

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

SAFEMOBILE

Москва

2024

СОДЕРЖАНИЕ

Перечень используемых терминов и сокращений	4
1 Введение	6
2 Назначение и условия применения	9
2.1 Назначение «UEM SafeMobile»	9
2.2 Требования к программному обеспечению	9
2.3 Системные требования	10
2.4 Требования к сетевому окружению	12
2.5 Требования к серверу БД	14
2.6 Требования к сертификатам HTTPS	16
3 Установка и настройка ПО Docker	17
4 Установка и настройка серверных компонентов «UEM SafeMobile»	17
4.1 Распаковка архивов серверных компонентов	18
4.2 Установка схемы БД PostgreSQL	18
4.2.1 Стандартная установка на сервер с уже имеющейся СУБД PostgreSQL	19
4.2.2 Первоначальная установка на новом сервере	20
4.2.3 Минимальная установка	20
4.2.4 Ручная оптимизация настроек СУБД PostgreSQL	21
4.2.5 Настройка СУБД PostgreSQL при работе в отдельной подсети	21
4.2.6 Подключение к СУБД PostgreSQL по сертификату	22
4.3 Запуск скрипта первоначальной настройки серверных компонентов	24
4.4 Конфигурационные файлы	27
4.5 Настройки сервиса отправки почты	28
4.6 Создание docker-контейнеров	30
4.7 Настройка раздела «Подключения к серверам» в APM	30

5	Получение цифровых сертификатов и ключей.....	32
5.1	Сертификаты HTTPS	32
5.2	Сертификат Push MDM.....	34
5.3	Приватный ключ пуш-сервера FCM.....	37
5.4	Сертификат SCEP	38
6	Обновление до версии 8.x.....	39
6.1	Обновление серверной части до версии 8.x.....	46
6.2	Особенность применения профилей после обновления с версии 4.4.x до 8.x48	
6.3	Работа с дампом БД, полученным перед патчем до новой версии	49
6.4	Особенности обновления БД с версии 5.0.3 и более ранних.....	50
7	Управление серверными компонентами «UEM SafeMobile»	51
8	Проверка работоспособности «UEM SafeMobile»	52
9	Приложение А – Диагностические сообщения при запуске APM.	54

Перечень используемых терминов и сокращений

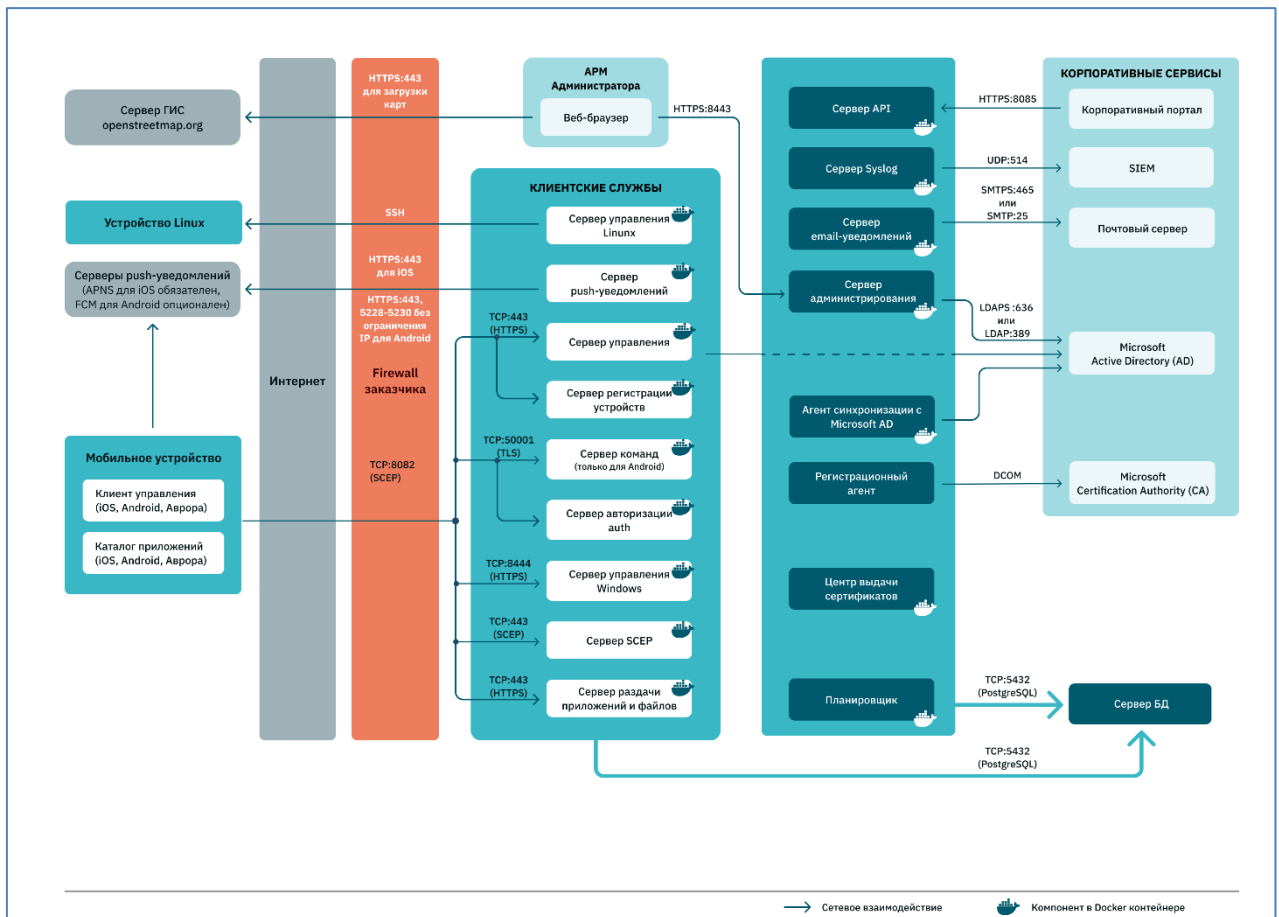
Таблица 1 – Перечень терминов и сокращений

Сокращение	Полное наименование
AD	Служба каталогов (Active Directory)
API	Интерфейс прикладного программирования (Application Programming Interface)
APNS	Служба push-уведомлений устройств Apple (Apple Push Notification Service)
AUTH	Сервер авторизации для SS
CA	Встроенный удостоверяющий центр для выпуска сертификатов mTLS
CPU	Центральное процессорное устройство (Central Processing Unit)
CSR	Запрос на получение сертификата (Certificate Signing Request)
DCOM	Расширение стандарта Component Object Model (Distributed COM)
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)
SCEP	Упрощенный протокол запроса и получения сертификатов (Simple Certificate Enrollment Protocol)
SIEM	Управление информацией и событиями безопасности (Security information and event management)
SMTP	Упрощенный протокол передачи почты (Simple Mail Transfer Protocol)
SSD	Запоминающее устройство, твердотельный накопитель (Solid State Drive)
TCP	Протокол управления передачей (Transmission Control Protocol)
UDP	Протокол пользовательских датаграмм (User Datagram Protocol)
UEM	Unified Endpoint management
APM	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

Сокращение	Полное наименование
СУБД	Система управления базами данных
УЦ	Удостоверяющий центр

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».



Состав UEM «SafeMobile»

Клиентские компоненты:

- мобильный клиент:
 - iOS – приложение EMM Client и встроенный системный MDM клиент;
 - Android – приложение «Monitor»;
 - Аврора – приложение EMM-Client «Monitor»;
 - Windows – встроенный системный MDM клиент;
- АРМ Администратора.

Серверные компоненты:

- **adagent** – агент синхронизации с Microsoft AD;
- **apple-mdm-push** – сервис пуш-уведомлений для управления устройствами iOS;
- **arm** – сервер администрирования;
- **auth-server** - сервер авторизации для компонента **socket-server**. Устанавливается автоматически вместе с компонентом **socet-server** и не требует дополнительных настроек;
- **ca** - встроенный УЦ для выпуска сертификатов mTLS. Устанавливается автоматически вместе с компонентом **arm** и не требует дополнительных настроек;
- **db** – сервер баз данных;
- **fcmpushserver** – сервис отправки пуш-уведомлений FCM (для некоторых Android). Использование пуш-сервиса FCM на данный момент опционально и может потребоваться только для управления некоторыми Android-устройствам с урезанной прошивкой, не обеспечивающей автозапуск и защиту MDM-агента от остановки операционной системой.
- **file-distr-server** - сервер раздачи корпоративных приложений и файлов;
- **iosmdm** – сервер управления MDM (для Android, iOS, Windows и АврораОС);
- **apple-monitor-push** – сервис отправки пуш-уведомлений приложению EMM Client на iOS;
- **lmsrv** – сервер управления Linux;
- **mail-agent** – сервис отправки электронной почты;
- **nginx** – прокси-сервер, обеспечивающий внешние подключения по портам 443, 8443, 50001, 8444, 8082, 8085(стандартные значения, могут быть изменены);
- **regportal** – сервер регистрации устройств;
- **scep** – сервер получения пользовательских сертификатов из УЦ, устанавливается автоматически при установке iosmdm;
- **scep-standalone** – scep сервер устанавливаемый отдельно. Устаревший вариант комопонента. Используется только в случае, если в прежней версии был развернут и настроен сервер scep;
- **scheduler** – планировщик БД, автоочистка;

- **sesl** – сервис отправки системных логов;
- **smapi** – сервер публичного API;
- **socket-server** – сервер команд (для Android);
- **winmdm** – сервер управления Windows. Назначение и условия применения.

В версиях «UEM SafeMobile» 8.x, для аутентификации устройств, используется протокол mTLS (см. раздел 6).

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 2.1 – Системные требования для основных компонентов

Количество МСК	ВМ	CPU	ОЗУ, ГБ	Диск, ГБ
1 – 100	Сервер SafeMobile (db+arm+iosmdm+apple-mdm-push+regportal+apple-monitor-push+socket-server+fcmpushserver+scep+ca+auth-server+file-distr-server+scheduler)	2	4	20
101 – 500	Сервер SafeMobile (db+arm+iosmdm+apple-mdm-push+regportal+apple-monitor-push+socket-server+fcmpushserver+scep+ca+auth-server+file-distr-server+scheduler)	2	6	30
501 – 1000	Сервер Управления и Администрирования (arm+iosmdm+apple-mdm-push+regportal+apple-monitor-push+socket-server+fcmpushserver+scep+ca+auth-server+file-distr-server+scheduler)	2	4	30
	Сервер БД (db)	2	4	100
1001 – 2000	Сервер Управления (iosmdm+apple-mdm-push+regportal+apple-monitor-push+socket-server+fcmpushserver+scep+auth-server+file-distr-server+scheduler)	2	4	30
	Сервер Администрирования (arm+ca)	2	7	30
	Сервер БД (db)	2	6	200
2001 – 10000	Сервер Команд (socket-server+auth-server+fcmpushserver)	2	4	20
	Сервер Управления (iosmdm+apple-mdm-push+regportal+apple-monitor-push+file-distr-server+scheduler+scep)	4	4	20
	Сервер Администрирования (arm+ca)	2	7	20
	Сервер БД (db)	4	16	300

Таблица 2.2 – Системные требования для опциональных компонентов

ВМ	CPU	ОЗУ, ГБ	Диск, ГБ
Сервер Интеграций (scep-standalone+adagent+mail-agent+sesl)	2	4	20
Сервер Управления Linux/Windows (lmsrv/winmdm)	2	4	20
Сервер SMAPI	1	3	20

Размер диска указан из расчёта, что всё пространство, кроме разделов boot и swar, будет отдано под корень файловой системы.

Таблица 2.3 – Системные требования для 10к+ устройств iOS, Android, Аврора

Контейнер	CPU	ОЗУ, ГБ	Число серверов для 10- 20к	Число серверов для 20- 30к	Число серверов для 30- 40к	Число серверов для 40- 50к
adagent	1	1	1	1	1	1
apple-mdm-push	1	1	2	4	6	8
arm+ca	2	6	1	1	1	1
fcmpushserver	1	1	2	4	6	8
file-distr-server	1	1	3	6	9	12
iosmdm	2	2	2	4	6	8
apple-monitor-push	1	1	2	4	6	8
mail-agent	1	1	1	1	1	1
regportal	1	2	1	1	1	4
scep	1	1	2	4	6	8
scheduler	1	0,5	1	1	1	1
sesl	1	1	1	1	1	1
smapl	1	3	1	1	1	2
socket-server+auth-server	1	1	1	1	1	4

Таблица 2.4 - Системные требования для работы компонента «Сервер БД (db)» для 10к+ устройств

Количество устройств	CPU	ОЗУ, ГБ	Диск, ГБ
10-20к	8	32	600
20-30к	12	48	800
30-40к	16	64	1000
40-50к	20	80	1200

Таблица 2.5 - Системные требования для опциональных компонентов

ВМ	CPU	ОЗУ, ГБ	Диск, ГБ
Сервер Управления Linux/Windows (lmsrv/winmdm)	2	4	20

2.4 Требования к сетевому окружению

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

1. клиентских подключений по следующим TCP-портам (указаны значения по умолчанию):

- 8443 (https) – от ПК администратора к Серверу Администрирования;
- 443 (https) – от МСК всех платформ к Серверу Управления;
- 50001 (tcp) – от МСК с ОС Android, к Серверу Команд;
- 8082 (scep) – от МСК с ОС Android, iOS, Аврора к Серверу SCEP. Используется только если установлен компонент **scep-standalone**.
- 8085 (https) – от внешних сервисов к Серверу API;
- 8444 (https)– от МСК с ОС Windows к Серверу Управления Windows.

2. сетевых подключений серверных компонентов (указаны значения TCP-портов по умолчанию):

- 5432 (tcp)– от всех серверных компонентов к Серверу БД;
- 636 (ldaps) или 389 (ldap) – от Серверов Администрирования, Регистрации и Агента Синхронизации к Microsoft AD;
- 465 (smtps) или 25 (smtp) – от Сервера email-уведомлений к почтовому

серверу;

- 514 (syslog) – от Сервиса отправки системных логов к хранилищу логов/событий;
- 443 (https) – от рабочего места администратора к серверу ГИС для отображения карт (по умолчанию *.openstreetmap.org).

3. (для управления iOS-устройствами) подключения Сервера Управления к серверам APNS посредством:

- доступа к DNS-серверу, разрешающему доменное имя 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 device-provisioning.googleapis.com, android.apis.google.com, mtalk.google.com, mtalk4.google.com, mtalk-staging.google.com, mtalk-dev.google.com, alt1-mtalk.google.com, alt2-mtalk.google.com, alt3-mtalk.google.com, alt4-mtalk.google.com, alt5-mtalk.google.com, alt6-mtalk.google.com, alt7-mtalk.google.com, alt8-mtalk.google.com, firebaseinstallations.googleapis.com;
- разрешения прохождения IP-трафика к перечисленным серверам, TCP-порты 443, 5228-5230;

Внимание!

*Для корректной работы серверных компонентов и рабочего места администратора **обязательна** 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. Должен быть создан пользователь с правами подключения к этой БД и на создание в ней временных таблиц (далее – пользователь БД SafeMobile). Имя и пароль этого пользователя должны быть впоследствии указаны в мастере первоначальной настройки сервера SafeMobile (параметры **user** и **password** в файле db.yml);
3. Должна быть создана схема в этой БД, владельцем которой должен быть назначен пользователь БД SafeMobile. А также схема для планировщика с фиксированным названием pgagent.
4. В указанной БД в стандартной схеме public должно быть установлено расширение pgcrypto.
5. Переменная сессии SEARCH_PATH для роли пользователя БД SafeMobile (п. 2.) должна содержать: <имя схемы БД SafeMobile (п. 2.)>, public.
6. В файле pg_hba.conf необходимо проверить и при необходимости добавить строку

```
hostnossl all all 0.0.0.0/0 md5
```

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

```
jit=off  
listen_addresses = '*'  
max_connections = 1000
```

Примечание.

Для Astra Linux 1.7_x86-64.

При создании БД в ручную есть вероятность получения ошибки:

```
«psql:./sql/schema.sql:10141: ОШИБКА: незавершённая строка в кавычках».
```

Необходимо выполнить настройку БД:

```
ALTER DATABASE namebd SET standard_conforming_strings = on
```

namebd – название БД.

Пример:

Создаем БД smdb, пользователя smuser, схему smschema

```
root@debian:/tmp# su - postgres -c psql
create database smdb with encoding 'UTF-8' lc_collate 'en_US.UTF-8' lc_ctype 'en_US.UTF-8';
\connect smdb
create role smuser with login password '123';
create schema smschema;
grant create, usage on schema smschema to smuser;
create schema pgagent;
grant create, usage on schema pgagent to smuser;
create extension pgcrypto schema public;
alter role smuser set search_path = 'smschema,public';
```

Наполняем БД и проверяем результат

```
emm@debian:/tmp$ ./install.sh --user smuser --db smdb --schema smschema -- -h 127.0.0.1
emm@debian:/tmp$ PGPASSWORD=123 psql -U smuser -d smdb -h 127.0.0.1 -c "select *
from instlog;"
```

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 проверить и установить на сервере локаль «en_US.UTF-8» и 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

Установку Docker рекомендуется выполнять из скриптов `docker` и `docker compose` для CentOS и Debian, расположенных в каталоге **utility**, который находится в каталоге **/opt/emm** (создается после разворачивания архив **emm-config.tar.gz**).

4 Установка и настройка серверных компонентов «UEM SafeMobile»

Установка и настройка серверных компонентов «UEM SafeMobile» проще и удобнее выполняется от пользователя `root`, но может быть произведена и от непривилегированного пользователя, при соблюдении условий (на примере пользователя `emm` и каталога установки `/opt/emm/`):

1) Предварительно установлены все необходимые системные компоненты, включая СУБД Postgres, и создан каталог установки

```
mkdir /opt/emm
```

2) Для каталога установки назначен соответствующий владелец:

```
chown -R emm:emm /opt/emm/
```

3) Пользователь добавлен в группу `docker`:

```
groupadd docker; usermod -aG docker emm
```

После этого, все необходимые `docker`-команды, скрипт первоначальной настройки SafeMobile `setup.sh`, а также инсталляцию/обновление БД SafeMobile (скрипт `install.sh`) можно выполнять от пользователя `emm`.

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**:

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

2. Распаковать файлы **db-postgresql.tar.gz** и **emm-config.tar.gz**:

```
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 ОС Debian 11 или CentOS 7, 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
```

```
debian11_pg14_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:

```
./setup.sh
```

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

Для получения справки по параметрам скрипта требуется запустить его с ключом **-h**:

```
./setup.sh -h
```

Затем установить схему БД командой:

```
./install.sh -- -h 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 не указан, будет включено значение параметра по умолчанию.

Для получения справки по параметрам скрипта требуется запустить его с ключом **-h**:

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

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

```
./install.sh --user smadmin --db smdb -- -h 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 ОС Debian 11 или CentOS 7, 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:

```
./debian11_pg14_install.sh
```

или

```
./centos7_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**.

Ручная оптимизация настроек описана в разделе 4.2.4.

Затем установить схему БД командой:

```
./install.sh -- -h 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 -- -h 127.0.0.1 -p 5433
```

“-p 5433” – указывается, если используется нестандартный порт, отличный от 5432.

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).

Для получения списка рекомендуемых настроек следует запустить скрипт *./make_pg_conf.sh* на компьютере, где установлен PostgreSQL, список отобразится на экране.

После внесения изменений необходимо перезапустить БД:

systemctl restart postgresql-11.service

4.2.5 Настройка СУБД PostgreSQL при работе в отдельной подсети

Серверные компоненты SafeMobile поддерживают пул соединений с сервером БД, на случай всплеска активности мобильных клиентов. Если сервер БД находится в отдельной подсети, пограничное активное сетевое оборудование может разрывать соединения, находящиеся в резерве. При этом, в логах PostgreSQL появляется множество ошибок "could not receive data from client: Connection timed out".

В этом случае необходимо скорректировать параметры PostgreSQL. Например, если активное сетевое оборудование разрывает все соединения, неактивные в течение 30 секунд, рекомендуется выставить следующие параметры в файле *postgresql.conf*

```
tcp_keepalives_idle = 20 # TCP_KEEPIDL, in seconds;
tcp_keepalives_interval = 1 # TCP_KEEPINTVL, in seconds;
tcp_keepalives_count = 9 # TCP_KEEPCNT;
```

и перезапустить сервис PostgreSQL.

Для просмотра параметров, использующихся сервером в данный момент, необходимо выполнить команду:

```
psql -U sphone -h 127.0.0.1 -c " select name, setting, unit from
pg_settings where name like 'tcp%';"
```

4.2.6 Подключение к СУБД PostgreSQL по сертификату

Скрипт установки и обновления схемы БД `install.sh` поддерживает подключение по сертификату. Для этого необходимо указать параметр `--ssl` и отредактировать файл настроек `ssl-connection-settings.sh`, находящийся в том же каталоге, что и скрипт. В файле настроек указаны пути к файлам клиентского сертификата, ключа клиентского сертификата и сертификата CA.

Для подключения по сертификату необходимо выпустить сертификат для сервера СУБД PostgreSQL, настроить СУБД PostgreSQL, выпустить клиентский сертификат для подключения.

Информация ниже приводится для ознакомления, подробная информация содержится в документации PostgreSQL.

4.2.6.1 Выпуск сертификатов, подписанных самоподписанным сертификатом CA

Создание ключа сертификата CA:

- `openssl genrsa -out root.key 4096`

Создание сертификата CA. В интерактивном режиме в Common Name (CN) указать не IP-адрес сервера, а любое название, например "MyCompanyCA":

- `openssl req -x509 -new -nodes -key root.key -sha256 -days 365 -out root.crt`

Создание ключа сертификата сервера:

- `openssl genrsa -out server.key 2048`

Создание запроса на сертификат сервера. В интерактивном режиме в Common Name (CN) указать IP-адрес сервера, например "10.17.7.88":

- `openssl req -new -key server.key -out server.csr`

Создание и подпись сертификата сервера:

- `openssl x509 -req -in server.csr -CA root.crt -CAkey root.key -`

```
CACreateserial -out server.crt -days 365 -sha256
```

Создание ключа сертификата клиента:

- *openssl genrsa -out client.key 2048*

Создание запроса на сертификат клиента. В интерактивном режиме в Common Name (CN) указать имя пользователя PostgreSQL, обычно "sphone":

- *openssl req -new -key client.key -out client.csr*

Создание и подпись сертификата клиента:

- *openssl x509 -req -in client.csr -CA root.crt -CAkey root.key -CACreateserial -out client.crt -days 365 -sha256*

4.2.6.2 Настройка СУБД PostgreSQL

Файлы сертификатов root.crt, server.crt, server.key скопировать в каталог установки кластера PostgreSQL. Для файлов выполнить:

- *chown postgres*
- *chmod 400*

Указать параметры в postgresql.conf:

- *ssl = on*
- *ssl_ca_file = 'root.crt'*
- *ssl_cert_file = 'server.crt'*
- *ssl_key_file = 'server.key'*

В pg_hba.conf добавить:

Для версии PostgreSQL 11:

- *hostssl all all 0.0.0.0/0 cert clientcert=1 #*

Для версии PostgreSQL 12 и выше:

- *hostssl all all 0.0.0.0/0 cert clientcert=verify-full #*

Перезапустить кластер PostgreSQL.

4.2.6.3 Подключение по сертификату

```
psql "host=10.17.7.88 port=5438 dbname=sphone user=sphone sslmode=verify-full  
sslcert=/distrib/certs/client.crt sslkey=/distrib/certs/client.key sslrootcert=/distrib/certs/root.crt"
```

- host - как в Common Name server.crt
- user - как в Common Name client.crt

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):

1. *Bind IP: 0.0.0.0*

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

2. *MDM: behind external proxy? [y/n/q/?] y*

Указать, расположены ли Сервера Управления (**iosmdm** и **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 Сервера Управления. Пример настройки внешнего прокси-сервера приведен разделе 6.

3. *ARM [y/n/q/?]? y*

Сформировать конфигурацию Сервера администрирования.

4. *ARM: Use HTTPS [y/n/q/?]? y*

Использовать протокол HTTPS для сервера администрирования.

5. *ARM: Create TLS certificate [y/n/q/?]? y*
Создать самоподписанный сертификат HTTPS сервера администрирования.
6. *ARM: Common Name (IP or domain name): 192.168.1.1*
Адрес или доменное имя для сертификата сервера администрирования.
7. *MDM server [y/n/q/?]? y*
Сформировать конфигурацию сервера управления MDM
8. *Windows MDM? [y/n/q/?] y*
Сформировать конфигурацию сервера WinMDM
9. *FCM Push Server? [y/n/q/?] y*
Сформировать конфигурацию пуш-сервера FCM
10. *iOS MDM: Create TLS certificate [y/n/q/?]? y*
Создать самоподписанный сертификат HTTPS сервера управления MDM.
11. *iOS MDM: Common Name (IP or domain name): 192.168.1.1*
Адрес или доменное имя для сертификата Сервера управления MDM.
12. *Socket server [y/n/q/?]? y*
Сформировать конфигурацию Сервера команд (Socket server)
13. *Socket server: Create TLS certificate [y/n/q/?]? y*
Создать самоподписанный сертификат HTTPS Сервера команд
14. *Socket server: Common Name (IP or domain name): 192.168.1.1*
Адрес или доменное имя для сертификата Сервера команд
15. *Linux Management Server? [y/n/q/?] y*
Сформировать конфигурацию Сервера управления Linux
16. *AD Sync Agent? [y/n/q/?] y*
Сформировать конфигурацию Сервера синхронизации с Microsoft AD
17. *SafeMobile API Server? [y/n/q/?] y*
Сформировать конфигурацию Сервера API
18. *SafeMobile API Server: Create TLS certificate? [y/n/q/?] y*
Создать самоподписанный сертификат HTTPS Сервера API

19. *SafeMobile API Server: Common Name (IP or domain name):*
192.168.1.1

Адрес или доменное имя для сертификата Сервера API

20. *Mail Service? [y/n/q/?] y*

Сформировать конфигурацию Сервера email-уведомлений

21. *Syslog Forward Service? [y/n/q/?] y*

Сформировать конфигурацию Сервера syslog

22. *SCEP server [y/n/q/?]? (deprecated) y*

Сформировать конфигурацию SCEP сервера.

Соглашаться следует, если до версии 8.2 был развернут сервер SCEP и не планируется его замена на сервер SCEP устанавливаемый вместе с Сервером Управления.

23. *SCEP server: Create TLS certificate [y/n/q/?]? y*

Создать самоподписанный сертификат HTTPS SCEP сервера?

Соглашаться следует, если до версии 8.2 был развернут сервер SCEP и не планируется его замена на сервер SCEP устанавливаемый вместе с Сервером Управления.

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

Адрес или доменное имя для сертификата SCEP сервера.

Соглашаться следует, если до версии 8.2 был развернут сервер SCEP и не планируется его замена на сервер SCEP устанавливаемый вместе с Сервером Управления.

25. *SCIM server - y*

"SafeMobile SCIM Server: Create TLS certificate?" - y

"SafeMobile SCIM Server: Old TLS certificate exists, create new?" (если SCIM сервер уже был установлен) - y

"SafeMobile SCIM Server: Common Name (IP or domain name)" - Адрес или доменное имя SCIM сервера

26. *Database hostname: 192.168.1.1*

Адрес сервера БД

27. *Database port (default: 5432): 5432*

Порт сервера БД

28. `Database name: sphone`

Имя БД

29. `Database username: sphone`

Пользователь БД

30. `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 `«config/nginx/arm.http.conf»`, в параметре `rate=*`. 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 `«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
```

Также в конфигурационном файле `«config/arm.yml»` можно изменить ссылку на Монитор для QR-кода, генерируемого в разделе Загрузчик, добавив параметр:

```
safemobile.url_for_monitor_download: https://my.url/monitor.apk
```

4.5 Настройки сервиса отправки почты

В конфигурационном файле «**config/mail.yml**» компонента **mail-agent** нужно указать настройки SMTP-сервера и учетную запись для отправки пользователям писем правил несоответствия и кодов приглашения, а также уведомлений администраторов о блокировке/разблокировке их учётных записей.

```
mail.yml
smtp:
  host: 127.0.0.1
  port: 25
  user: safemobile@safe-mobile.ru
  password: P@ssw0rd
  sender: safemobile@safe-mobile.ru
  # serverCertificate: /config/ca.cer
  # checkRevocation: false
  # checkHostname: false
  # checkCertificate: true
  ### None, Auto, SslOnConnect, StartTls, StartTlsWhenAvailable
  # tlsOptions: Auto
logging:
  logLevel:
    default: information
ratelimit:
  # max number of emails
  limit: 100
  # in time window (in seconds)
  window: 60
```

Параметры mail.yml

- **password** – Если закомментировать пароль, то будет использована анонимная аутентификация;
- **sender** – Пользователь отправитель сообщений. Задается в виде

user@domain.ru. Если параметр не задан, то вместо sender будет применяться параметр user.

- serverCertificate – путь к сетевому сертификату;
- checkRevocation – проверять отзыв серверного сертификата;
- checkHostname – проверять соответствие имени хоста серверному сертификату;
- checkCertificate – проверять ли серверный сертификат;
- tlsOptions – Настройки TLS. Возможные значения:
 - None – не использовать шифрование TLS;
 - Auto – автоматически определять, какие параметры TLS будут использованы. Если сервер не поддерживает TLS, соединение продолжится без какого-либо шифрования;
 - SslOnConnect – Соединение должно сразу при подключении к серверу использовать шифрование TLS;
 - StartTls – шифрование TLS включается после получения приветствия и параметров совместимости сервера. Если сервер не поддерживает опцию STARTTLS, соединение завершится неудачей;
 - StartTlsWhenAvailable – шифрование TLS включается после получения приветствия и параметров совместимости сервера, но только когда сервер поддерживает опцию STARTTLS.
- limit – максимальное количество писем которое может быть отправлено за промежуток времени, заданный в параметре window;
- window – расчетный промежуток времени в секундах для параметра limit.

4.6 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.

4.7 Настройка раздела «Подключения к серверам» в APM

После настройки всех серверных компонентов, входа в консоль администрирования и ввода лицензии, в первую очередь необходимо произвести настройки, необходимые мобильным устройствам для подключения к серверу. Для этого предназначен раздел «Подключения к серверам». С его помощью можно настроить только параметры, передаваемые мобильным клиентам для связи с сервером. Физическая настройка адресов, портов и сертификатов, отдаваемых сервером по сети, происходит в мастере первоначальной настройки SafeMobile и конфигурационных файлах, и представлена ранее в этом документе.

При первичной установке, настройке SCEPServer следует задать те же настройки, что и в MDMServer. Указание настройки обязательно. Если настройки SCEPServer не

заданы, то подключение устройств к системе будет невозможно, т.к устройство не сможет получить сертификат mTLS.

1) Если сервер использует сертификаты, выданные общедоступным доверенным УЦ(GlobalSign, DigiCert, Let's Encrypt и т.п.), доверие серверу со стороны мобильных клиентов не требует дополнительной настройки и достаточно указать только адреса:порты сервера.

Тип сервера ▲	URL	Сертификаты
MDMServer	https://sso2.safe-mobile.ru	
SCEPServer	https://sso2.safe-mobile.ru	
SocketServer	sso2.safe-mobile.ru:50042	
WinMDM Enrollment	https://sso2.safe-mobile.ru:8444	
WinMDM Management	https://sso2.safe-mobile.ru	

Рисунок – пример адреса и порты сервера

2) Если сервер использует сертификаты, выданные корпоративным УЦ или полученные с помощью мастера первоначальной настройки SafeMobile, мобильным клиентам при подключении необходимо передать корневой сертификат УЦ, для доверия серверу. В случае мастера первоначальной настройки SafeMobile создается свой мини-УЦ и его корневой сертификат лежит в каталоге установки сервера, в файле CA.pem.

Корневой сертификат УЦ необходимо загрузить в APM, в раздел «Серверные сертификаты», после чего в разделе «Подключения к серверам» появится возможность назначить этот доверенный сертификат на URL.

Тип сервера ▲	URL	Сертификаты
MDMServer	https://sso2.safe-mobile.ru	Russian Trusted Root CA
SCEPServer	https://sso2.safe-mobile.ru	SCEP Server
SocketServer	sso2.safe-mobile.ru:50042	Russian Trusted Root CA
WinMDM Enrollment	https://sso2.safe-mobile.ru:8444	Russian Trusted Root CA
WinMDM Management	https://sso2.safe-mobile.ru	Russian Trusted Root CA

Рисунок – назначенные серверные сертификаты

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 4.2.5.

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 apple-mdm-push 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 приложить к заявке на Портале Технической Поддержки НИИ СОКБ <https://service.niisokb.ru/>. Подписанный файл CSR будет возвращён в формате PLIST.

4. После получения PLIST-файла, необходимо 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/.

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. 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. Можно использовать исходный файл MdmPush.csr, или 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. Файл MdmPush.csr следует приложить к заявке на Портале Технической Поддержки НИИ СОКБ <https://service.niisokb.ru/>. 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 apple-mdm-push
```

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 создать заявку на Портале Технической Поддержки НИИ СОКБ <https://service.niisokb.ru/>. В ответ будет прислан файл **firebase.json**, который необходимо разместить в каталог **/opt/emm/config/**, при условии, что SafeMobile установлен в **/opt/emm/**.

5.4 Сертификат SCEP

Сертификат SCEP генерируется автоматически инсталлятором в каталоге установки (файл `scep.p12`). Сертификат используется для подписи запросов сертификата. Если используется схема с несколькими серверами MDM расположенными за внешним балансировщиком, то необходимо обеспечить чтобы все сервера использовали один сертификат `scep`.

6 Обновление до версии 8.x

Внимание!

- В версии 8.2 введена аутентификация подключаемых устройств по протоколу *mTLS*. Это изменение может привести к **ПОТЕРЕ УПРАВЛЕНИЯ УСТРОЙСТВАМИ ПРИ НЕСОБЛЮДЕНИИ РЕГЛАМЕНТА ОБНОВЛЕНИЯ**. *mTLS* (*Mutual TLS*) протокол предназначен для взаимной аутентификации по сертификатам *x509* как сервера, так и клиента.
- Решение об использовании внешнего прокси-сервера принимается при запуске скрипта первоначальной настройки.
- Для корректной работы серверных компонентов и рабочего места администратора перед началом обновления **обязательна** настройка синхронизации времени по протоколу **NTP, UDP-порт 123**.
- В случае использования внешнего прокси-сервера, отличного от *nginx*, необходимо убедиться, что прокси-сервер можно настроить для корректной обработки *mTLS* трафика.

Для реализации *mTLS* в составе системы добавлены новые компоненты:

- **са** - встроенный УЦ для выпуска сертификатов *mTLS*. Устанавливается автоматически вместе с Сервером Администрирования (**arm**) и не требует дополнительных настроек.
- **auth-server** - сервер авторизации для Сервера Команд (**socket-server**). Устанавливается автоматически вместе с Сервером Команд и не требует дополнительных настроек.

Помимо новых компонент в 8.2 обязательным компонентом стал Сервер SCEP. С версии 8.2 он автоматически устанавливается вместе с Сервером Управления (**mdm**) и использует тот же URL, что и Сервер Управления. В

зависимости от того использовался Сервер SCEP до 8.2 (см. п.4.3, шаг 23) после обновления системы необходимо:

- Если в системе не использовался ранее сервер SCEP, то в разделе APM "Объекты учета" -> "Подключения к серверам" скопировать настройки из MDMServer в настройки SCEPServer и отказаться от у установки компонента **scep-standalone**: `SCEP server [y/n/q/?]? (deprecated) n.`
 - Если в системе ранее был установлен сервер SCEP возможны два варианта: либо продолжить использовать его, либо перейти на использование сервера SCEP устанавливаемого вместе с MDM. Для продолжения использования Сервера SCEP, установленного с предыдущей версией, необходимо при установке выбрать установку компонента **scep-standalone**: `SCEP server [y/n/q/?]? (deprecated) y.` Во втором случае необходимо в разделе APM "Объекты учета" -> "Подключения к серверам" скопировать настройки из MDMServer в настройки SCEPServer и отказаться от у установки компонента **scep-standalone**: `SCEP server [y/n/q/?]? (deprecated) n.`
 - Если трафик TLS в сторону Серверов управления (компоненты mdm и winmdm) терминируется на внешнем прокси сервере, необходимо настроить внешний прокси сервер:
 - Прокси сервер не должен проверять, что сертификат mTLS клиента выпущен публичным доверенным УЦ. Клиентский сертификат mTLS в версии 8.2 выпускается встроенным УЦ. Корневой сертификат встроенного УЦ самоподписанный.
- Пример настройки внешнего прокси-сервера:

```
http {
    # ...
    server {
        # ...
        ssl_verify_client optional_no_ca;
        error_page 495 = @fallback;
        location @fallback {
            try_files ----- $request_uri;
        }
        # ...
    }
    # ...
}
```

- Прокси сервер должен передавать в http заголовках параметры клиентского сертификата mTLS.

Пример настройки внешнего прокси-сервер:

```
http {
    ...
    server {
        ...
        location {
            ...
            proxy_set_header X-Client-Certificate $ssl_client_escaped_cert;
            proxy_set_header X-Client-Certificate-Sha1 $ssl_client_fingerprint;
            ...
        }
        ...
    }
    ...
}
```

- Если трафик TLS в сторону Сервера Команд (socket-server) терминируется на внешнем прокси сервере, возможны два варианта. Перенастроить внешний прокси сервер так, чтобы TLS трафик приходил на сервер SS.

Пример настроек внешнего прокси-сервера:

```
server {
    listen 50068 ssl;
    proxy_pass x.x.x.x:50001;
    proxy_ssl on; #mTLS
    ssl_certificate ../../../../certs/cert.pem;
    ssl_certificate_key ../../../../certs/key.pem;
    ssl_protocols TLSv1.2 TLSv1.3;
    ssl_prefer_server_ciphers on;
    ssl_ciphers
    ECDH+AESGCM:ECDH+AES256:ECDH+AES128:DH+3DES:!ADH:!AECDH:!MD5;
    ssl_verify_client optional_no_ca; #mTLS
}
```

```
js_preread main.preread_verify; #mTLS

}
```

Либо оставить завершение TLS трафика на внешнем прокси сервере, но в этом случае проверка сертификата клиента при обращении к Серверу Команд производится не будет.

Переход на сертификаты mTLS, ранее подключенных устройств iOS будет происходить не сразу. Из-за особенностей реализации смену сертификата можно произвести только после того, как устройство обновит свой токен. Как правило обновление токенов производится раз в месяц.

При обновлении из журнала синхронизации с AD будут удалены все записи. Обусловлено изменением способа синхронизации и состава записей в журнале.

После миграции изменения правил синхронизации возможно только при отключенной автосинхронизации.

При использовании внешнего прокси-сервера, для установки актуального nginx и модуля nginx-module-njs для реализации mTLS на стороне socket-server (для Debian 11) необходимо выполнить следующие действия:

1. Выполнить:

```
wget https://nginx.org/keys/nginx_signing.key

apt-key add nginx_signing.key

nano /etc/apt/sources.list и добавляем в файл следующие строки:

deb https://nginx.org/packages/mainline/debian/ bullseye nginx

deb-src https://nginx.org/packages/mainline/debian bullseye nginx

apt update && apt install nginx nginx-module-njs
```

- После установки необходимо добавить в самое начало файла */etc/nginx/nginx.conf* следующую строку:

```
load_module modules/nginx_stream_js_module.so;
```

Настройка конфигурационных файлов nginx на внешнем прокси-сервере, для работы mTLS в socket-server:

Файл */etc/nginx/conf.d/ss.stream.conf*

```
js_path "/etc/nginx/conf.d/njs/";
js_import main from auth.js;

server {
    listen 50001 ssl;
    js_preread main.preread_verify; #mTLS
    proxy_pass x.x.x.x:50001;
    ssl_certificate /etc/nginx/conf.d/fullchain.cer;
    ssl_certificate_key /etc/nginx/conf.d/snt.safephone4.ru.key;
    ssl_protocols TLSv1.2 TLSv1.3;
    ssl_prefer_server_ciphers on;
    ssl_ciphers
    ECDH+AESGCM:ECDH+AES256:ECDH+AES128:DH+3DES:!ADH:!AECDH:!MD5;
}
```

- `proxy_pass x.x.x.x:` - ip-адрес сервера, на котором размещен socket-server
- `ssl_certificate /.../.../....cer` – ссылка на сертификат;
- `ssl_certificate_key /.../.../.../....key` – ссылка на ключ.

Файл `/etc/nginx/conf.d/njs/auth.js`

```
function preread_verify(s) {
    var collect = "";

    s.on('upload', async function (data, flags) {
        collect += data;

        if(collect.length >= 32) {
            var len = collect.charCodeAt(4) + collect.charCodeAt(5)*256 +
collect.charCodeAt(6)*256*256 + collect.charCodeAt(7)*256*256*256;
            if(collect.length >= 32 + Math.min(len,16)){
                s.off('upload');
                let payload = collect.slice(32);
                let e = payload.indexOf(String.fromCharCode(31));
                if(e == -1){
                    s.deny();
                    return;
                }
                let id = payload.slice(0,e);
                let reply = await ngx.fetch('http://y.y.y.y:2080/auth',
                    {headers: {"Host":'auth', "X-MCC-Id": id, "X-Client-Certificate-
Fingerprint": s.variables.ssl_client_fingerprint}});
                (reply.status == 200) ? s.done(): s.deny();
            }

        }
    });
}

export default {preread_verify};
```

- `y.y.y.y` - ip-адрес сервера, на котором размещен сервис auth.

Если в Вашей системе использовался запрет Google Play в профилях, то необходимо выполнить следующие действия (ДО обновления к версии 8.2):

- 1 Если в разделе "Объекты учета" -> "Приложения" нет приложения Google Play со следующими параметрами, то его необходимо добавить:
 - Платформа: Android.
 - Тип приложения: Некорпоративное,
 - Наименование: "Google Play",
 - UID: "com.android.vending",
 - Владелец: root,
- 2 Создать правило управления приложениями на удаление приложения Google Play со следующими параметрами:
 - Название произвольное (например: "Заблокировать Google Play"),
 - Место установки: Устройство,
 - Приложение должно быть установлено: Нет,
 - Владелец: root,
- 3 Назначить правило на корень дерева ОШС.

Внимание!

Если помимо общего запрета нужно разрешить использовать Google Play в каком-либо подразделении, то в закладке "Назначения" правила, необходимо снять действие правила с соответствующих узлов.

- 4 Если в Вашей компании имеются устройства, использующие контейнер KNOX или Рабочий профиль Android и нужно обеспечить запрет Google Play внутри контейнеров, то необходимо дополнительно создать правило аналогичное п.2 и п.3, но местом установки выбрать - контейнер.
- 5 После настройки всех правил необходимо задать значение политики управления Google Play (во всех профилях ограничений) в значение - Не задано.

6 Провести обновление.

Внимание!

В версии 8.2 были изменены порты серверов Windows. Если у Вас имеются подключенные устройства на платформе Windows, то перед проведением обновления Вам необходимо обратиться в службу поддержки за дополнительными материалами.

6.1 Обновление серверной части до версии 8.x

Для обновления уже установленной «UEM SafeMobile» до текущей версии дополнительно в установочный комплект входит файл `db-postgresql-patch-8.xxx.tar.gz`, который рекомендуется распаковать в каталог `/tmp/` командой:

```
tar xzvf db-postgresql-patch-8.*.tar.gz -C /tmp/
```

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

1. Остановить docker-контейнеры на всех серверах 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 /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 патчи БД из каталога **/tmp/** посредством скрипта **install_patch.sh** следующей командой:

```
mkdir /tmp/ && ./install_patch.sh -- -h 127.0.0.1
```

При запуске скрипта **./install_patch.sh**, до первого патча автоматически создаётся бэкап БД в каталоге **/tmp**

Дополнительные настройки скрипта можно уточнить командой:

```
./install_patch.sh --help
```

6. В каталоге **«/opt/emm/config»** содержатся сформированные конфигурационные файлы компонентов SafeMobile. Следует сравнить конфигурационные файлы релиза 8.x в каталоге **«emm»** с файлами в каталоге **«emm-old»** и при необходимости дополнить их 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 на всех серверах 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
```

После запуска и настройки всех контейнеров можно выполнить команду

```
docker image prune -a
```

она удаляет docker-образы, которые не задействованы.

6.2 Особенность применения профилей после обновления с версии 4.4.x до 8.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 8.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 8.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.

После обновления необходимо зайти суперпользователем root и раздать необходимые полномочия локальным администраторам, созданным в предыдущих версиях.

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_9.0-20240329_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_6.0.1-20230513_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
```


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».

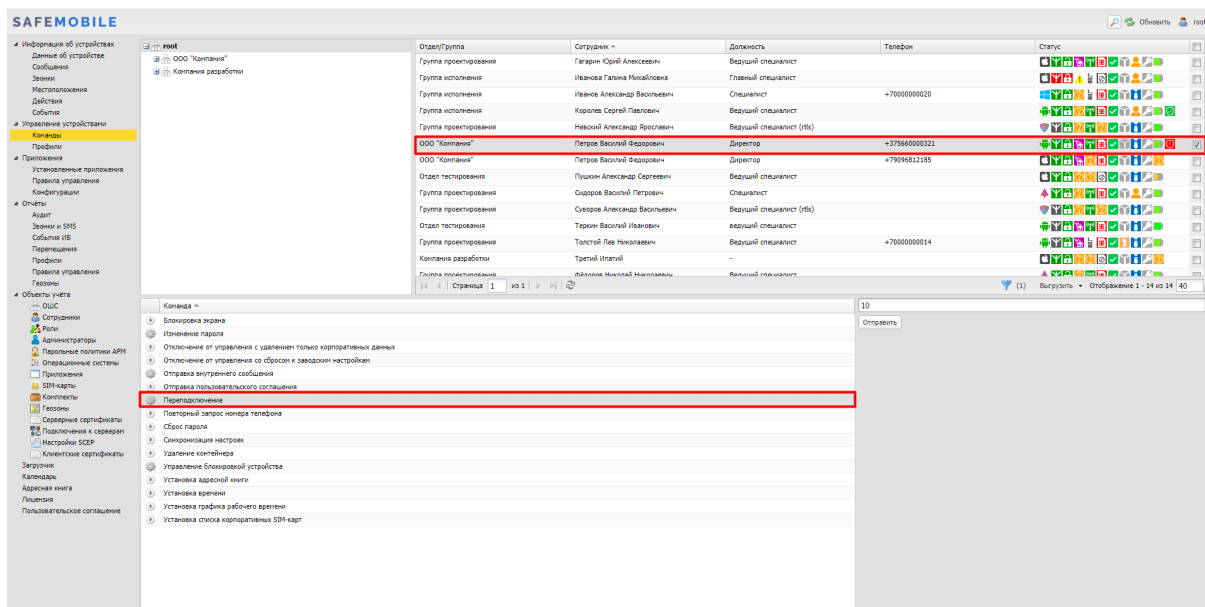


Рисунок 8.2 – Отправка команды «Переподключение»

4. Дождаться результата выполнения действия: когда значение в разделе «Действие» изменится на значение, отличное от «Ожидание результата»:
- результат «Нормальное завершение» свидетельствует о работоспособности «UEM SafeMobile» (рисунок 8.3);

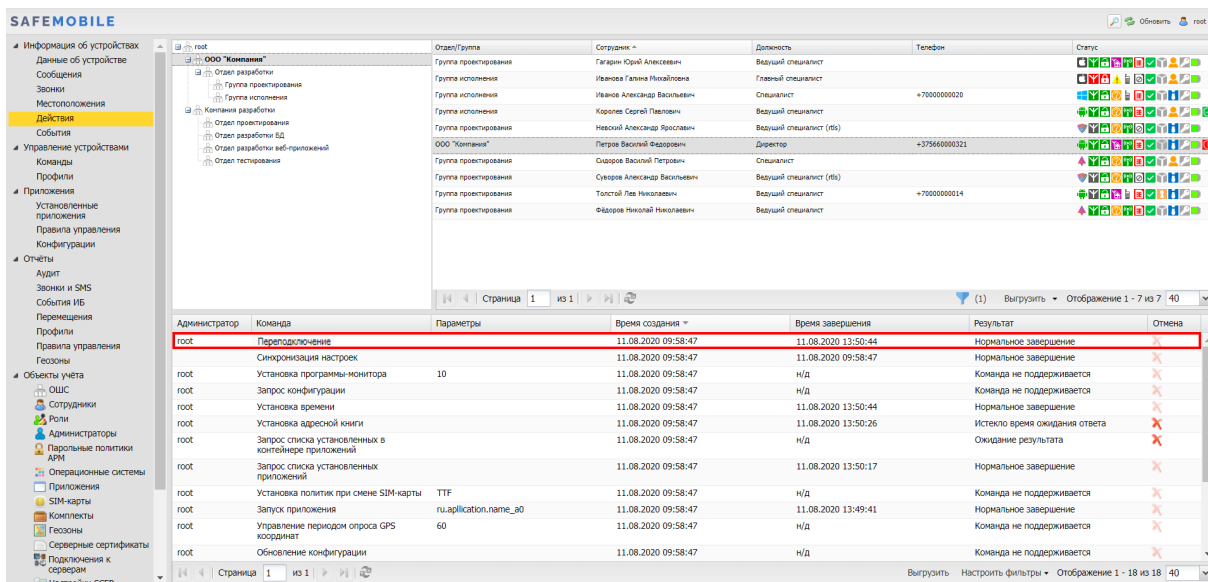


Рисунок 8.3 – Результат команды «Переподключение»

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

9 Приложение А – Диагностические сообщения при запуске АРМ.

1. Установлена настройка: *ad.cert_disable_validation: true*

Имитация текущей даты: 2023-09-12T07:00Z

Содержание файла настроек:

```
ad:
  domain: safephone.pro
  url: ldaps://192.168.15.150
  cert_disable_validation: true

  cert: "RuntimeUtils/src/test/resources/192_168_15_150__636.pem"

# ИГНОРИРУЕТСЯ
# mode-ldap.certs:
# - d:\\_vpv\\sp\\safephone\\safephone-arm\\ldapsrvr.pem

arm.dirname-tmp-file: ./
```

Сообщение системы:

```
*****

***      PREPARATION FOR EXECUTION STARTED      ***

*****

INFO: ad.cert_disable_validation: true

No need to verify certificates

Check and apply settings for mail...

INFO: notification by mail disabled
```

Checking the presence of a directory for temporary report files...

*INFO: directory for temporary report files [arm.dirname-tmp-file] exists:
D:_vpv\sp\safephone\safephone-arm\RuntimeUtils\.*

Settings check completed

2. Установлена настройка:

'auth-provider.active-directory.on: true', 'ad.url: ldap://192.168.15.150'

Имитация текущей даты: 2023-09-12T07:00Z

Содержание файла настроек:

```
# совместимость со старыми версиями
# включена идентификация/аутентификация по ldap
auth-provider.active-directory.on: true
ad:

  domain: safephone.pro
  url: ldap://192.168.15.150
  cert_disable_validation: false

  cert: "RuntimeUtils/src/test/resources/192_168_15_150__636.pem"

# mode-ldap.certs:
# - d:\_vpv\sp\safephone\safephone-arm\ldapsrvr.pem
# - d:\_vpv\sp\safephone\safephone-arm\ldapsrvr.pem
# - "d:/_vpv/sp/safephone/safephone-arm/192_168_15_150__636.pem"
# - "d:\Program files\sp\safephone\safephone-arm\aaa aaa aaa.pem"
# - "aaa"

arm.dirname-tmp-file: ./
```

Сообщение системы:

*** PREPARATION FOR EXECUTION STARTED ***

INFO: ad.cert_disable_validation: false

Check and apply settings for LOCAL auth mode...

auth-provider.active-directory.on:true

INFO: Idaps url: ldap://192.168.15.150

There is no need to validate certificates for 'LDAP auth mode'

Check and apply settings for mail...

INFO: notification by mail disabled

Checking the presence of a directory for temporary report files...

INFO: directory for temporary report files [arm.dirname-tmp-file] exists:

D:_vpv\sp\safephone\safephone-arm\RuntimeUtils\.

Settings check completed

3. Установлена настройка:

auth-provider.active-directory.on: false

Имитация текущей даты: 2023-09-12T07:00Z

Содержание файла настроек:

```
# совместимость со старыми версиями

# выключена идентификация/аутентификация по ldap

auth-provider.active-directory.on: false


ad:

  domain: safephone.pro

  url: ldaps://192.168.15.150

  cert_disable_validation: false


  cert: "RuntimeUtils/src/test/resources/192_168_15_150__636.pem-bad"


# mode-ldap.certs:

# - d:\_vpv\sp\safephone\safephone-arm\ldapserver.pem

# - d:\_vpv\sp\safephone\safephone-arm\ldapserver.pem

# - "d:/_vpv/sp/safephone/safephone-arm/192_168_15_150__636.pem"

# - "d:\\Program files\\sp\\safephone\\safephone-arm\\aaa aaa aaa.pem"

# - "aaa"

arm.dirname-tmp-file: ./
```

Сообщение системы:

```
*****  
  
***      PREPARATION FOR EXECUTION STARTED      ***  
  
*****  
  
INFO: ad.cert_disable_validation: false  
  
Check and apply settings for LOCAL auth mode...  
  
auth-provider.active-directory.on:false  
  
AD:auth-provider.active-directory.on: no need to check the ldaps certificate  
  
There is no need to validate certificates for 'LDAP auth mode'  
  
Check and apply settings for mail...  
  
INFO: notification by mail disabled  
  
Checking the presence of a directory for temporary report files...  
  
INFO: directory for temporary report files [arm.dirname-tmp-file] exists:  
D:\_vpv\sp\safephone\safephone-arm\RuntimeUtils\  
  
Settings check completed
```

4. Установлена настройка:

ad.cert: file_any_no_exists - файл с сертификатом не существует'

Имитация текущей даты: 2023-09-12T07:00Z

Содержание файла настроек:

```
# совместимость со старыми версиями

# включена идентификация/аутентификация по ldap

auth-provider.active-directory.on: true


ad:

  domain: safephone.pro

  url: ldaps://192.168.15.150

  cert_disable_validation: false


# УКАЗАН НЕСУЩЕСТВУЮЩИЙ ФАЙЛ СЕРТИФИКАТА

cert: "file_any_no_exists"


# mode-ldap.certs:

# - d:\\_vpv\\sp\\safephone\\safephone-arm\\ldapsrvr.pem

# - d:\\_vpv\\sp\\safephone\\safephone-arm\\ldapsrvr.pem

# - "d:/_vpv/sp/safephone/safephone-arm/192_168_15_150__636.pem"

# - "d:\\Program files\\sp\\safephone\\safephone-arm\\aaa aaa aaa.pem"

# - "aaa"

arm.dirname-tmp-file: ./
```

Сообщение системы:

```
*****

***      PREPARATION FOR EXECUTION STARTED      ***

*****

INFO: ad.cert_disable_validation: false

Check and apply settings for LOCAL auth mode...

auth-provider.active-directory.on:true

INFO: Idaps url: Idaps://192.168.15.150

INFO: AD cert: file_any_no_exists

ERROR: Cert file not found: D:\_vpv\sp\safephone\safephone-
arm\RuntimeUtils\file_any_no_exists

*****

ERROR: There can be problems when working with active directory

      Check settings 'ad.url' and 'ad.cert'

*****

There is no need to validate certificates for 'LDAP auth mode'

Check and apply settings for mail...

INFO: notification by mail disabled

Checking the presence of a directory for temporary report files...

INFO: directory for temporary report files [arm.dirname-tmp-file] exists:
D:\_vpv\sp\safephone\safephone-arm\RuntimeUtils\

Settings check completed
```

5. Установлена настройка:

ad.cert - файл с сертификатом совпадает с серверным.

Имитация текущей даты: 2023-09-12T07:00Z

Содержание файла настроек:

```
# совместимость со старыми версиями

# включена идентификация/аутентификация по ldap

auth-provider.active-directory.on: true

ad:

  domain: safephone.pro

  url: ldaps://192.168.15.150

  cert_disable_validation: false


# УКАЗАН СУЩЕСТВУЮЩИЙ ФАЙЛ С ВАЛИДНЫМ СЕРТИФИКАТОМ

cert: "src/test/resources/192_168_15_150__636.pem"

# mode-ldap.certs:

# - d:\\_vpv\\sp\\safephone\\safephone-arm\\ldapsrvr.pem

# - d:\\_vpv\\sp\\safephone\\safephone-arm\\ldapsrvr.pem

# - "d:/_vpv/sp/safephone/safephone-arm/192_168_15_150__636.pem"

# - "d:\\Program files\\sp\\safephone\\safephone-arm\\aaa aaa aaa.pem"

# - "aaa"

arm.dirname-tmp-file: ./
```

Сообщение системы:

```
*****

***      PREPARATION FOR EXECUTION STARTED      ***

*****

INFO: ad.cert_disable_validation: false

Check and apply settings for LOCAL auth mode...

auth-provider.active-directory.on:true

INFO: Idaps url: Idaps://192.168.15.150

INFO: AD cert: src/test/resources/192_168_15_150__636.pem

Local cert(s):

Issuer:CN=safemobile-CA,DC=safemobile,DC=pro, Subject:CN=pdc.safemobile.pro,
NotBefore:2022-12-02T07:05Z, NotAfter:2023-12-02T07:05Z

*****

ad.url: Idaps://192.168.15.150

protocol = Idaps

authority = 192.168.15.150

host = 192.168.15.150

port = 636

path =

query = null

*****

The certificate matches the trusted certificate
```

There is no need to validate certificates for 'LDAP auth mode'

Check and apply settings for mail...

INFO: notification by mail disabled

Checking the presence of a directory for temporary report files...

INFO: directory for temporary report files [arm.dirname-tmp-file] exists:

D:_vpv\sp\safephone\safephone-arm\RuntimeUtils\.

Settings check completed

6. Установлена настройка:

ad.cert - файл с сертификатом валидный

Текущее время раньше сертификатного.

Имитация текущей даты: 2022-12-01T07:05Z

The certificate has not yet started

validity:src/test/resources/192_168_15_150__636.pem

У сертификата: NotBefore:2022-12-02T07:05Z, NotAfter:2023-12-02T07:05Z

Содержание файла настроек:

совместимость со старыми версиями

включена идентификация/аутентификация по ldap

auth-provider.active-directory.on: true

ad:

domain: safephone.pro

```
url: ldaps://192.168.15.150

cert_disable_validation: false

# УКАЗАН СУЩЕСТВУЮЩИЙ ФАЙЛ С ВАЛИДНЫМ СЕРТИФИКАТОМ

cert: "src/test/resources/192_168_15_150__636.pem"

# mode-ldap.certs:

# - d:\_vpv\sp\safephone\safephone-arm\ldapserver.pem

# - d:\_vpv\sp\safephone\safephone-arm\ldapserver.pem

# - "d:/_vpv/sp/safephone/safephone-arm/192_168_15_150__636.pem"

# - "d:\\Program files\\sp\\safephone\\safephone-arm\\aaa aaa aaa.pem"

# - "aaa"

arm.dirname-tmp-file: ./
```

Сообщение системы:

```
*****

***      PREPARATION FOR EXECUTION STARTED      ***

*****

INFO: ad.cert_disable_validation: false

Check and apply settings for LOCAL auth mode...

auth-provider.active-directory.on:true
```

INFO: Idaps url: ldaps://192.168.15.150

INFO: AD cert: src/test/resources/192_168_15_150__636.pem

Local cert(s):

Issuer:CN=safemobile-CA,DC=safemobile,DC=pro, Subject:CN=pdc.safemobile.pro,
NotBefore:2022-12-02T07:05Z, NotAfter:2023-12-02T07:05Z

ad.url: ldaps://192.168.15.150

protocol = ldaps

authority = 192.168.15.150

host = 192.168.15.150

port = 636

path =

query = null

The certificate matches the trusted certificate

WARN: The certificate has not yet started validity:

src/test/resources/192_168_15_150__636.pem

WARNING: There can be problems when working with active directory

Check settings 'ad.url' and 'ad.cert'

There is no need to validate certificates for 'LDAP auth mode'

Check and apply settings for mail...

INFO: notification by mail disabled

Checking the presence of a directory for temporary report files...

INFO: directory for temporary report files [arm.dirname-tmp-file] exists:

D:_vpv\sp\safephone\safephone-arm\RuntimeUtils\.

Settings check completed

7. Установлена настройка:

ad.cert - файл с сертификатом валидный

Текущее время позже сертификатного.

Имитация текущей даты: 2023-12-03T07:05Z

The certificate has not yet started

validity:src/test/resources/192_168_15_150__636.pem

У сертификата: NotBefore:2022-12-02T07:05Z, NotAfter:2023-12-02T07:05Z

Содержание файла настроек:

совместимость со старыми версиями

включена идентификация/аутентификация по ldap

auth-provider.active-directory.on: true

ad:

domain: safephone.pro

url: ldaps://192.168.15.150

cert_disable_validation: false

```
# УКАЗАН СУЩЕСТВУЮЩИЙ ФАЙЛ С ВАЛИДНЫМ СЕРТИФИКАТОМ
```

```
cert: "src/test/resources/192_168_15_150__636.pem"
```

```
# mode-ldap.certs:
```

```
# - d:\\_vpv\\sp\\safephone\\safephone-arm\\ldapserver.pem
```

```
# - d:\\_vpv\\sp\\safephone\\safephone-arm\\ldapserver.pem
```

```
# - "d:/_vpv/sp/safephone/safephone-arm/192_168_15_150__636.pem"
```

```
# - "d:\\Program files\\sp\\safephone\\safephone-arm\\aaa aaa aaa.pem"
```

```
# - "aaa"
```

```
arm.dirname-tmp-file: ./
```

Сообщение системы:

```
*****
```

```
***      PREPARATION FOR EXECUTION STARTED      ***
```

```
*****
```

```
INFO: ad.cert_disable_validation: false
```

```
Check and apply settings for LOCAL auth mode...
```

```
auth-provider.active-directory.on:true
```

```
INFO: Idaps url: Idaps://192.168.15.150
```

```
INFO: AD cert: src/test/resources/192_168_15_150__636.pem
```

```
Local cert(s):
```

Issuer:CN=safemobile-CA,DC=safemobile,DC=pro, Subject:CN=pdc.safemobile.pro,
NotBefore:2022-12-02T07:05Z, NotAfter:2023-12-02T07:05Z

ad.url: ldaps://192.168.15.150

protocol = ldaps

authority = 192.168.15.150

host = 192.168.15.150

port = 636

path =

query = null

The certificate matches the trusted certificate

WARN: The certificate has already expired: src/test/resources/192_168_15_150__636.pem

WARNING: There can be problems when working with active directory

Check settings 'ad.url' and 'ad.cert'

There is no need to validate certificates for 'LDAP auth mode'

Check and apply settings for mail...

INFO: notification by mail disabled

Checking the presence of a directory for temporary report files...

INFO: directory for temporary report files [arm.dirname-tmp-file] exists:

D:_vpv\sp\safephone\safephone-arm\RuntimeUtils\.

Settings check completed

8. Установлена настройка:

ad.cert - файл с сертификатом чужой

Имитация текущей даты: 2022-06-25T08:01Z

Содержание файла настроек:

```
# совместимость со старыми версиями

# включение/выключение идентификации/аутентификации

auth-provider.active-directory.on: true


ad:

  domain: safephone.pro

  url: ldaps://192.168.15.150

  cert_disable_validation: false


  cert: "src/test/resources/example-chain.pem"


# mode-ldap.certs:

# - d:\_vpv\sp\safephone\safephone-arm\ldapsrvr.pem

# - d:\_vpv\sp\safephone\safephone-arm\ldapsrvr.pem

# - "d:/_vpv/sp/safephone/safephone-arm/192_168_15_150__636.pem"
```

```
# - "d:\\Program files\\sp\\safephone\\safephone-arm\\aaa aaa aaa.pem"

# - "aaa"

arm.dirname-tmp-file: ./
```

Сообщение системы:

```
*****

***      PREPARATION FOR EXECUTION STARTED      ***

*****

INFO: ad.cert_disable_validation: false

Check and apply settings for LOCAL auth mode...

auth-provider.active-directory.on:true

INFO: Idaps url: Idaps://192.168.15.150

INFO: AD cert: src/test/resources/example-chain.pem

Local cert(s):

Issuer:CN=Safephone Root CA, Subject:CN=10.17.7.93, NotBefore:2022-06-24T08:01Z,
NotAfter:2024-09-25T08:01Z

Issuer:CN=Safephone Root CA, Subject:CN=Safephone Root CA, NotBefore:2020-10-
13T06:24Z, NotAfter:2030-10-11T06:24Z

*****

ad.url: Idaps://192.168.15.150

protocol = Idaps

authority = 192.168.15.150
```

host = 192.168.15.150

port = 636

path =

query = null

ERROR: setting:ad.cert:src/test/resources/example-chain.pem:java.security.cert.CertPathValidatorException: Path does not chain with any of the trust anchors

ERROR: There can be problems when working with active directory

Check settings 'ad.url' and 'ad.cert'

There is no need to validate certificates for 'LDAP auth mode'

Check and apply settings for mail...

INFO: notification by mail disabled

Checking the presence of a directory for temporary report files...

INFO: directory for temporary report files [arm.dirname-tmp-file] exists:

D:_vpv\sp\safephone\safephone-arm\RuntimeUtils\.

Settings check completed

9. Настройки секции *mail* с ССО2, выключена

Имитация текущей даты: 2022-06-25T08:01Z

Содержание файла настроек:

```
#####  
  
# файл с ССО2 2023-09-15  
  
#####  
  
server:  
  
  servlet:  
  
    context-path:  
  
    session-timeout: 30  
  
    forward-headers-strategy: native  
  
#Logging  
logging:  
  
  level:  
  
    root: WARN  
  
  jdbc:  
  
    sqlonly: OFF  
  
    audit: OFF  
  
    connection: OFF  
  
    sqltiming: OFF
```

com.safephone.dao.resultcode: OFF

session.control:

enabled: false

maximum-sessions: 2

max-session-prevents-login: false

auth-provider:

database.on: true

active-directory.on: false

use ad.cert: "cert file name"

active-directory.on: true

gis:

servers:

- name: openstreetmap

label: openstreetmap.org

url: http://{a-c}.tile.openstreetmap.org/{z}/{x}/{y}.png

E-Mail

mail:

notification:

to_admin:

true - for use notification

enabled: false

template:

lock_subject: "СУМТС: Аккаунт заблокирован"

Uncomment for use

lock: "/config/admin-lock.html"

unlock_subject: "СУМТС: Аккаунт разблокирован"

Uncomment for use

unlock: "/config/admin-unlock.html"

to_employee:

Шаблоны содержания писем

тема письма (subject)

По умолчанию "QR код для подключения мобильного устройства к SafeMobile"

qr_send_subject: "QR код для подключения мобильного устройства к SafeMobile"

```
# ссылка на файл текста с QR-кодом

# Текст по умолчанию содержит "{{QR}}".

# Для изменения содержания укажите ссылку на файл с новым содержанием.

# Путь к файлу указывается в рамках файловой системы docker-образа, а не host-
машины

# qr_send_template: "/home/safephone/message_templates/employee-qr-send.html"


# Рекомендация: заблокировать администратора root после настройки APM

# safephone.disable-root: true


# Максимальное количество записей для включения в xlsx отчёты

# По умолчанию - 10000. Максимально возможное: 1 048 576, если превышает, то APM
установит в 1 048 576

# safephone.max-page-size: 1048576


# каталог для временных файлов отчётов

arm.dirname-tmp-file: ./


# URL для скачивания монитора

safemobile.url_for_monitor_download: https://safemobile.store/android/<version>/monitor.apk
```

Сообщение системы:

```
*****  
  
***      PREPARATION FOR EXECUTION STARTED      ***  
  
*****  
  
INFO: ad.cert_disable_validation: false  
  
Check and apply settings for LOCAL auth mode...  
  
auth-provider.active-directory.on:false  
  
AD:auth-provider.active-directory.on: no need to check the Idaps certificate  
  
There is no need to validate certificates for 'LDAP auth mode'  
  
Check and apply settings for mail...  
  
INFO: notification by mail disabled  
  
Checking the presence of a directory for temporary report files...  
  
INFO: directory for temporary report files [arm.dirname-tmp-file] exists:  
D:\_vpv\sp\safephone\safephone-arm\RuntimeUtils\  
  
Settings check completed
```

10. *Настройки секции mail с ССО2, включена.*

Имитация текущей даты: 2022-06-25T08:01Z

Содержание файла настроек:

```
#####  
  
# файл с ССО2 2023-09-15  
  
#####  
  
server:  
  
  servlet:  
  
    context-path:  
  
    session-timeout: 30  
  
    forward-headers-strategy: native  
  
#Logging  
logging:  
  
  level:  
  
    root: WARN  
  
  jdbc:  
  
    sqlonly: OFF  
  
    audit: OFF  
  
    connection: OFF  
  
    sqltiming: OFF
```

com.safephone.dao.resultcode: OFF

session.control:

enabled: false

maximum-sessions: 2

max-session-prevents-login: false

auth-provider:

database.on: true

active-directory.on: false

use ad.cert: "cert file name"

active-directory.on: true

gis:

servers:

- name: openstreetmap

label: openstreetmap.org

url: http://{a-c}.tile.openstreetmap.org/{z}/{x}/{y}.png

E-Mail

mail:

notification:

to_admin:

true - for use notification

enabled: true

template:

lock_subject: "СУМТС: Аккаунт заблокирован"

Uncomment for use

lock: "/config/admin-lock.html"

unlock_subject: "СУМТС: Аккаунт разблокирован"

Uncomment for use

unlock: "/config/admin-unlock.html"

to_employee:

Шаблоны содержания писем

тема письма (subject)

По умолчанию "QR код для подключения мобильного устройства к SafeMobile"

qr_send_subject: "QR код для подключения мобильного устройства к SafeMobile"

ссылка на файл текста с QR-кодом

Текст по умолчанию содержит "{{QR}}".

Для изменения содержания укажите ссылку на файл с новым содержанием.

Путь к файлу указывается в рамках файловой системы docker-образа, а не host-машины

qr_send_template: "/home/safephone/message_templates/employee-qr-send.html"

Рекомендация: заблокировать администратора root после настройки APM

safephone.disable-root: true

Максимальное количество записей для включения в xlsx отчёты

По умолчанию - 10000. Максимально возможное: 1 048 576, если превышает, то APM установит в 1 048 576

safephone.max-page-size: 1048576

каталог для временных файлов отчётов

arm.dirname-tmp-file: ./

URL для скачивания монитора

safemobile.url_for_monitor_download: https://safemobile.store/android/<version>/monitor.apk

Сообщение системы:

PREPARATION FOR EXECUTION STARTED

INFO: ad.cert_disable_validation: false

Check and apply settings for LOCAL auth mode...

auth-provider.active-directory.on:false

AD:auth-provider.active-directory.on: no need to check the ldaps certificate

There is no need to validate certificates for 'LDAP auth mode'

Check and apply settings for mail...

INFO: notification by mail enabled

Checking the presence of a directory for temporary report files...

INFO: directory for temporary report files [arm.dirname-tmp-file] exists:

D:_vpv\sp\safephone\safephone-arm\RuntimeUtils\.

Settings check completed

11. Проверка наличия каталога для временных файлов отчётов - не существует.

Имитация текущей даты: 2022-06-25T08:01Z

Содержание файла настроек:

#####

файл с ССО2 2023-09-15

#####

server:

servlet:

context-path:

session-timeout: 30

forward-headers-strategy: native

#Logging

logging:

level:

root: WARN

jdbc:

sqlonly: OFF

audit: OFF

connection: OFF

sqltiming: OFF

com.safephone.dao.resultcode: OFF

session.control:

enabled: false

maximum-sessions: 2

max-session-prevents-login: false

auth-provider:

database.on: true

```
active-directory.on: false
```

```
# use ad.cert: "cert file name"
```

```
# active-directory.on: true
```

```
gis:
```

```
servers:
```

```
- name: openstreetmap
```

```
label: openstreetmap.org
```

```
url: http://{a-c}.tile.openstreetmap.org/{z}/{x}/{y}.png
```

```
# E-Mail
```

```
mail:
```

```
notification:
```

```
to_admin:
```

```
# true - for use notification
```

```
enabled: false
```

```
# template:
```

```
lock_subject: "СУМТС: Аккаунт заблокирован"
```

```
# Uncomment for use
```

```
# lock: "/config/admin-lock.html"
```

```
unlock_subject: "СУМТС: Аккаунт разблокирован"
```

```
# Uncomment for use
```

```
# unlock: "/config/admin-unlock.html"
```

```
to_employee:
```

```
### Шаблоны содержания писем
```

```
# тема письма (subject)
```

```
# По умолчанию "QR код для подключения мобильного устройства к SafeMobile"
```

```
qr_send_subject: "QR код для подключения мобильного устройства к SafeMobile"
```

```
# ссылка на файл текста с QR-кодом
```

```
# Текст по умолчанию содержит "{{QR}}".
```

```
# Для изменения содержания укажите ссылку на файл с новым содержанием.
```

```
# Путь к файлу указывается в рамках файловой системы docker-образа, а не host-машины
```

```
# qr_send_template: "/home/safephone/message_templates/employee-qr-send.html"
```

```
# Рекомендация: заблокировать администратора root после настройки APM

# safephone.disable-root: true


# Максимальное количество записей для включения в XLSX отчёты

# По умолчанию - 10000. Максимально возможное: 1 048 576, если превышает, то APM
установит в 1 048 576

# safephone.max-page-size: 1048576


# каталог для временных файлов отчётов

arm.dirname-tmp-file: /run/arm


# URL для скачивания монитора

safemobile.url_for_monitor_download: https://safemobile.store/android/<version>/monitor.apk
```

Сообщение системы:

```
*****

***      PREPARATION FOR EXECUTION STARTED      ***

*****

INFO: ad.cert_disable_validation: false

Check and apply settings for LOCAL auth mode...

auth-provider.active-directory.on:false
```

AD:auth-provider.active-directory.on: no need to check the ldaps certificate

There is no need to validate certificates for 'LDAP auth mode'

Check and apply settings for mail...

INFO: notification by mail disabled

Checking the presence of a directory for temporary report files...

ERROR: bad setting for 'arm.dirname-tmp-file': /run/arm

12. Проверка наличия каталога для временных файлов отчётов –
существует.

Имитация текущей даты: 2022-06-25T08:01Z

Содержание файла настроек:

```
#####  
# файл с ССО2 2023-09-15  
#####  
server:  
  
  servlet:  
  
    context-path:  
  
    session-timeout: 30  
  
    forward-headers-strategy: native  
  
#Logging  
  
logging:
```

level:

root: WARN

jdbc:

sqlonly: OFF

audit: OFF

connection: OFF

sqltiming: OFF

com.safephone.dao.resultcode: OFF

session.control:

enabled: false

maximum-sessions: 2

max-session-prevents-login: false

auth-provider:

database.on: true

active-directory.on: false

use ad.cert: "cert file name"

active-directory.on: true

gis:

servers:

- name: openstreetmap

label: openstreetmap.org

url: http://{a-c}.tile.openstreetmap.org/{z}/{x}/{y}.png

E-Mail

mail:

notification:

to_admin:

true - for use notification

enabled: false

template:

lock_subject: "СУМТС: Аккаунт заблокирован"

Uncomment for use

lock: "/config/admin-lock.html"

unlock_subject: "СУМТС: Аккаунт разблокирован"

Uncomment for use

unlock: "/config/admin-unlock.html"

to_employee:

Шаблоны содержания писем

тема письма (subject)

По умолчанию "QR код для подключения мобильного устройства к SafeMobile"

qr_send_subject: "QR код для подключения мобильного устройства к SafeMobile"

ссылка на файл текста с QR-кодом

Текст по умолчанию содержит "{{QR}}".

Для изменения содержания укажите ссылку на файл с новым содержанием.

Путь к файлу указывается в рамках файловой системы docker-образа, а не host-машины

qr_send_template: "/home/safephone/message_templates/employee-qr-send.html"

Рекомендация: заблокировать администратора root после настройки APM

safephone.disable-root: true

Максимальное количество записей для включения в xlsx отчёты

По умолчанию - 10000. Максимально возможное: 1 048 576, если превышает, то APM установит в 1 048 576

safephone.max-page-size: 1048576

каталог для временных файлов отчётов

arm.dirname-tmp-file: ./

URL для скачивания монитора

safemobile.url_for_monitor_download: <https://safemobile.store/android/<version>/monitor.apk>

Сообщение системы:

```
*****  
  
***      PREPARATION FOR EXECUTION STARTED      ***  
  
*****  
  
INFO: ad.cert_disable_validation: false  
  
Check and apply settings for LOCAL auth mode...  
  
auth-provider.active-directory.on:false  
  
AD:auth-provider.active-directory.on: no need to check the ldaps certificate  
  
There is no need to validate certificates for 'LDAP auth mode'  
  
Check and apply settings for mail...  
  
INFO: notification by mail disabled  
  
Checking the presence of a directory for temporary report files...  
  
INFO: directory for temporary report files [arm.dirname-tmp-file] exists:  
D:\_vpv\sp\safephone\safephone-arm\RuntimeUtils\  
  
Settings check completed
```