

КОМПЛЕКСНАЯ ЦИФРОВАЯ МУЛЬТИПЛАТФОРМА УПРАВЛЕНИЯ
МОБИЛЬНЫМИ СРЕДСТВАМИ КОММУНИКАЦИЙ
РУКОВОДСТВО ПО УСТАНОВКЕ И НАСТРОЙКЕ

SAFEMOBILE

Москва

2022

СОДЕРЖАНИЕ

Перечень используемых терминов и сокращений	4
1 Введение	5
2 Назначение и условия применения	7
2.1 Назначение «UEM SafeMobile»	7
2.2 Требования к программному обеспечению	7
2.3 Системные требования	7
2.4 Требования к сетевому окружению	8
2.5 Требования к серверу БД	9
2.6 Требования к сертификатам HTTPS	10
3 Установка и настройка ПО Docker	11
4 Установка и настройка серверных компонентов «UEM SafeMobile»	12
4.1 Распаковка архивов серверных компонентов	12
4.2 Установка схемы БД PostgreSQL	12
4.2.1 Стандартная установка на сервер с уже имеющейся СУБД PostgreSQL	13
4.2.2 Первоначальная установка на новом сервере	14
4.2.3 Минимальная установка	15
4.2.4 Ручная оптимизация настроек СУБД PostgreSQL	15
4.3 Запуск скрипта первоначальной настройки серверных компонентов	16
4.4 Конфигурационные файлы	18
4.5 Создание docker-контейнеров	19
4.6 Настройка интеграции с AD	19
5 Получение цифровых сертификатов и ключей	23
5.1 Сертификаты HTTPS	23
5.2 Сертификат Push MDM	24

5.3	Приватный ключ пуш-сервера FCM.....	28
6	Обновление до версии 6.x	29
6.1	Обновление серверной части до версии 6.x.....	29
6.2	Особенность применения профилей после обновления с версии 4.4.x до 6.x	30
6.3	Работа с дампом БД, полученным перед патчем до новой версии.....	31
6.4	Особенности обновления БД с версии 5.0.3 и более ранних	32
7	Управление серверными компонентами «UEM SafeMobile»	33
8	Проверка работоспособности «UEM SafeMobile»	34
	Приложение А Настройки для внешнего прокси-сервера Nginx.....	36
	Приложение Б Особенности настройки LDAPS	37
	Приложение В Подготовка компьютера для агента регистрации.....	41

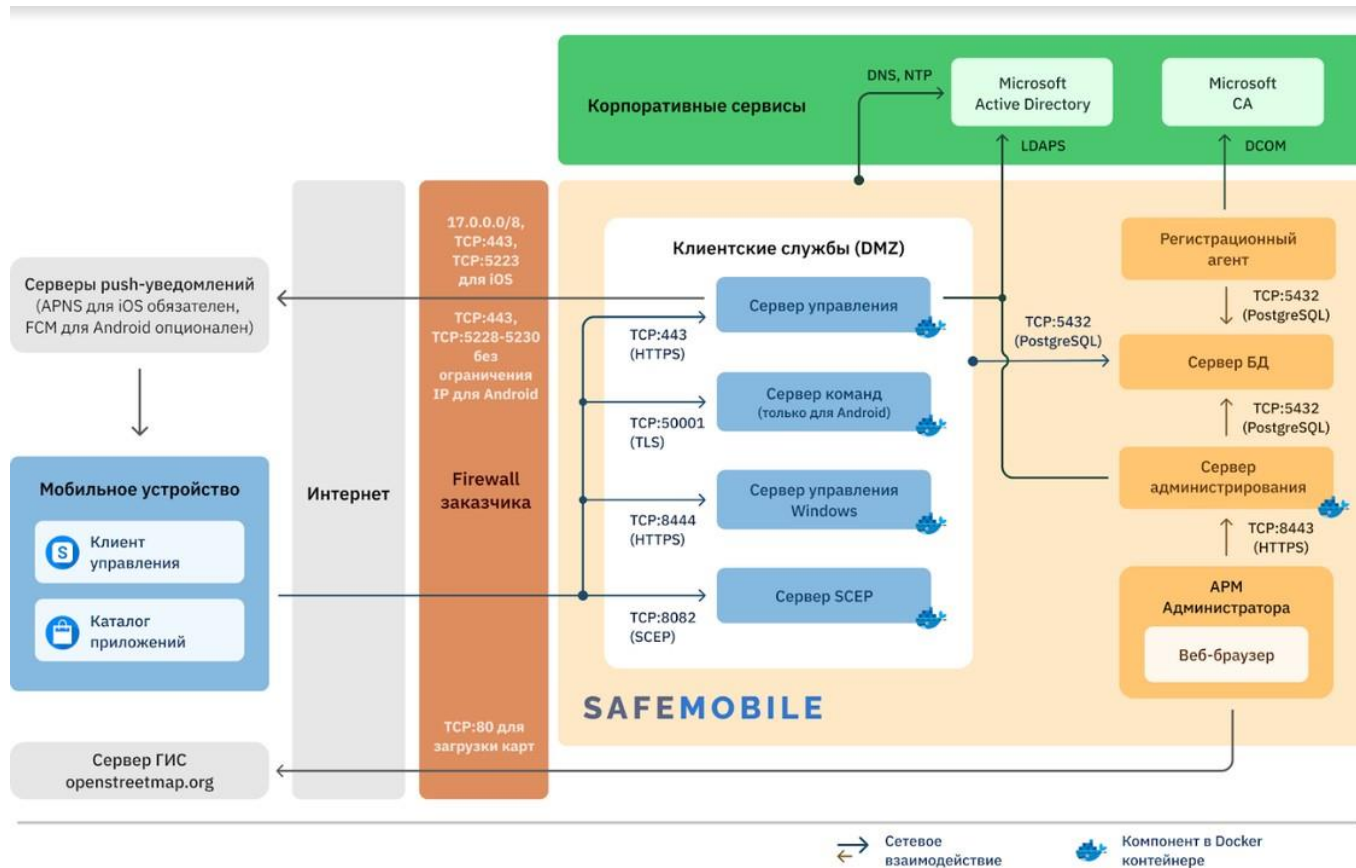
Перечень используемых терминов и сокращений

Таблица 1 – Перечень терминов и сокращений

Сокращение	Полное наименование
AD	Служба каталогов (Active Directory)
ADEP	Программа управления корпоративными приложениями на устройствах Apple (Apple Developer Enterprise Program)
APNS	Служба отправки push-уведомлений на устройства Apple (Apple Push Notification Service)
CPU	Центральное процессорное устройство (Central Processing Unit)
CSR	Запрос на получение сертификата (Certificate Signing Request)
DNS	Система доменных имён (Domain Name System)
FCM	Служба отправки push-уведомлений (Firebase Cloud Messaging)
HTTPS	Расширение протокола HTTP для поддержки шифрования в целях повышения безопасности (HyperText Transfer Protocol Secure)
IP	Интернет-протокол (Internet Protocol)
MDM	Система управления мобильными устройствами (Mobile Device Management)
NTP	Протокол сетевого времени (Network Time Protocol)
TCP	Протокол управления передачей (Transmission Control Protocol)
SLES	Операционная система SUSE Linux Enterprise Server
SSD	Запоминающее устройство, твердотельный накопитель (Solid State Drive)
UDP	Протокол пользовательских датаграмм (User Datagram Protocol)
UEM	Unified Endpoint management
АРМ	Автоматизированное рабочее место
БД	База данных
ГИС	Географическая информационная система
ВМ	Виртуальная машина
МСК	Мобильное средство коммуникации (смартфон, планшетный компьютер)
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПО	Программное обеспечение
СУБД	Система управления базами данных
УЦ	Удостоверяющий центр
ЦС	Центр сертификации

1 Введение

Настоящее руководство предназначено для установки комплексной цифровой мультиплатформы управления мобильными средствами коммуникаций «UEM SafeMobile» (далее по тексту – UEM SafeMobile) и содержит указания по установке и настройке программного окружения и серверных компонентов «UEM SafeMobile».



Архитектурная схема

«SafeMobile» состоит из следующих компонентов:

Клиентские компоненты:

- мобильный клиент¹;
- АРМ Администратора.

Серверные компоненты:

- db – сервер баз данных;
- arm – сервер администрирования;
- iosmdm – сервер управления MDM
(для Android, iOS, Windows и АврораОС);
- socket-server – сервер команд (для Android);
- winmdm – сервер управления WinMDM (для Windows);
- fcmpushserver – пуш-сервер FCM (для некоторых Android);
- scep – сервер получения пользовательских сертификатов из УЦ.

Использование пуш-сервера FCM на данный момент опционально и может потребоваться только для управления некоторыми Android-устройствами, не обеспечивающими защиту MDM-агента от остановки операционной системой.

¹ Мобильный клиент для iOS состоит из клиентского ПО SafeMobile и конфигурационного профиля управления MCK.

2 Назначение и условия применения

2.1 Назначение «UEM SafeMobile»

«UEM SafeMobile» представляет из себя аппаратно-программный комплекс для защиты информации, обрабатываемой на мобильных устройствах, от несанкционированного доступа.

2.2 Требования к программному обеспечению

Установка серверных компонентов «UEM SafeMobile» возможна на любой современный 64-разрядный Linux-дистрибутив, если для него доступны пакеты `docker`, `docker-compose`, `git`, `postgresql`, `postgresql-contrib`, которые необходимо предварительно установить, в соответствии с документацией вендора ОС.

Работоспособность «UEM SafeMobile» протестирована на следующих ОС:

1. Debian, Ubuntu, AstraLinux;
2. RedHat Enterprise Linux, CentOS, OracleLinux, RockyLinux, ПЕД ОС;
3. OpenSUSE, SUSE Linux Enterprise Server (SLES);
4. ALT Linux, Alpine Linux.

«UEM SafeMobile» может работать с любым современным сервером PostgreSQL.

Работоспособность протестирована на следующих версиях:

1. PostgreSQL 11, 12, 14;
2. PostgreSQL Pro 14.

Для примера установки и настройки СУБД на сервере с CentOS7 и Debian 11, в комплекте с дистрибутивом «UEM SafeMobile» поставляются скрипты `centos7_pg11_install.sh` и `debian11_pg14_install.sh`

Для входа в веб-консоль администратора требуется один из перечисленных браузеров актуальной версии: Mozilla Firefox, Google Chrome, Яндекс.Браузер.

2.3 Системные требования

В таблице 2 указаны рекомендованные системные требования в зависимости от количества МСК, подключаемых к системе. В скобках указаны рекомендуемые серверные компоненты.

Таблица 2 – Системные требования

Количество МСК	ВМ	СРU	ОЗУ, ГБ	Диск, ГБ
1 – 100	Сервер SafeMobile (db+arm+iosmdm+socket-server+winmdm+fcmpushserver)	2	2	20
101 – 500	Сервер SafeMobile (db+arm+iosmdm+socket-server+winmdm+fcmpushserver)	2	4	30
501 – 1000	Сервер Управления и Администрирования (arm+iosmdm+socket-server+winmdm+fcmpushserver)	2	4	20
	Сервер БД (db)	2	4	100
1001 – 2000	Сервер Управления (iosmdm+socket-server+winmdm+fcmpushserver)	2	4	20
	Сервер Администрирования (arm)	2	4	20
	Сервер БД (db)	2	4	200
2001 – 10000	Сервер Команд (socket-server+fcmpushserver+scep)	2	4	20
	Сервер Управления (iosmdm)	4	4	20
	Сервер WinMDM (winmdm)	4	4	20
	Сервер Администрирования (arm)	2	6	20
	Сервер БД (db)	4	8	300

2.4 Требования к сетевому окружению

Для работы серверных компонентов «UEM SafeMobile» в сетевом окружении требуются следующие разрешения:

- внешних подключений по следующим TCP-портам¹ (указаны значения по умолчанию):
 - 8443(https) или 8080(http) – для подключения браузером к Серверу Администрирования.
 - 443 – для подключения МСК всех платформ к Серверу Управления;
 - 8444 – для подключения МСК с ОС Windows к Серверу WinMDM;

¹ После стандартной установки CentOS 7.x и выше в системе включен брандмауэр и разрешены входящие соединения только на порт 22.

- 50001 – для подключения МСК с ОС Android, к Серверу Команд;
2. сетевых подключений серверных компонентов (указаны значения TCP-портов по умолчанию):
- 5432 – от всех серверных компонентов в адрес Сервера БД;
 - 80 – от рабочего места администратора в адрес сервера ГИС (по умолчанию *.openstreetmap.org).
3. (для управления iOS-устройствами) подключения Сервера Управления к серверам APNS посредством:
- доступа к DNS-серверу, разрешающему доменные имена api.push.apple.com, gateway.push.apple.com, api.push.apple.com;
 - прохождения IP-трафика к адресам 17.0.0.0/8, TCP-порт 443;
4. (для управления Android-устройствами, которым требуется Firebase Cloud Messaging) подключения пуш-сервера к серверам FCM посредством:
- доступа к DNS-серверу, разрешающему доменные имена fcm.googleapis.com, apis.google.com, ajax.googleapis.com;
 - разрешения прохождения IP-трафика к серверам apis.google.com, ajax.googleapis.com, TCP-порт 443;
 - разрешения прохождения IP-трафика к серверам fcm.googleapis.com, TCP-порты 443, 5228-5230;

Для корректной работы серверных компонентов и рабочего места администратора необходима настройка синхронизации времени по протоколу NTP, UDP-порт 123.

2.5 Требования к серверу БД

Для установки схемы БД SafeMobile можно воспользоваться подготовленными скриптами, приведенными в разделе 4.2, либо настроить кластер PostgreSQL вручную, тогда он должен соответствовать следующим требованиям, необходимыми для работы с SafeMobile:

1. На сервере должна быть создана база данных с именем, которое впоследствии нужно указать в мастере первоначальной настройки сервера SafeMobile (параметр **name** в файле db.yml). Кодировка этой БД должна быть en_US.UTF-8.
2. На сервере должен быть создан пользователь с правами подключения к этой БД и на создание в ней временных таблиц (далее – пользователь SafeMobile). Login-имя и пароль этого пользователя должны впоследствии нужно указать в

мастере первоначальной настройки сервера SafeMobile (параметры **user** и **password** в файле db.yml); должна быть создана схема в этой БД, владельцем которой должен быть назначен пользователь SafeMobile.

3. В указанной БД в стандартной схеме public должно быть установлено расширение pgcrypto.

4. Переменная сессии SEARCH_PATH для роли пользователя БД SafeMobile (п. 2.) должна содержать: <имя схемы БД SafeMobile (п. 2.)>, public.

5. В файле pg_hba.conf необходимо проверить и при необходимости скорректировать

```
host all all 0.0.0.0/0 md5
```

6. В файле postgresql.conf необходимо проверить и при необходимости скорректировать параметры:

```
listen_addresses = '*'  
max_connections = 1000
```

Примечание: Если СУБД инициализирована без поддержки кодировки en_US.UTF-8, при работе скриптов разворачивания БД SafeMobile возникают сообщения:

ПРЕДУПРЕЖДЕНИЕ: несовпадение версии для правила сортировки "default"

ПОДРОБНОСТИ: Правило сортировки в базе данных было создано с версией 153.88.34, но операционная система предоставляет версию 153.88.

ERROR: invalid locale name: "en_US.utf8"

Необходимо переинициализировать СУБД командой

```
su - postgres -c "initdb --locale=en_US.UTF-8 -D <путь к хранилищу>"
```

2.6 Требования к сертификатам HTTPS

1. Сертификаты сервера должны использовать ключи RSA длиной не менее 2048 бит.

2. Сертификаты сервера должны использовать алгоритм хеширования из семейства SHA-2 для создания цифровой подписи.

3. Сертификаты сервера должны содержать имя или IP-адрес сервера в поле Subject Alternative Name.

4. Сертификаты сервера должны включать расширение ExtendedKeyUsage (EKU), содержащее идентификатор объекта id-kp-serverAuth.

5. Срок действия сертификатов сервера должен составлять не более 825 дней (как указано в полях NotBefore и NotAfter).

3 Установка и настройка ПО Docker

Установка демонстрируется на примере CentOS7. Для установки Docker требуется выполнить следующие действия:

1. Осуществить установку и настройку актуального пакета docker из официального репозитория:

```
yum install -y yum-utils  
yum-config-manager --add-repo  
https://download.docker.com/linux/centos/docker-ce.repo  
yum makecache fast  
yum -y install docker-ce
```

2. Настроить запуск Docker со стартом системы:

```
systemctl enable docker
```

3. Запустить Docker с помощью команды:

```
systemctl start docker
```

4. Выполнить установку компонента docker-compose:

```
curl -L  
https://github.com/docker/compose/releases/download/1.29.2/docker  
-compose-Linux-x86\_64 > /usr/local/bin/docker-compose
```

5. Настроить права доступа к установленным компонентам:

```
chmod +x /usr/local/bin/docker-compose  
ln -s /usr/local/bin/docker-compose /usr/bin/docker-compose
```

6. Осуществить проверку версии установленных компонентов:

```
docker --version  
  
docker-compose --version
```

4 Установка и настройка серверных компонентов «UEM SafeMobile»

Комплект ПО для установки «UEM SafeMobile» состоит из следующих файлов:

- `emm-config.tar.gz`;
- `emm-docker.tar.gz`;
- `db-postgresql.tar.gz`.

Для установки серверных компонентов следует выполнить следующие операции.

4.1 Распаковка архивов серверных компонентов

1. Установить docker-образы серверных компонентов из архива **emm-docker.tar.gz** посредством команды:

```
docker load -i emm-docker.tar.gz
```

2. Создать каталог **/opt/emm** и распаковать файлы **db-postgresql.tar.gz** и **emm-config.tar.gz**:

```
mkdir /opt/emm
```

```
tar xzvf emm-config.tar.gz -C /opt/emm
```

```
tar xzvf db-postgresql.tar.gz -C /tmp/
```

4.2 Установка схемы БД PostgreSQL

Для сервера баз данных PostgreSQL (в терминологии PostgreSQL – кластер PostgreSQL) возможны три сценария установки ПО БД SafeMobile:

- **стандартная установка**, на сервер с уже имеющейся СУБД PostgreSQL.
- **первоначальная установка** на новом сервере с CentOS7 или Debian 11, обычно с минимальным набором пакетов, не включающим в себя PostgreSQL;
- **минимальная установка**, на сервер с уже имеющейся СУБД PostgreSQL, на котором уже проведена предварительная настройка в соответствии с разделом 2.5.

Для начала установки необходимо перейти в каталог «`/tmp/`», в котором после распаковки архива находятся:

```
каталог sql
```

```
centos7_pg11_install.sh
```

```
INSTALL.md
```

```
install.sh
```

```
setup.sh
```

4.2.1 Стандартная установка на сервер с уже имеющейся СУБД PostgreSQL

Пользователям, на сервере которых СУБД PostgreSQL уже установлена, предлагается возможность ее автоматической настройки.

Для этого следует от пользователя postgres выполнить скрипт setup.sh следующей командой:

```
su - postgres -c "$( cd "$(dirname "${BASH_SOURCE[0]}") " >/dev/null  
2>&1 && pwd )/setup.sh -y"
```

В результате выполнения данной команды будет создана БД со следующими параметрами по умолчанию: имя базы данных – **sphone**, имя пользователя – **sphone**, пароль пользователя – **111**.

Затем установить схему БД командой:

```
./install.sh -- --host 127.0.0.1
```

После запуска скрипта будет предложена установка схемы БД с параметрами по умолчанию, а именно:

```
File: ./sql/schema.sql # Название файла для установки
```

```
Database: sphone # Имя базы данных
```

```
User: sphone # Имя пользователя
```

```
Schema: sphone # Название схемы
```

```
Continue (y/n)?
```

Для продолжения работы с предложенными параметрами следует нажать «**y**». В противном случае нажать «**n**» и запустить скрипт с указанием требуемых параметров. Если какой-то из параметров схемы не будет указан, следовательно, в схему будет включен параметр по умолчанию.

Для получения справки по параметрам схемы требуется запустить скрипт с ключом **-h** или **--help**:

```
./install.sh -h
```

Пример команды, где **smadmin** – имя пользователя, **smdb** – имя базы данных:

```
./install.sh --user smadmin --db smdb -- --host 127.0.0.1
```

После выбора параметров требуется подтвердить установку схемы БД вводом пароля пользователя.

После этого можно переходить к разделу 4.2.4 для ручной оптимизации настроек СУБД PostgreSQL

4.2.2 Первоначальная установка на новом сервере

Пользователям, использующим CentOS7 или Debian 11, на сервере которых СУБД PostgreSQL не установлена, предлагается возможность ее автоматической установки и настройки с оптимальными параметрами.

Для этого следует от пользователя root запустить скрипт командой, соответствующей вашей ОС:

```
./centos7_pg11_install.sh
```

или

```
./debian11_pg14_install.sh
```

В результате выполнения данной команды будет установлена СУБД PostgreSQL и создана БД со следующими параметрами по умолчанию: имя базы данных – **sphone**, имя пользователя – **sphone**, пароль пользователя – **111**.

На последнем этапе выполнения команды будет задан вопрос "Введите количество МСК:". Необходимо выбрать значение в соответствии с планируемым количеством МСК в системе: «1 – 1-1000», «2 – 1000-10000» или «3 – Более 10000». На основе выбранного значения будут подобраны параметры оптимизации СУБД PostgreSQL. Ручная оптимизация настроек описана в разделе 4.2.4.

Затем установить схему БД командой:

```
./install.sh -- --host 127.0.0.1
```

Затем выбрать параметры схемы БД согласно описанию, при стандартной установке после запуска скрипта *install.sh*.

После этого можно переходить к разделу 4.3 и запускать скрипт первоначальной настройки серверных компонентов

4.2.3 Минимальная установка

Предназначена для пользователей, у которых уже установлена СУБД PostgreSQL, создана БД и настроена в соответствии с требованиями в разделе 2.5.

Для того, чтобы установить схему БД необходимо запустить скрипт командой:

```
./install.sh -- --host 127.0.0.1
```

Затем выбрать параметры схемы БД согласно описанию, при стандартной установке после запуска скрипта *install.sh*.

После выбора параметров требуется подтвердить установку схемы БД вводом пароля пользователя.

4.2.4 Ручная оптимизация настроек СУБД PostgreSQL

Для оптимизации настроек СУБД PostgreSQL с целью обеспечения хорошей производительности сервера, необходимо внести изменения в файл postgresql.conf (стандартный путь для PostgreSQL 11: /var/lib/pgsql/11/data/postgresql.conf).

Следует раскомментировать и заменить стандартные настройки следующим значениями:

```
max_connections=500
shared_buffers=512MB # Рекомендуемое значение составляет 25% от
общего объема оперативной памяти компьютера
work_mem=128MB
maintenance_work_mem=1024MB
random_page_cost=4.0 # При использовании SSD понизить до 1.1
```

После внесения изменений необходимо перезапустить БД:

```
systemctl restart postgresql-11.service
```

4.3 Запуск скрипта первоначальной настройки серверных компонентов

Для работы скрипта первоначальной настройки необходимо ПО Git.

Скрипт первоначальной настройки **setup.sh**, находится в каталоге **«/opt/emm»**. После его запуска необходимо ответить на вопросы для создания конфигурационных файлов серверных компонентов и файла **«docker-compose.yml»**, выбранных для установки на этом сервере (для ответов на вопросы предоставляются подсказки: **y** – да, **n** – нет, **q** – выход из настройки, **?** – справочная информация):

```
Bind IP: 0.0.0.0
```

Изменение дефолтного значения 0.0.0.0 может потребоваться при особых условиях настройки сервера с несколькими ip

```
ARM [y/n/q/?]? y
```

Сформировать конфигурацию сервера администрирования.

```
ARM: Use HTTPS [y/n/q/?]? y
```

Использовать протокол HTTPS для сервера администрирования.

```
ARM: Create TLS certificate [y/n/q/?]? y
```

Создать самоподписанный сертификат HTTPS сервера администрирования.

```
ARM: Common Name (IP or domain name): 192.168.1.1
```

Адрес или доменное имя для сертификата сервера администрирования.

```
ARM: use LDAP auth? [y/n/q/?] y
```

Добавить аутентификацию с помощью доменных учётных записей, если выбран ответ «у», то будут запрошены два дополнительных параметра (Адрес и домен сервера AD):

```
ARM: LDAP address: 192.168.1.100
```

```
ARM: LDAP domain: example.com
```

```
iOS MDM [y/n/q/?]? y
```

Сформировать конфигурацию сервера управления MDM

```
iOS MDM: use LDAP auth? [y/n/q/?] y
```


Добавить аутентификацию с помощью доменных учётных записей, если ответ «у», то будут запрошены два дополнительных параметра (Адрес и домен сервера AD):

```
iOS MDM: LDAP address: 192.168.1.100
```

```
iOS MDM: LDAP domain: example.com
```

```
Windows MDM? [y/n/q/?] y
```

Сформировать конфигурацию сервера WinMDM

```
Windows MDM: behind external proxy? [y/n/q/?] y
```

Указать, расположен ли WinMDM за каким-либо внешним прокси-сервером. При выборе режима работы за внешним прокси-сервером, на внешнем прокси-сервере необходимо настроить передачу клиентских сертификатов с прокси-сервера на сервер WinMDM. Пример настройки внешнего прокси-сервера приведен в приложении А.

```
FCM Push Server? [y/n/q/?] y
```

Сформировать конфигурацию пуш-сервера FCM

```
iOS MDM: Create TLS certificate [y/n/q/?]? y
```

Создать самоподписанный сертификат HTTPS сервера управления MDM

```
iOS MDM: Common Name (IP or domain name): 192.168.1.1
```

Адрес или доменное имя для сертификата сервера управления MDM

```
Socket server [y/n/q/?]? y
```

Сформировать конфигурацию сервера команд (Socket server)

```
Socket server: Create TLS certificate [y/n/q/?]? y
```

Создать самоподписанный сертификат HTTPS сервера команд

```
Socket server: Common Name (IP or domain name): 192.168.1.1
```

Адрес или доменное имя для сертификата сервера команд

```
SCEP server [y/n/q/?]? y
```

Сформировать конфигурацию SCEP сервера

```
SCEP server: Create TLS certificate [y/n/q/?]? y
```

Создать самоподписанный сертификат HTTPS SCEP сервера?

```
SCEP server: Common Name (IP or domain name): 192.168.XX.XX
```

Адрес или доменное имя для сертификата SCEP сервера

```
Database hostname: 192.168.1.1
```

Адрес сервера БД

```
Database port (default: 5432): 5432
```

Порт сервера БД

```
Database name: sphone
```

Имя БД

```
Database username: sphone
```

Пользователь БД

```
Database password:
```

Пароль пользователя БД

4.4 Конфигурационные файлы

В результате выполнения скрипта `setup.sh` в каталоге `«/opt/emm»` сформируются конфигурационные файлы серверных компонентов SafeMobile(в подкаталоге `«config»`) и файл `«docker-compose.yml»`, состав и настройки которых будут соответствовать заданным параметрам.

Затем можно изменить количество неправильных попыток ввода пароля в конфигурационном файле `«arm.http.conf»`, который доступен в каталоге `«config/nginx»`. Пример файла приведен ниже, в котором по умолчанию количество попыток авторизаций в минуту равно 3.

```
map $server_name $arm_external_url {  
...  
limit_req_zone $arm_login_zone_key zone=arm_login:10m rate=3r/m  
# Количество попыток авторизаций в минуту = `3`  
...  
}
```

В конфигурационном файле `«/opt/emm/config/arm.yml»` можно выполнить настройку максимального размера файла для отправки командой «Отправить файл», изменив значение по умолчанию 100МБ:

```
arm.cmd-send-file.max-file-size: 100MB
```

В конфигурационном файле `«/opt/emm/config/arm.yml»` можно выполнить настройку уведомлений администраторов о блокировке/разблокировке их учётных записей в

подсекции «mail». В этой подсекции указываются настройки SMTP-сервера, а также настройки темы и содержания отправляемых писем.

4.5 Создание docker-контейнеров

Запустить установку docker-контейнеров с помощью команды:

```
docker-compose up -d
```

Проверить наличие загруженных docker-образов и созданных docker-контейнеров следующими командами:

```
docker images -a
```

```
docker ps -a
```

Если в результате проверки, кроме созданных компонентов, отобразились docker-образы и docker-контейнеры от более ранних версий системы, их следует удалить.

4.6 Настройка интеграции с AD

Если при первоначальной настройке сервера(setup.sh) была выбрана поддержка ldap, то в конфигурационных файлах соответствующих серверных компонентов появятся настройки, которые можно редактировать впоследствии:

1) Сервер Администрирования (arm.yml):

```
ad:
```

```
domain: niisokb.ru
```

```
url: ldap://192.168.1.2
```

```
# search-filter:
```

```
(&(objectClass=user)(userPrincipalName={0})(memberOf=CN=usersy,CN=users,DC=niisokb,DC=ru
```

При необходимости контроля группы пользователей, которым разрешен доступ к АРМ, следует раскомментировать и править строку *search-filter*, где **CN=usersy** – имя группы пользователи, из которой имеют право на доступ к АРМ, **CN=users** – группа верхнего уровня, **DC=niisokb** – имя домена, **DC=ru** – имя домена.

Примечание: Интеграция с AD в АРМ используется, чтобы проверить доменный пароль пользователя и его вхождение в заданную доменную группу, но AD ничего не знает про роль(полномочия) и область управления администратора в SafeMobile.

Поэтому необходимо создать в SafeMobile администратора с тем же логином. Пароль локальной учетной записи совсем не обязан совпадать с доменным, но должен соответствовать парольным политикам APM.

Помимо прочего, это дает резервный способ входа в SafeMobile с локальным паролем, на случай проблем с AD, но его можно отключить через параметр настройки APM

```
database.on: false
```

2) Сервер управления(iosmdm.yml):

```
ldap:
```

```
addr: 192.168.1.2
```

```
basedn: dc=niisokb,dc=ru
```

```
account_lockout_threshold # Количество возможных неудачных  
попыток аутентификации
```

```
account_lockout_duration # Время в минутах на которые будет  
заблокирована учетная запись, если кол-во неудачных попыток  
аутентификации будет превышено
```

```
reset_account_lockout_counter_after # Время через которое будет  
сброшен счетчик неудачных попыток после последней неудачной попытки  
аутентификации (не может быть больше account_lockout_duration )
```

```
group: ""
```

При необходимости контроля группы пользователей, которым разрешено подключение, правим строку `group ""`, например, присваивая значение `group: "CN=usersy, CN=users, DC=niisokb, DC=ru"` – где **CN=usersy** – имя группы, пользователи из которой, имеют право на подключение к серверу Safephone, **CN=users** – группа верхнего уровня, **DC=niisokb** – имя домена, **DC=ru** – имя домена.

Поддержка LDAPS

Для настройки LDAPS, необходимо загрузить на сервер SafeMobile корневой сертификат удостоверяющего центра и внести изменения в конфигурационные файлы соответствующих серверных компонентов.

1. Выгрузка корневого сертификата УЦ

Сертификат в формате PEM необходимо запросить у Администратора УЦ или выгрузить из веб-интерфейса УЦ, если такая функция активирована. На рисунке 4.1

приведен пример, в соответствии с которым необходимо выбрать параметр «Base64» и нажать на ссылку «Загрузка сертификата ЦС».

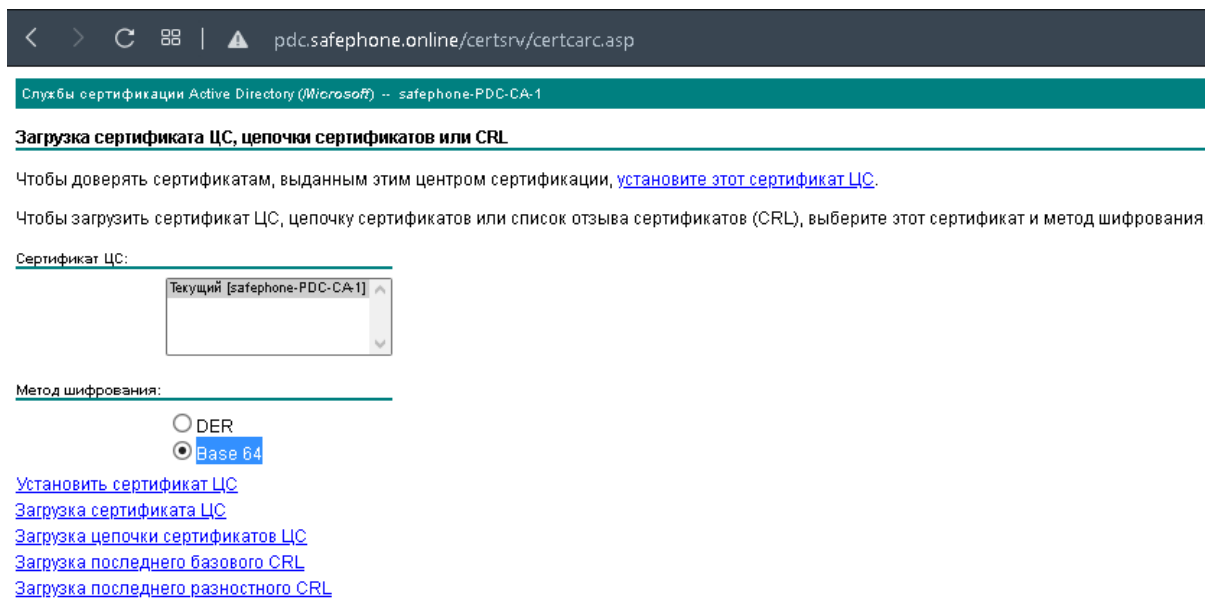


Рисунок 4.1 – Пример загрузки сертификата ЦС

Вместо **pdc.safemobile.online** следует указать имя вашего УЦ. Стандартное имя сертификата «**certnew.cer**» рекомендуется сразу поменять, например, на CN УЦ и скопировать в каталог **config**. На рисунке 4.1 это «**SafeMobile-PDC-CA-1.pem**».

2. Настройка сервера администрирования SafeMobile на поддержку ldaps для входа администраторов с помощью доменной учетной записи

В файл **config/arm.yml** необходимо внести следующие настройки:

`ad:`

`domain: safemobile.online`

`url: ldaps://pdc.safemobile.online:636`

`cert: "/config/SafeMobile-PDC-CA-1.pem"`

где:

safemobile.online – домен, в который входят проверяемые пользователи;

pdc.safemobile.online – DNS-имя сервера ldaps. CN или SAN отдаваемого им SSL-сертификата должен совпадать с этим именем. 636 - стандартный порт при использовании LDAPS;

SafeMobile-PDC-CA-1.pem – имя файла корневого УЦ.

3. Настройка сервера управления SafeMobile на поддержку Idaps для подключения устройств пользователями с помощью доменной учетной записи

В файл **config/iosmdm.yml** необходимо внести следующие настройки:

```
ldap:
```

```
  addr: pdc.safemobile.online
```

```
  port: 636
```

```
  basedn: dc=safemobile,dc=online
```

```
  use_ssl: true
```

```
  cert: /etc/safemobile/iosmdm/SafeMobile-PDC-CA-1.pem
```

где:

dc=safemobile,dc=online – домен, в который входят проверяемые пользователи;
pdc.safemobile.online – DNS-имя сервера Idap. CN или SAN отдаваемого им SSL-сертификата должен совпадать с этим именем. 636 - стандартный порт при использовании LDAPS;

SafeMobile-PDC-CA-1.pem – имя файла корневого УЦ.

После внесения изменений необходимо пересоздать контейнеры командами:

```
docker-compose down -v
```

```
docker-compose up -d
```

Особенности настройки LDAPS приведены в приложении Б.

5 Получение цифровых сертификатов и ключей

Для создания запроса и генерации ключа используется криптографический пакет OpenSSL.

5.1 Сертификаты HTTPS

Для работы серверных компонентов SafeMobile по протоколу HTTPS, потребуются сертификаты и ключи:

- iosmdm.crt – сертификат сервера управления MDM;
- iosmdm.key – приватный ключ сервера управления MDM;
- arm.crt – сертификат сервера администрирования;
- arm.key – приватный ключ сервера администрирования;
- ss.crt – сертификат сервера команд;
- ss.key – приватный ключ сервера команд.

Генерация приватных ключей с формированием долгосрочных самоподписанных сертификатов выполняется при запуске скрипта первоначальной настройки в соответствии с описанием в 4.3.

Проверить, что сертификаты и ключи автоматически помещены в конфигурационный каталог, а именно:

iosmdm.crt и iosmdm.key в /opt/emm/config/;

ss.crt, ss.key, arm.crt и arm.key в /opt/emm/config/nginx/.

Если серверные компоненты, которым требуются HTTPS сертификаты и ключи расположены на разных серверах, следует сертификаты и ключи переместить на целевые серверы в указанные каталоги.

При нежелании использовать самоподписанные сертификаты, следует получить HTTPS-сертификаты в доверенном УЦ. Для этого необходимо выполнить следующие действия:

1. Сгенерировать ключи и сформировать запросы на выпуск сертификатов в формате CSR следующей командой (пример для сервера управления MDM):

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

2. Направить csr-файлы в УЦ. После проверки данных, указанных в запросе, будет выписан сертификат.
3. Полученные сертификаты и ключи поместить в конфигурационный каталог, как было описано в данном подразделе.
4. В файл «iosmdm.crt» сертификата сервера управления MDM необходимо занести всю цепочку сертификатов следующим образом:

```
-----BEGIN CERTIFICATE-----  
сертификат сервера  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
промежуточный сертификат  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
корневой сертификат  
-----END CERTIFICATE-----
```

5.2 Сертификат Push MDM

Для возможности управления МСК на платформе iOS потребуется сертификат и ключ APNS для сервера управления MDM.

После установки и запуска сервис iosmdm-bg будет находиться в циклической перезагрузке, пока не будет получен валидный файл MDMPush.pem.

Для **получения** сертификата Push MDM необходимо выполнить следующие действия:

1. Для запуска процесса генерации приватного ключа и формирования запроса на сертификат в формате CSR выполнить команду:

```
openssl req -new -newkey rsa:2048 -nodes -keyout MdmPush.key -subj  
'/C=RU/ST=Moscow/CN=MdmPush' -out MdmPush.csr
```

В запросе допустимо заменить город Москва на любой другой город Российской Федерации.

2. По окончании генерации ключа и запроса на сертификат будут сформированы два файла:

- MdmPush.csr– запрос на сертификат;
- MdmPush.key – приватный ключ.

3. Файл MdmPush.csr следует отправить/передать в службу технической поддержки «UEM SafeMobile» по электронной почте. Подписанный файл CSR будет возвращён в формате PLIST.

4. После получения PLIST-файла, в браузере перейти на страницу <https://identity.apple.com/pushcert/> и зайти на портал регистрации сертификатов для push-уведомлений (Apple Push Certificates Portal) посредством своей учетной записи (Apple ID).

Примечание – Рекомендуется отдельная учетная запись для должности администратора (не персональная) с целью сохранения возможности управления корпоративными сертификатами при увольнении ответственного сотрудника.

5. На портале регистрации сертификатов для push-уведомлений следует выполнить следующие действия:

- нажать **«Create a Certificate»** (Создать сертификат);
- ознакомиться и согласиться с предложенными условиями, установив галочку в поле **«I have read and agree to these terms and conditions»** и нажав на **«Accept»** (Принять);
- нажать **«Browse»** (Обзор), перейти на подписанный файл MdmPush.plist на своем компьютере, выбрать его и нажать **«Upload»** (Загрузить);

– для получения файла сертификата в формате PEM нажать «**Download**» (Скачать) и скачать файл с названием MDM_Certificate.pem.

6. Файлы MdmPush.key и MDM_Certificate.pem поместить в конфигурационный каталог /opt/emm/config/, при условии, что SafeMobile будет установлен в /opt/emm/, совместно с файлом docker-compose.yml.

7. Объединить файлы сертификата и приватного ключа в один файл MdmPush.pem:

```
echo >> MDM_Certificate.pem;cat MDM_Certificate.pem MdmPush.key |  
grep -Ev "^$" > MdmPush.pem
```

8. В дальнейшем используется только файл MdmPush.pem, поэтому остальные использованные файлы следует удалить для обеспечения безошибочной работы:

```
rm -f MDM_Certificate.pem MdmPush.key
```

9. Полученный сертификат выдается на один год и должен быть своевременно обновлен в соответствии с регламентом, изложенным в этом подразделе.

Для **обновления** сертификата Push MDM необходимо выполнить следующие действия:

1. Сформировать новый запрос с использованием старого ключа следующей командой:

```
openssl req -new -key MdmPush.key -subj  
'/C=RU/ST=Moscow/CN=MdmPush' -out MdmPush.csr
```

2. По окончании генерации запроса на сертификат, сформированный файл MdmPush.csr следует отправить/передать в службу технической поддержки «UEM SafeMobile» по электронной почте. Подписанный файл CSR будет возвращён в формате PLIST.

3. В браузере перейти на страницу <https://identity.apple.com/pushcert/> и зайти на портал регистрации сертификатов для push-уведомлений (Apple Push Certificates Portal) посредством своей учетной записи (Apple ID/Password).

4. На портале регистрации сертификатов для push-уведомлений следует выполнить следующие действия:

– выбрать строку с сертификатом, подлежащим обновлению, и нажать **«Renew»** (Обновить);

Примечание - При обновлении сертификата не следует нажимать «Download» (Скачать) или «Revoke» (Отозвать), т.к. оба эти параметра потребуют повторной регистрации всех МСК на платформе iOS.

– нажать **«Browse»** (Обзор), перейти на подписанный файл MdmPush.plist на своем компьютере, выбрать его и нажать **«Upload»** (Загрузить);

– для получения файла сертификата в формате PEM нажать **«Download»** (Скачать).

5. В конфигурационном каталоге /opt/emm/config/ открыть файл MdmPush.pem и скопировать в него строки из обновленного сертификата, заменив информацию об истекшем сертификате, а информацию о приватном ключе оставив без изменений. Сохранить внесенные изменения.

Пример файла MdmPush.pem приведен ниже:

```
-----BEGIN CERTIFICATE-----  
вставить содержимое обновленного сертификата  
-----END CERTIFICATE-----  
-----BEGIN RSA PRIVATE KEY-----  
оставить без изменений  
-----END RSA PRIVATE KEY-----
```

6. Перезапустить docker-контейнеры для сервера управления MDM следующей командой:

```
docker-compose restart iosmdm iosmdm-bg
```

7. При необходимости отзыва сертификата Push MDM следует на портале регистрации в строке с выбранным сертификатом нажать **«Revoke»** (Отозвать).

5.3 Приватный ключ пуш-сервера FCM

После установки и запуска серверный компонент **fcmpushserver** находится в циклической перезагрузке, пока не будет получен валидный файл **firebase.json**.

Для включения пуш-сервера следует отправить запрос в службу технической поддержки НИИ СОКБ по электронной почте. В ответ будет прислан файл **firebase.json**, который необходимо разместить в каталог **/opt/emm/config/** при условии, что SafeMobile установлен в **/opt/emm/**.

6 Обновление до версии 6.x

6.1 Обновление серверной части до версии 6.x

Для обновления уже установленной «UEM SafeMobile» до текущей версии дополнительно в установочный комплект входит файл `update_by_patch_list-master_to_60.tar.gz`, который рекомендуется распаковать в каталог `/tmp/` командой:

```
tar xzvf update_by_patch_list-master_to_60.tar.gz -C /tmp/
```

Чтобы обновить систему следует выполнить следующие операции (предполагается, что система установлена в `/opt/emm`):

1. Остановить docker-контейнеры следующей командой:

```
cd /opt/emm; docker-compose down -v
```

2. Установить новые docker-образы серверных компонентов из архива **emm-docker.tar.gz** посредством команды:

```
docker load -i emm-docker.tar.gz
```

3. Переименовать каталог «**emm**» в «**emm-old**»:

```
mv -R /opt/emm /opt/emm-old
```

4. Создать каталог «**/opt/emm**», распаковать в него архив с конфигурацией компонентов и скрипт обновления БД с помощью команд:

```
mkdir /opt/emm
```

```
tar xzvf emm-config.tar.gz -C /opt/emm
```

И пройти мастер первоначальной настройки `setup.sh`, выбирая компоненты, необходимые на данном сервере. SSL сертификаты генерировать не нужно, т.к. они уже есть в каталоге «`emm-old`».

5. Установить патч БД из каталога **/tmp/** посредством скрипта **install.sh** следующей командой:

```
./install_patch.sh -- --host=127.0.0.1
```

При запуске скрипта `./install_patch.sh`, до начала наката первого патча, автоматически создается бэкап БД в каталоге `/tmp`.

6. В каталоге «**/opt/emm/config**» содержатся сформированные конфигурационные файлы компонентов SafeMobile. Следует сравнить

конфигурационные файлы релиза 6.x в каталоге «**emm**» с файлами в каталоге «**emm-old**» и дополнить их, при необходимости, измененными настройками из старых файлов.

7. Скопировать файлы формата CRT, KEY, PEM из каталога «**emm-old/**» в «**emm/**». Пример команд приведен ниже:

```
cp /opt/emm-old/ca.pem /opt/emm/
```

```
cd /opt/emm-old/config
```

```
cp /opt/emm-old/config/$(ls *.crt *.key MdmPush.pem) /opt/emm/config/
```

```
cd /opt/emm-old/config/nginx/
```

```
cp /opt/emm-old/config/nginx/$(ls *.crt *.key) /opt/emm/config/nginx/
```

8. Запустить docker-контейнеры с помощью команды:

```
cd /opt/emm; docker-compose up -d
```

9. Проверить наличие созданных docker-образов и docker-контейнеров следующими командами:

```
docker images -a
```

```
docker ps -a
```

Docker-образы и docker-контейнеры более ранних версий следует удалить.

6.2 Особенность применения профилей после обновления с версии 4.4.x до 6.x

В версии 4.5 и последующих, изменился способ расчета результирующих политик профилей: «Профили парольных политик», «Профили ограничений», «Профили режима киоска», «Профиль настроек монитора Android», «Профиль настроек монитора Android», «Профиль управления датой и временем Samsung Knox». Если в предыдущей версии применялись самые строгие политики из всех назначенных профилей, то в SafeMobile 6.x, после обновления будет применяться политика из ближайшего к МСК профиля. Под «**ближайшим**» понимается назначение, сделанное на ближайший к устройству узел в цепочке: устройство - пользователь - подразделение - корень ОШС.

Перед обновлением SafeMobile с версии 4.4.x до версии 6.x выполнить следующие действия:

- Проверить содержимое профилей: необходимо, чтобы в профилях одного типа, назначенных и подразделениям, и сотрудникам и, возможно, отдельным устройствам не были заданы разные значения одних и тех же политик. Чтобы сохранить поведение системы после обновления следует выбрать самое строгое значение политики, указать его в самом «верхнем» профиле, назначенном выше всего в ОШС, а в профилях «ниже» указать значение «не задано».
- Убедиться, что нет профилей одного типа, назначенных на одно и то же подразделение или сотрудника. Если такие профили найдутся, оставить только один.

6.3 Работа с дампом БД, полученным перед патчем до новой версии

При обновлении будет сформирован дамп БД в каталоге /tmp. Имя файла дампа <"имя-бд"_"имя-схемы"_"версия-БД-до-патча"-"дата-время-создания".dmp>.

Например: если имя БД и имя схемы **sphone**, а версия до обновления 5.0.4, то файл дампа будет иметь имя **sphone_sphone_5.0.4-20220613_1214.dmp**. В том же каталоге будет находиться файл лога снятия дампа. Он будет иметь такое же имя, а расширение .log.

Если потребуется восстановление БД из дампа, сначала необходимо очистить схему БД. Для этого выполнить следующие действия:

1. Распаковать архив инсталлятора БД нужной версии в любой каталог на сервере (или если он уже распакован, то следует перейти в этот каталог).
2. Очистить схему БД, выполнив команду от пользователя postgres (из-под root-а выполнить su - postgres):

```
./setup.sh --dump-prepare
```

После этого можно приступить к восстановлению БД из дампа:

```
pg_restore -O -h 127.0.0.1 -U sphone -d sphone  
/tmp/sphone_sphone_5.0.4-20220613_1214.dmp
```

где:

pg_restore – команда для восстановления БД из дампа;

-h 127.0.0.1 – установить соединение с хостом указанного IP;

-U sphone – соединиться как пользователь postgresql sphone (можно посмотреть в конфигурационном файле db.yml параметр user);

-d sphone – имя целевой БД (можно посмотреть в конфигурационном файле db.yml параметр name);

sphone_sphone_4.4.8.4-20211013_1214.dmp – имя файла дампа.

При восстановлении дампа вначале может возникнуть ошибка:

```
pg_restore: error: could not execute query: ERROR: permission denied for database sphone
```

```
Command was: CREATE SCHEMA sphone;
```

Это происходит потому, что схема уже существует, но, если в дальнейшем ошибок не возникает, значит импорт проходит нормально.

6.4 Особенности обновления БД с версии 5.0.3 и более ранних

Для обновления уже установленной «UEM SafeMobile» версии 5.0.3 и более ранних, в установочный комплект дополнительно входит патч, посредством которого задания, выполняющиеся по расписанию (job's), удаляются из БД postgres и создаются в БД sphone. Для этого в БД sphone создается схема pgagent, в которой и будет храниться информация об этих заданиях.

После установки патча следует выполнить следующие действия:

1. Вывести список процессов, в названии которых есть подстрока pgagent:

```
systemctl list-units | grep pgagent
```

Для PostgreSQL 11, установленного в CentOS сервис будет называться pgagent_11.service.

2. Следует остановить сервис и убрать его из автозагрузки:

```
systemctl stop pgagent_11
```

```
systemctl disable pgagent_11
```

3. Удалить пакет pgagent_11 из системы:

```
yum remove pgagent_11
```


7 Управление серверными компонентами «UEM SafeMobile»

1. Просмотреть текущие версии установленных компонентов можно следующими командами:

```
docker ps -a
```

2. При изменениях в конфигурации серверных компонентов следует перезапустить docker-контейнеры следующей командой:

```
cd /opt/emm; docker-compose restart <ИМЯ КОМПОНЕНТА>
```

3. Обновление docker-образов осуществляется следующими командами, при этом необходимо сначала остановить и удалить docker-контейнеры, затем обновить версии в файле **«.env»** и запустить docker-контейнеры:

```
docker-compose down -v
```

```
docker load -i emm-docker.tar.gz
```

```
docker-compose up -d
```




4. При внесении изменений в файлы **«.env»** или **«docker-compose.yml»**, следует пересоздать docker-контейнеры командой:

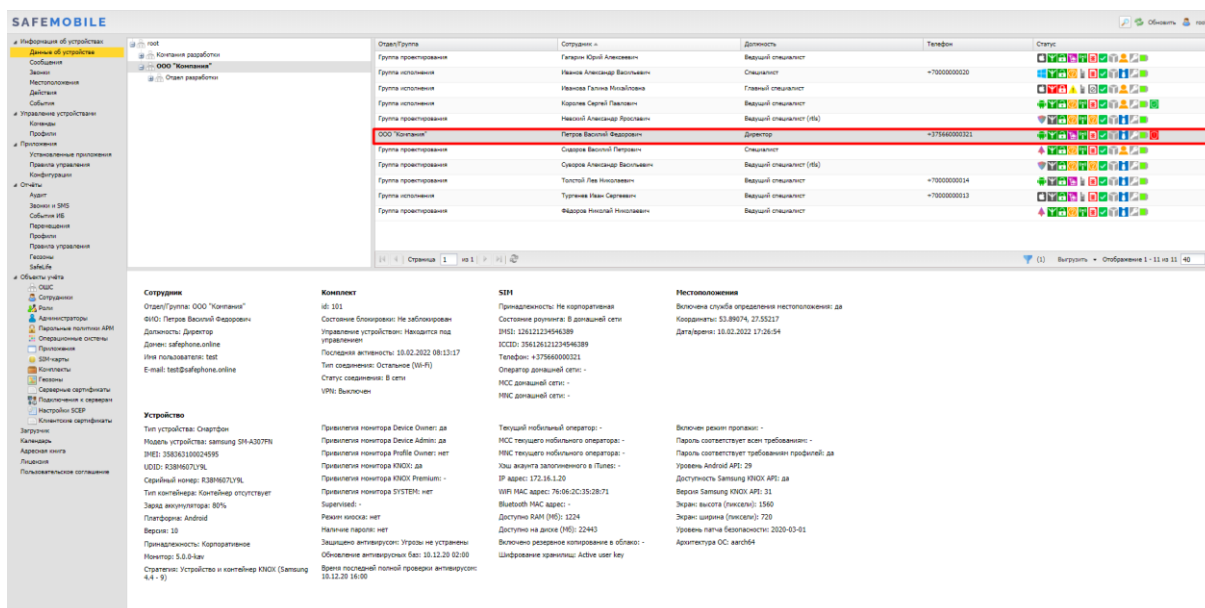
```
docker-compose up -d
```

8 Проверка работоспособности «UEM SafeMobile»

После установки и запуска сервисы iomdm-bg и fcsmrpushserver будут находиться в циклической перезагрузке, пока не будут получены валидные файлы MDMPush.pem и firebase.json, соответственно.

Для контроля работоспособности «UEM SafeMobile» требуется:

1. Войти в APM Администратора SafeMobile, для этого в адресной строке браузера ввести <https://ip-address:8443>, (вместо <ip-address> следует указать адрес сервера администрирования). Должна отобразиться страница авторизации, для входа понадобится ввести логин и пароль действующей учетной записи администратора.
2. В таблице MCK главного окна выбрать **подключенный, незаблокированный и доступный для управления** комплект в соответствии с рисунком 8.1, у которого:
 - состояние соединения MCK, которое отображается в столбце «Статус»,  – в сети;
 - состояние блокировки MCK, которое отображается в столбце «Статус»,  – не заблокирован;
 - состояние управления устройством, которое отображается в столбце «Статус»,  – доступно для управления.



Группа	Имя	Роль	Статус	Управление
Группа администраторов	Григорьев Юрий Александрович	Ведущий специалист		
Группа исполнителей	Николаев Александр Васильевич	Специалист		
Группа исполнителей	Королева Сергей Павлович	Ведущий специалист		
Группа исполнителей	Николаев Александр Васильевич	Ведущий специалист (M)		
ООО "Компания"	Петров Василий Федорович	Директор		
Группа администраторов	Смирнов Василий Григорьевич	Специалист		
Группа исполнителей	Смирнов Александр Васильевич	Ведущий специалист (M)		
Группа администраторов	Туркина Гали Николаевна	Ведущий специалист		
Группа исполнителей	Туркина Иван Сергеевич	Ведущий специалист		
Группа администраторов	Федоров Николай Николаевич	Ведущий специалист		

Сотрудник
 Отдел/Группа: ООО "Компания"
 ФИО: Петров Василий Федорович
 Должность: Директор
 Данные профиля: test@safermobile.online
 Имя пользователя: test
 E-mail: test@safermobile.online

Комплект
 ID: 101
 Состояние блокировки: Не заблокирован
 Управление устройством: Находится под контролем
 Последняя активность: 18.02.2022 08:13:17
 Тип соединения: Остаточное (M-F)
 Статус соединения: В сети
 VPN: Выключен

СМН
 Принадлежность: Не корпоративная
 Состояние роуминга: В домашней сети
 IMEI: 29612121494389
 ICCID: 29612612323494389
 Телефон: +37566000021
 Оператор домашней сети: -
 MCC домашней сети: -
 MNC домашней сети: -

Нестационализация
 Включена служба определения местоположения: да
 Координаты: 53.89074, 27.55217
 Дата/время: 18.02.2022 17:26:54

Устройство
 Тип устройства: Смартфон
 Модель устройства: samsung SM-A207N
 IMEI: 35836310024595
 UUID: 8388607196
 Серийный номер: R3888607196
 Тип контейнера: Контейнер отсутствует
 Заряд аккумулятора: 99%
 Платформа: Android
 Версия: 10
 Принадлежность: Корпоративное
 Номер: 5.0.0-kay
 Состояние: Устройство и контейнер Knox (Samsung 4.4 - 9)
 Привилегия монитора Device Owner: да
 Привилегия монитора Profile Owner: нет
 Привилегия монитора Knox: да
 Привилегия монитора Knox Premium: -
 Привилегия монитора SYSTEM: нет
 Выключен: -
 Режим вывоза: нет
 Наличие пароля: нет
 Защита авторизации: Угрозы не устранены
 Обновление авторизации: 18.12.20 02:00
 Форма последней полной проверки авторизации: 18.12.20 16:00

Телефонный оператор:
 Текущий мобильный оператор: -
 MCC текущего мобильного оператора: -
 MNC текущего мобильного оператора: -
 Оши аккаунта заполненного в Плате: -
 IP адрес: 172.16.1.20
 WAP NAS адрес: 76.06.202.35:2871
 IPv6/WAN NAS адрес: -
 Доступно RAM (M): 1224
 Доступно на ядре (M): 2243
 Включено резервное копирование в облако: -
 Шафрование клавиатуры: Active user key

Включен режим прошивки:
 Пароль соответствует всем требованиям: -
 Пароль соответствует требованиям прошивки: да
 Уровень Android API: 29
 Доступность Samsung Knox API: да
 Версия Samsung Knox API: 31
 Экран вывоза (пиксели): 1560
 Экран ширины (пиксели): 720
 Уровень языка безопасности: 2020-03-01
 Архитектура ОС: arm64

Рисунок 8.1 – Выбор подключенного незаблокированного комплекта

3. В главном меню выбрать раздел «Команды» и отправить на устройство команду «Переподключение» соответствии с рисунком 8.2, с параметром 10 с. Затем в окне «Уведомления» нажать кнопку «ОК».

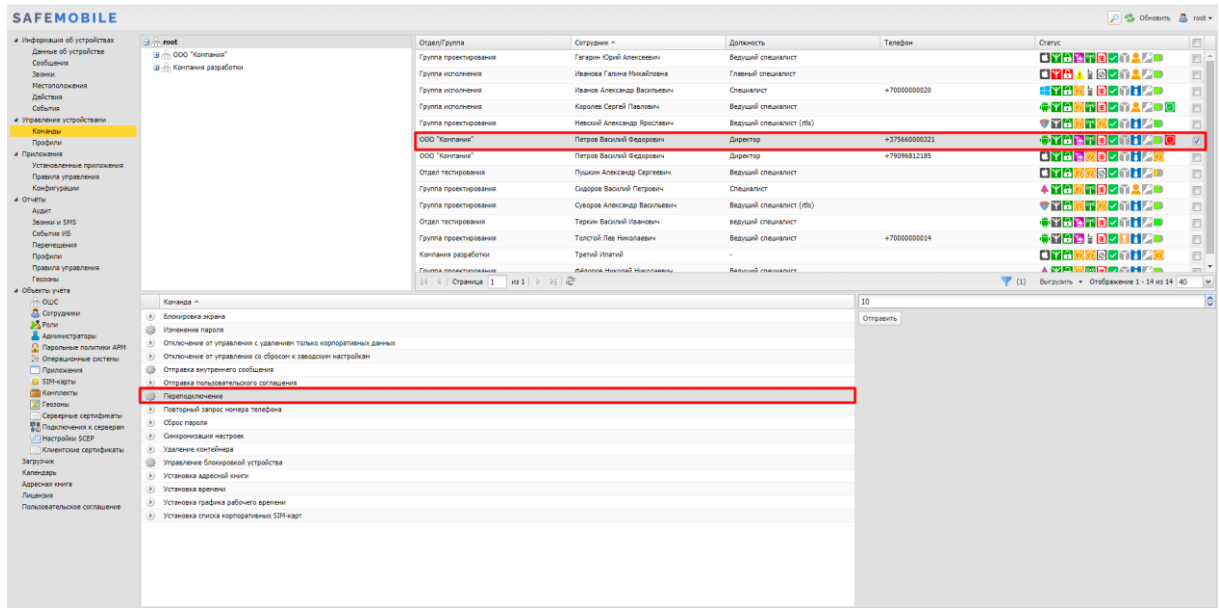


Рисунок 8.2 – Отправка команды «Переподключение»

4. Дождаться результата выполнения действия: когда значение в разделе «Действие» изменится на значение, отличное от «Ожидание результата»:

- о результат «Нормальное завершение» свидетельствует о работоспособности «UEM SafeMobile» (рисунок 8.3);

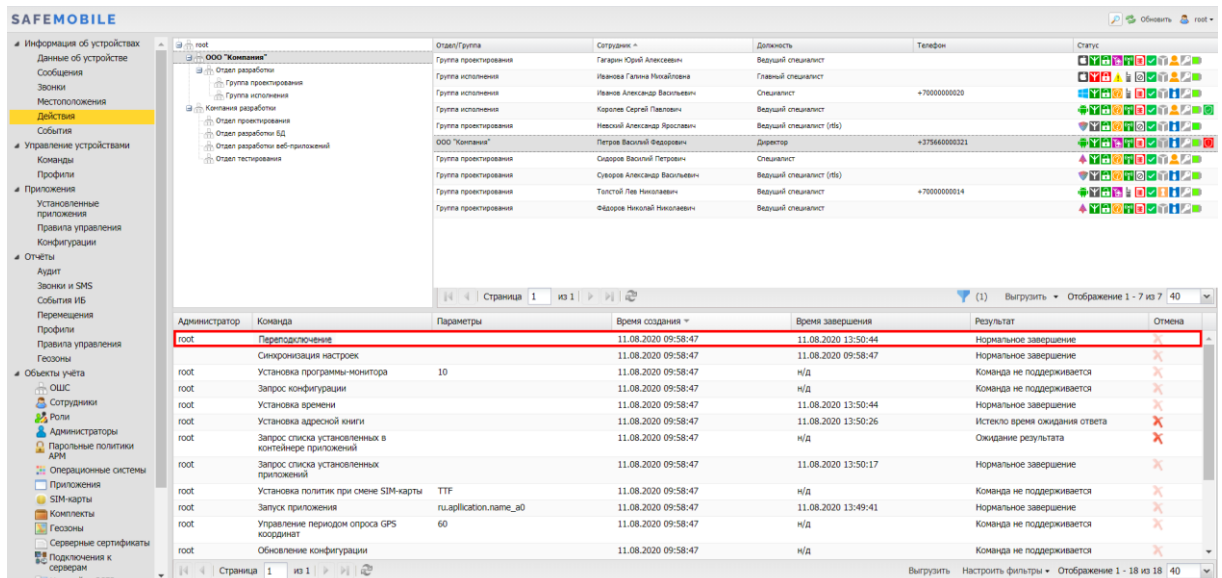


Рисунок 8.3 – Результат команды «Переподключение»

- о значение результата, отличное от «Нормальное завершение», свидетельствует о возможном нарушении работоспособности системы.

Приложение А

Настройки для внешнего прокси-сервера Nginx

Решение об использовании внешнего прокси-сервера принимается при запуске скрипта первоначальной настройки.

Пример необходимых настроек для внешнего прокси-сервера Nginx:

```
server {  
    listen 443 ssl;  
    server_name win.sso3.sp4x.ru;  
    ....  
    ssl_verify_client optional_no_ca;  
    location{  
        proxy_pass https://10.17.7.47:8444;  
        ....  
        proxy_set_header X-Client-  
Certificate $ssl_client_escaped_cert;  
    }  
}
```

Приложение Б Особенности настройки LDAPS

Порядок использования сертификатов LDAP (Active Directory)

Краткое описание

Сертификат LDAP необходим для взаимодействия с LDAP-сервером. Как правило, это Active Directory.

Docker-образ APM при старте, после проверки необходимости использования сертификатов, сохраняет сертификаты во внутреннее хранилище. После остановки docker-образа APM, внутреннее хранилище сертификатов уничтожается.

Настройки APM для работы с сертификатом АД

Путь к сертификату указывается в настройках с учётом нахождения в файловой системе docker-образа.

Как правило, в docker-образе используется каталог /config/, который ассоциирован с каким-либо каталогом хостовой ОС в файле docker-compose.yml.

```
ad:  
  cert: "/config/<название файла>"
```

Сертификат копируется в хранилище сертификатов (внутри Docker-container) в случае использования настроек:

```
auth-provider:  
  active-directory.on: true  
ad:  
  url: "ldaps:<адрес и, возможно, порт>"
```

ВАЖНО! Значение настройки `ad.url` должно начинаться с `ldaps`.

При неправильных настройках APM для работы сертификатами запуск APM будет неуспешным.

Контроль успешности запуска возможен с помощью команды:

```
docker-compose logs arm > arm.log && cat arm.log
```

Примеры настроек AD

Для доступа к AD используется сертификат из файла safemobile_pdc_ca.cer

```
#
auth-provider:
  database.on: true
  active-directory.on: true
ad:
  domain: safemobile.online
  url: ldaps://10.17.7.44:636
  cert: "/config/safemobile_pdc_ca.cer"
```

Контроль сертификата LDAP

Нужно проверить:

1. наличие сертификата CA, предоставленного настройкой cert: и то, что это именно сертификат
2. доступность ресурса, предоставленного настройкой url: и то, что там именно SSL
3. сертификат, выдаваемый по url: должен быть выдан именно тем УЦ, который представлен сертификатом cert:

Сначала можно провести сразу три проверки одним запросом, пример:

```
>>> openssl s_client -connect pdc.safemobile.online:636 -CAfile
/opt/safemobile/postgresql/config/safephone-PDC-CA-1.pem
```

Диагностические сообщения

Вывод диагностических сообщений не зависит от уровня логирования.

Сообщение	Категория	Комментарий
AD:auth-provider.active-directory.on: no need to check the ldaps certificate	INFO	Сообщение об отсутствии необходимости контроля сертификата. Идентификация и аутентификация по LDAP отключены.
AD:ldaps not found: no need to check the certificate	INFO	Сообщение об отсутствии необходимости контроля сертификата. Идентификация и аутентификация по LDAP настроена на незащищённый протокол (например: ad.url: ldap://safemobile.online:389).

Сообщение	Категория	Комментарий
AD:ldaps: Check "ad.url" setting. The url is bad:[]	ERROR	Сообщение об отсутствии адреса ldap-сервера (например: AD:ldaps: Check "ad.url" setting. The url is bad:[]).
AD:config cert filename: filename	INFO	Сообщение об имени файла сертификата из настроек
AD:ldaps: Check "ad.cert" setting. The certificate file not found:[<имя файла сертификата>]	ERROR	Файл сертификата не найден
AD:remove: <имя временного файла>	INFO	Сообщение об удалении временного файла
AD:connect:test...	INFO	Начало проверки возможности соединения с ldap-сервером, только для ldaps-протокола
строки с данными сертификата	INFO	Выполнение команды openssl s_client -connect <ldap_addr> -showcerts </dev/null
AD:connect:test...ERROR	ERROR	Сообщение об ошибке соединения с ldap-сервером, только для ldaps-протокола
AD:connect:test...OK	INFO	Сообщение об успехе соединения с ldap-сервером, только для ldaps-протокола
AD:Get PEM from:<ldap_addr>	INFO	Начало попытки получения сертификата ldap-сервера
AD:Get PEM from:ERROR	ERROR	Ошибка получения сертификата ldap-сервера
AD:PEM format:ERROR	ERROR	Ошибка просмотра содержания сертификата с ldap-сервера
AD:CERT CONFIG:PEM format:<имя файла сертификата из настроек>:ERROR:	ERROR	Ошибка просмотра содержания сертификата, указанного в настройках. Значения искать в документации к openssl
AD:diff:[<cert_config_filename>] vs [<ldap_addr>]:Certificates do not match each other:ERROR	ERROR	Сертификат из настроек не соответствует сертификату с ldap-сервера
AD:check:OK	INFO	Контроль сертификата LDAP закончен

Сообщение	Категория	Комментарий
ERROR: There can be problems when working with active directory	ERROR	Предупреждение о возможных проблемах работы с ldap-сервером

Основные диагностические сообщения

Certificate was added to keystore - сертификат добавлен во внутреннее хранилище сертификатов

ERROR: ARM settings file not found: - не найден файл с настройками APM.

ERROR: Cert file not found: - не найден файл сертификата. Возможно, неправильно указано имя файла.

WARN: AD cert not defined - не указан файл сертификата АД

Add AD cert to keystore: - успешное добавление сертификатов во внутреннее хранилище APM

Пример сообщений

Успешный запуск APM:

```
arm_1 | Certificate was added to keystore
arm_1 | Certificate was added to keystore
arm_1 | AD enabled: True
arm_1 | ldaps url:ldaps://10.17.7.44:636
arm_1 | AD cert: /config/safemobile_pdc_ca.cer
arm_1 | Add AD cert to keystore:/config/safemobile_pdc_ca.cer
```

Неуспешный запуск APM:

```
arm_1 | AD enabled: True
arm_1 | ldaps url:ldaps://10.17.7.44:636
arm_1 | AD cert: /config/safemobile_pdc_ca.cert
arm_1 | ERROR: Cert file not found:
/config/safemobile_pdc_ca.cert
```

Неуспешный запуск APM:

```
arm_1 | Certificate was added to keystore
arm_1 | AD enabled: True
arm_1 | ldaps url:ldaps://10.17.7.44:636
arm_1 | AD cert: /config/safemobile_pdc_ca.cer
arm_1 | Add AD cert to keystore:/config/safemobile_pdc_ca.cer
arm_1 | ERROR: Cert file not found: /config/exch-lync.cert
arm_1 | Certificate was added to keystore
```


Приложение В

Подготовка компьютера для агента регистрации

Регистрационный агент представляет собой Windows сервис, который устанавливается на компьютер с ОС Windows в инфраструктуре заказчика.

Для инсталляции Агента регистрации необходимо выполнить следующие действия:

В.1 Установка Агента регистрации должна производиться на компьютере, включенном в тот же домен, что и сервер СА.

В.2 Все действия должны выполняться от имени доменного администратора.

В.3 Скачать и установить пакет **.NET Framework 4.7.2**, если данный пакет еще не был установлен.

В.4 Скачать и установить Агент регистрации. Файл **«SafeMobileEnrollmentAgentSetup.msi»** входит в комплект ПО для установки «UEM SafeMobile» по требованию заказчика.

В.5 Создать доменного пользователя, от имени которого будет запускаться служба Агента регистрации.

В.6 Добавить пользователя в группу **CERTSVC_DCOM_ACCESS** или Certificate Service DCOM Access, на контролере домена или на любом компьютере домена с установленным RSAT.

В.7 На компьютере с установленным Агентом регистрации следует выполнить следующие действия:

В.7.1.1 Запустить оснастку Services (mmc.exe services.msc).

В.7.1.2 В параметрах службы агента регистрации **SafeMobile EnrollmentSrv** настроить вход в систему от имени созданного пользователя.

В.8 В каталоге установки агента регистрации (обычно C:\Program Files (x86)\NIISOKB\SafeMobile Enrollment Agent) настроить параметры подключения к СА и БД в файле conf.yml:

Агент регистрации может поддерживать несколько СА.

```
# SafeMobile database connection settings

ca:

pdc.example.com\CA

# - pdc2.example.com\CA2

enrollmentTemplate: EnrollmentAgent #template certificate for
enrollment agent. Default EnrollmentAgent

db:

type: postgresql

user: sphone

password: 111

host: 127.0.0.1

port: 5432

name: sphone # "database name" for postgresql
```

B.9 Адрес удостоверяющего центра можно посмотреть в файле C:\Windows\System32\certsrv\certdat.inc (переменная sServerConfig) на сервере CA.

B.10 На сервере CA в оснастке mmc Component Services выбрать свойства компонента: Console root -> Component Services -> Computers -> My computer -> DCOM config -> CertSrv request. В закладке Security в свойствах Launch and Activation permissions выбрать Customize -> Edit. Убедится, что доменной группе CERTSVC_DCOM_ACCESS или Certificate Service DCOM Access разрешены права: Remote Launch и Remote Activation. Для свойства Access Permissions группе CERTSVC_DCOM_ACCESS или Certificate Service DCOM Access должны быть разрешены права Remote Access.

B.11 На сервере CA в оснастке **mmc Certificate Templates** выбрать шаблон **Enrollment Agent** в закладке **Security** задать для пользователя службы агента регистрации разрешения: **Read** и **Enroll**.

B.12 На сервере CA в оснастке **mmc Certification Authority** в каталог **Certificate Templates** добавить шаблон **Enrollment agent**, если еще не добавлен.

B.12.1 Проверить доступность CA можно следующим образом:

V.12.1.1 Запустить интерпретатор командной строки от имени созданного пользователя. Например,

```
runas /user: SafeMobile \enrollment_agent cmd.
```

V.12.1.2 В командном интерпретаторе набрать:

```
certutil -ping -config "<Адрес удостоверяющего центра>".
```

V.12.1.3 Если настройки выполнены правильно, то будет результат:

```
CertUtil: -ping - command completed successfully.
```

V.13 На компьютере агента регистрации запустить сервис **SafeMobileEnrollmentSrv**.

V.14 Перейти в системный журнал событий компьютера агента регистрации и убедиться, что в ветке: **Event viewer -> Windows Logs -> Application** нет событий с ошибками от источника **SafeMobile Enrollment Agent**.