НИИ СОКБ
ЦЕНТР РАЗРАБОТКИ

КОМПЛЕКСНАЯ ЦИФРОВАЯ МУЛЬТИПЛАТФОРМА УПРАВЛЕНИЯ МОБИЛЬНЫМИ СРЕДСТВАМИ КОММУНИКАЦИЙ

РУКОВОДСТВО ПО УСТАНОВКЕ И НАСТРОЙКЕ

SAFEMOBILE

Москва

2026

СОДЕРЖАНИЕ

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
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

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».

2 Состав UEM «SafeMobile»

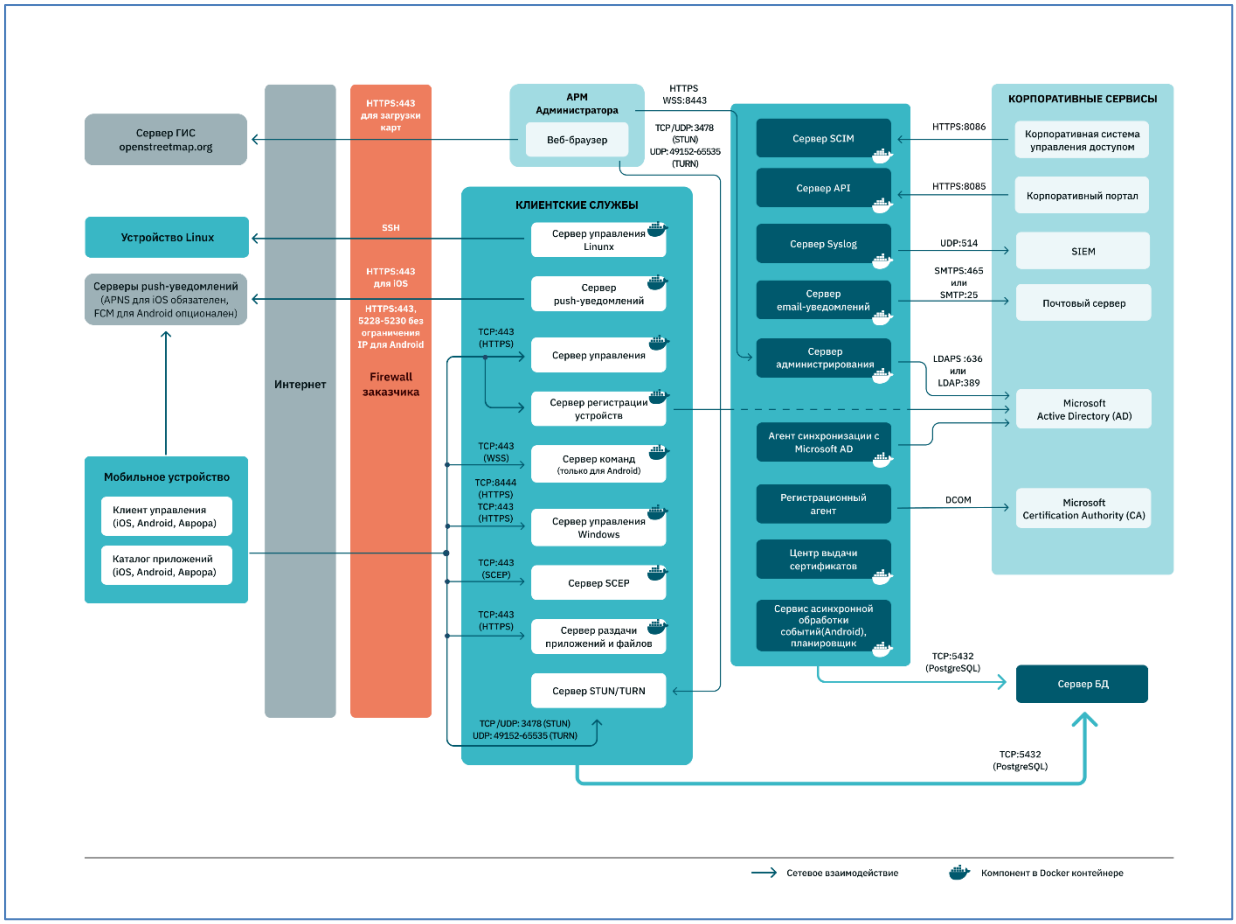

Рисунок 1.1 — Архитектурная схема

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. Компонент опционален. Установка требуется, если необходима интеграция системы с Microsoft AD;
- **apple-mdm-push** — сервис пуш-уведомлений для управления устройствами iOS. Компонент опционален. Установка требуется, если планируется управление устройствами на платформе iOS;

- **arm** — сервер администрирования. Компонент обязателен;
- **ca** — встроенный УЦ для выпуска сертификатов mTLS. Устанавливается автоматически вместе с компонентом **arm** и не требует дополнительных настроек;
- **db** — сервер баз данных. Компонент обязателен;
- **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 устройствами с ограниченной прошивкой, не обеспечивающей автозапуск и защиту MDM-агента от остановки операционной системой.
- **file-distr-server** — сервер раздачи корпоративных приложений и файлов. Компонент обязателен;
- **mdm** — сервер управления MDM (для Android, iOS, Windows и Аврора) Компонент обязателен. Предназначен для раздачи профилей, правил управления приложениями, конфигураций приложений на устройства с платформами: iOS, Android и Аврора. Также компонент обеспечивает доставку команд на устройства платформами: Android и Аврора;
- **apple-monitor-push** — сервис отправки пуш-уведомлений приложению EMM Client на iOS. Компонент опционален. Установка требуется, если планируется управление устройствами на платформе iOS и при этом планируется использование Монитора iOS;
- **lmsrv** — сервер управления Linux. Компонент опционален. Установка требуется, если планируется управление устройствами на платформе Linux;
- **mail-agent** — сервис отправки электронной почты. Компонент опционален. Установка требуется, если планируется использовать доставку уведомлений Администраторам и Сотрудникам по электронной почте;
- **nginx** — прокси-сервер, обеспечивающий внешние подключения по портам 443, 8443, 8444, 8085(стандартные значения, могут быть изменены). Компонент обязателен. Обеспечивает сетевую связанность компонентов;
- **regportal (Enrollment Server)** — сервер регистрации устройств. Компонент обязателен. Предназначен для регистрации устройств на платформах: iOS, Android, Аврора;
- **scep** — сервер получения пользовательских сертификатов из УЦ по протоколу SCEP. Компонент обязателен. Полученные сертификаты используются для подключения устройств по протоколу mTLS и для профилей, использующих клиентские сертификаты;
- **sesl** — сервис отправки системных логов. Компонент опционален. Установка требуется, если планируется подключение системы к корпоративному агрегатору логов;
- **smapi** — сервер публичного API. Компонент опционален;
- **scim** — сервер SCIM. Компонент опционален. Компонент реализует протокол SCIM v2.

Для внедрения может быть нужна кастомизация под конкретную реализацию OIDC.

- **mdmwss** — сервер команд (command-server для Android). Компонент опционален. Предназначен для доставки команд приложению Монитор начиная с версии 10.0. Установка требуется, если планируется управление устройствами на платформе Android;
- **winmdm —** сервер управления Windows. Назначение и условия применения. Компонент опционален. Установка требуется, если планируется управление устройствами на платформе Windows.
- **bgworker** — Компонент обязателен. Сервис асинхронной обработки событий (Android). А так же обеспечивает автоматическое удаление в БД устаревших данных

3 Системные требования

3.1 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, OracleLinux, RockyLinux, РЕД ОС;
3. OpenSUSE, SUSE Linux Enterprise Server (SLES);
4. ALT Linux, Alpine Linux.

«UEM SafeMobile» может работать с сервером PostgreSQL любой поддерживаемой версии. Работоспособность протестирована на следующих версиях:

1. PostgreSQL 14, 15;
2. PostgreSQL Pro 14;
3. Pangolin 5.

Примечание

UEM SafeMobile не работает с менеджерами коннектов, в том числе PGBOUNCER и HikariCP.

Для примера установки и настройки СУБД на сервере Debian 12, в комплекте с дистрибутивом «UEM SafeMobile» поставляются скрипт debian12_pg14_install.sh

Для управления 10К и более мобильных устройств рекомендуется размещать серверные компоненты SafeMobile, кроме сервера БД, в оркестраторе. Поддерживается работа с оркестраторами K8S и OpenShift.

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

3.2 Требования к серверным мощностям

3.2.1 До 10К управляемых устройств

В таблицах 3.1 и 3.2 указаны рекомендованные системные требования в зависимости от количества МСК, подключаемых к системе. В скобках указаны рекомендуемые серверные компоненты.

Таблица 3.1 — Системные требования для основных компонентов

Количество МСК	ВМ	CPU	ОЗУ, ГБ	Диск, ГБ
1 — 100	Сервер SafeMobile (db+arm+mdm+apple-mdm-push+regportal+apple-monitor-push+mdmwss+fcmpushserver+scep+ca++file-distr-server+bgworker)	4	8	30
101 — 500	Сервер SafeMobile (db+arm+mdm+apple-mdm-push+regportal+apple-monitor-push+mdmwss+fcmpushserver+scep+ca++file-distr-server+bgworker)	6	12	50
501 — 1000	Сервер Управления и Администрирования (arm+mdm+apple-mdm-push+regportal +apple-monitor-push +mdmwss+fcmpushserver+scep+ca+file-distr-server+bgworker)	6	10	30
	Сервер БД (db)	4	8	100
1001 — 2000	Сервер Управления (mdm+apple-mdm-push+regportal+apple-monitor-push +mdmwss+fcmpushserver+scep+file-distr-server+bgworker)	4	8	30
	Сервер Администрирования (arm+ca)	2	8	30
	Сервер БД (db)	4	8	200
2001 — 10000	Сервер Команд (mdmwss+fcmpushserver)	2	4	20
	Сервер Управления (mdm+apple-mdm-push+regportal+apple-monitor-push+file-distr-server+bgworker+scep)	4	8	20
	Сервер Администрирования (arm+ca)	2	8	30
	Сервер БД (db)	6	16	300

Таблица 3.2 — Системные требования для опциональных компонентов

ВМ	CPU	ОЗУ, ГБ	Диск, ГБ
Сервер Интеграций (adagent+mail-agent+sesl)	2	6	20
Сервер Управления Linux/Windows (lmsrv/winmdm)*	2	4	20
Сервер SMAPI	2	4	20

При установке winmdm и lmvsrv на отдельной машине следует **обязательно устанавливать MDM TLS сертификат.*

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

3.2.2 Более 10К управляемых устройств

Для управления 10К и более мобильных устройств рекомендуется размещать серверные компоненты SafeMobile, кроме сервера БД, в оркестраторе. Поддерживается работа с оркестраторами K8S и OpenShift.

В таблице 3.3 перечислены системные требования и рекомендуемое количество подов серверных компонентов SafeMobile в зависимости от числа управляемых устройств. В таблице 3.4 перечислены требования к серверу БД.

Таблица 3.3 — Системные требования для 10К устройств iOS, Android, Аврора

Контейнер	CPU	ОЗУ, ГБ	Серверов для 10-20К	Серверов для 20-30К	Серверов для 30-40К	Серверов для 40-50К	Серверов для 50-100К
adagent	1	1	1	1	1	1	1
apple-mdm-push	1	1	2	4	6	8	16
arm+ca	2	6	1	1	1	1	1
fcmpushserver	1	1	2	4	6	8	16
file-distr-server	1	1	3	6	9	12	24
mdm	2	2	2	4	6	8	16
apple-monitor-push	1	1	2	4	6	8	16
mail-agent	1	1	1	1	1	1	1
regportal	1	2	1	1	1	4	8
scep	1	1	2	4	6	8	16
bgworker	1	0,5	1	1	1	1	1
sesl	1	1	1	1	1	1	1
smapi	1	3	1	1	1	2	4
mdmwss	1	1	1	2	4	6	12

Таблица 3.4 — Системные требования для работы компонента «Сервер БД (db)» для 10К и более 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

Дальнейшее увеличение числа управляемых устройств достигается с помощью горизонтального масштабирования, исходя из одной инсталляции для 100К устройств.

3.3 Требования к сетевому окружению

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

1. Клиентских подключений по следующим TCP-портам (указаны значения по умолчанию):
   - 8443 (https) — от ПК администратора к Серверу Администрирования;
   - 3478 (tcp/udp) и 49152-65535 (udp) — от ПК администратора к Серверу STUN/TURN;
   - 3478 (tcp/udp) и 49152-65535 (udp) — от МСК к Серверу STUN/TURN;
   - 443 (https) — от МСК всех платформ к Серверу Управления, Серверу регистрации устройств, Серверу SCEP и Серверу раздачи приложений и файлов;
   - 443 (https) — от МСК с ОС Windows к Серверу Управления Windows;
   - 8085 (https) — от внешних сервисов к Серверу API;
   - 8086 (https) — от внешних сервисов к Серверу SCIM;
   - 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. Трафика wss между рабочим местом администратора, с которого запускается консоль администрирования АРМ, и сервером администрирования.
4. Трафика wss от МСК с ОС Android к Серверу команд;
5. (Для управления iOS-устройствами) подключения Сервера Управления к серверам APNS обеспечения работы AppStore посредством:
   - доступа к DNS-серверу, разрешающему доменное имя:
     - api.push.apple.com (для APNS);
     - itunes.apple.com и *.mzstatic.com (для доступа к AppStore и загрузки приложений).

- прохождения IP-трафика к адресам 17.0.0.0/8, TCP-порт 443 (для APNS);

> ***Примечание***
> *Для возможности добавления приложений из AppStore в АРМ необходимо также обеспечить доступ к доменам itunes.apple.com и *.mzstatic.com с компьютера, на котором запущена АРМ.*

6. (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.

7. Доступ к Appstore — для получения списка приложений.
8. Доступ к странице списка протестированных устройств: https://safe-mobile.ru/product/devices-os/

> ***Внимание!***
>
> *Для корректной работы серверных компонентов и рабочего места администратора* ***обязательна*** *настройка синхронизации времени по протоколу* ***NTP, UDP-порт 123****.*

3.4 Требования к серверу БД

Для установки схемы БД SafeMobile можно воспользоваться подготовленными скриптами, приведенными в разделе 5.2, 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 заново инициализировать СУБД командой:

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

3.5 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).

4. Установка и настройка ПО Docker

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

На момент написания документации актуальная версия докера 27.5.1 (согласно оф.сайту docker.com).

Минимальная версия Docker для Debian — 27.5.1, для АстраЛинукс — 25.0.5~astra1. В дальнейшем необходимо поддерживать актуальные версии docker с учетом дистрибутива Linux.

Минимальная поддерживаемая версия Docker compose — 2.x. Версии 1.x более не поддерживаются.

5. 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.

5.1 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/
```

5.2 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 12**,** 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 5.2.

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

- *каталог sql*
- *debian12_pg14_install.sh*
- *INSTALL.md*
- *install.sh*
- *setup.sh*

5.2.1 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
Continuie (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 «5.2.4 Ручная оптимизация настроек СУБД PostgreSQL».

5.2.2 Первоначальная установка на новом сервере

Пользователям, использующим ОС Debian 12, 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:

```
./debian12_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 5.2.4.

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 « 5.3 Запуск скрипта первоначальной настройки серверных компонентов».

5.2.3 Минимальная установка

Предназначена для пользователей, у которых уже установлена СУБД PostgreSQL, создана БД и настроена в соответствии с требованиями в разделе 3.4.

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.

5.2.4 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
```

5.2.5 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 следующе параметры в файле postgresql.conf

```
tcp_keepalives_idle = 20 # TCP_KEEPIDLE, 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 данным момент, необходимо выполнить команду:

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

5.2.6 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 сертфикат для подключения.

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

5.2.6.1 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*

5.2.6.2 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.

5.2.6.3 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*

chown root client.key

chgrp 2000 client.key

chmod 640 client.key

5.3 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 «ДА», если сервера управления (mdm и winmdm) расположены 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 7.

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

Сформировать конфигурацию Сервера администрирования. Установка обязательна, т.к. компонент отвечает за консоль администрирования.

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

Использовать протокол HTTPS для сервера администрирования. Установка обязательна.

- Если конфиг уже был установлен:
  ARM: Old TLS certificate exists, create new? [y/n/q/?]? y
- При установке в первый раз:
  ARM: Create TLS certificate? [y/n/q/?]? y

5. ARM: Common Name (IP or domain name): 192.168.1.1

Адрес или доменное имя для сертификата сервера администрирования.

6. MDM server [y/n/q/?]? y

Сформировать конфигурацию сервера управления MDM. Установка обязательна, используется для всех устройств, за исключением Linux.

7. APNS MDM push server? [y/n/q/?]? y

Сформировать конфигурацию push server управления устройствами iOS. Установить, если будут использоваться устройства iOS.

8. APNS SafeMobile monitor push server? [y/n/q/?]? y

Сформировать конфигурацию push server клиента SafeMobile (iOS). Установить, если будут использоваться устройства iOS.

9. SCEP server? [y/n/q/?]? y

Сформировать конфигурацию SCEP сервера. Установка обязательна, т.к. компонент отвечает за рассылку mTLS сертификатов.

10. File Distribution Server? [y/n/q/?]? y

Сформировать конфигурацию сервера раздачи приложений. Установка обязательна, т.к. компонент используется для установки приложений и передачи файлов на устройства.

11. Android command server (WebSocket) [y/n/q/?]? y

Сформировать конфигурацию Сервера команд (MDM WebSocket server). Установить, если будут использоваться устройства Android.

12. Windows MDM? [y/n/q/?] y

Сформировать конфигурацию сервера WinMDM. Установить, если будут использоваться устройства Windows.

13. Registration portal (Enrollment server)? [y/n/q/?] y

Сформировать конфигурацию сервера регистрации устройств (Enrollment server). Устанавливается безусловно при установке Windows MDM.

14. FCM Push Server? [y/n/q/?] y

Сформировать конфигурацию пуш-сервера FCM. Установить, если ранее использовался и есть сертификат firebase.json. Используется для запуска приложения «Монитор» на некоторых устройствах.

15. Linux Management Server? y

Сформировать конфигурацию Сервера управления Linux. Установить, если будут использоваться устройства ОС Linux.

16. AD Sync Agent? y

Сформировать конфигурацию Сервера синхронизации с Microsoft AD. Установить, если планируется использовать синхронизацию с AD.

17. SafeMobile API Server? y

Сформировать конфигурацию Сервера API. Установить, если планируется работа в внешним API.

- При установке в первый раз:
  SafeMobile API Server: Create TLS certificate? y
- Если конфиг уже был установлен:
  SafeMobile API Server: Old TLS certificate exists, create new? y

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

Адрес или доменное имя для сертификата Сервера API

19. Mail Service? y

Сформировать конфигурацию Сервера email-уведомлений. Установить, если планируется выполнять рассылку на почту сотрудников.

20. Syslog Forward Service? y

Сформировать конфигурацию Сервера syslog. Установить, если планируется выгрузка во внешние SIEM-системы.

21. SCIM server? y

Сформировать конфигурацию SCIM server (API для управления учетными данными администратора). Не обязателен к установке.

- При установке в первый раз:
  SafeMobile SCIM Server: Create TLS certificate? y
- Если конфиг уже был установлен:
  SafeMobile SCIM Server: Old TLS certificate exists, create new? y

22. SCIM Server: Common Name (IP or domain name): 192.168.1.1

Адрес или доменное имя для сертификата SCIM сервера.

23. Database hostname: 192.168.1.1

Указать реальный IP-адрес сервера БД.

24. Database port (default: 5432): 5432

Порт сервера БД.

25. Database name: sphone

Имя БД.

26. Database username: sphone

Пользователь БД.

27. Database password:

Пароль пользователя БД.

- Если конфиг уже был установлен:
  MDM: Old TLS certificate exists, create new? y
- При установке в первый раз:
  MDM: Create TLS certificate? y

28. MDM: Common Name (IP or domain name): 192.168.1.1

Адрес или доменное имя для сертификата MDM сервера (а также для прочих серверов, работающих на порту 443: Сервер управления, Сервера регистрации устройств, Сервера команд, Сервера SCEP, Сервера раздачи приложений и файлов).

5.4 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
```

Чтобы установить максимальный размер шаблонов писем следует изменить параметр:

```
 mail:

 template.max_total_size: 50MB
```

Срок действия mTLS-сертификата настраивается в файле **«config/ca.yml»**. Дата окончания срока действия не должна превышать 2049 год.

5.5 Размещение приложения Монитор на web-сервере организации

Допускается размещение дистрибутива приложения «Монитор» на web-сервере организации.

По умолчанию приложение Монитор расположено по адресу:

https://safemobile.store/android/<версия_SafeMobile>/monitor.apk

(например, для SM 15.0 адрес выглядит так: https://safemobile.store/android/15.0/monitor.apk)

Для обеспечения генерации QR-кодов со ссылкой на внутренний web-сервер организации необходимо выполнить настройку следующих конфигурационных файлов:

1. В файле **config/arm.yml** добавить строку:
   safemobile.url_for_monitor_download: https://my.url/monitor.apk
2. В файле **config/regportal.yml** изменить значение параметра url:
   - Исходное значение:
     - url: https://safemobile.store/android/%7Bversion%7D/monitor.apk
   - Измененное значение:
     - url: https://my.url/monitor/apk
3. В АРМ перезапустить компонент regportal (см. Руководство администратора 2.14 «Информация—Компоненты»)

Ответственность за поддержание актуальной версии приложения «Монитор» на web-сервере организации возлагается на администратора программного комплекса.

5.6 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.

5.7 Создание docker-контейнеров

Установку docker-контейнеров следует запустить из каталога:

```
/opt/emm
```

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.

5.8 Настройка раздела «Подключения к серверам» в АРМ

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 (рисунок 3.1).

Тип сервера	Описание	URL	Сертификаты
Command Server	Сервер команд. Обеспечивает доставку команд устройствам с монитором версии 10.0 и выше	https://k8s-messy3.safe-mobile.ru	
Enrollment Server	Сервер регистрации устройств Android, iOS и Aurora	https://k8s-messy3.safe-mobile.ru:443	
File Distribution Server	Сервер предназначен для раздачи файлов и приложений. Если не используется внешний кэширующий сервер, то URL должен совпадать с URL MDMServer	https://k8s-messy3.safe-mobile.ru:443	
MDMServer	Сервер управления. Обеспечивает доставку профилей, конфигураций и правил управления приложениями устройствам Android, iOS и Аврора. А так же команд для устройств iOS и Аврора	https://k8s-messy3.safe-mobile.ru	
SCEPServer	Сервер получения пользовательских сертификатов для устройств Android, iOS и Аврора	https://k8s-messy3.safe-mobile.ru:8082	SCEP Server
TURN Server	Подключение для удалённого управления мобильным устройством по протоколу TURN	turn.safe-mobile.ru:3478	
WinMDM Enrollment	Сервер регистрации устройств Windows	https://k8s-messy3.safe-mobile.ru	
WinMDM Management	Сервер управления устройствами Windows	https://k8s-messy3.safe-mobile.ru:8444	

Рисунок 3.1 — 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 АРМ, в раздел «Серверные сертификаты», после чего в разделе «Подключения к серверам» появится возможность назначить этот доверенный сертификат на URL (рисунок 3.2).

Тип сервера	Описание	URL	Сертификаты
Command Server	Сервер команд. Обеспечивает доставку команд устройствам с монитором версии 10.0 и выше	https://k8s-messy2.safe-mobile.ru	Russian Trusted Root CA
File Distribution Server	Сервер предназначен для раздачи файлов и приложений. Если не используется внешний кэширующий сервер, то URL должен совпадать с URL MDMServer	https://k8s-messy2.safe-mobile.ru:443	Russian Trusted Root CA
MDMServer	Сервер управления. Обеспечивает доставку профилей, конфигураций и правил управления приложениями устройствам Android, iOS и Аврора. А так же команд для устройств iOS и Аврора	https://k8s-messy2.safe-mobile.ru	
SCEPServer	Сервер получения пользовательских сертификатов для устройств Android, iOS и Аврора	https://k8s-messy2.safe-mobile.ru:8082	SCEP Server
TURN Server	Подключение для удалённого управления мобильным устройством по протоколу TURN	k8s-messy2.safe-mobile.ru:3478	
WinMDM Enrollment	Сервер регистрации устройств Windows	https://k8s-messy2.safe-mobile.ru	
WinMDM Management	Сервер управления устройствами Windows	https://k8s-messy2.safe-mobile.ru:8444	

Рисунок 3.2 — Назначенные серверные сертификаты

5.9 Обеспечение доступности

Показатели доступности UEM SafeMobile определяются настройками резервного копирования и кластеризации СУБД, выполненными администратором баз данных (DBA) заказчика. Чем чаще будут делаться резервные копии, тем меньшими будут значения RPO (recovery point objective, допустимая потеря данных) и RTO (recovery time objective, допустимое время восстановления данных).

Дополнительные меры для обеспечения доступности и отказоустойчивости:

1. Кластеризация серверных компонентов SafeMobile. При этом могут использоваться пробы, описанные в разделе 10.2.
2. Кластеризация СУБД. Настраивается администратором баз данных (DBA) заказчика. Поддерживается работа с кластерной СУБД через внешний балансировщик, который предоставляет серверным компонентам активную ноду кластера. Например, HAProxy.
3. Очередь событий на мобильных клиентах. Мобильные клиенты сохраняют события в очереди до их доставки на сервер. Длина очереди управляется администратором. По умолчанию в очереди сохраняются до 20 000 событий. Это позволяет сохранить информацию о мобильном устройстве при длительной недоступности сервера.

6. Получение цифровых сертификатов и ключей

Для создания запроса и генерации ключа используется криптографический пакет OpenSSL.

6.1 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.

Генерация приватных ключей с формированием долгосрочных самоподписанных сертификатов выполняется при запуске скрипта первоначальной настройки в соответствии с описанием в 5.2.5.

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

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

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:

```
1.  -----BEGIN CERTIFICATE-----
2.  сертификат сервера
3.  -----END CERTIFICATE-----
4.  -----BEGIN CERTIFICATE-----
5.  промежуточный сертификат
6.  -----END CERTIFICATE-----
7.  -----BEGIN CERTIFICATE-----
8.  корневой сертификат
9.  -----END CERTIFICATE-----
```

5. Если используется внешний прокси-сервер, то на нем также должна использоваться цепочка сертификатов (см. п.4).

6.2 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.

Получение сертификата:

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 окончанию 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:

1. Нажать **«Create a Certificate»** (Создать сертификат).
2. 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).
3. Нажать **«Browse»** (Обзор), перейти на подписанный файл MdmPush.plist на своем компьютере, выбрать его и нажать **«Upload»** (Загрузить).
4. 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.

Обновление сертификата:

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:

1. 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.*

2. Нажать **«Browse»** (Обзор), перейти на подписанный файл MdmPush.plist на своем компьютере, выбрать его и нажать **«Upload»** (Загрузить).
3. 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 mdm apple-mdm-push

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

6.3 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/**.

6.4 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.

7. Обновление системы

7.1 Особенности обновления с версий 8.2 — 10.x

В версии 10.x экземпляр Сервера SCEP более не устанавливается автоматически вместе с Сервером MDM. При установке обновления, Сервер SCEP должен быть установлен вручную. Если ранее использовался автоматически установленный Сервер SCEP, то при обновлении его предпочтительнее устанавливать на ту же виртуальную машину, что и Сервер MDM (см. таблицу 2.1 — Системные требования для основных компонентов).

В версии 10.0 компонент SocketServer работающий по проприетарному TCP протоколу был заменен на компонент Command Server (mdmwss). Но для выполнения обновления приложений Монитор Андроид с версий старше 10.0 — необходима установка обоих компонентов и SocketServer, и Command Server. Компонент SocketServer можно отключить и удалить после того, как будут обновлены приложения Монитор на всех подключенных устройствах Android.

7.2 Особенности обновления с версии 7.x и более ранних

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:

- **ca** — встроенный УЦ для выпуска сертификатов mTLS. Устанавливается автоматически вместе с Сервером Администрирования (**arm)** и не требует дополнительных настроек.

Помимо новых компонент в 8.2 обязательным компонентом стал Сервер SCEP. Если SCEP ранее не использовался, то его лучше размещать на той же виртуальной машине, что и Сервер MDM (см. таблицу 2.1 — Системные требования для основных компонентов). после обновления системы необходимо:

- Если в системе ранее не использовался сервер SCEP, то в разделе АРМ «Объекты учета» -> «Подключения к серверам» скопировать настройки из MDMServer в настройки SCEPServer. В этом случае Сервер SCEP будет использовать тот же порт, что и Сервер MDM.
- Если в системе ранее был установлен сервер SCEP возможны два варианта: либо продолжить использовать его на старом порту, либо перейти на использование порта Сервера MDM.. Для продолжения использования прежнего порта Сервера SCEP,

установленного с предыдущей версией, необходимо открыть порт в конфигурационном файле docker-compose server (раскомментировать строку # — ${BIND_ADDR}:8082:8082 # scep (old port)). Во втором случае необходимо в разделе APM «Объекты учета» -> «Подключения к серверам» скопировать настройки из MDMServer в настройки SCEPServer.

- 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 начиная с 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 и параметры подключения по WebSocket. Пример настройки внешнего прокси-сервер:

```
http {
  # ...
  map $http_upgrade $connection_upgrade {
    default upgrade;
    '' close;
  }

  server {
    # ...
```

```
    location / {
      # ...

      proxy_set_header        X-Forwarded-Proto $scheme;
      proxy_set_header        Host $host;
      proxy_set_header        X-Forwarded-For
$remote_addr;
      proxy_set_header        X-Real-IP $remote_addr;
      proxy_set_header        X-Forwarded-For
$proxy_add_x_forwarded_for;
      proxy_set_header        X-Client-Certificate
$ssl_client_escaped_cert;
      proxy_set_header        X-Client-Certificate-Sha1
$ssl_client_fingerprint;

      proxy_read_timeout 360;

      proxy_http_version 1.1;
      proxy_set_header Upgrade $http_upgrade;
      proxy_set_header Connection $connection_upgrade;
    }
  }

}
```

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.

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.

7 Если используются файрволл, антивирус, или DLP система, проверьте, что они не блокируют трафик wss между рабочим местом администратора, с которого запускается консоль администрирования арм, и сервером администрирования.

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 обратится в службу поддержки за дополнительными материалами.

7.3 Обновление до версии 15.x

Обновление серверных компонентов

Для обновления уже установленной «UEM SafeMobile» до текущей версии дополнительно в установочный комплект входит файл *db-postgresql-patch-<version>.tar.gz,* (например db-postgresql-patch-9.0-34-g23dd384.tar.gz) , который рекомендуется распаковать в каталог /tmp/ командой:

```
tar xzvf db-postgresql-patch-*.*.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:

   ```
   cd /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 новые

конфигурационные файлы (в каталоге **«emm»**) с файлами ранее используемого релиза (в каталоге **«emm-old»**). 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.

Перемещение политики «URL ссылка для скачивания фонового изображения».

Если используется профиль «Режим киоска Android» и в нем задана политика «URL ссылка для скачивания фонового изображения ...», то после обновления Монитора на устройствах, данная политика работать не будет. Если необходимо задавать фоновое изображение в киоске, то перед обновлением мониторов необходимо создать профиль «Обои Android» и назначить его на устройства с киоском.

7.4 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.

7.5 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.

7.6 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
   ```

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
   ```

7.7 Обратная совместимость

Новые версии серверных компонентов UEM SafeMobile поддерживают обратную совместимость на уровне API, необходимого для обновления мобильных клиентов предыдущий версий до актуальный. Полноценная работоспособность системы гарантируется при совпадении мажорных версий серверных и клиентских компонентов.

8 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
```

9 Описание конфигурационных файлов

9.1 Конфигурационный файл сервера управления MDM

9.1.1 Название файла

iosmdm.yml

9.1.2 Параметры и секции

Параметры:

- iosmdm.sowa
- iosmdm.mdm_cert
- iosmdm.mdm_key
- iosmdm.log_format
- iosmdm.log
- iosmdm.default_ownership

Секции:

- iosmdm.lost_mode_messages
- iosmdm.server
- iosmdm.db_pool

9.1.3 Подробный пример

В данном примере представлен наиболее подробный конфигурационный файл с максимальным количеством настроек. В продакшене нужны не все настройки.

```
iosmdm:
  log: d # уровни логирования DEBUG (D, T), INFO (I), WARNING (W), ERROR
(E), FATAL (F, CRITICAL, C) — регистр любой
  timing: c # только для разработчиков — логирование хронометража ХП
  # для подписи профиля Apple
  mdm_cert: \config\iosmdm.crt
  mdm_key: \config\iosmdm.key

  # настройки МСК (экран блокировки при потере устройства)
  lost_mode_messages:
    message: Устройство заблокировано
    footnote: Обратитесь к администратору
  # настройки MDM-сервера
  sowa: true                                  # только для разработчиков —
true|false включение проверки json body запроса
  server:
    numthreads: 19                      # количество потоков МДМ-сервера

  db_pool:
    minconn: 3
    maxconn: 40
```

9.1.4 Изменения в версии 8.2

Начиная с версии 8.2 параметры MDM сервера, относящиеся к порталу регистрации и пуш серверу MDM были перенесены в отдельные конфигурационные файлы в связи с появлением отдельных сервисов. Далее представлен список перенесённых параметров.

Все параметры, отсутствующие в данном файле относительно версии 7.0 более не поддерживаются.

Новые секции:

- Секция db_pool — настройка подключений к БД

(Подробности о параметрах см. раздел Конфигурационный файл REGPORTAL).

- Секция providers — отвечает за способы регистрации
- Секция monitor — отвечает за url мониторов, скачиваемых на странице регистрации
- Секция ldap — отвечает за настройки блокировки попыток входа через ldap
- Параметры mdm_cert и mdm_key продублированы в конфигах regportal.yml и iosmdm.yml

9.1.5 Изменения в версии 9.0

1. Подсекция cache была полностью удалена, так как за раздачу файлов отвечает FDS.
2. Подсекция monitorpush также удалена в связи с переписанным пуш сервером.

9.1.6 Подсекция lost_mode_messages

Отвечает за сообщения, показываемые на экране при блокировке устройства (режиме пропажи).

Обязательная: нет.

```
lost_mode_messages:
    message: Устройство заблокировано
    footnote: Обратитесь к администратору
```

message — текст в верхней части экрана
footnote — текст в нижней части экрана

9.1.7 Подсекция server

Отвечает за настройки http сервера MDM

Обязательная: нет

```
server:
    numthreads: 19
```

numthreads — количество потоков, обслуживающих http-запросы. По умолчанию: 20.

9.1.8 Подсекция db_pool

Отвечает за настройки базы данных

Обязательная: нет

```
db_pool:
    minconn: 3
    maxconn: 40
```

minconn — минимальное количество соединений с БД. По умолчанию 5. maxconn — максимальное количество соединений с БД. По умолчанию 40.

9.1.9 Подсекция sowa

Значения: false/true

Обязательное: нет

По умолчанию: false

Управляет включением компонента проверки json-содержащих body во входящих запросах. Компонент предназначен для эмуляции работы шлюза безопасности SOWA, применяемого в ПАО «Сбербанк».

В случае отсутствия параметра принимает значение по умолчанию false — компонент отключен. Проверка осуществляется по описанию ожидаемого json согласно стандарту JSON-schema draft-07.

9.1.10 Подсекция iosmdm.mdm_cert

Сертификат для подписи профиля iOS

Значения: str

Обязательное: да

По умолчанию: config/iosmdm.crt

```
iosmdm:
    ...
    mdm_cert: /config/iosmdm1.crt
```

Параметр mdm_cert определяет путь к сертификату мдм-сервера.

Если параметр не указан, то мдм-сервер использует путь к сертификату iOS устройств (config/iosmdm.crt). Требуется только для управления iOS

9.1.11 Подсекция iosmdm.mdm_key

Ключ для подписи профиля iOS

```
iosmdm:
    ...
    mdm_key: /config/iosmdm.key
```

Параметр mdm_key определяет путь к приватному ключу сертификата MDM сервера.

Если параметр не указан, то MDM сервер использует путь к сертификату iOS устройств (config/iosmdm.key).

Ключ участвует в подписи профиля управления mdm. Требуется только для управления iOS

9.1.12 Подсекция iosmdm.log_format

Формат логирования. Если параметр не указан используется формат по умолчанию

```
iosmdm:
    ...
    log_format:   %(levelname).1s:(%(threadName)-10s):   %(filename)s:
%(funcName)s: %(lineno)s: %(message)s
    ...
```

Параметр log_format определяет формат логирования

9.1.13 Подсекция iosmdm.log

Уровень логирования

Значения: DEBUG/D/T/INFO/I/WARNING/W/ERROR/E/FATAL/F/CRITICAL/C

```
iosmdm:
    ...
    log: D
    ...
```

9.2 Конфигурационный файл REGPORTAL

9.2.1 Название файла

regportal.yml

9.2.2 Параметры и секции

Параметры:

- regportal.log
- regportal.log_format
- regportal.mdm_cert
- regportal.mdm_key

Секции:

- regportal.server
- regportal.providers
- regportal.ldap
- regportal.monitor

9.2.3 Подробный пример

```
regportal:
  log: D    # уровни логирования DEBUG (D, T), INFO (I), WARNING (W),
ERROR (E), FATAL (F, CRITICAL, C) — регистр любой

  # для подписи профиля Apple
  mdm_cert: /config/iosmdm.crt
  mdm_key: /iosmdm.key

  server:
    numthreads: 19                    # количество потоков сервера

  providers: # способы регистрации
    — code
    — ldap

  ldap: # настройка сервера ldap
    account_lockout_threshold: 3             # количество попыток входа
до блокировки
    reset_account_lockout_counter_after: 1       # таймаут до сброса
количества попыток, минуты
    account_lockout_duration: 2              # длительность блокировки,
минуты

  monitor: # каким ОС откуда брать свои Мониторы
    — descr: Android
      regex: \bandroid
      url: https://safemobile.store/android/9.0/monitor.apk
    — descr: Aurora 3
      regex: \bsailfish
      url: https://safemobile.store/aurora/9.0/monitor.rpm
    — descr: Aurora 4
      regex: ^(?!.*\b(?:Windows|Mac|iPhone)\b).*\bGecko\/.*$
      url: https://safemobile.store/aurora/monitor.rpm
    — descr: iOS
      regex: \biphone|\bmac
      url: https://apps.apple.com/ru/app/id1462613087

  jwt_expiration = 30
```

9.2.4 Параметр regportal.log

Уровень логирования.

Значения: DEBUG/D/T/INFO/I/WARNING/W/ERROR/E/FATAL/F/CRITICAL/C

```
regportal:
    ...
    log: D
    ...
```

Параметр log_format определяет формат логирования.

9.2.5 Параметр regportal.log_format

Формат логирования.

Если параметр не указан используется формат по умолчанию.

```
regportal:
    ...
    log_format:   %(levelname).1s:(%(threadName)-10s):   %(filename)s:
%(funcName)s: %(lineno)s: %(message)s
    ...
```

9.2.6 Параметр regportal.mdm_cert

Сертификат для подписи профиля iOS. Требуется только для подключения iOS.

Значения: str

Обязательное: да

По умолчанию: config/iosmdm.crt

```
     regportal:
    ...
    mdm_cert: ../config/iosmdm.crt
```

9.2.7 Параметр regportal.mdm_key

Ключ для подписи профиля iOS. Требуется только для подключения iOS.

Параметр mdm_key определяет путь к приватному ключу сертификата MDM сервера.

Если параметр не указан, то MDM сервер использует путь к сертификату iOS устройств (config/iosmdm.key).

```
regportal:
    ...
    mdm_key: ../config/iosmdm.key
```

9.2.8 Подсекция server

Отвечает за настройки http сервера MDM.

Обязательная: нет.

numthreads — количество потоков, обслуживающих http-запросы. По умолчанию: 19.

```
        server:
    numthreads: 19
```

9.2.9 Подсекция providers

Отвечает за параметры авторизации. Обязательная: да

code — авторизация по коду приглашения, ldap — авторизация по учётным данным LDAP

```
providers:
    - code
    - ldap
```

9.2.10 Подсекция ldap

Отвечает за настройки авторизации по LDAP. Обязательная: нет

account_lockout_threshold — количество неудачных попыток входа до блокировки, reset_account_lockout_counter_after — таймаут до сброса счетчика неудачных попыток, минуты account_lockout_duration — длительность блокировки, минуты.

```
  ldap:
    account_lockout_threshold: 3
    reset_account_lockout_counter_after: 1
    account_lockout_duration: 2
```

9.2.11 Подсекция monitor

Отвечает за ссылки на мониторы для разных ОС Обязательная: да.

Представляет собой массив словарей, каждый новый элемент начинается с:

– descr — описание, regex — регулярное выражение для определения типа ОС (используется для определения платформы по user-agent), url — ссылка на монитор.

```
monitor: # каким ОС откуда брать свои Мониторы
    – descr: Android
      regex: \bandroid
      url: https://safemobile.store/android/6.1/monitor.apk
```

9.2.12 Параметр jwt_expiration

Время жизни jwt сессии в минутах. По умолчанию равно 30.

9.3 Конфигурационный файл пуш сервера системного монитора iOS

9.3.1 Название файла

apple-mdm-push.yml

9.3.2 Параметры и секции

Параметры:

- apnspush.log_format
- apnspush.log

Секции:

- apnspush.db_pool
- apnspush.apns_settings

9.3.3 Подробный пример

В данном примере представлен наиболее подробный конфигурационный файл с максимальным количеством настроек. В продакшене нужны не все настройки.

```
apple-mdm-push:
  log: W

  db_pool:
    minconn: 5
    maxconn: 5
#  Стандартные параметры
# apns_settings:
#   apns_addr: api.push.apple.com
#   apns_port: 443
#   client_cert: /config/MdmPush.pem

# Параметры для прокси
  apns_settings:
    apns_addr: mdmproxy.local
    apns_port: 17443
    client_cert: /config/MdmProxy.pem
    ca_cert: /config/ProxyRootCA.crt
```

9.3.4 Параметр mdmpush.log_format

Формат логирования.

Если параметр не указан используется формат по умолчанию.

```
apple-mdm-push:
    ...
    log_format:   %(levelname).1s:(%(threadName)-10s):   %(filename)s:
%(funcName)s: %(lineno)s: %(message)s
    ...
```

9.3.5 Параметр mdmpush.log

Уровень логирования.

Значения: DEBUG/D/T/INFO/I/WARNING/W/ERROR/E/FATAL/F/CRITICAL/C

```
apple-mdm-push:
    ...
    log: D
    ...
```

9.3.6 Подсекция apns_settings

Отвечает за настройки пуш сервера встроенного клиента ios. Обязательная: нет

apns_addr — адрес апнс сервера (или прокси на него)

apns_port — порт

client_cert — путь к клиентскому сертификату

ca_cert — путь к сертификату удостоверяющего центра

```
apns_settings:
    apns_addr: proxy.safe-mobile.ru
    apns_port: 8085
    client_cert: /config/MdmProxy.pem
    ca_cert: /config/ca.pem
```

9.3.7 Подсекция db_pool

Отвечает за настройки базы данных. Обязательная: нет.

minconn — минимальное количество соединений с БД. По умолчанию 5.

maxconn — максимальное количество соединений с БД. По умолчанию 40.

```
db_pool:
    minconn: 3
    maxconn: 40
```

9.4 Конфигурационный файл пуш сервера монитора iOS (EMM Client)

9.4.1 Название файла

apple-monitor-push.yml

9.4.2 Параметры и секции

Параметры:

- apnspush.log_format
- apnspush.log

Секции:

- apnspush.db_pool
- apnspush.apns_settings

9.4.3 Подробный пример

В данном примере представлен наиболее подробный конфигурационный файл с максимальным количеством настроек. В продакшене нужны не все настройки.

```
apple-monitor-push:
  log: W

  db_pool:
    minconn: 5
    maxconn: 5

#  Стандартные параметры
# apns_settings:
#   apns_addr: api.push.apple.com
#   apns_port: 443
#   client_cert: /config/MdmPush.pem

# Параметры для прокси
  apns_settings:
    apns_addr: mdmproxy.local
    apns_port: 17443
    client_cert: /config/MdmProxy.pem
    ca_cert: /config/ProxyRootCA.crt
```

9.4.4 Параметр monitorpush.log_format

Формат логирования.

Если параметр не указан используется формат по умолчанию.

```
apple-monitor-push:
    ...
    log_format:   %(levelname).1s:(%(threadName)-10s):   %(filename)s:
%(funcName)s: %(lineno)s: %(message)s
    ...
```

9.4.5 Параметр monitorpush.log

Значения: DEBUG/D/T/INFO/I/WARNING/W/ERROR/E/FATAL/F/CRITICAL/C

```
apple-monitor-push:
    ...
    log: D
    ...
```

9.4.6 Подсекция apns_settings

Отвечает за настройки пуш сервера встроенного клиента ios. Обязательная: нет.

apns_addr — адрес апнс сервера (или прокси на него)

apns_port — порт

client_cert — путь к клиентскому сертификату

ca_cert — путь к сертификату удостоверяющего центра

monitor_uuid — uuid монитора aps — содержимое пуша (не требует изменения без необходимости).

```
apns_settings:
    apns_addr: proxy.safe-mobile.ru
    apns_port: 8085
    client_cert: /config/MdmProxy.pem
    ca_cert: /config/ca.pem
    monitor_uuid: ru.safe-phone.Monitor
    push_content:
        aps:
            content-available: 1
            sound:
```

9.4.7 Подсекция db_pool

Отвечает за настройки базы данных. Обязательная: нет.

minconn — минимальное количество соединений с БД. По умолчанию 5. maxconn — максимальное количество соединений с БД. По умолчанию 40.

```
db_pool:
    minconn: 3
    maxconn: 40
```

10 Проверка работоспособности «UEM SafeMobile»

10.1 С помощью АРМ Администратора

После установки и запуска сервисы apple-mdm-push и fcmpushserver 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 АРМ 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 МСК главного окна выбрать **подключенный, незаблокированный и доступный для управления** комплект в соответствии с рисунком 5.1, у которого:
   - состояние соединения МСК, которое отображается в столбце «Статус», — в сети;
   - состояние блокировки МСК, которое отображается в столбце «Статус», — не заблокирован;
   - состояние управления устройством, которое отображается в столбце «Статус», — доступно для управления.

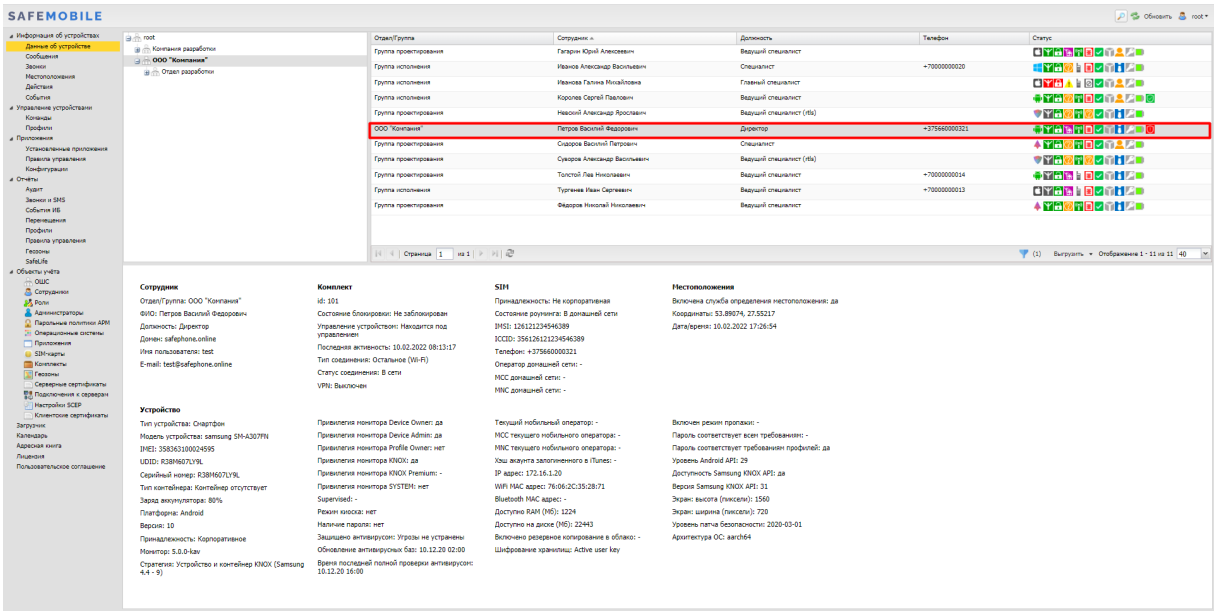

Рисунок 5.1 — Выбор подключенного незаблокированного комплекта

3. В главном меню выбрать раздел «Команды» и отправить на устройство команду «Переподключение» соответствии с рисунком 5.2, с параметром 10 с. Затем в окне «Уведомления» нажать кнопку «ОК».

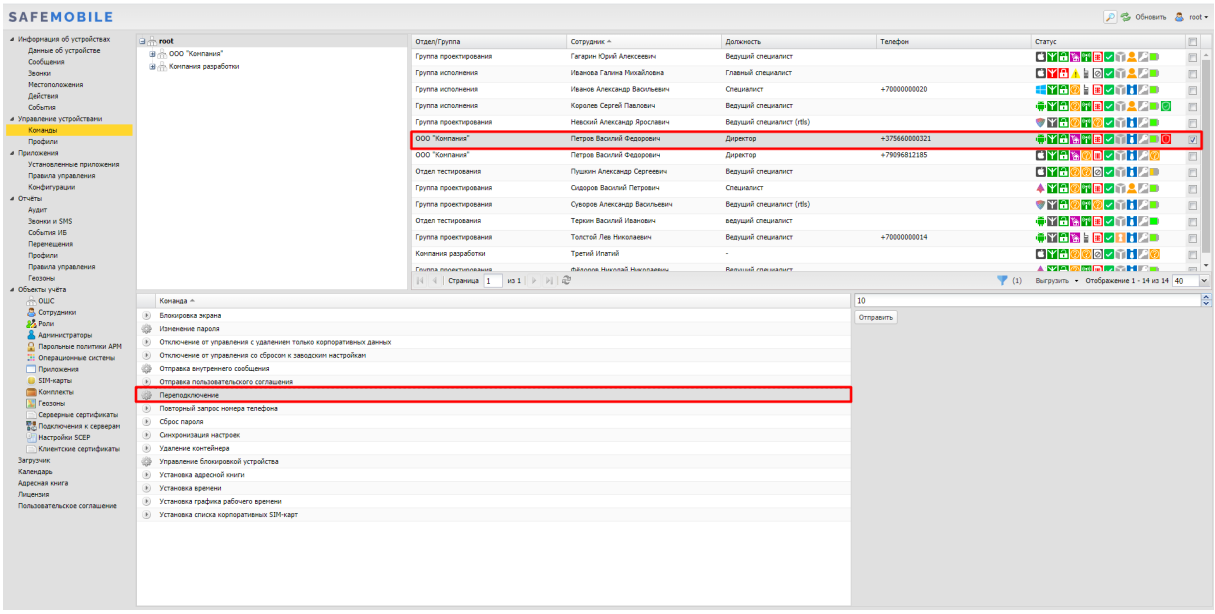

Рисунок 5.2 — Отправка команды «Переподключение»

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 5.3);

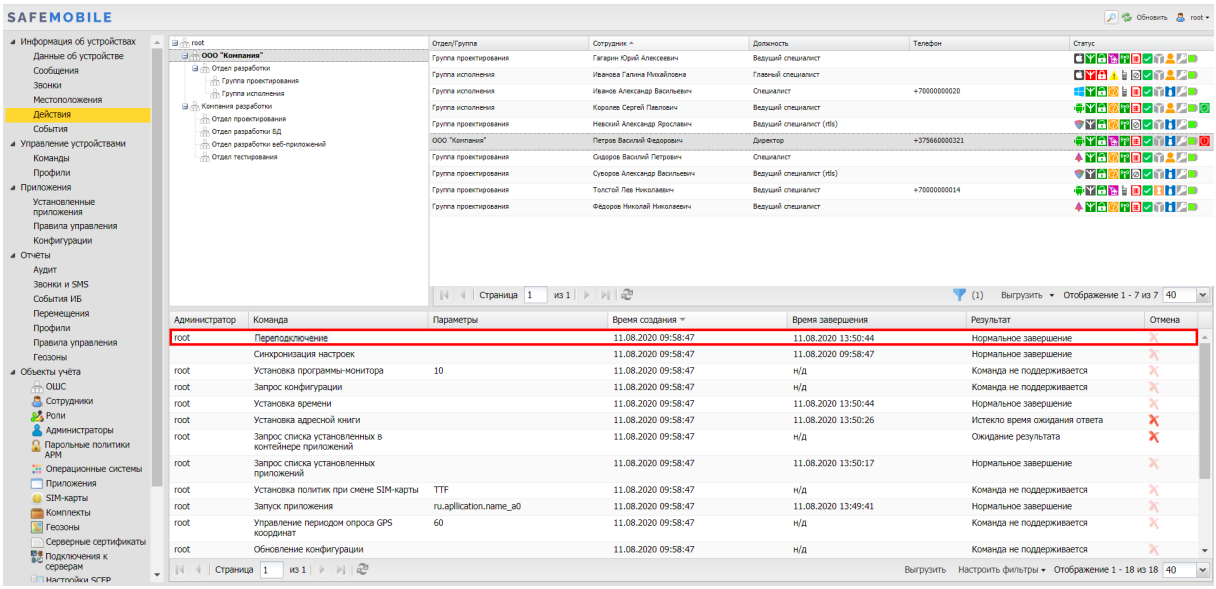

Рисунок 5.3 — Результат команды «Переподключение»

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

10.2 С помощью http health-check проверок

Для непосредственного мониторинга основных компонентов SM реализованы HTTP Health Checks — проверки здоровья.

При получении запроса на health-check URL компонент проверяет:

- Работоспособность основного процесса.
- Доступность базы данных.

В случае успешной проверки возвращается HTTP-код ответа 200. Все остальные коды ответа, а также их отсутствие или таймаут, говорят о неработоспособности или ошибках в работе компонента.

Проверки могут быть использованы как для систем мониторинга доступности, так и для получения статуса компонентов со стороны вышестоящих балансировщиков в случае HA-архитектуры.

Для получения возможности использования проверок необходимо создать файл health.mdm.conf в директории config/nginx установленного дистрибутива со следующим содержанием:

```
# сервер команд
location = /health-check/wss/liveness/ {
    proxy_pass http://wss/health/liveness;
}

# сервер управления
location = /health-check/mdm/liveness/ {
    proxy_pass http://mdm/health/liveness;
}

location = /health-check/arm/liveness/ {
    proxy_pass http://arm-frontend/health/liveness;
}

location = /health-check/regportal/liveness/ {
    proxy_pass http://regportal/health/liveness;
}

# сервер File Distribution
location = /health-check/fds/liveness/ {
    proxy_pass http://fds/health/liveness;
}

# сервер API
location = /health-check/smapi/liveness/ {
```

```
    proxy_pass http://smapi/health/liveness;
}

# сервер SCEP
location = /health-check/scep/liveness/ {
    proxy_pass http://scep/health/liveness;
}
```

После добавления файла необходимо перезапустить компоненты SM:

```
docker compose down && docker compose up -d
```

Внимание!

1. *Для каждого компонента формируется отдельная секция **location**. Если компонент не установлен на данной машине (например, если у вас разные компоненты расположены на разных VM), его секцию необходимо убрать из файла. В противном случае nginx будет давать ошибку host not found in upstream.*
2. *Пробы не имеют аутентификации, поэтому для каждого location крайне рекомендуется добавить список разрешенных IP-адресов. Пример:*

```
location = /health-check/wss/liveness/ {

    proxy_pass http://wss/health/liveness;

    allow 192.168.1.100; # Разрешенный локальный адрес 1

    allow 192.168.1.101; # Разрешенный локальный адрес 2

    deny all; # Запрет для всех остальных адресов

}
```

Список URL для проверок с учетом указанного выше конфигурационного файла nginx:

URL	**Название компонента**
https://<ваш_домен>/health-check/wss/liveness/	Сервер команд
https://<ваш_домен>/health-check/mdm/liveness/	Сервер управления
https://<ваш_домен>/health-check/arm/liveness/	Сервер администрирования
https://<ваш_домен>/health-check/regportal/liveness/	Портал регистрации
https://<ваш_домен>/health-check/fds/liveness/	Сервер File Distribution
https://<ваш_домен>/health-check/smapi/liveness/	Сервер API
https://<ваш_домен>/health-check/scep/liveness/	Сервер SCEP

Приложение А — Диагностические сообщения при запуске АРМ

В случае необходимости получения логов уровня debug следует сменить уровень логирования. Для этого необходимо выполнить следующие действия:

1. Остановить контейнер winmdm
2. Создать файл config/winmdm.json:

```
{
  "Logging": {
    "LogLevel": {
      "Default": "Debug",
      "Microsoft": "Debug",
      "Microsoft.Hosting.Lifetime": "Information"
    }
  }
}
```

3. Запустить контейнер winmdm

Диагностические сообщения

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\\ldapserver.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\\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: ldaps 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\\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: ldaps url: ldaps://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\\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: ldaps 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
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: ldaps 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: ldaps 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      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\\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: ldaps url: ldaps://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: ldaps://192.168.15.150
protocol = ldaps
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 CCO2, выключена*

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

   Содержание файла настроек:

```
############################################################
# файл с CCO2 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 АРМ
# safephone.disable-root: true

# Максимальное количество записей для включения в xlsx отчёты
# По умолчанию — 10000. Максимально возможное: 1 048 576, если
превышает, то АРМ 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
```

10. *Настройки секции mail с CCO2, включена.*

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

    Содержание файла настроек:

```
############################################################
# файл с CCO2 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 АРМ
# safephone.disable-root: true
```

```
# Максимальное количество записей для включения в xlsx отчёты
# По умолчанию — 10000. Максимально возможное: 1 048 576, если
превышает, то АРМ 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 CCO2 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 CCO2 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 АРМ
# safephone.disable-root: true

# Максимальное количество записей для включения в xlsx отчёты
```

```
# По умолчанию — 10000. Максимально возможное: 1 048 576, если
превышает, то АРМ 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
```

Приложение Б — Поддержка удаленного управления

Для поддержки «удаленного управления» необходимо развернуть TURN сервер, для этого используйте документ »Инструкция_по_установке_и_настройке_TURN_STUN_серверов» из состава документации SafeMobile.

При формировании конфигурационного файла TURN сервера генерируется парольная фраза для аутентификации клиентов, укажите ее в SafeMobile в файле /opt/emm/config/arm.yml

Секция:
 # Удалённое управление

Параметр:
secret:

После чего выполните рестарт докер контейнера arm , выполнив команду:

cd /opt/emm && docker-compose restart arm