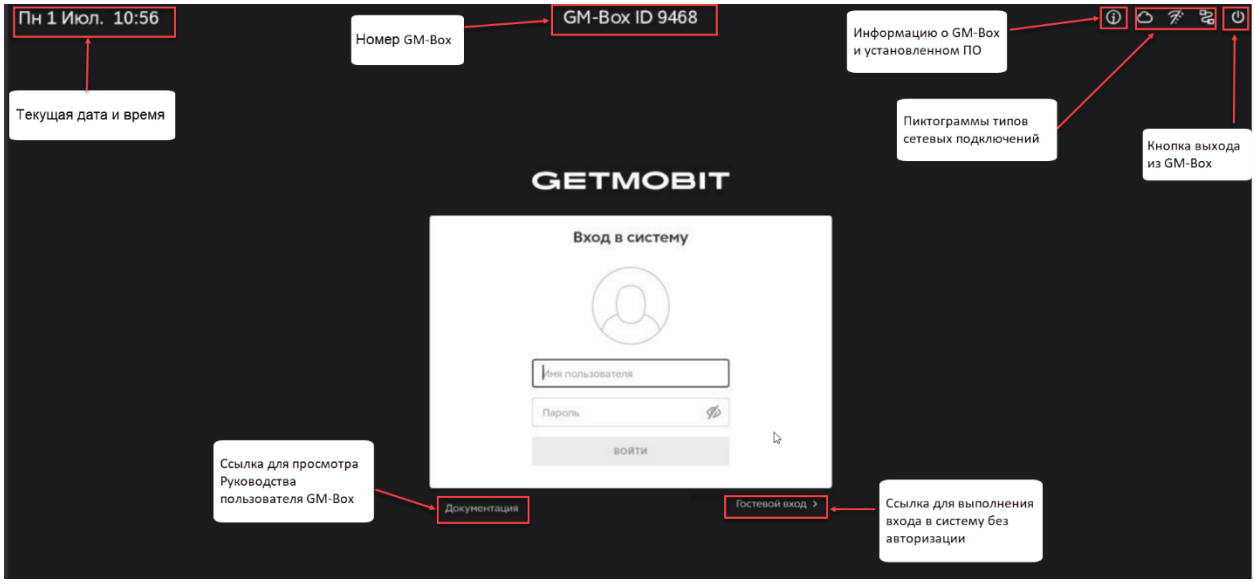


Рисунок 140 – Вид экрана приветствия GM-Box

При нажатии на пиктограмму  откроется окно с информацией, содержащей UUID устройства, версию прошивки и сервисов, установленных на GM-Box (Рисунок *141*).

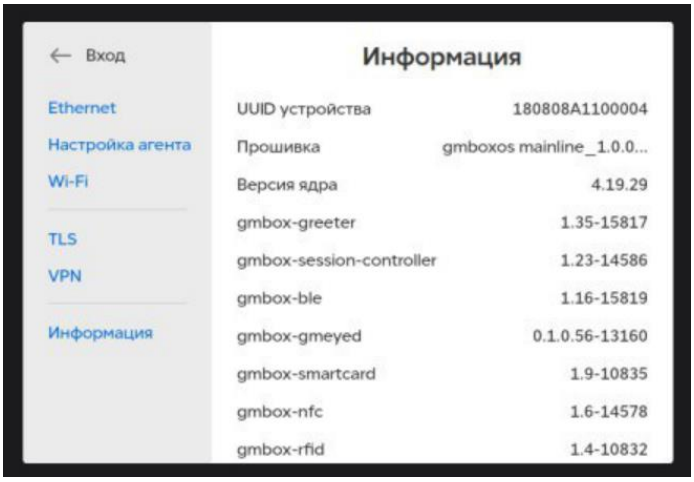


Рисунок 141 – Вид окна с информацией

При нажатии на пиктограмму сетевого подключения открывается окно с соответствующими настройками.

Приложение Б. Конфигурационный файл greeter.conf

Файл *greeter.conf* содержит конфигурации загружаемых плагинов, которые обеспечивают процедуры идентификации и аутентификации пользователя, настройку сетевых интерфейсов.

Для изменения стандартных настроек загружаемых плагинов вы можете создать конфигурационный файл *greeter.conf* аналогично следующему примеру:

```
{
  "plugins": [
    {
      "pluginName": "Wifi",
      "isEnabled": true,
      "isUsable": true
    },
    {
      "pluginName": "Ethernet",
      "isEnabled": true,
      "isUsable": true
    },
    {
      "pluginName": "Gmeye",
      "isEnabled": true,
      "isUsable": true
    },
    {
      "pluginName": "Modem",
      "isEnabled": false,
      "isUsable": false
    },
    {
      "pluginName": "BLE",
      "isEnabled": true,
      "isUsable": true
    },
    {
      "pluginName": "IdAndPassword",
      "isEnabled": true,
      "isUsable": true
    },
    {
      "pluginName": "Information",
```

```
      "isEnabled": true,
      "isUsable": true
    },
    {
      "pluginName": "NFC",
      "isEnabled": true,
      "isUsable": true
    },
    {
      "pluginName": "PasswordWithCancel",
      "isEnabled": true,
      "isUsable": true
    },
    {
      "pluginName": "RFID",
      "isEnabled": true,
      "isUsable": true
    },
    {
      "pluginName": "SessionController",
      "isEnabled": true,
      "isUsable": true
    },
     {
      "pluginName": "System",
      "isEnabled": true,
      "isUsable": true
     },
     {
      "pluginName": "Token",
      "isEnabled": true,
      "isUsable": true
    },
    {
      "pluginName": "VPN",
      "isEnabled": false,
      "isUsable": false
    },
    {
      "pluginName": "Tunnel",
      "isEnabled": false,
      "isUsable": false
    }
  ],
  "canShowPassword": true,
```

```
  "canUseGuestLogin": true,
  "guestLogin": "guestUserWeb",
  "guestPassword": "guest"
}
```

В Таблица 15 приведен перечень и описание параметров конфигурационного файла.

Таблица 15 – Перечень и описание параметров конфигурационного файла

Параметр	Описание
"pluginName": "Wifi"	Настройки беспроводных сетевых интерфейсов.
"pluginName": "Ethernet"	Настройки проводных сетевых интерфейсов.
"pluginName": "Gmeye"	Настройки агента, который позволяет получить информацию о статусе соединения с СУ и о загруженных сертификатах, также перевести соединение в защищенный режим.
"pluginName": "Modem"	Настройки соединения с использованием 3G/LTE модема.
"pluginName": "BLE"	Настройки идентификации пользователя с использованием смартфона
"pluginName": "idAndPassword"	Настройки идентификации пользователя с использованием логина и пароля учетной записи
"pluginName": "Information"	Информация о версиях сервисов, используемых на GM-Box
"pluginName": "NFC"	Настройки идентификации пользователя с использованием NFC-карт.
"pluginName": "PasswordWithCancel"	Дополнительная настройка, отображающая кнопку отмены процедуры в случае неуспешной идентификации пользователя.
"pluginName": "RFID"	Настройки идентификации пользователя с использованием RFID-карт.
"pluginName": "SessionController"	Плагин, контролирующий пользовательскую сессию. Обязательный параметр. Редактирование запрещено.
"pluginName": "System"	Настройки, позволяющие пользователю обновить прошивку GM-Box до первоначальных настроек
"pluginName": "Token"	Настройки идентификации пользователя с использованием токена.

Параметр	Описание
"pluginName": "VPN"	Настройки для использования OpenVPN-соединения
"pluginName": "Tunnel"	Настройки для использования TLS-соединения
canShowPassword	Возможность просмотра введенного пароля
canUseGuestLogin	Возможность использовать гостевую учетную запись для входа в систему. Обязательные параметры: guestLogin guestPassword

У параметров возможны следующие значения:

- *"isEnabled": true* –настройки, задаваемые параметром, отображаются на экране приветствия GM-Box;
- *"isEnabled": false* – настройки, задаваемые параметром, не отображаются на экране приветствия GM-Box;
- *"isUsable": true* – настройки параметры доступны для редактирования;
- *"isUsable": false* –настройки параметра недоступны для редактирования.

Например, если в конфигурационном файле задано:

```
{
  "pluginName": "Wifi",
  "isEnabled": true,
  "isUsable": true
},
```

На экране приветствия GM-Box отображается пиктограмма Wi-Fi и настройки доступны для редактирования (Рисунок *142*).



Рисунок 142 –Варианты отображения информации в окне приветствия GM-Box