UNLIMITED PRODUCTION

eXpress

Система коммуникаций

Руководство администратора

Установка

Версия 4
Сборка 3.6
12.10.2023

Почтовый адрес:	127055, г. Москва, ул. Новослободская, д.24, стр.1
Телефон:	+7 (495) 968-96-58
E-mail:	support@express.ms
Web:	https://express.ms/

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Руководство предназначено для администраторов изделия «Система коммуникаций «Express» 05262609.62.01.29.000.001 (далее – СК «Express», Express, система). В нем содержатся сведения, необходимые для установки и настройки системы.

Служба технической поддержки. Связаться со службой технической поддержки можно по электронной почте support@express.ms. Страница службы технической поддержки на сайте компании «Анлимитед продакшен» https://express.ms/ru/support.

Сайт в интернете. Информацию о продукте компании «Анлимитед продакшен» представлена на сайте https://express.ms/.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термин	Определение
API	Application programming interface — интерфейс для взаимодействия программ и приложений
APNS	Apple Push Notification Service — сервис push-уведомлений Apple
botX	Платформа для разработки чат-ботов
CTS	Corporate Transport Server — корпоративный сервер
ETS	Enterprise Transport Server — сервер предприятия
FCM	Firebase Cloud Messaging — служба, которая упрощает обмен сообщениями между мобильными приложениями и серверных приложений
JSON	Текстовый формат обмена данными, основанный на JavaScript
NTLM	Протокол сетевой аутентификации, разработанный фирмой Microsoft для Windows NT
RTS	Regional Transport Server — региональный сервер
SIEM	Security information and event management — управление информацией о безопасности и событиями безопасности
Single CTS	Единый корпоративный сервер
SMTP	Сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP
SSL	Криптографический протокол для безопасной связи
STUN	Сетевой протокол для определения внешнего IP-адреса, используемый для установления соединения UDP между двумя хостами в случае, если они оба находятся за маршрутизатором NAT
TLS	Протокол защиты транспортного уровня
TURN	Протокол для получения входящих данных через TCP или UDP соединения
VAPID-ключи	Voluntary Application Server Identification — пара ключей: открытый и закрытый. Закрытый ключ сервер хранит в тайне, а открытый передаёт клиенту. Ключи позволяют сервису push-уведомлений знать о том, какой сервер приложения подписал пользователя, и быть уверенным в том, что это — тот же самый сервер, который отправляет уведомления конкретному пользователю
Виджет	Конструктивный элемент панели, отвечающий за визуальный вывод части информации, собранной системой
ВКС	Видео- и конференц-связь
КСПД	Корпоративная сеть передачи данных
Кэш	Промежуточный буфер с быстрым доступом, содержащий информацию, которая может быть запрошена с наибольшей вероятностью
ПДС	Платформа доверенных сервисов
ПК	Персональный компьютер
Разделенный CTS	Разделенный корпоративный сервер: Front CTS и Back CTS
Роутинг	Контур, в котором существует чат (корпоративный, публичный, смешанный)
Траст	Сервис для передачи данных между CTS и RTS и другими сервисами, входящими в их контур

Глава 1

ОБЩИЕ СВЕДЕНИЯ

НАЗНАЧЕНИЕ КОМПЛЕКСА

СК «Express» предназначено для предоставления качественной и непрерывной связи между сотрудниками компании и снижения рисков утечек информации за счет перемещения каналов обмена из сети Интернет в периметр локальных вычислительных сетей Компании.

ОСНОВНЫЕ ФУНКЦИИ

Express реализует следующие основные функции:

- быстрый обмен пользователей текстовыми сообщениями и файлами с помощью мобильных устройств и веб-клиента на ПК в рамках персональных и групповых чатов;
- осуществление персональных и групповых аудио- и видеозвонков;
- обеспечение безопасного хранения и передачи конфиденциальных данных;
- создание копии данных для восстановления работоспособности подсистемы в случае ее повреждения или разрушения;
- оптимизация использования ресурсов.

ОСНОВНЫЕ КОМПОНЕНТЫ

СК «Express» предусматривает три контура взаимодействия пользователей (которые могут поставляться в трех исполнениях):

- публичный (внешний);
- контур предприятия (внутренний контур компании, объединяющий несколько внутренних серверов);
- корпоративный (внутренний).

Публичный (внешний) контур взаимодействия пользователей используется для:

- первичной регистрации пользователей;
- отправки push-уведомлений;
- обмена сообщениями и файлами с пользователями, не подключенными к какому-либо внутреннему контуру;
- совершения звонков пользователями, не подключенным к какому-либо внутреннему контуру;
- маршрутизации сообщений и файлов между внутренними контурами, не имеющими прямых доверенных подключений.

Контур предприятия (внутренний контур компании) используется для:

- регистрации пользователей;
- отправки push-уведомлений;
- маршрутизации сообщений и файлов между корпоративными контурами, не имеющими прямых доверенных подключений.

Корпоративный (внутренний) контур взаимодействия пользователей используется для:

- регистрации корпоративных пользователей;
- обмена сообщениями, файлами и совершения звонков с пользователями компании;
- предоставления корпоративной адресной книги;
- маршрутизации сообщений и файлов между корпоративным контуром компании и корпоративными контурами партнеров, с которыми установлены доверенные подключения.

СК «Express» включает следующие отдельно устанавливаемые компоненты:

- региональный сервер Express (далее — RTS);
- сервер предприятия (далее — ETS);
- корпоративный сервер Express (далее — CTS);
- мобильное приложение;
- десктоп-приложение;
- веб-приложение.

RTS, ETS и CTS являются основными элементами в структуре комплекса.

RTS объединяют и обслуживают компьютерные сети внутри одного региона и отвечают за функционирование публичного контура взаимодействия.

ETS объединяют и обслуживают компьютерные сети и корпоративные серверы внутри одной большой компании и отвечают за функционирование контура предприятия. Под ETS выпускается отдельное приложение, которое управляется компанией, использующей ETS. Пользователи CTS, подключенные к ETS, получают СМС и push-уведомления с этого ETS.

CTS объединяют и обслуживают клиентские устройства в пределах организации, подключаются к ETS или RTS и выполняют роль посредника между клиентским устройством и ETS/RTS. CTS отвечает за функционирование корпоративного контура. При установленном ETS информационный обмен между корпоративными серверами происходит внутри предприятия, данные с CTS передаются на ETS, ETS осуществляет информационный обмен с внешним контуром.

Клиентское устройство может подключаться как к CTS, так и к ETS или RTS напрямую. Для каждого сервера пользователь регистрирует свой профиль. В зависимости от активного профиля пользователю доступны свои ресурсы в виде чатов, контактов и истории обмена сообщениями. Подключение клиента к CTS возможно после подключения к RTS или ETS. Все сообщения, переданные между корпоративными пользователями, хранятся на CTS в зашифрованном виде и не доступны администраторам сервера. Для обеспечения работы голосовых вызовов используется сервер STUN/TURN (VoEx), который может быть расположен отдельно, совмещен с CTS или расположен на RTS/ETS.

Для обеспечения работы голосовых вызовов используется сервер STUN/TURN (VoEx), который может быть расположен отдельно, совмещен с CTS или расположен на RTS/ETS.

Для интеграции системы АТС используется модуль SIP-телефонии, который позволяет совершать и принимать голосовые вызовы, вести телефонную книгу и сопоставлять пользователей с номерами АТС («Определитель номера»).

Сопоставление функций и возможностей системы:

Таблица 1

Функции	Возможности
Исходящие вызов	• Совершение голосовых вызовов на АТС с использованием мобильного устройства или ПК; • вызов абонента путем набора номера
Входящий вызовов	Прием голосовых вызовов, поступающих с АТС с использованием мобильного устройства или ПК
Ведение телефонной книги	Интеграция телефонной книги модуля телефонии с: • телефонной книгой устройства, на котором установлен СК «Express»; • записями, сохраненными в СК «Express»;
Определитель номера	Сопоставление номера вызывающего абонента с соответствующим пользователем СК «Express» при поступлении входящего вызова с АТС на устройство с установленным СК «Express». В результате вызываемый пользователь получает информацию о звонящем (имя, аватар и т. п.). При совершении исходящего вызова с устройства с установленным СК «Express» на АТС, автоматически определяется вызываемый пользователь и отображается информация о нем

Управление комплексом осуществляется с помощью веб-интерфейса — консоли администратора, которая предоставляет возможности для настройки Express и контроля функционирования приложения.

ДОСТУПНЫЕ РОЛИ

Управление комплексом осуществляют сотрудники организации, обладающие правами администратора. Административные права системы назначаются иерархически.

Для безопасной и успешной эксплуатации Express определяются следующие роли:

Таблица 2

Роль	Права	Тип учетной записи
Администратор	• назначение ролей; • просмотр журнала безопасности; • управление чатами; • управление учетными записями пользователей; • подключение чат-ботов; • управление настройками системы	Внутренний пользователь
Корпоративный пользователь	• отправка сообщений; • создание чата; • просмотр адресной книги сервера; • подключение к чат-ботам	Внутренний пользователь
Региональный пользователь	• отправка сообщений; • создание чата	Внешний пользователь
Администратор безопасности	• просмотр сообщений в консоли DLP; • просмотр журналов в консоли DLP	Внутренний пользователь

Тип учетной записи зависит от положения сервера, на котором авторизован пользователь. Если в защитном контуре находится RTS, то региональный пользователь становится внутренним.

СК «Express» предусматривает создание администраторов с ограниченными правами для решения конкретных задач.

Задачи администраторов:

- установка и управление обновлениями общесистемного и прикладного ПО;
- настройка, поддержка в работоспособном состоянии и мониторинг работы серверного оборудования;
- управление резервным копированием и восстановление данных;
- централизованная настройка мобильного приложения;
- управление учетными записями пользователей.

АРХИТЕКТУРА

СК «Express» состоит из внешнего контура и внутреннего контура. Связь между внешним и внутренним контуром средства в локальной сети осуществляется с помощью специального сервиса — траста. Внешний контур состоит из регионального сервера (RTS), внутренний контур состоит из корпоративного сервера (CTS) или сервера предприятия (ETS) и CTS, которые к нему подключаются.

Серверная часть Express основана на микросервисной архитектуре с использованием контейнеризации на основе Docker. Данное решение позволяет максимально автоматизировать развертывание и обновление серверного ПО Express.

CTS поддерживает 2 вида развертывания:

- единый сервер Express (Single CTS), см. стр. 13;
- разделенный сервер Express (Front CTS и Back CTS), см. стр. 14.

ETS поддерживает 2 вида развертывания:

- ETS и единый сервер Express (Single CTS), см. стр. 16;
- ETS и разделенный сервер Express (Front CTS и Back CTS), см. стр. 17.

Сервер видеосвязи (VoEx) размещается в сети Интернет либо в демилитаризованной сетевой зоне компании. При размещении в сети Интернет, VoEx располагается на выделенном сервере. При размещении в демилитаризованной сетевой зоне компании, VoEx может располагаться на выделенном сервере, на сервере Single CTS или Front CTS (в случае развертывания разделенного сервера).

Сервер чат-ботов (Bot-сервер) размещается во внутренней сети компании и предназначен для размещения чат-ботов и необходимых компонентов для их функционирования, например баз данных. Соединение с Bot-сервером выполняются с помощью docker-контейнера botx.

Для эксплуатации изделия требуется наличие межсетевого экрана на границе периметра сети с ограничением доступа к следующим компонентам:

- сервис интеграции с единым каталогом учетных записей (ad_integration);
- сервис обмена текстовыми и голосовыми сообщениями (messaging);
- сервис аутентификации пользователей (authentication);
- сервис администрирования (admin);
- сервис маршрутизации сообщений (routing_schema);
- сервис передачи паролей (kdc);
- сервис управления настройками сервера (etcd, settings).

Дополнительно должна применяться политика безопасности контента (Content Security Policy) в целях предотвращения и минимизации атак типа XSS.

РЕГИОНАЛЬНЫЙ СЕРВЕР

Для всех вариантов развертывания системы региональный сервер (RTS) размещается в сети Интернет и содержит в себе следующие контейнеры:

- admin (интерфейс администратора);
- audit (сервис аудита подключений);
- authentication_service (отвечает за авторизацию на RTS);
- email_notifications (отвечает за рассылку e-mail сообщений с кодом аутентификации);
- etcd (дополнение к settings, отвечает за хранение настроек сервисов);
- events (сервис информирования пользователей о событиях в чатах);
- file_service (сервис загрузки файлов);
- homescreen-smartapp (смартапп «Главная страница»);
- kafka (диспетчер сообщений между сервисами);
- kdc (хранилище ключей);
- messaging (сервис обмена сообщениями, отвечает за подключение клиентов через протокол websocket);
- nginx (веб-сервер, который принимает подключения извне и отвечает за маршрутизацию подключений);
- phonebook (адресная книга);
- postgres (основная база данных сервисов);
- preview_service (сервис предпросмотра страниц, на которые отправлены ссылки);
- prometheus (отвечает за снятие, обработку и хранение метрик сервисов);
- push_service (сервис отправки push-уведомлений);
- redis (KV-хранилище);
- routing_schema_service (сервис построения схем роутинга, визуализирует схему маршрутизации в чатах);
- settings (отвечает за хранение настроек сервисов);
- sms_service (сервис для отправки СМС-сообщений);
- stickers (сервис для управления стикерами);
- trusts(отвечает за взаимодействие с ETS и CTS);
- voex (сервис для совершения аудиовызовов);
- bot (отвечает за интеграцию с ботами);
- conference_bot (бот, отвечающий за уведомления о конференциях);
- notifications_bot (бот для отправки сообщений в глобальный чат).

ЕДИНЫЙ КОРПОРАТИВНЫЙ СЕРВЕР

Типовая схема развертывания Single CTS изображена ниже (Рисунок 1).

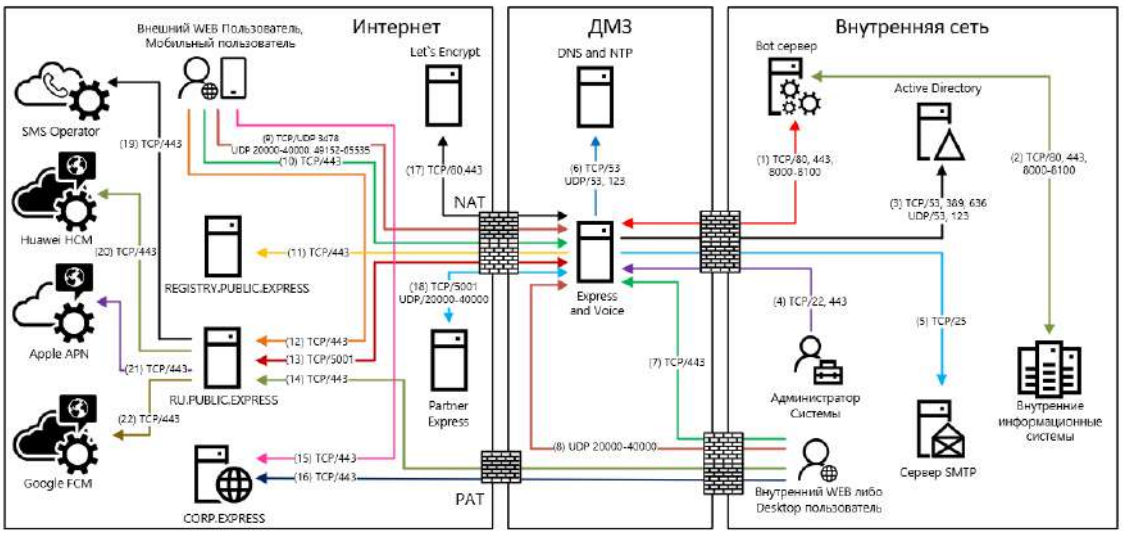


Рисунок 1. Типовая схема развертывания Single CTS

Внимание! Partner Express – партнерский сервер Express CTS, с которым можно установить доверенное соединение. Он расположен в локальной сети другой организации или сети интернет. Пользователи такого сервера принимают участие в аудио- и видеозвонках с пользователями CTS сервера, поэтому для обмена медиаданными по протоколу SRTP необходимо открыть соответствующие порты

Номера сетевых взаимодействий соответствуют номеру строки в Приложении 1.

Single CTS размещается в демилитаризованной сетевой зоне компании и содержит в себе следующие контейнеры docker:

- admin (интерфейс администратора);
- apigw (сервис информирования пользователей о событиях в чатах);
- audit (сервис аудита подключений);
- botx (отвечает за интеграцию с ботами);
- conference_bot (бот, отвечающий за уведомления о конференциях);
- corporate_directory (каталог открытых ботов и чатов);
- dlps (DLP-система Express);
- email_notifications (отвечает за рассылку e-mail сообщений с кодом аутентификации);
- etcd (дополнение к settings, отвечает за хранение настроек сервисов);
- events (сервис информирования пользователей о событиях в чатах);
- file_service (сервис загрузки файлов);
- kafka (диспетчер сообщений между сервисами);
- kdc (хранилище ключей);
- messaging (сервис обмена сообщениями, отвечает за подключение клиентов через протокол websocket);
- metrics_service (сервис сбора индивидуальных показателей ETS/CTS серверов);

- nginx (веб-сервер, который отвечает за маршрутизацию внутренних подключений);
- notifications_bot (бот для отправки сообщений в глобальный чат);
- ad_phonebook (адресная книга);
- postgres (основная база данных сервисов);
- prometheus (отвечает за снятие, обработку и хранение метрик сервисов);
- redis (KV-хранилище);
- routing_schema (сервис построения схем роутинга, визуализирует схему маршрутизации в чатах);
- settings (отвечает за хранение настроек сервисов);
- traefik (отвечает за получение сертификатов от LE и терминация TLS на входе);
- trusts (отвечает за обмен событиями между RTS, ETS и CTS, а также за взаимодействие с другими серверами Express);
- preview_service (сервис предпросмотра страниц, на которые отправлены ссылки);
- stickers (сервис для управления стикерами);
- voex (сервис для совершения аудиовызовов).

РАЗДЕЛЕННЫЙ КОРПОРАТИВНЫЙ СЕРВЕР

Типовая схема развертывания Front CTS и Back CTS изображена ниже (Рисунок 2).

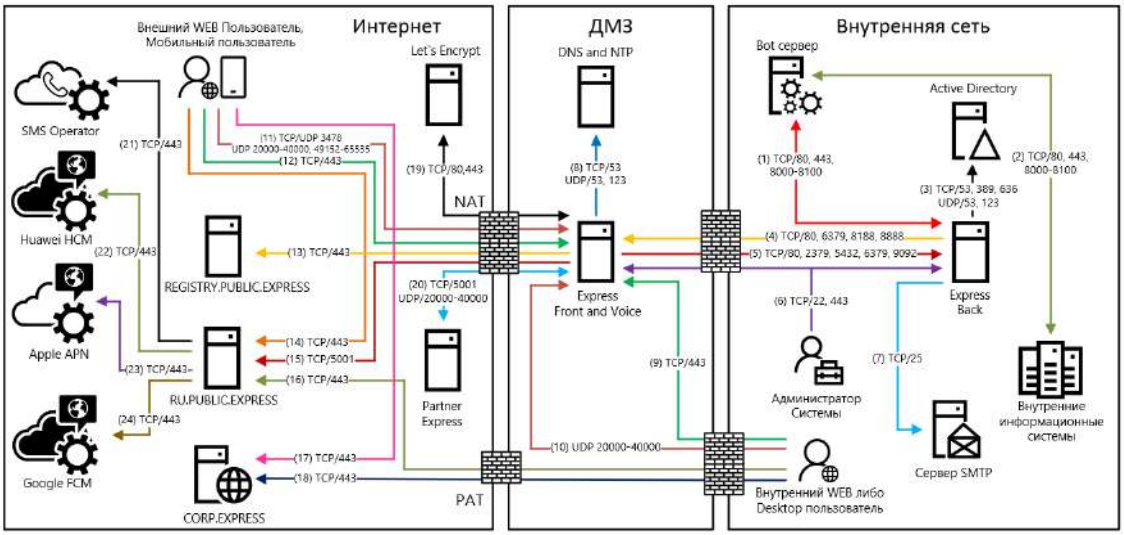


Рисунок 2. Типовая схема развертывания разделенного CTS (Front/Back)

Внимание! Partner Express – партнерский сервер Express CTS, с которым можно установить доверенное соединение. Он расположен в локальной сети другой организации или сети интернет. Пользователи такого сервера принимают участие в аудио- и видеозвонках с пользователями CTS сервера, поэтому для обмена медиаданными по протоколу SRTP необходимо открыть соответствующие порты.

Номера сетевых взаимодействий соответствуют номеру строки в Приложении 2.

Разделенный сервер состоит из Front CTS и Back CTS серверов.

Front CTS сервер размещается в демилитаризованной сетевой зоне компании и содержит в себе два контейнера и локальный прокси-сервер:

- nginx (веб-сервер, который принимает подключения извне и отвечает за маршрутизацию подключений);
- trusts (обеспечивает взаимодействие с сервером ETS/RTS и другими доверенными корпоративными CTS).
- tinyproxy (обеспечивает доступ Back CTS к репозиторию express).

Примечание. Если на том же сервере развернут компонент VoEx, перечень контейнеров дополнится следующими:

- coturn (сервер STUN/TURN);
- redis (KV-хранилище);

При установке рекомендуется использовать отдельный системный Redis.

Back CTS сервер размещается в локальной сети компании и содержит в себе следующие контейнеры docker:

- admin (интерфейс администратора);
- audit (сервис аудита подключений);
- apigw (сервис информирования пользователей о событиях в чатах);
- botx (отвечает за интеграцию с ботами);
- conference_bot (бот, отвечающий за уведомления о конференциях);
- corporate_directory (каталог открытых ботов и чатов);
- dlps (DLP-система Express);
- email_notifications (отвечает за рассылку e-mail сообщений с кодом аутентификации);
- etcd (дополнение к settings, отвечает за хранение настроек сервисов);
- events (сервис информирования пользователей о событиях в чатах);
- file_service (сервис загрузки файлов);
- kafka (диспетчер сообщений между сервисами);
- kdc (хранилище ключей);
- messaging (сервис обмена сообщениями, отвечает за подключение клиентов через протокол websocket);
- metrics_service (сервис сбора индивидуальных показателей ETS/CTS серверов);
- nginx (веб-сервер, который отвечает за внутреннюю маршрутизацию подключений);
- notifications_bot (бот для отправки сообщений в глобальный чат);
- ad_phonebook (адресная книга);
- postgres (основная база данных сервисов);
- prometheus (отвечает за снятие, обработку и хранение метрик сервисов);
- redis (KV-хранилище)[1];

[1] При установке рекомендуется использовать отдельный системный Redis. Встроенные контейнер Redis предназначен для демонстраций возможностей изделия.

- routing_schema (сервис построения схем роутинга, визуализирует схему маршрутизации в чатах);
- settings (отвечает за хранение настроек сервисов);
- tinyproxy (локальный прокси-сервер, обеспечивает подключение Back CTS к репозиторию образов docker, используемых для установки и обновления изделия). Устанавливается отдельно при отсутствии доступа с сервера к registry.public.express;
- stickers (сервис для управления стикерами);
- preview_service (сервис предпросмотра страниц, на которые отправлены ссылки);
- voex (сервис для совершения аудиовызовов).

СЕРВЕР ПРЕДПРИЯТИЯ И ЕДИНЫЙ КОРПОРАТИВНЫЙ СЕРВЕР

Типовая схема развертывания ETS и Single CTS изображена ниже (Рисунок 3).

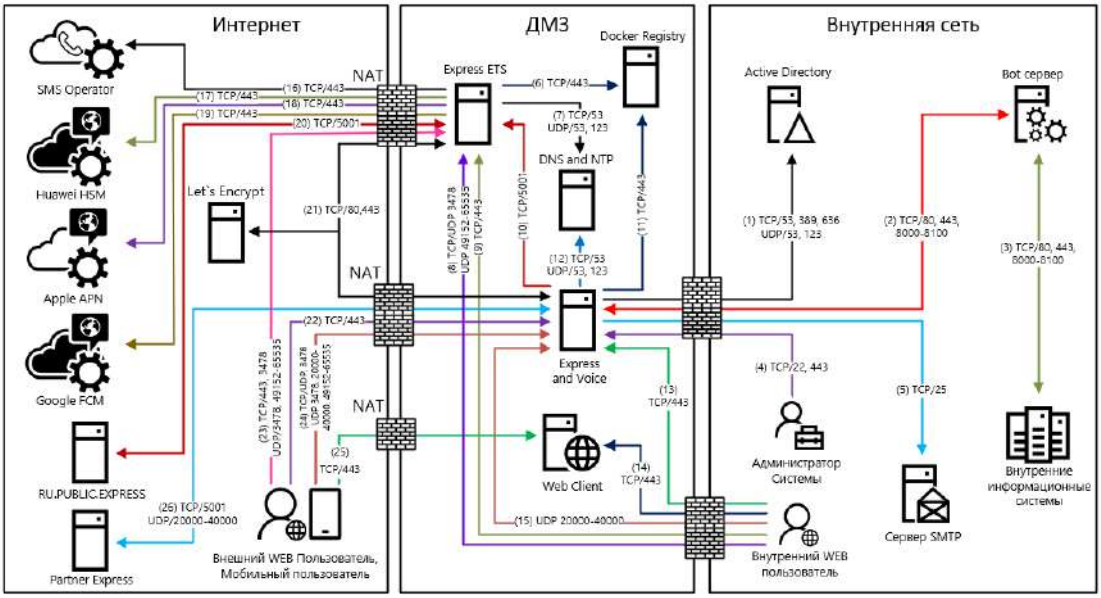


Рисунок 3. Типовая схема развертывания ETS и Single CTS

Внимание! Partner Express – партнерский сервер Express CTS, с которым можно установить доверенное соединение. Он расположен в локальной сети другой организации или сети интернет. Пользователи такого сервера принимают участие в аудио- и видеозвонках с пользователями CTS сервера, поэтому для обмена медиаданными по протоколу SRTP необходимо открыть соответствующие порты.

Номера сетевых взаимодействий соответствуют номеру строки в Приложении 3.

Сервер ETS размещается в демилитаризованной сетевой зоне компании и содержит в себе следующие контейнеры:

- audit (сервис аудита подключений);
- authentication_service (отвечает за авторизацию на ETS и RTS);
- email_notifications (отвечает за рассылку по электронной почте сообщений с кодом аутентификации);
- etcd (дополнение к settings, отвечает за хранение настроек сервисов);
- events (сервис информирования пользователей о событиях в чатах);

- file_service (сервис загрузки файлов);
- kafka (диспетчер сообщений между сервисами);
- kdc (хранилище ключей);
- ets_messaging (сервис обмена сообщениями, отвечает за подключение клиентов через протокол websocket);
- metrics_service (сервис сбора индивидуальных показателей ETS/CTS серверов);
- nginx (веб-сервер, который отвечает за маршрутизацию внутренних подключений);
- botx (отвечает за интеграцию с ботами);
- conference_bot (бот, отвечающий за уведомления о конференциях);
- notifications_bot (бот для отправки сообщений в глобальный чат);
- ets_phonebook (адресная книга);
- postgres (основная база данных сервисов);
- preview_service (сервис предпросмотра страниц, на которые отправлены ссылки);
- prometheus (отвечает за снятие, обработку и хранение метрик сервисов);
- push_service (сервис отправки push-сообщений);
- redis (KV-хранилище);
- settings (отвечает за хранение настроек сервисов);
- sms_service (сервис для отправки СМС-сообщений);
- stickers (сервис для управления стикерами);
- trusts (отвечает за взаимодействие с RTS и CTS);
- voex (сервис для совершения аудиовызовов).

Список контейнеров Single CTS представлен в п. «Единый корпоративный сервер», стр. 13.

СЕРВЕР ПРЕДПРИЯТИЯ И РАЗДЕЛЕННЫЙ КОРПОРАТИВНЫЙ СЕРВЕР

Типовая схема развертывания ETS, Front CTS и Back CTS изображена ниже (Рисунок 4).

Номера сетевых взаимодействий соответствуют номеру строки в Приложении 4.

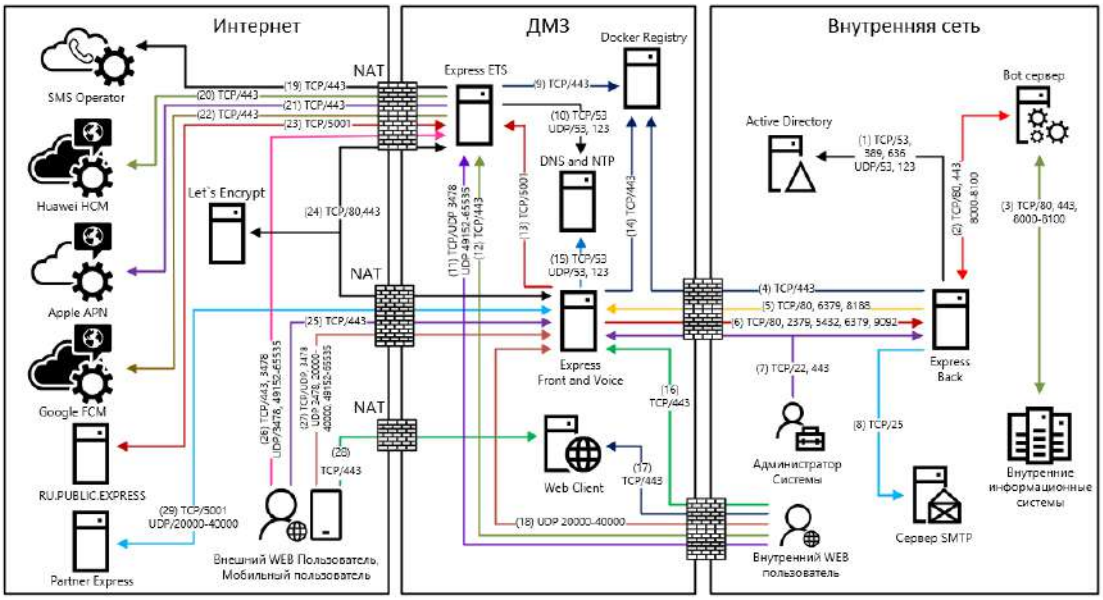


Рисунок 4. Типовая схема развертывания ETS, Front CTS и Back CTS

Сервер ETS размещается в демилитаризованной сетевой зоне компании и содержит в себе следующие контейнеры:

- audit (сервис аудита подключений);
- authentication_service (отвечает за авторизацию на ETS и RTS);
- email_notifications (отвечает за рассылку по электронной почте сообщений с кодом аутентификации);
- etcd (дополнение к settings, отвечает за хранение настроек сервисов);
- events (сервис информирования пользователей о событиях в чатах);
- file_service (сервис загрузки файлов);
- kafka (диспетчер сообщений между сервисами);
- kdc (хранилище ключей);
- ets_messaging (сервис обмена сообщениями, отвечает за подключение клиентов через протокол websocket);
- metrics_service (сервис сбора индивидуальных показателей ETS/CTS серверов);
- nginx (веб-сервер, который отвечает за маршрутизацию внутренних подключений);
- botx (отвечает за интеграцию с ботами);
- conference_bot (бот, отвечающий за уведомления о конференциях);
- notifications_bot (бот для отправки сообщений в глобальный чат);
- ets_phonebook (адресная книга);
- postgres (основная база данных сервисов);
- preview_service (сервис предпросмотра страниц, на которые отправлены ссылки);
- prometheus (отвечает за снятие, обработку и хранение метрик сервисов);
- push_service (сервис отправки push-сообщений);
- redis (KV-хранилище);

- settings (отвечает за хранение настроек сервисов);
- sms_service (сервис для отправки СМС-сообщений);
- stickers (сервис для управления стикерами);
- trusts (отвечает за взаимодействие с RTS и CTS);
- voex (сервис для совершения аудиовызовов).

Список контейнеров разделенного CTS представлен в п. «Разделенный корпоративный сервер», стр. 14.

СИСТЕМНЫЕ ТРЕБОВАНИЯ

ТРЕБОВАНИЯ К ПЛАТФОРМЕ

Примечание. В данном подразделе рассматриваются требования к платформе неотказоустойчивой конфигурации из расчета количества пользователей менее 3000. Если предполагается большее количество пользователей, обратитесь за индивидуальным проектом к разработчику.

CTS может быть развернут на аппаратной платформе или в среде виртуализации.

У Front CTS должен быть один сетевой интерфейс с поддержкой IPv6 (необходим для запуска сервисов, маршрутизация трафика ipv6 не требуется).

Важно! Для получения минимальных системных требований при установке сервера Single CTS требуется сложить соответствующие параметры для Front CTS и Back CTS.

Минимальные системные требования к аппаратным платформам в зависимости от количества пользователей:

Таблица 3 – Количество пользователей:100

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Front CTS	2	2	45	13
Back CTS	4	8	211	33
Bot	1	2	65	7
Всего	**7**	**12**	**321**	**53**

Таблица 4 – Количество пользователей:200

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Front CTS	2	2	45	13
Back CTS	4	10	358	43
Bot	2	4	85	9
Всего	**8**	**16**	**488**	**65**

Таблица 5 – Количество пользователей:300

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Front CTS	2	3	45	13
Back CTS	6	12	504	53
Bot	3	5	105	11
Всего	**11**	**20**	**654**	**77**

Таблица 6 – Количество пользователей:400

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Front CTS	2	3	45	13

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Back CTS	6	14	651	63
Bot	3	6	125	13
Всего	**11**	**23**	**821**	**89**

Таблица 7 – Количество пользователей:500

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Front CTS	3	4	45	13
Back CTS	8	16	797	73
Bot	4	7	145	15
Всего	**15**	**27**	**987**	**101**

Таблица 8 – Количество пользователей:600

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Front CTS	3	5	45	13
Back CTS	8	18	944	83
Bot	4	8	165	17
Всего	**15**	**31**	**1154**	**113**

Таблица 9 – Количество пользователей:700

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Front CTS	4	6	45	13
Back CTS	10	18	1090	93
Bot	4	9	185	19
Всего	**18**	**33**	**1320**	**125**

Таблица 10 – Количество пользователей:800

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Front CTS	4	7	45	13
Back CTS	10	20	1237	103
Bot	5	10	205	21
Всего	**19**	**37**	**1487**	**137**

Таблица 11 – Количество пользователей:900

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Front CTS	6	8	45	13
Back CTS	12	22	1383	113
Bot	5	11	225	23
Всего	**23**	**41**	**1653**	**149**

Таблица 12 – Количество пользователей:1000

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Front CTS	6	10	45	13
Back CTS	12	24	1530	123
Bot	6	12	245	25
Всего	**24**	**46**	**1820**	**161**

Таблица 13 – Количество пользователей:2000

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Front CTS	10	12	45	13
Back CTS	16	30	2995	223

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Bot	7	14	445	45
Всего	**33**	**56**	**3485**	**281**

Таблица 14 – Количество пользователей:3000

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Front CTS	14	14	45	13
Back CTS	20	36	4460	323
Bot	8	16	645	65
Всего	**42**	**66**	**5150**	**401**

Примечание. Объем SSD взят из расчета глубины хранения журналов (1 Гб) и пользовательских данных (4 Гб) за 4 года. Данные по требуемому месту могут значительно отличаться от расчетных при более активном использовании изделия.

Минимальные системные требования к серверу CTS для установки подсистем:

Таблица 15

Элемент	Параметры
Процессор	4 ядра, частота не менее 3.60 ГГц
Оперативная память	16 ГБ
Операционная система	Astra Linux Special Edition 1.7
Жесткий диск	Не менее 500 ГБ
Предустановленное ПО	• Docker-ce версии 18 или 20; • PostgreSQL версии 9, 10 или 14; • Postgres Pro Enterprise 9.6, 10, 11.13.1, 13.4.1, 11.14.1, 13.5.1, 11.15.1. и 13.6.1; • Postgres Pro Standard 9.6 или 10; • Postgres Pro Enterprise Certified 9.6 или 10; • Postgres Pro Certified 9.6 или 10
Сетевой адаптер	Ethernet

Минимальные системные требования к серверу ETS для установки подсистем:

Таблица 16

Элемент	Параметры
Процессор	4 ядра, частота не менее 3.60 ГГц
Оперативная память	16 ГБ
Операционная система	Astra Linux Special Edition 1.7
Жесткий диск	Не менее 500 ГБ
Предустановленное ПО	• Docker-ce версии 18 или 20; • PostgreSQL версии 9,10 или 14; • Postgres Pro Enterprise 9.6, 10, 11.13.1, 13.4.1, 11.14.1, 13.5.1, 11.15.1. и 13.6.1; • Postgres Pro Standard 9.6 или 10; • Postgres Pro Enterprise Certified 9.6 или 10; • Postgres Pro Certified 9.6 или 10
Сетевой адаптер	Ethernet

Минимальные системные требования к серверу RTS для установки подсистем:

Таблица 17

Элемент	Параметры
Процессор	4 ядра, частота не менее 3.60 ГГц
Оперативная память	16 ГБ
Операционная система	Astra Linux Special Edition 1.7
Жесткий диск	Не менее 500 ГБ

Элемент	Параметры
Предустановленное ПО	• Docker-ce версии 18 или 20; • PostgreSQL версии 9, 10 или 14; • Postgres Pro Enterprise 9.6, 10, 11.13.1, 13.4.1, 11.14.1, 13.5.1, 11.15.1. и 13.6.1; • Postgres Pro Standard 9.6 или 10; • Postgres Pro Enterprise Certified 9.6 или 10; • Postgres Pro Certified 9.6 или 10 • Apache Cassandra версии 3.11.4
Сетевой адаптер	Ethernet

Требование к операционной системе: Серверы CTS, ETC, RTS поддерживают любую ОС семейства Linux, на который устанавливается Docker 20.10.23. Рекомендуется Linux Astra 1.7.

Примечание. Серверы CTS, ETC, RTS поддерживают ОС Astra Linux 2.12.43 Common Edition «Орёл».

Требование к ПО контейнеризации: Docker: 20.10.23 (настоятельно рекомендуется установка из репозитория docker, https://docs.docker.com/install/linux/docker-ce/ubuntu/).

Требование к синхронизации времени: Необходим установленный и настроенный локальный сервер NTP с уровнем stratum не ниже 15.

Для воспроизведения веб-интерфейса рекомендуется использовать браузеры:

Таблица 18

Браузер	Версия
Google Chrome	68
Chromium	68
Yandex Browser	19
Firefox	79
Opera	56
Edge	79

Для воспроизведения десктоп-интерфейса рекомендуется использовать персональные компьютеры с операционными системами, перечисленными в таблице ниже (Таблица 19)

Таблица 19

ОС	Версия
Linux Astra "Смоленск"	1.7
Linux Astra "Воронеж"	1.7

ТРЕБОВАНИЯ К ПЛАТФОРМЕ STUN/TURN

Сервер STUN/TURN может быть развернут на аппаратном сервере или в среде виртуализации. Требования к аппаратной платформе сервера STUN/TURN в зависимости от количества пользователей:

Таблица 20

Кол-во пользователей	vCPU/CPU Core	RAM Гб	HDD Гб
10	2	1	42
25	4	2	42
50	4	2	42
100	8	4	42
200	10	5	42

500	12	6	42
1000	16	8	42
2000	18	9	42
5000	32	16	42
10000	64	32	42

При развертывании сервера STUN/TURN на сервер Single CTS требования суммируются.

ТРЕБОВАНИЯ К DNS

Для корректной работы СК «Экспресс» используется технология Split DNS:

- требуется DNS-имя для сервера CTS, разрешаемое в сети Интернет и ссылающиеся на внешний IP-адрес публикации сервера Single CTS или Front CTS. Рекомендуется имя третьего уровня, например express.mydomain.tld.
- во внутренней сети компании DNS-имя должно разрешаться во внутренний IP-адрес сервера CTS. При использовании раздельной установки (Front + Back CTS) каждому серверу назначается внутреннее DNS-имя, отличное от имени CTS-сервера.

Важно! **Если нет возможности использовать Split DNS, допускается настройка средствами ОС linux (служба systemd-resolved) с преобразованием во внутренней сети компании имен во внутренний IP-адрес.**

Требования к DNS-имени STUN/TURN сервера аналогичны требованиям к DNS-имени сервера CTS.

ТРЕБОВАНИЯ К СЕРТИФИКАТУ

Для работы изделия требуется оформить сертификат на внешнее имя сервиса Express (FQDN или wildcard), выпущенный публичным доверенным центром сертификации и удовлетворяющий следующим требованиям:

- версия 3 и не ниже TLS 1.2;
- длина ключа не меньше 2048 бит;
- алгоритм подписи SHA 256;
- версия синтаксиса X.509 3;
- незашифрованный закрытый ключ.

Файл должен содержать в себе сертификат сервера, сертификаты промежуточного центра сертификации и корневого центра сертификации. Формат сертификатов должен соответствовать кодировке Base64. Файл закрытого ключа должен содержать нешифрованный закрытый ключ кодировки Base64.

Примерная структура файла сертификата изображена на рисунке ниже (Рисунок 5).

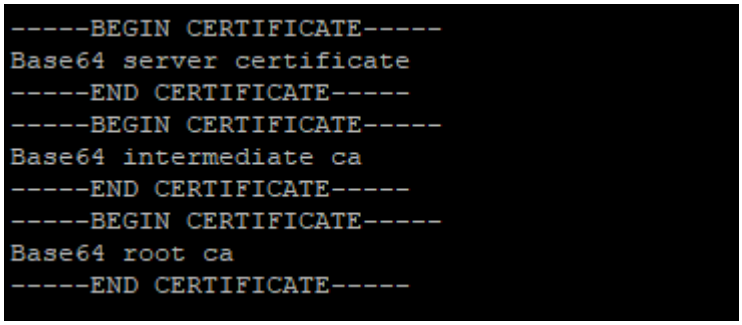


Рисунок 5

Поддерживается использование бесплатного сертификата от компании Let`s Encrypt.

ТРЕБОВАНИЯ К СЕРВЕРУ SMTP

Для возможности отправки ПИН-кодов аутентификации устройства пользователя требуется создание на почтовом сервер учетной записи, под которой будет производиться отправка электронной почты.

ТРЕБОВАНИЯ К СЕТЕВЫМ ВЗАИМОДЕЙСТВИЯМ

Требования к сетевым взаимодействиям описаны в Приложении 1, Приложении 2, Приложении 3, и Приложении 4.

ТРЕБОВАНИЯ К СЕРВЕРУ VOEX

Сервер VoEx может быть развернут на аппаратном сервер или в среде виртуализации. Минимальные системные требования к серверу VoEx в зависимости от количества пользователей:

Таблица 21

Кол-во пользователей	vCPU/CPU Core	RAM Гб	HDD Гб
10	2	1	42
25	4	2	42
50	4	2	42
100	8	4	42
200	10	5	42
500	12	6	42
1000	16	8	42
2000	18	9	42
5000	32	16	42
10000	64	32	42

Примечание. При развертывании сервера VoEx на сервер Single CTS или Front CTS требования суммируются.

ТРЕБОВАНИЯ К DLP

Для обеспечения работы DLP необходим доступ к следующим объектам и функционалу:

- подсистеме kafka для получения событий «admin-events» и «system-events»;
- API подсистем kdc (БД ключей безопасности) и messaging (БД сообщений);
- базам данных messaging (БД сообщений) и DLP;

- скачиванию файлов.

Требования к сетевой инфраструктуре входящих соединений:

Таблица 22

Модуль/сервис	Протокол	Порт
Веб-клиент	TCP	80, 443

Требования к сетевой инфраструктуре исходящих соединений:

Таблица 23

Модуль/сервис	Протокол	Порт
Kafka	TCP/UDP	9092/9093
Zookeeper	TCP	2182
Postgresql	TCP	5432
CTS-app	TCP	80, 443

Требования к объему памяти:

Таблица 24

Параметр	Значение
Процессор	8 ядер
Оперативная память	8 Гб
Жесткий диск	40 Гб
Пропускная способность сети	1 Гбит/с

Глава 2

УСТАНОВКА EXPRESS

Установка сервера Express включает в себя следующие этапы:

1) предварительная настройка (см. стр. 26);
2) предварительная настройка VoEx (см. стр. 29);
3) установка сервера VoEx (см. стр. 29);
4) установка корпоративного сервера (см. стр. 31);
5) настройка сервера VoEx (см. стр. 37);
6) установка регионального сервера и/или сервера предприятия (см. стр. 39);
7) запуск сервера (см. стр. 40);
8) настройка сервера:

- RTS (см. стр. 43);
- ETS (см. стр. 55);
- CTS (см. стр. 68).

ПРЕДВАРИТЕЛЬНАЯ НАСТРОЙКА

Для корректной работы сервера выполните предварительную настройку.

Внимание! Установку Express должен осуществлять пользователь Linux с опытом администрирования.

Ниже приведены требования удовлетворяющие ОС Astra Linux Смоленск и ОС Astra Linux Воронеж. Требования к ОС Astra Linux Воронеж являются менее жесткими и выбор служб (в частности служба синхронизации времени) может отличаться от заявленных ниже.

ОС ASTRA LINUX

Для предварительной настройки при использовании ОС Astra Linux:

1. Установите ОС Astra Linux. Во время установки на шаге выбора «Выбор программного обеспечения» выделите Базовые средства, Средства удаленного доступа SSH.
2. Установите Docker помощью команды:

```
sudo apt install docker.io
```

3. Установите дополнительное ПО (см. ниже).

СЛУЖБА СИНХРОНИЗАЦИИ ВРЕМЕНИ

В качестве службы синхронизации времени рекомендуется использовать службу timesyncd.

Примечание. Служба timesyncd не может выполнять функции сервера, это исключительно клиентская служба

Для использования timesyncd:

1. Удалите службы NTP и openntpd, если они были установлены ранее, с помощью команды:

```
sudo apt purge ntp openntpd
```

для удаления службы времени chronyd используйте команду:

```
sudo apt purge chronyd
```

2. Запустите службу timesyncd:

```
sudo systemctl start systemd-timesyncd
```

3. Проверьте работоспособность службы timesyncd командой:

```
sudo timedatectl status
```

4. Если имеются источники точного времени внутри компании, в файл /etc/systemd/timesyncd.conf внесите серверы NTP.

Укажите опции в конфигурационном файле:

- NTP= - разделённый пробелами основной список имён NTP-серверов.
- FallbackNTP= разделённый пробелами список имён резервных NTP-серверов.

Пример:

```
NTP=ntp1.local ntp2.local
FallbackNTP=ntp3.local
```

НАСТРОЙКА КОНФИГУРАЦИИ DOCKER

Для настройки конфигурации:

1. Откройте (создайте) конфигурационный файл:

```
sudo nano /etc/docker/daemon.json
```

2. Укажите параметры хранения журналов в Docker в каталоге /etc/docker/daemon.json:

```
{
"log-driver": "json-file",
 "log-opts": {
       "max-size": "1g"
 }
}
```

3. Выполните:

```
systemctl restart docker
```

ДОПОЛНИТЕЛЬНЫЕ ОПЕРАЦИИ

Для завершения предварительной настройки:

1. Проверьте цепочку SSL-сертификатов и убедитесь в правильном порядке набора сертификатов (см. стр. 23).
2. Проверьте правильность настроек сервера[1]:

Таблица 25

Название настройки	Определение	Решаемая задача
Открытые порты CTS	22, TCP	Удаленное подключение к SSH для управления сервером
Открытые порты DNS сервера	53, UDP/TCP	DNS-запросы
Открытые порты NTP сервера	123, UDP	Синхронизация времени по протоколу NTP

[1] Данные настройки подходят для установки всех компонентов на одном сервере. Подробные настройки сетевых взаимодействий для Single CTS и комбинации Front CTS и Back CTS см. стр. 45 «Приложение 2» и стр. 46 «Приложение 3» соответственно.

Название настройки	Определение	Решаемая задача
Открытые порты CTS	443, TCP	HTTPS-подключение мобильных клиентов к CTS
Открытые порты registry.public.express:443	443, TCP	Установка и обновление пакетов CTS
Открытый порт VoEX-сервера	6379, TCP	Подключение к REDIS на VoEx-сервере
Открытый порт ru.public.express: 5001	5001, TCP	Трастовое подключение к Российскому региональному серверу
DNS-имя	• рекомендуется иметь третий уровень DNS; • во внутренней сети компании DNS-имя должно разрешаться во внутренний IP сервера Single CTS; • требования к DNS-имени STUN/TURN сервера аналогичны требованиям к DNS-имени сервера CTS	
Сертификат для DNS-имени	• SSL версии 3 и не ниже TLS 1.2; • длина ключа равна 2048 или больше; • X.509 версия 3; • незашифрованный ключ для сертификата[1]	

3. Запросите у разработчика следующие индивидуальные параметры для установки (параметры предоставляются по FQDN конкретного сервера):
   - cts_id – идентификатор данного сервера;
   - rts_host – FQDN адрес сервера RTS, к которому будет подключен данный CTS;
   - rts_id – идентификатор сервера RTS;
   - rts_token – токен для авторизации на сервере RTS. Имеет следующий формат <token_for_accept>:<token_for_connect>, где token_for_accept – то-кен для приема подключения от удаленного сервера, token_for_connect – токен для подключения к удаленному серверу.

[1] Могут быть предоставлены компанией разработчиком.

УСТАНОВКА СЕРВЕРА VOEX

Сервер VoEx (STUN/TURN сервер) предназначен для организации видео- и аудиосвязи между пользователями. Видео использует по умолчанию кодек VP8, битрейт 120kbps, 360kbps, 1080kbps на участника (в зависимости от выбранного качества на стороне клиента). Аудио использует по умолчанию кодек OPUS, битрейт 16 kbps на участника.

Установка сервера VoEx проходит в следующем порядке: необходимо выполнить предварительную настройку, затем установить сервер VoEx, установить корпоративный сервер и после — выполнить настройку VoEx (все этапы см. стр. 26).

ПРЕДВАРИТЕЛЬНАЯ НАСТРОЙКА

Для корректной работы сервера выполните предварительную настройку.

Примечание. Задержки при передаче голосовой информации в режиме TURN зависят от удаленности конечного пользователя от TURN-сервера. Для обеспечения качественной связи между сотрудниками компании в разных филиалах рекомендуется устанавливать сервер VoEx для каждого филиала.

Перед установкой сервера VoEx:

1. Определите одинаково доступный для обращений из локальной сети предприятия и интернета глобальный IP-адрес для сервера VoEx.
2. Проверьте правильность выставленных настроек сервера.

Таблица 26

Направление	Источник	Приемник	Порт	Протокол	Предназначение порта
Входящий	Admin IP	STUN/TURN	22	TCP	SSH
Входящий	CTS	STUN/TURN	6379	TCP	REDIS
Входящий	CTS	MCU	8188	TCP	Management conference
Входящий	Любой	STUN/TURN	3478-3479	TCP/UDP	TURN
Входящий	Любой	STUN/TURN	5349-5350	TCP/UDP	TURN TLS
Входящий	Любой	MCU	20000-40000	UDP	SRTP media
Входящий	Любой	STUN/TURN	49152-65535	UDP	SRTP media
Исходящий	STUN/TURN	Любой	Любой	UDP	SRTP media
Исходящий	STUN/TURN	DNS	53	TCP/UDP	DNS
Исходящий	STUN/TURN	NTP	123	UDP	NTP
Исходящий	STUN/TURN	registry.public.express	443	TCP	Docker registry

3. Присвойте доменное имя серверу VoEx.
4. Подготовьте цепочку сертификатов SSL в формате PEM и нешифрованный приватный ключ.

УСТАНОВКА СЕРВЕРА VOEX

Следующий набор команд выполняется в командной строке сервера, на котором устанавливается VoEx.

Для установки сервера VoEx:

1. Запустите командную строку.

2. Подключитесь к репозиторию разработчика в Docker для скачивания контейнеров.

```
docker login -u Login -p Password registry.public.express
```

Примечание. В качестве логина и пароля используются Login и Password, которые выдаются разработчиком.

В случае установки сертифицированной версии подключите твердотельный накопитель с программным обеспечением к платформе, на которой происходит установка, и распакуйте архивный файл cts_X.XX.X.zip.

3. Запустите операцию инсталляции.

```
docker run -d --rm --name dpl-install \
    registry.public.express/dpl:master sleep 10 && \
    docker cp dpl-install:/deployka /usr/local/bin/dpl
```

Из репозитория на сервер скачается файл в формате YAML с контейнерами и инсталлятор.

4. Создайте рабочий каталог проекта:

```
mkdir -p /opt/express-voice
cd /opt/express-voice
dpl --init express-voice
```

5. Установите цепочку сертификатов и ключа SSL для TURN и STUN серверов.

```
mkdir -p certs
cp /somewhere/my-certificate-chain.crt certs/coturn.crt
cp /somewhere/my-unencrypted-key.key certs/coturn.key
```

6. Создайте DH (Diffie Hellman) ключ.

```
openssl dhparam -out certs/dhparam.pem 2048
```

7. Откройте файл конфигурации для редактирования:

```
external_interface: eth0
permit_ip: []
project_type: express-voice
turnserver_listening_ip: 2.3.4.5
turnserver_server_name: localhost
```

8. Внесите изменения в настройки по умолчанию и добавьте следующие параметры:

```
turnserver_external_ip:
  - 1.2.3.4
redis_options:
  command:
    - redis-server
    - --requirepass verystrongpassword
redis_userdb: ip=localhost password=verystrongpassword dbname=1
port=6379
redis_statsdb: ip=localhost password=verystrongpassword dbname=1
port=6379
```

Таблица 27

Название настройки	Значение
external_interface	Наименование интерфейса с внешним IP-адресом[1]
permit_ip	Список разрешенных IP-адресов: • для одного CTS-сервера — его адрес: [1.2.3.4]; • если CTS и VoEx сервер находятся на одном сервере — пустой список: []

[1] IP-адрес должен быть «белым».

Название настройки	Значение
turnserver_listening_ip	Внешний или внутренний IP-адрес интерфейса для TURN и STUN серверов
turnserver_server_name	Полное имя домена данного сервера, совпадающее с адресом, прописанным в сертификате
turnserver_external_ip	Внешний IP-адрес
redis_options	Включение аутентификации в voice redis, пароль verystrongpassword будет использоваться для доступа к базе данных, и он же указывается для сервера CTS в параметре voex_redis_connection_string. Замените пароль verystrongpassword при первой возможности
nat_1_1_mapping keep_private_host	При использовании NAT 1:1 указывается внешний IP-адрес и включается режим сохранения приватного IP-адреса

9. Добавьте следующие параметры и установите параметр «janus_nat_1_1_mapping» равным значению внешнего IP-адреса в сети Интернет, с которого производится переброс портов:

```
janus_enabled: true
janus_keep_private_host: true
janus_ws_ip: 172.17.0.1
janus_ws_acl: 172.18.0.
janus_nat_1_1_mapping: 1.2.3.4
```

10. Выполните команду предварительного генерирования файлов конфигураций:

```
dpl -p
```

Для ограничения доступа к базе данных Redis по IP-адресам укажите IP-адрес сервера Back CTS в конфигурационном файле:

```
express-voice/express-voice.service
```

11. Установите systemd unit в систему и запустите:

```
cp express-voice/express-voice.service /etc/systemd/system/ \
 && systemctl daemon-reload \
 && systemctl enable express-voice.service \
 && systemctl start       express-voice.service
```

УСТАНОВКА КОРПОРАТИВНОГО СЕРВЕРА EXPRESS

Важно! Перед началом процедуры установки необходимо подключиться к серверу VoEx (см. стр. 29),

УСТАНОВКА SINGLE CTS

Следующий набор команд выполняется в командной строке сервера, на котором устанавливается CTS.

Для установки CTS:

1. Подключите твердотельный накопитель с программным обеспечением к платформе, на которой происходит установка.
2. Запустите командную строку.
3. Выполните распаковку архивов с контейнерами для CTS:

```
tar -xvf project_backend_3.6.tar.gz
```

4. Перейдите в каталог с распакованными файлами и выполните загрузку docker images в репозиторий:

```
docker load <  service_name.tar.gz
```

5. Запустите операцию инсталляции.

```
docker run -d --rm --name dpl-install \
    registry.public.express/dpl:master sleep 10 && \
    docker cp dpl-install:/deployka /usr/local/bin/dpl
```

Из репозитория на сервер скачается файл в формате YAML с контейнерами и инсталлятор.

6. Создайте рабочий каталог CTS.

```
mkdir -p /opt/express
cd /opt/express
dpl --init cts
```

После выполнения команды dpl --init cts создается файл settings.

7. Установите цепочки сертификатов и ключа SSL.

- при использовании собственного сертификата создайте директорию для сертификатов.

  Важно! Имя файла сертификата и имя ключа должны соответствовать примеру ниже:

  ```
  mkdir -p nginx/certs
  cp /somewhere/my-certificate-chain.crt nginx/certs/nginx.crt
  cp /somewhere/my-unencrypted-key.key nginx/certs/nginx.key
  ```

  Конструкции /somewhere/my-certificate-chain.crt и /somewhere/my-unencrypted-key.key индивидуальны для каждого конкретного случая.

  Конструкции nginx/certs/nginx.crt и nginx/certs/nginx.key являются обязательными.

  Требования к сертификатам изложены на стр. 23.

- при использовании сертификата от Let's Encrypt в файл settings добавьте параметр le_email: admin@company-mail.ru

Проверка подключения сертификатов после инсталляции описана на стр. 40.

8. Выполните настройку DLP для доступа администраторов безопасности к содержимому сообщений (параметры настройки см. стр.73).

9. Установите cAdvisor (установка выполняется из каталога /opt/express).

```
dpl cadvinstall
...
ps ax|grep cadvisor | grep -v grep
```

Вывод команды:

```
17605 ? Ssl 44:20 /usr/bin/cadvisor -listen_ip 172.17.0.1 -port
9100
```

10. Установите Prometheus node exporter из каталога /opt/express с помощью команды:

```
dpl nxinstall
...
ps ax|grep node_exporter | grep -v grep
```

Вывод команды:

```
17802 ?        Ssl  322:51 /usr/bin/node_exporter --web.listen-
address=172.17.0.1:9200
```

По завершении установки CTS и вспомогательного ПО создается файл конфигурации, в котором необходимо задать параметры для подключения к RTS, получения push-уведомлений, SMS-сообщений и других функций.

Созданный по умолчанию файл конфигурации имеет следующий вид и требует редактирования:

Примечание: Значения параметров cts_id, rts_host, rts_id и rts_token должны находиться внутри кавычек ('value'). На другие параметры данное требование не распространяется. Для предотвращения ошибок рекомендуется заменить параметры сгенерированного файла параметрами, выданными разработчиками.

```
project_type: cts
api_internal_token: verystrongpassword
ccs_host: 'cts_name.somedomain.sometld'
cts_id: 'aaaa-bbbb-cccc-dddd'
phoenix_secret_key_base: verystrongpassword
postgres_password: verystrongpassword
project_type: cts
prometheus_users: verystrongpassword
    prometheus: verystrongpassword
rts_host: 'rts_name.somedomain.sometld'
rts_id: 'aaaa-bbbb-cccc-dddd'
rts_token: verystrongpassword
```

Для изменения файла конфигурации воспользуйтесь любым текстовым редактором и внесите исправления в файл:

Таблица 28

Название настройки	Значение
project_type	Тип сервера
ccs_host	Полное имя домена данного сервера, прописанное в DNS и соответствующее имени, на которое приобретался сертификат
cts_id	Идентификатор установленного сервера, предоставляется разработчиком
prometheus_users	Список пользователей с паролями, генерируемыми утилитой htpasswd, для доступа к интегрированному в систему стеку Prometheus
rts_host	Полное имя домена сервера RTS, к которому будет подключен установленный CTS (предоставляется разработчиком)
rts_id	Идентификатор сервера RTS (предоставляется разработчиком)
rts_token	Токен для авторизации на сервере RTS (предоставляется разработчиком)
le_email	Параметр устанавливается при использовании сертификата от компании Let`s Encrypt. Значение параметра должно соответствовать e-mail, на который будут приходить оповещения от Let`s Encrypt
janus_enabled	Установите значение «true»
janus_url	ws://172.17.0.1:8188
voex_redis_connection_string	redis://:verystrongpassword@172.17.0.1:6379/1. Можно сгенерировать через «openssl rand -hex 16»
admin_url	Параметр указывается для переопределения стандартного пути (/admin) к веб интерфейсу администратора: например /not-admin

Для подключения сервера VoEx к CTS добавьте в конфигурацию:

```
voex_enabled: true
voex_redis_connection_string: redis://:
verystrongpassword@voex_fqdn_address:6379/1
```

Параметр voex_redis_connection_string измените в соответствии с настройками подключения к серверу VoEx и базе Redis, функционирующей на нем. Значение verystrongpassword — это пароль к базе данных redis, который должен совпадать со значением на стр.33:

```
- --requirepass verystrongpassword
redis_userdb: ip=localhost password=verystrongpassword
```

При первой возможности замените значение verystrongpassword на более сложное.

УСТАНОВКА BACK CTS И FRONT CTS СЕРВЕРОВ

Установка комбинации Front CTS и Back CTS серверов осуществляется в определенном порядке.

Для установки Front CTS:

1. Подключите твердотельный накопитель с программным обеспечением к платформе, на которой происходит установка.
2. Запустите командную строку.
3. Выполните распаковку архивов с контейнерами для Front CTS:

```
tar -xvf project_backend_3.6.tar.gz
```

4. Перейдите в каталог с распакованными файлами и выполните загрузку docker images в репозиторий:

```
docker load <  service_name.tar.gz
```

5. Запустите операцию инсталляции.

```
docker run -d --rm --name dpl-install \
    registry.public.express/dpl:master sleep 10 && \
    docker cp dpl-install:/deployka /usr/local/bin/dpl.
```

6. Создайте рабочий каталог Front CTS:

```
mkdir -p /opt/express
cd /opt/express
echo DPL_IMAGE_TAG=cts-release > dpl.env
dpl --init
```

7. Установите цепочки сертификатов и ключа SSL.
   - при использовании собственного сертификата создайте директорию для сертификатов.

     Важно! Имя файла сертификата и имя ключа должны соответствовать примеру ниже:

     ```
     mkdir -p certs
     cp /somewhere/my-certificate-chain.crt certs/express.crt
     cp /somewhere/my-unencrypted-key.key certs/express.key
     ```

     Конструкции /somewhere/my-certificate-chain.crt и /somewhere/my-unencrypted-key.key индивидуальны для каждого конкретного случая.

     Конструкции certs/express.crt и certs/express.key являются обязательными.

     Требования к сертификатам изложены на стр. 23.
   - при использовании сертификата от Let's Encrypt в файл settings.yaml добавьте параметр le_email: admin@company-mail.ru

   Проверка подключения сертификатов после инсталляции описана на стр. 40.
8. Откройте для редактирования конфигурационный файл settings.yaml (Файл использует язык разметки YAML):

```
api_internal_token: verystrongpassword
ccs_host: cts_name.somedomain.sometld
cts_id: 'aaaa-bbbb-cccc-dddd'
janus_url: ws://172.17.0.1:8188
phoenix_secret_key_base: verystrongpassword
postgres_password: verystrongpassword
prometheus_users:
  prometheus: verystrongpassword
```

```
rts_host: 'rts_name.somedomain.sometld'
rts_id: 'aaaa-bbbb-cccc-dddd'
rts_token: 'verystrongpassword'
voex_redis_connection_string: redis://172.17.0.1:6379/1
```

Для корректного функционирования сервера рекомендуется исправлять параметры cts_id, rts_host, rts_id и rts_token; в примере выше они выделены красным цветом.

Примечание:

- Значения параметров cts_id, rts_host, rts_id и rts_token должны находиться внутри кавычек ('value'). На другие параметры данное требование не распространяется. В случае ручного ввода значений символ кавычки не вводится.
- 25.10.2021 вырезана ELK из установки CTS сервера. При необходимости, используйте внешнюю инсталляцию, указав elk_host в settings.

9. Отредактируйте конфигурационный файл settings.yaml следующим образом: удалите строки содержащие prometheus_users, cts_backend и добавьте следующие параметры:

```
cts_frontend: true
kafka_host: backend_name.somedomain.sometld
postgres_host: backend_name.somedomain.sometld
frontend_host: frontend_name.somedomain.sometld
backend_host: backend_name.somedomain.sometld
```

Для установки Back CTS:

1. Подключите твердотельный накопитель с программным обеспечением к платформе, на которой происходит установка.
2. Запустите командную строку.
3. Выполните распаковку архивов с контейнерами для Back CTS:

```
tar -xvf project_backend_3.6.tar.gz
```

4. Перейдите в каталог с распакованными файлами и выполните загрузку docker images в репозиторий:

```
docker load <  service_name.tar.gz
```

5. Запустите операцию инсталляции.

```
docker run -d --rm --name dpl-install \
    registry.public.express/dpl:master sleep 10 && \
    docker cp dpl-install:/deployka /usr/local/bin/dpl
```

Из репозитория на сервер скачается файл в формате YAML с контейнерами и инсталлятор.

6. Создайте рабочий каталог Back CTS.

```
mkdir -p /opt/express
cd /opt/express
```

7. Установите цепочки сертификатов и ключа SSL.

- при использовании собственного сертификата создайте директорию для сертификатов.

  Важно! Имя файла сертификата и имя ключа должны соответствовать примеру ниже:

```
mkdir -p certs
cp /somewhere/my-certificate-chain.crt certs/express.crt
cp /somewhere/my-unencrypted-key.key certs/express.key
```

  Конструкции /somewhere/my-certificate-chain.crt и /somewhere/my-unencrypted-key.key индивидуальны для каждого конкретного случая.

Конструкции certs/express.crt и certs/express.key являются обязательными.

Требования к сертификатам изложены на стр. 23.

- при использовании сертификата от Let's Encrypt в файл settings.yaml добавьте параметр le_email: admin@company-mail.ru

Проверка подключения сертификатов после инсталляции описана на стр. 40.

8. Скопируйте файл конфигурации с Front CTS (/opt/express/settings.yaml) на сервер Back CTS и разместите его в папке /opt/express.
9. Откройте для редактирования конфигурационный файл settings.yaml (Файл использует язык разметки YAML):

```
api_internal_token: verystrongpassword
ccs_host: cts_name.somedomain.sometld
cts_id: 'aaaa-bbbb-cccc-dddd'
janus_url: ws://172.17.0.1:8188
phoenix_secret_key_base: verystrongpassword
postgres_password: verystrongpassword
prometheus_users:
  prometheus: verystrongpassword
rts_host: 'rts_name.somedomain.sometld'
rts_id: 'aaaa-bbbb-cccc-dddd'
rts_token: 'verystrongpassword'
voex_redis_connection_string: redis://172.17.0.1:6379/1
```

Для корректного функционирования сервера рекомендуется исправлять параметры cts_id, rts_host, rts_id и rts_token; на примере выше они выделены красным цветом.

Примечание:

- Значения параметров cts_id, rts_host, rts_id и rts_token должны находиться внутри кавычек ('value'). На другие параметры данное требование не распространяется. В случае ручного ввода значений символ кавычки не вводится.
- 25.10.2021 вырезана ELK из установки CTS сервера. При необходимости, используйте внешнюю инсталляцию, указав elk_host в settings.

10. При редактировании файла конфигурации удалите дополнительные настройки:

```
cts_frontend: true
kafka_host: backend_name.somedomain.sometld
postgres_host: backend_name.somedomain.sometld
```

11. При редактировании файла конфигурации внесите дополнительные настройки:

```
cts_backend: true
set_real_ip_from:
  - 10.4.151.168 #IP frontend
```

12. Установите cAdvisor (установка выполняется из каталога /opt/express).

```
dpl cadvinstall
ps ax|grep cadvisor | grep -v grep
```

Вывод команды:

```
17605 ? Ssl 44:20 /usr/bin/cadvisor -listen_ip 172.17.0.1 -port
9100
```

13. Установите Prometheus node exporter из каталога /opt/express с помощью команды:

```
dpl nxinstall
ps ax|grep node_exporter | grep -v grep
```

Внимание! Если по требованиям информационной безопасности выход в Интернет с Back CTS должен быть ограничен, предусмотрено использование TinyProxy. При необходимости использовать proxy, рекомендуем ознакомиться с настройкой proxy для службы Docker по ссылке:

- https://docs.docker.com/config/daemon/systemd/

Для установки TinyProxy:

1. В каталоге, в котором установлена ОС, запустите команду:

```
Ubuntu\Debian - sudo apt-get install -y tinyproxy
RHEL\CentOS – sudo yum install -y epel-release
RHEL\CentOS - sudo yum install -y tinyproxy
```

2. Создайте файл /etc/tinyproxy/filter, в котором перечисляются хосты для доступа через прокси:

```
registry.public.express
registry-auth.public.express
```

   Автоматически будет создан файл конфигурации для tinyproxy: /etc/tinyproxy/tinyproxy.conf.

3. В файл /etc/tinyproxy/tinyproxy.conf внесите настройки:

```
User tinyproxy
Group tinyproxy
Port 8888
Timeout 600
DefaultErrorFile "/usr/share/tinyproxy/default.html"
StatFile "/usr/share/tinyproxy/stats.html"
LogFile "/var/log/tinyproxy/tinyproxy.log"
LogLevel Info
PidFile "/var/run/tinyproxy/tinyproxy.pid"
MaxClients 10
MinSpareServers 1
MaxSpareServers 5
StartServers 1
MaxRequestsPerChild 0
#BackIP
Allow 192.168.80.22
ViaProxyName "tinyproxy"
Filter "/etc/tinyproxy/filter"
FilterDefaultDeny Yes
ConnectPort 443
ConnectPort 563
```

4. Перезапустите сервис tinyproxy с помощью команды:

```
sudo systemctl restart tinyproxy
```

НАСТРОЙКА СЕРВЕРА VOEX

Настройка сервера VoEx включает в себя:

- настройку серверов STUN и TURN (см. стр. 37);
- настройку IP-телефонии (опционально, см. стр. 38).

НАСТРОЙКА СЕРВЕРА VOEX

Для настройки сервера VoEx (STUN и TURN):

1. Запустите сервер VoEx в командной строке командой:

```
dpl -d
```

2. Откройте консоль администратора.

Перейдите в раздел «VoEx» (Рисунок 6) и укажите адрес сервера (FQDN) и порт turn/stun сервера:

- в поле «TURN Server (через запятую)» введите внешний FQDN вашего сервера и через двоеточие номер порта, например «express.firma.ru:3478»;
- поле «STUN Server (через запятую)» заполняется аналогично.

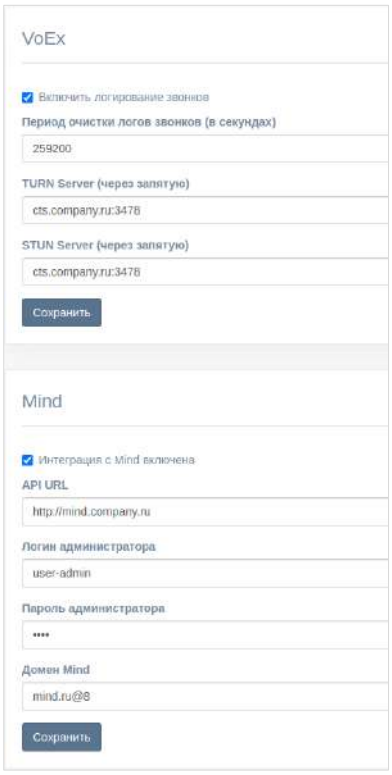


Рисунок 6

3. Введите внешние IP-адреса в соответствующие поля и нажмите кнопку «Сохранить».

НАСТРОЙКА IP-ТЕЛЕФОНИИ

Для настройки IP-телефонии:

1. В секции «SIP» установите флаг «SIP включен» (Рисунок 7).

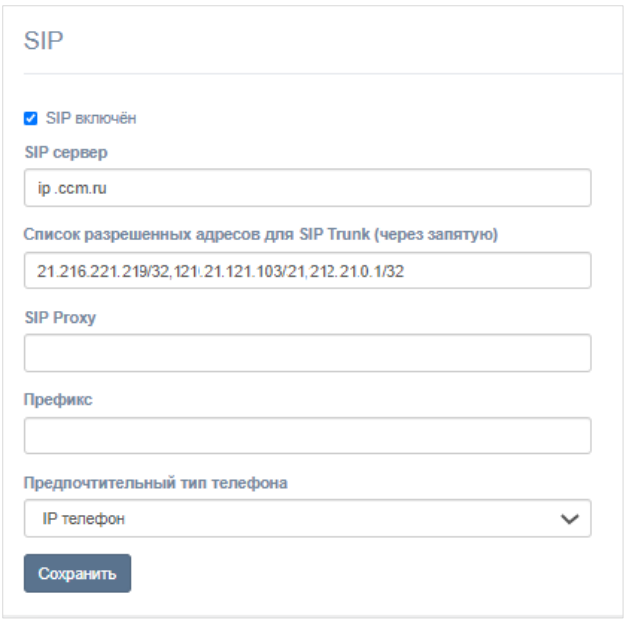


Рисунок 7

2. Заполните поля:

Таблица 29

Поле	Назначение
SIP сервер	Адрес SIP сервера
Список разрешенных адресов SIP Trunk	
SIP Proxy	Адрес прокси-сервера SIP
Префикс	Префикс номера телефона
Предпочтительный тип телефона	Тип телефона, с которого будут осуществляться звонки. Выбирается из списка

3. Нажмите кнопку «Сохранить».

ЗАПУСК СЕРВЕРА VOEX

Для запуска сервера VoEx выполните команды, аналогичные командам запуска сервера CTS на стр. 40. Команды установки сервера VoEx выполняются из директории /opt/express-voice/.

УСТАНОВКА RTS И ETS

Установка сервера RTS для сертифицированной версии продукта выполняется по аналогии с установкой сервера Single CTS:

- при редактировании файла конфигурации задайте следующие параметры:

```
cassandra_host: 10.0.0.1
cassandra_keyspace_authentication: authentication
cassandra_keyspace_kdc: kdc
cassandra_keyspace_phonebook: phonebook
cassandra_keyspace_trusts: trusts
ccs_host: 'cts_name.somedomain.sometld'
phoenix_secret_key_base: ''
project_type: rts
prometheus_users:
```

```
    prometheus: $apr1$dafdabfg$18dafaOuAUoIp6KR9V.I3R1
    grafana: $apr1$skedsaFd$WIMfdafa0bhEBrAn4SzPZxDisA0
region: ru
rts_id: 'aaaa-bbbb-cccc-dddd'
rts_token:
```

Установка сервера ETS для сертифицированной версии продукта выполняется по аналогии с установкой сервера Single CTS:

- при редактировании файла конфигурации задайте следующие параметры:

```
project_type: ets
api_internal_token:
ccs_host: 'cts_name.somedomain.sometld'
ets_id:
phoenix_secret_key_base:
postgres_password:
prometheus_users:
  prometheus:
rts_host: 'rts_name.somedomain.sometld'
rts_id: 'aaaa-bbbb-cccc-dddd'
rts_token:
```

ПРОВЕРКА СЕРТИФИКАТОВ

Для тестирования корректности сертификата после инсталляции изделия выполните команду:

```
openssl s_client -connect fqnd-cts:443
```

Сообщение следующего вида сигнализирует об ошибке:

```
depth=0 CN = *.domain.ru
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 CN = *.domain.ru
verify error:num=21:unable to verify the first certificate
verify return:1
```

ЗАПУСК СЕРВЕРА

Для запуска сервера:

Примечание. Команды для запуска сервера выполняются из каталога установки /opt/express.

1. Выполните команду:

   Примечание. В случае использования разделенной установки. Данная команда выполняется с начала на сервере Back CTS затем на сервере Front CTS.

   ```
   dpl -d
   ```

2. Проверьте, запустились ли все контейнеры, с помощью команды:

   ```
   docker ps -a
   ```

   Если контейнеры не запустились, для просмотра журнала событий выполните команду:

   ```
   dpl --dc logs --tail=200  <не_запускаемый_контейнер>
   ```

   Если процедура установки сервера выполнена правильно, в течение пяти минут будет установлена и доступна консоль администратора (веб-интерфейс) https://ccs_host/admin.

Примечание. Для корректной работы консоли администратора **не рекомендуется** использовать Internet Explorer.

3. Создайте учетную запись администратора.

```
dpl --dc exec admin bin/admin add_admin -u admin -p
'veryinsecurepassword123'
```

Если консоль администратора не установилась, то произошла ошибка несовпадения по политике паролей.

4. В появившихся логах найдите наиболее частое упоминание с ошибками и перезапустите контейнер, выдающий ошибку, командой:

```
dpl --dc restart {имя_контейнера}
```

Например:

```
dpl --dc restart nginx
```

Примечание. Все имена контейнеров, соответствующих конкретной архитектуре, перечислены в разделе «Архитектура».

Если операция не поможет, свяжитесь с технической поддержкой компании разработчика.

Глава 3

НАСТРОЙКА СЕРВЕРА

Для нормального функционирования системы необходимо выполнить предварительную настройку сервера в веб-консоли администратора. Процедура настройки зависит от типа сервера и описывается в соответствующих пунктах ниже:

- RTS — см. стр. 43;
- ETS — стр. 55;
- CTS — стр. 68.

Для авторизации в консоли администратора:

1. В адресной строке браузера укажите адрес консоли администратора.

   Примечание. Для RTS вход выполняется в веб-интерфейсе консоли администратора https://rts_host/admin, для ETS — https://ets_host/admin, для CTS — https://cts_host/admin.

   Важно! Без https консоль администратора недоступна.

   Откроется окно авторизации (Рисунок 8).

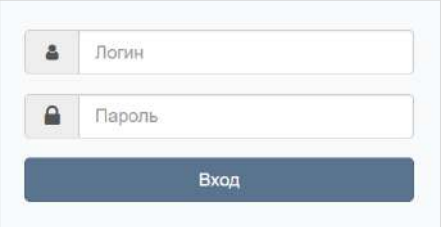


Рисунок 8

2. Введите имя учетной записи и пароль в соответствующие поля.
3. Нажмите кнопку «Вход».

   Откроется главное окно консоли администратора.

Для выхода из административной консоли нажмите кнопку в верхней левой части окна.

НАСТРОЙКА RTS

Настройка RTS включает в себя следующие процедуры:

- подключение TLS-сертификата (если это не было выполнено в процессе установки RTS) см. стр. 43;
- настройка видео- и голосовой связи см. стр. 44;
- подключение SMTP-сервера см. стр. 44;
- настройка push-уведомлений см. стр. 45;
- настройка подключений ETS и CTS см. стр.50.

ПОДКЛЮЧЕНИЕ TLS-СЕРТИФИКАТА

Для настройки TLS-сертификата:

1. В консоли администратора выберите пункт меню «Сервер»

Откроется окно с информацией о данном RTS сервере (Рисунок 9).

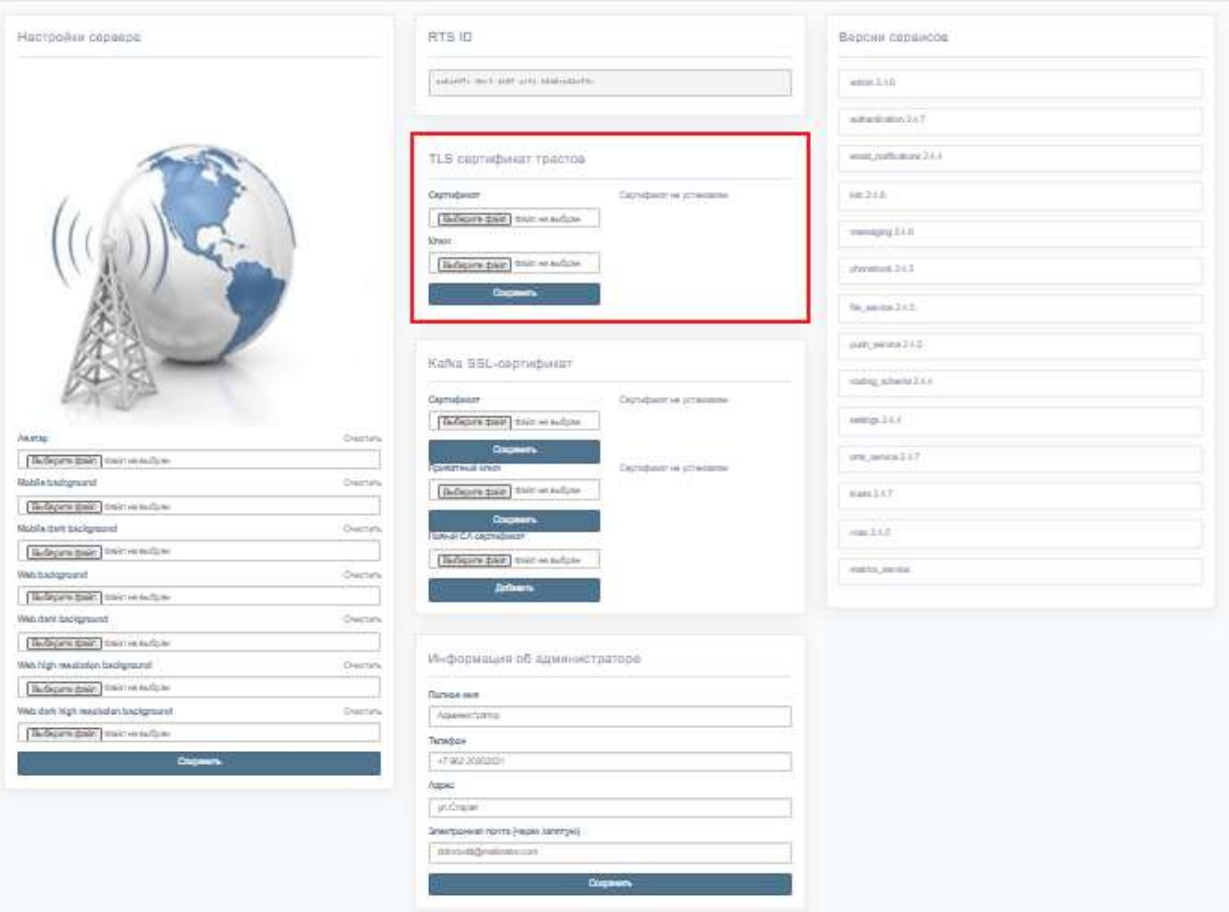


Рисунок 9

Для применения TLS-протокола в трастовых соединениях:

1. Внесите данные о сертификате и ключе в соответствующие поля области «TLS-сертификат трастов».
2. Нажмите кнопку «Сохранить».

Примечание. Допускается применение TLS-сертификата, использованного на этапе установки CTS.

НАСТРОЙКА ВИДЕО- И ГОЛОСОВОЙ СВЯЗИ

Настройка видео- и голосовой связи выполняется после установки сервера Voex и описана на стр. 37.

ПОДКЛЮЧЕНИЕ SMTP-СЕРВЕРА

Для подключения SMTP-сервера:

1. В меню выберите пункт «E-mail» (Рисунок 10).
2. В области «Настройки e-mail» заполните поля:
   - в поле «От» укажите обратный адрес;
   - в поле «Сервер» укажите SMTP-сервер;
   - в поле «Порт» укажите номер порта для ретрансляции исходящей почты: 25, 587 или 465. Номер порта зависит от типа защищенного соединения;

- В полях «Имя пользователя» и «Пароль» укажите данные для авторизации на SMTP-сервере.

3. Выберите тип защищенного соединения в выпадающем списке: SSL, Start/TLS или None.
4. Нажмите кнопку «Сохранить».

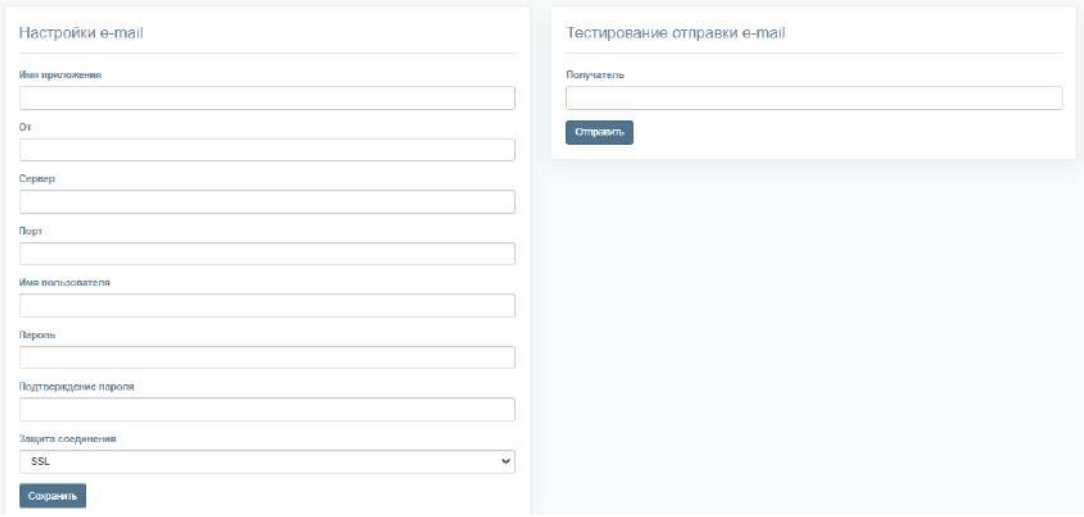


Рисунок 10

Для проверки настроек подключения воспользуйтесь областью «Тестирование отправки e-mail». Впишите в пустое поле адрес получателя и нажмите кнопку «Отправить».

НАСТРОЙКА PUSH-УВЕДОМЛЕНИЙ

Для подключения и настройки push-уведомлений перейдите в раздел «Push Service».

Интерфейс предназначен для подключения push-уведомлений (Рисунок 11).

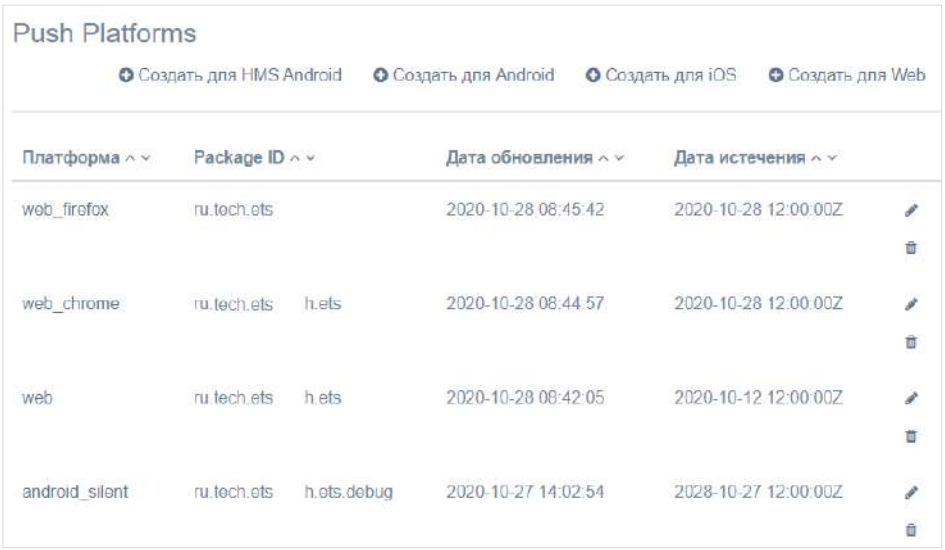


Рисунок 11

Таблица содержит следующую информацию:

Таблица 30

Название столбца	Информация
Платформа	Платформа, на которой подключены push-уведомления
Package ID	Название сборки приложения Express
Дата обновления	Дата последнего изменения настройки push-уведомлений
Дата истечения	Дата истечения поступления push-уведомлений

Для редактирования подключения нажмите кнопку и внесите изменения в открывшемся окне.

Для удаления подключения нажмите кнопку .

Механизм подключения push-уведомлений различен для платформ Android, iOS и веб-приложения. Для Android и веб-приложения push-уведомления подключаются через FCM, для iOS — через APNS.

Для создания подключения на Android/HMS Android

1. Откройте консоль Firebase.
2. В проекте (меню «Project Overview»), где сконфигурированы ключи для Android, выберите пункт «Project settings» (Рисунок 12).

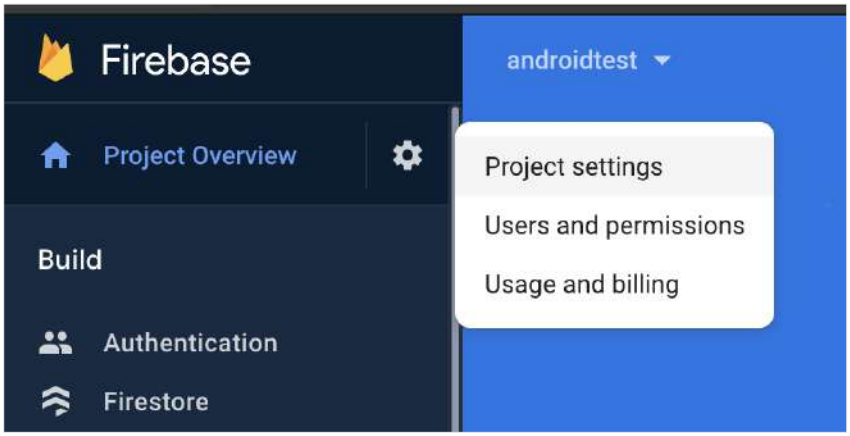


Рисунок 12

3. В консоли администратора Express в разделе «Push Service» нажмите кнопку «Создать для Android» в верхнем правом углу.

   Откроется окно создания подключения для платформы Android (Рисунок 13).

Рисунок 13

4. Заполните поля формы:

Таблица 31

Параметр	Описание	Значение
Платформа	Платформа, на которой подключены push-уведомления	android_silent
Package ID	Название сборки приложения Express	
Дата истечения	Дата истечения поступления push-уведомлений	
FCM URL	Адрес сервера Firebase Cloud Messaging	https://fcm.googleapis.com/fcm/send
FCM API Key	Ключ API, выдаваемый в консоли администратора Firebase	См. Рисунок 14

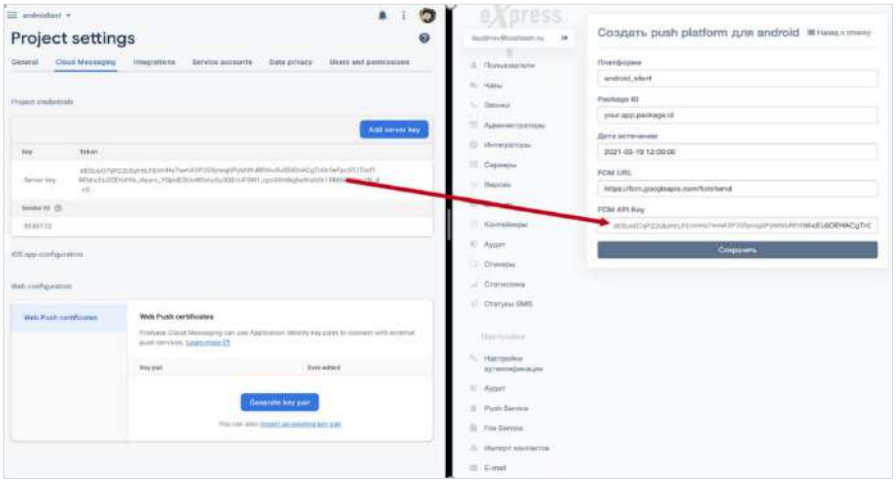


Рисунок 14

5. Нажмите кнопку «Сохранить».

Для создания подключения на iOS:

1. Нажмите кнопку «Создать для iOS» в верхнем правом углу.

   Откроется окно создания подключения для платформы iOS (Рисунок 15).

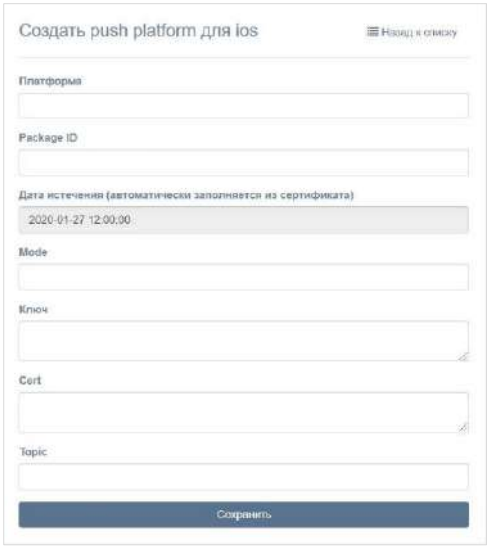


Рисунок 15

2. Заполните поля формы:

Таблица 32

Параметр	Описание	Значение
Платформа	Платформа, на которой подключены push-уведомления	• ios_apns (для alert push с сертификатом apns); • ios_voex (для push-уведомлений звонков с сертификатом voip)
Package ID	Название сборки приложения Express	
Дата истечения	Дата истечения поступления push-уведомлений	
Mode	Режим работы push-уведомлений. Возможные значения prod/dev	• dev (для сборки beta); • prod (для релиза/пререлиза)
Ключ	Приватный ключ	
Cert	Сертификат	
Topic	Название сборки приложения Express	Package ID (для ios_apns); пустое значение (для ios_voex)

3. Нажмите кнопку «Сохранить».

Для создания подключения в веб-приложении:

1. Откройте консоль Firebase.
2. В консоли Firebase создайте проект для веб-приложения (Рисунок 16).

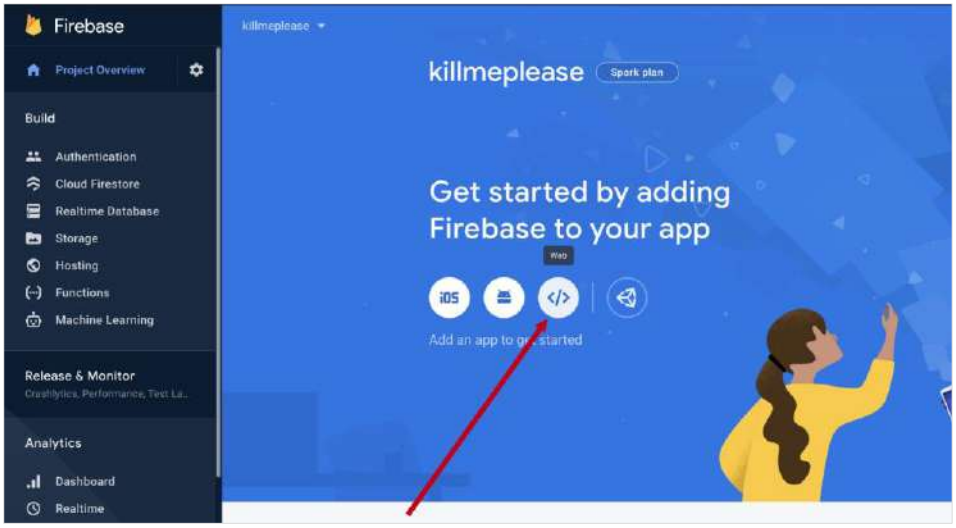


Рисунок 16

3. В открывшемся окне нажмите кнопку «Generate key pairs» (Рисунок 17).

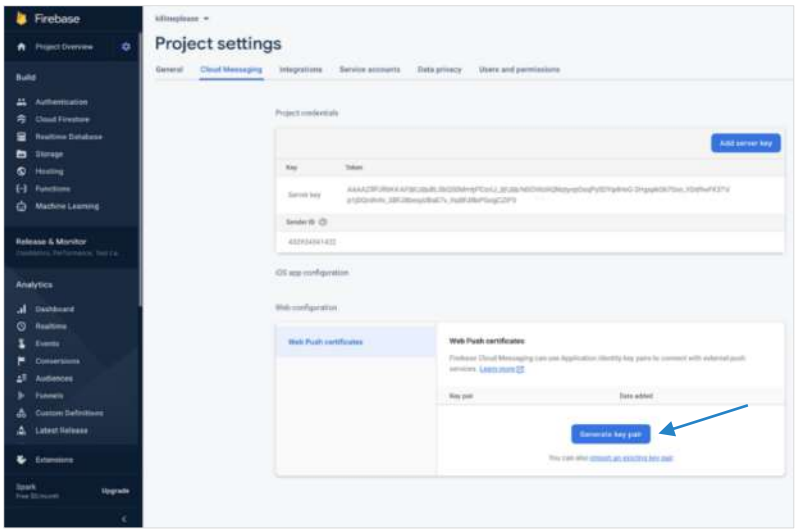


Рисунок 17

4. В консоли администратора в разделе «Push Service» нажмите кнопку «Создать для Web» в верхнем правом углу.

   Откроется окно создания подключения для веб-приложения (Рисунок 18).

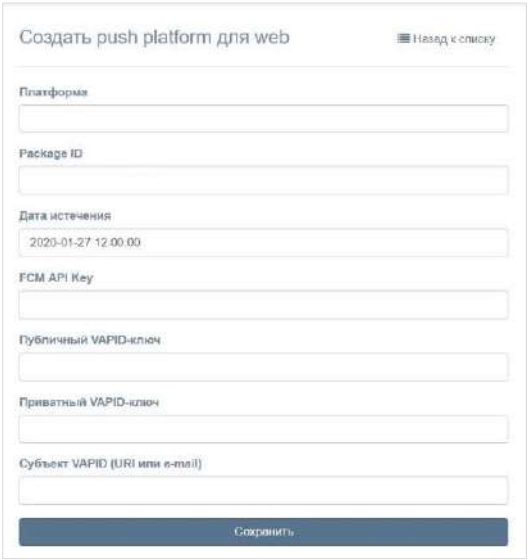


Рисунок 18

5. Заполните поля формы.

Примечание. В поле «Платформа» укажите значение «web».

Таблица 33

Параметр	Описание	Значение
Платформа	Платформа, на которой подключены push-уведомления	• web; • web_chrome; • web_firefox
Package ID	Название сборки приложения Express	
Дата истечения	Дата истечения поступления push-уведомлений	
FCM API Key	Ключ API, выдаваемый в консоли администратора Firebase	См. Рисунок 19
Публичный VAPID-ключ	Публичный ключ API, сгенерированный в консоли администратора Firebase	См. Рисунок 19

Параметр	Описание	Значение
Приватный VAPID-ключ	Приватный ключ API, сгенерированный в консоли администратора Firebase	См. Рисунок 19
Субъект VAPID (URI или e-mail)	Адрес электронной почты пользователя в firebase	mailto:<email аккаунта firebase>

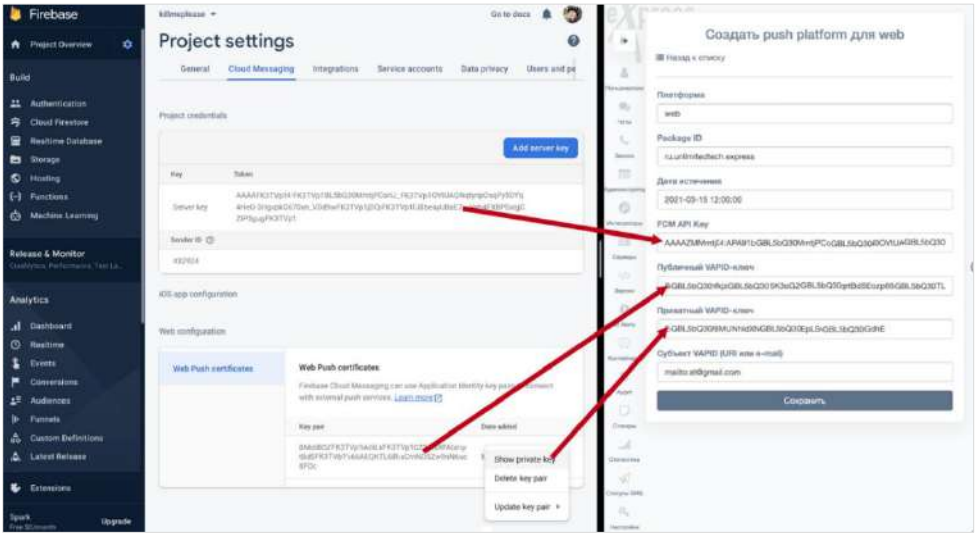


Рисунок 19

6. Нажмите кнопку «Сохранить».
7. Повторите действия 1 – 6 для Chrome, указав в поле «Платформа» значение «web_chrome».

   В разделе «Push Service» появятся две записи (для двух браузеров).
8. В конфигурационном файле docker-образа веб-приложения (WEB_CLIENT_CONFIG) измените параметр gcmSenderId на значение из Firebase (Рисунок 20).

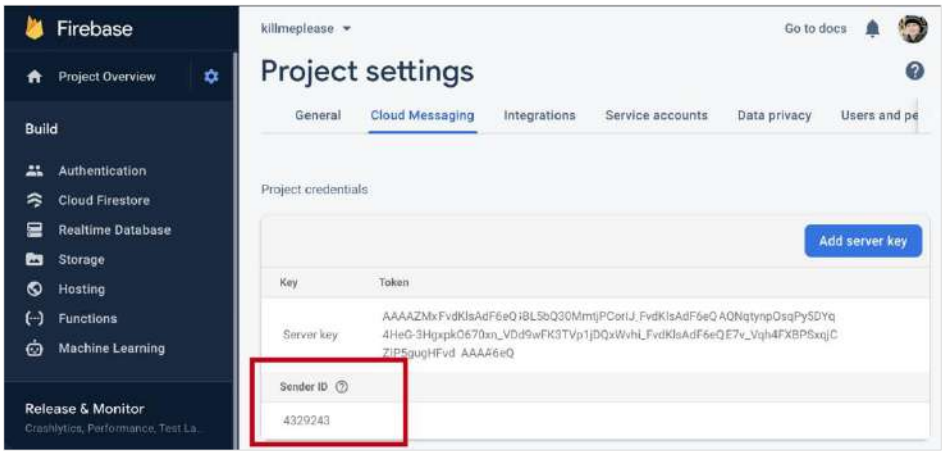


Рисунок 20

НАСТРОЙКА ПОДКЛЮЧЕНИЙ КОРПОРАТИВНЫХ СЕРВЕРОВ И СЕРВЕРОВ ПРЕДПРИЯТИЯ

Для настройки подключений ETS и CTS:

1. Перейдите в раздел «Серверы».

В разделе «Серверы» представлена информация о подключенных ETS и CTS.

В разделе «Серверы» представлена информация о серверах, подключенных к данному RTS (Рисунок 21, Рисунок 22, Рисунок 23).

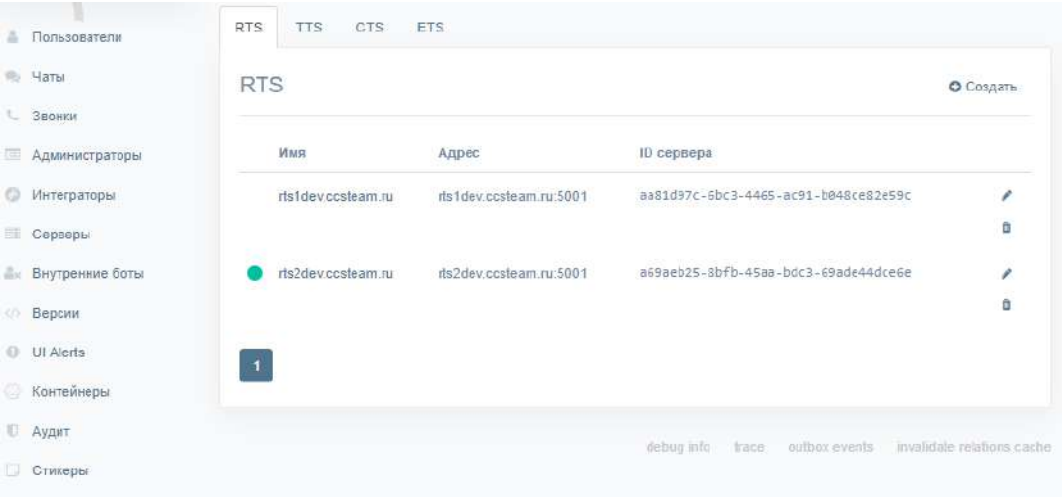


Рисунок 21

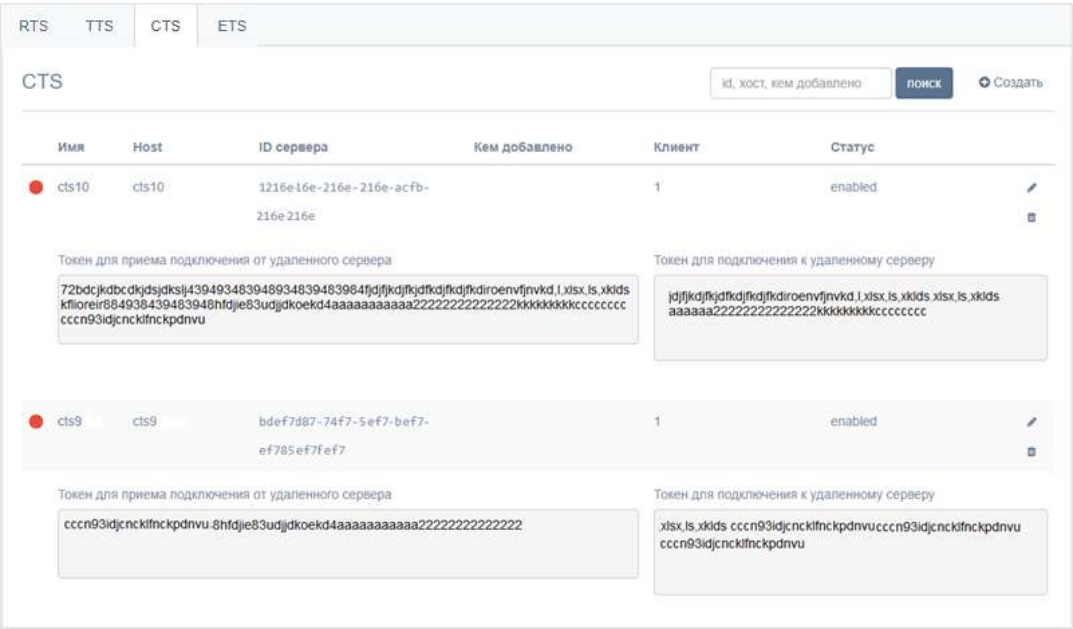


Рисунок 22

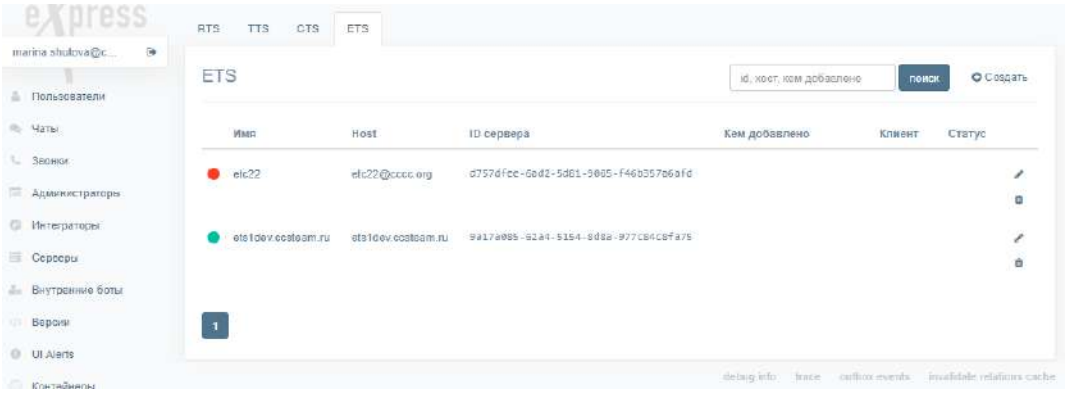


Рисунок 23

2. Проверьте статус подключения ETS и CTS с помощью цветовых маркеров рядом с именами серверов.
   - зеленый — сервер подключен и есть связь;
   - фиолетовый — сервер заблокирован;
   - красный — сервер подключен и нет связи;
   - пустое место — сервер подключен к другому RTS.
3. Подключите ETS и CTS (если они не подключены).

Для подключения CTS/ETS:

1. Нажмите кнопку «Создать» в правом верхнем углу в секции «CTS»/«ETS». Откроется окно (Рисунок 24 и Рисунок 25).

Рисунок 24

Рисунок 25

2. Заполните поля:

- в поле «ID» укажите идентификатор сервера, с которым будет установлено подключение (идентификатор CTS/ETS хранится в разделе «Сервер» административной консоли этого CTS/ETS);
- в поле «Имя» внесите краткое обозначение для создаваемого канала связи;
- в поле «Host» укажите реальный адрес подключения к серверу (URL), который будет отображаться в клиентском приложении;
- в полях «Токен для подключения от удаленного сервера» и «Токен для подключения к удаленному серверу» укажите токены;
- в поле «RTS ID» укажите идентификатор сервера RTS, к которому подключается данный CTS/ETS;
- в поле «Статус» выберите значение «включено» или «выключено»;
- в полях «Клиент», «Кто установил», «Контакт на стороне eXpress», «Контакт на стороне клиента», «Партнер», «Ссылка на документацию», «Ссылка на конфиг», «Описание проблем и их решений» введите соответствующие данные;
- в выпадающем списке «Ответственный за обновления» выберите «eXpress»/«Клиент»/«Партнер»;
- при необходимости подключите опцию «Позволять отправлять письма с этого CTS» (если подключаете CTS).

3. Нажмите на кнопку «Сохранить».

Для просмотра информации о подключенных TTS:

1. В разделе «Серверы» откройте вкладку «TTS».

   На экране отобразится информация о подключениях к транспортным серверам (Рисунок 26).

Рисунок 26

2. Нажмите на имя TTS.

   Откроется окно (Рисунок 27).

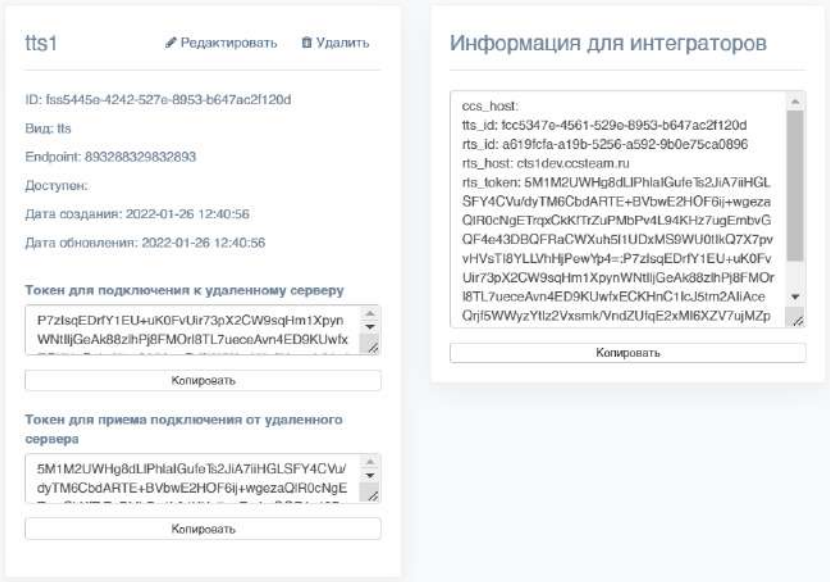


Рисунок 27

В открывшемся окне содержится следующая информация:

Параметр	Описание
ID	Идентификатор сервера TTS, с которым установлено соединение
Вид	Вид соединения
Endpoint	Адрес подключения к серверу TTS
Доступен	Дата и время последнего подключения
Дата создания	Дата создания подключения
Дата обновления	Дата последнего изменения подключения
Токен для подключения к удаленному серверу	Токен для подключения
Токен для приема подключения от удаленного сервера	Токен для приема подключения
Информация для интеграторов	Данные для настройки трастов между серверами

Для редактирования подключения к TTS нажмите кнопку и внесите изменения в открывшемся окне.

Для удаления подключения к TTS нажмите кнопку .

Для создания подключения к транспортному серверу нажмите кнопку «Создать» и заполните поля формы (Рисунок 28).

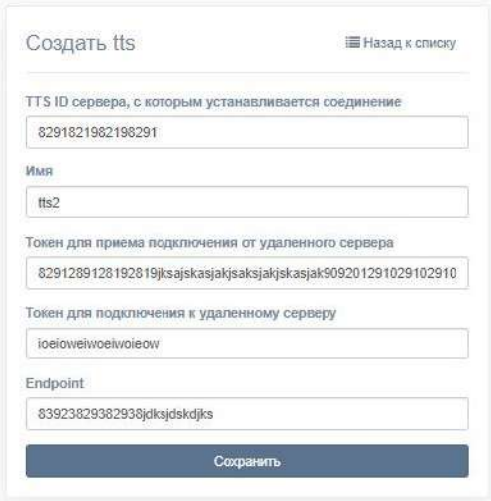


Рисунок 28

НАСТРОЙКА ETS

Настройка ETS включает в себя следующие процедуры:

- подключение TLS-сертификата (если это не было выполнено в процессе установки ETS) см. стр. 55;
- настройка видео- и голосовой связи см. стр. 44;
- подключение SMTP-сервера см. стр. 44;
- настройка push-уведомлений см. стр. 45;
- настройка подключений CTS см. стр. 62;
- установка веб-клиента (см. стр. 66).

ПОДКЛЮЧЕНИЕ TLS-СЕРТИФИКАТА

Для настройки TLS-сертификата:

- В консоли администратора выберите пункт меню «Сервер»

  Откроется окно с информацией о данном RTS-сервере (Рисунок 29).

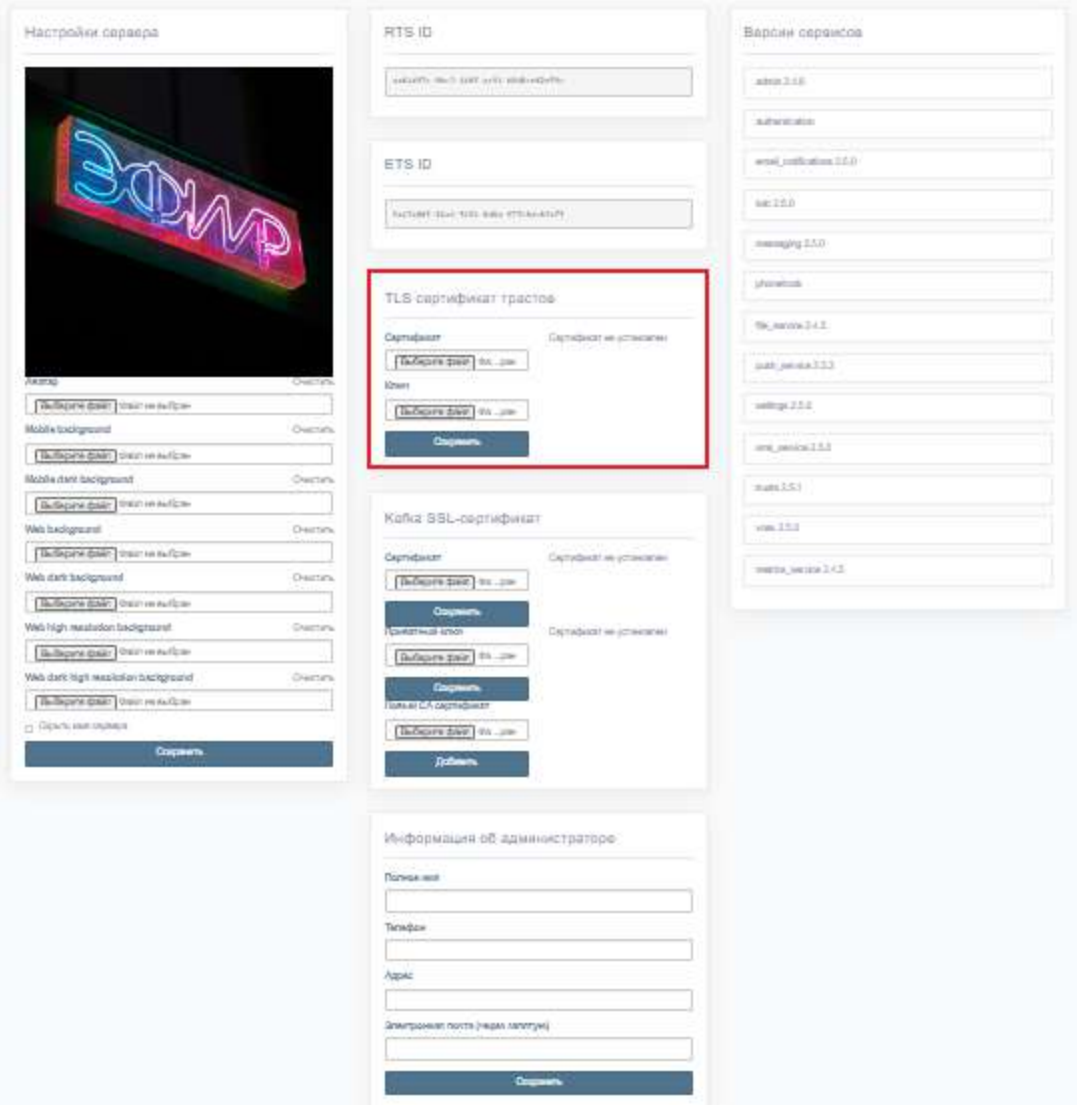


Рисунок 29

Для применения TLS-протокола в трастовых соединениях:

1. Внесите данные о сертификате и ключе в соответствующие поля области «TLS-сертификат трастов».
2. Нажмите кнопку «Сохранить».

Примечание. Допускается применение TLS-сертификата, использованного на этапе установки CTS.

НАСТРОЙКА ВИДЕО- И ГОЛОСОВОЙ СВЯЗИ

Настройка видео- и голосовой связи выполняется после установки сервера Voex и описана на стр. 37.

ПОДКЛЮЧЕНИЕ SMTP-СЕРВЕРА

Для подключения SMTP-сервера:

1. В меню выберите пункт «E-mail» (Рисунок 10).
2. В области «Настройки e-mail» заполните поля:
   - в поле «От» укажите обратный адрес;

- в поле «Сервер» укажите SMTP-сервер;
- в поле «Порт» укажите номер порта для ретрансляции исходящей почты: 25, 587 или 465. Номер порта зависит от типа защищенного соединения;
- В полях «Имя пользователя» и «Пароль» укажите данные для авторизации на SMTP-сервере.

3. Выберите тип защищенного соединения в выпадающем списке: SSL, Start/TLS или None.
4. Нажмите кнопку «Сохранить».

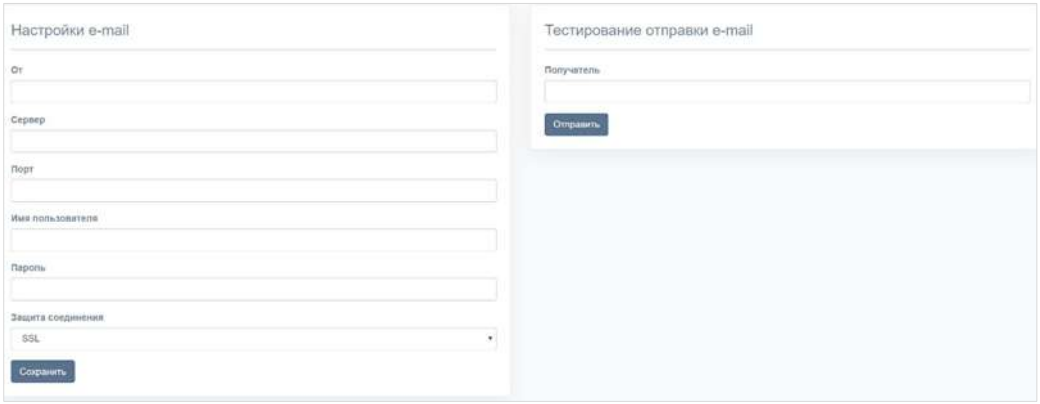


Рисунок 30

Для проверки настроек подключения воспользуйтесь областью «Тестирование отправки e-mail». Впишите в пустое поле адрес получателя и нажмите кнопку «Отправить».

НАСТРОЙКА PUSH-УВЕДОМЛЕНИЙ

Для подключения и настройки push-уведомлений перейдите в раздел «Push Service».

Интерфейс предназначен для подключения push-уведомлений (Рисунок 31).

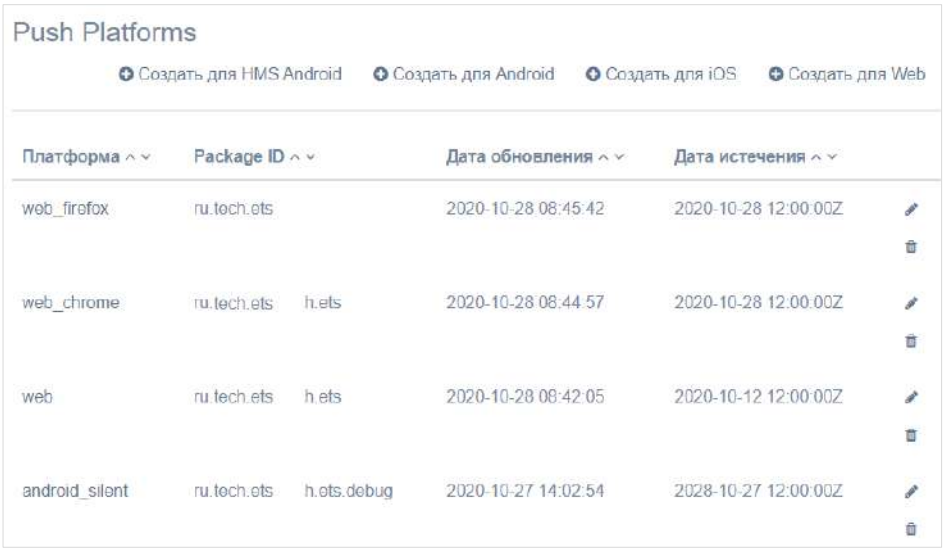


Рисунок 31

Таблица содержит следующую информацию:

Таблица 34

Название столбца	Информация
Платформа	Платформа, на которой подключены push-уведомления
Package ID	Название сборки приложения Express
Дата обновления	Дата последнего изменения настройки push-уведомлений
Дата истечения	Дата истечения поступления push-уведомлений

Для редактирования подключения нажмите кнопку и внесите изменения в открывшемся окне.

Для удаления подключения нажмите кнопку .

Механизм подключения push-уведомлений различен для платформ Android, iOS и веб-приложения. Для Android и веб-приложения push-уведомления подключаются через FCM, для iOS — через APNS.

Для создания подключения на Android/HMS Android

1. Откройте консоль Firebase.
2. В проекте (меню «Project Overview»), где сконфигурированы ключи для Android, выберите пункт «Project settings» (Рисунок 32).

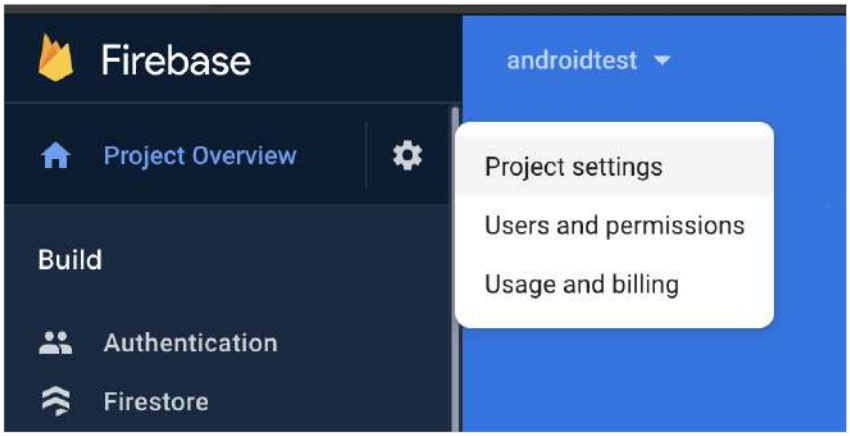


Рисунок 32

3. В консоли администратора Express в разделе «Push Service» нажмите кнопку «Создать для Android» в верхнем правом углу.

   Откроется окно создания подключения для платформы Android (Рисунок 33).

Рисунок 33

4. Заполните поля формы:

Таблица 35

Параметр	Описание	Значение
Платформа	Платформа, на которой подключены push-уведомления	android_silent
Package ID	Название сборки приложения Express	
Дата истечения	Дата истечения поступления push-уведомлений	
FCM URL	Адрес сервера Firebase Cloud Messaging	https://fcm.googleapis.com/fcm/send
FCM API Key	Ключ API, выдаваемый в консоли администратора Firebase	См. Рисунок 34

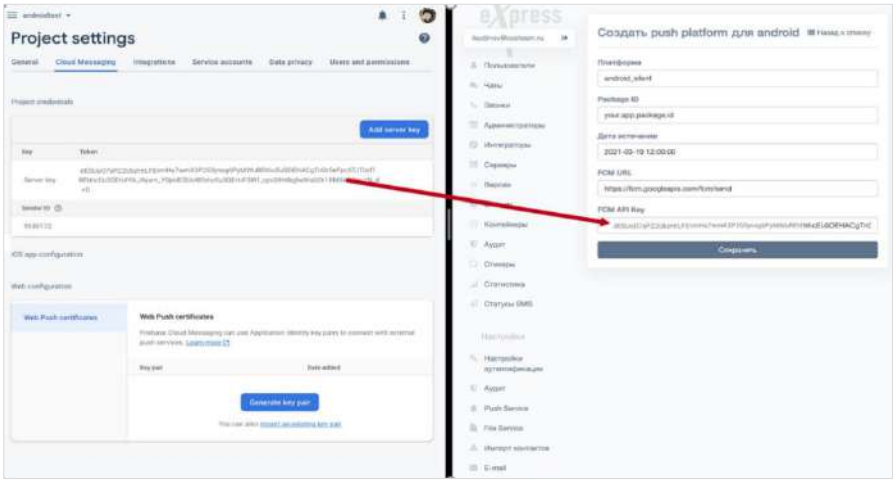


Рисунок 34

5. Нажмите кнопку «Сохранить».

Для создания подключения на iOS:

1. Нажмите кнопку «Создать для iOS» в верхнем правом углу.

   Откроется окно создания подключения для платформы iOS (Рисунок 35).

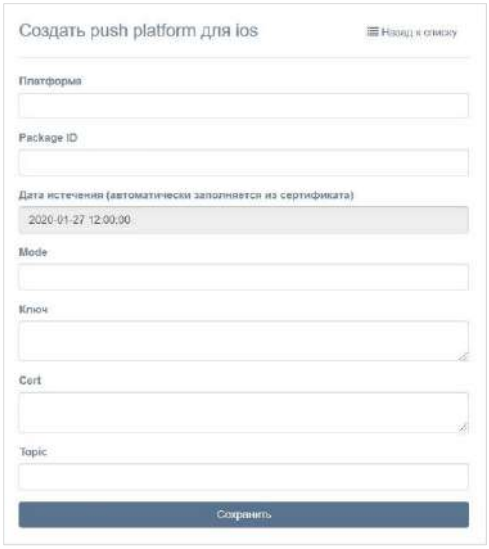


Рисунок 35

2. Заполните поля формы:

Таблица 36

Параметр	Описание	Значение
Платформа	Платформа, на которой подключены push-уведомления	• ios_apns (для alert push с сертификатом apns); • ios_voex (для push-уведомлений звонков с сертификатом voip)
Package ID	Название сборки приложения Express	
Дата истечения	Дата истечения поступления push-уведомлений	
Mode	Режим работы push-уведомлений. Возможные значения prod/dev	• dev (для сборки beta); • prod (для релиза/пререлиза)
Ключ	Приватный ключ	
Cert	Сертификат	
Topic	Название сборки приложения Express	Package ID (для ios_apns); пустое значение (для ios_voex)

3. Нажмите кнопку «Сохранить».

Для создания подключения в веб-приложении:

1. Откройте консоль Firebase.
2. В консоли Firebase создайте проект для веб-приложения (Рисунок 36).

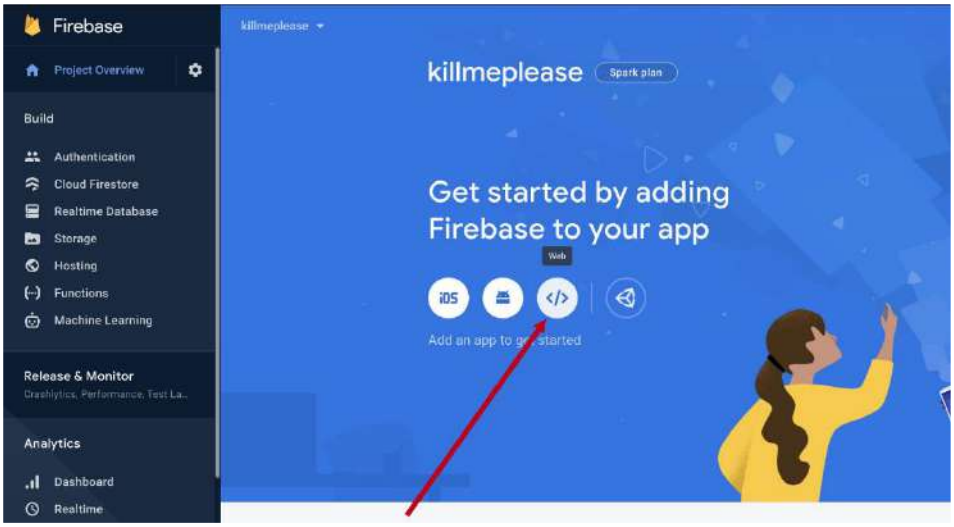


Рисунок 36

3. В открывшемся окне нажмите кнопку «Generate key pairs» (Рисунок 37).

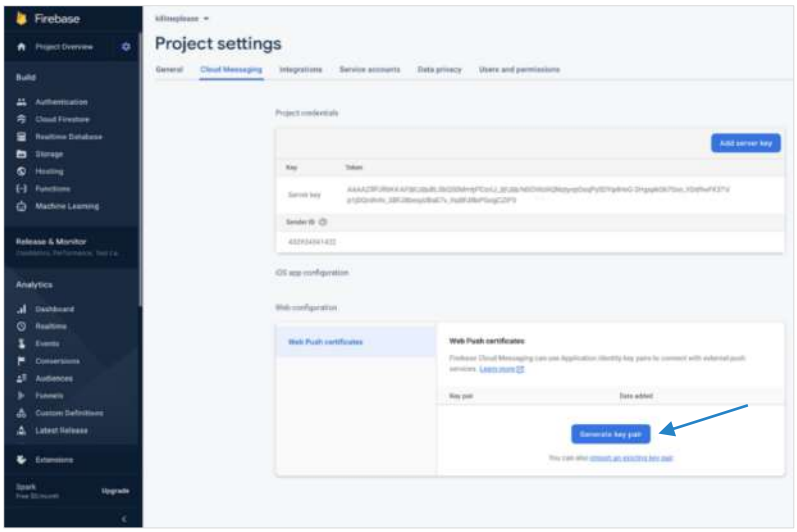


Рисунок 37

4. В консоли администратора в разделе «Push Service» нажмите кнопку «Создать для Web» в верхнем правом углу.

   Откроется окно создания подключения для веб-приложения (Рисунок 38).

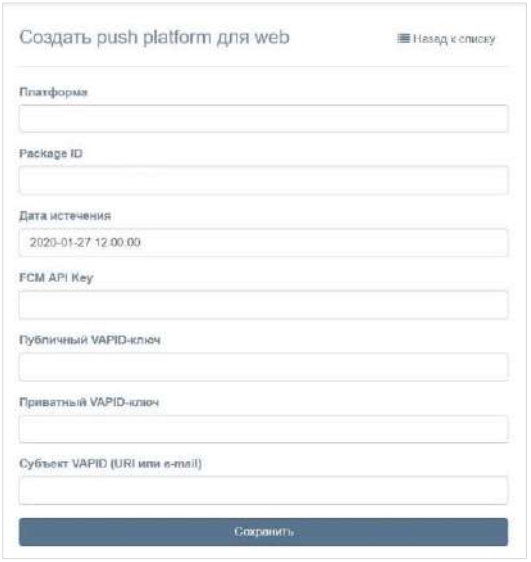


Рисунок 38

5. Заполните поля формы.

Примечание. В поле «Платформа» укажите значение «web».

Таблица 37

Параметр	Описание	Значение
Платформа	Платформа, на которой подключены push-уведомления	• web; • web_chrome; • web_firefox; • web_edge
Package ID	Название сборки приложения Express	
Дата истечения	Дата истечения поступления push-уведомлений	
FCM API Key	Ключ API, выдаваемый в консоли администратора Firebase	См. Рисунок 39
Публичный VAPID-ключ	Публичный ключ API, сгенерированный в консоли администратора Firebase	См. Рисунок 39

Параметр	Описание	Значение
Приватный VAPID-ключ	Приватный ключ API, сгенерированный в консоли администратора Firebase	См. Рисунок 39
Субъект VAPID (URI или e-mail)	Адрес электронной почты пользователя в firebase	mailto:<email аккаунта firebase>

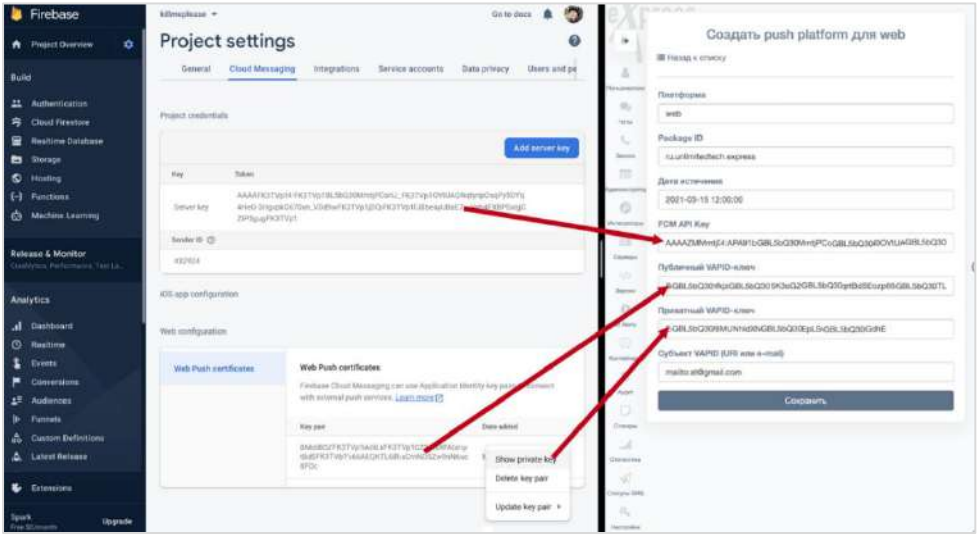


Рисунок 39

6. Нажмите кнопку «Сохранить».
7. Повторите действия 1–6 для Chrome, указав в поле «Платформа» значение «web_chrome».

   В разделе «Push Service» появятся две записи (для двух браузеров).
8. В конфигурационном файле docker-образа веб-приложения (WEB_CLIENT_CONFIG) измените параметр gcmSenderId на значение из Firebase (Рисунок 40).

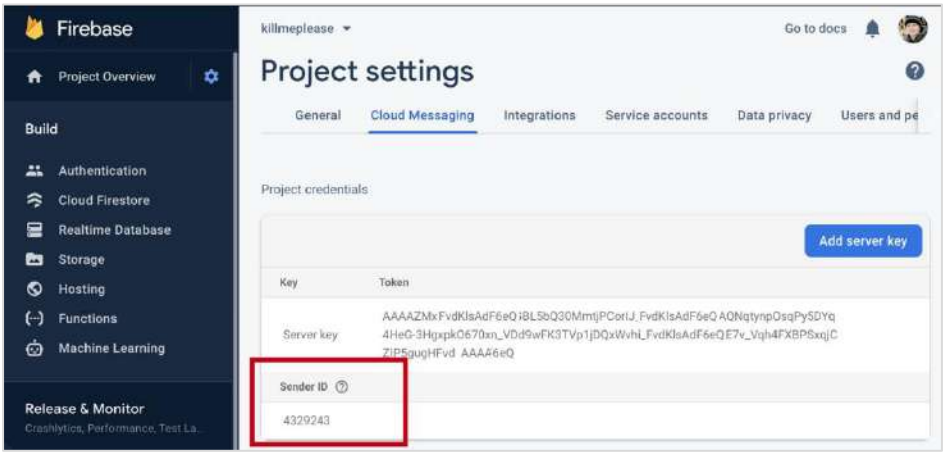


Рисунок 40

НАСТРОЙКА ПОДКЛЮЧЕНИЙ КОРПОРАТИВНЫХ СЕРВЕРОВ

Для настройки сервера:

1. Перейдите в раздел «Серверы».

В разделе «Серверы» представлена информация об RTS, к которому подключен данный ETS (Рисунок 41), и CTS, подключенных к данному ETS (Рисунок 42).

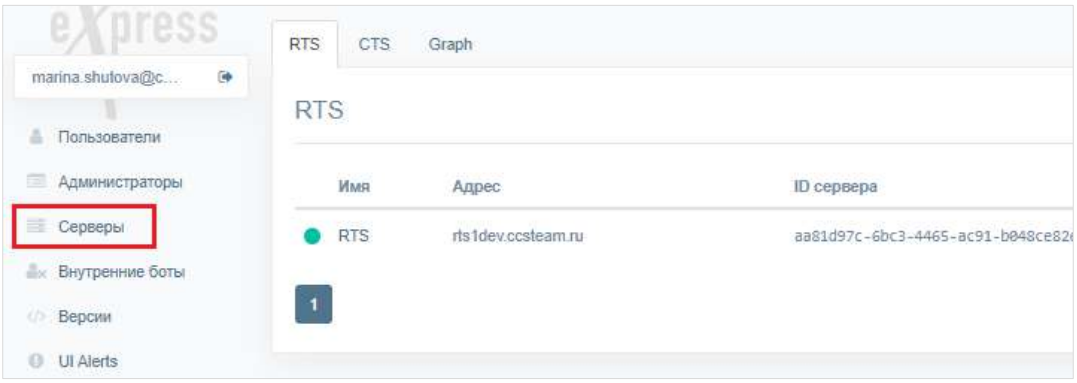


Рисунок 41

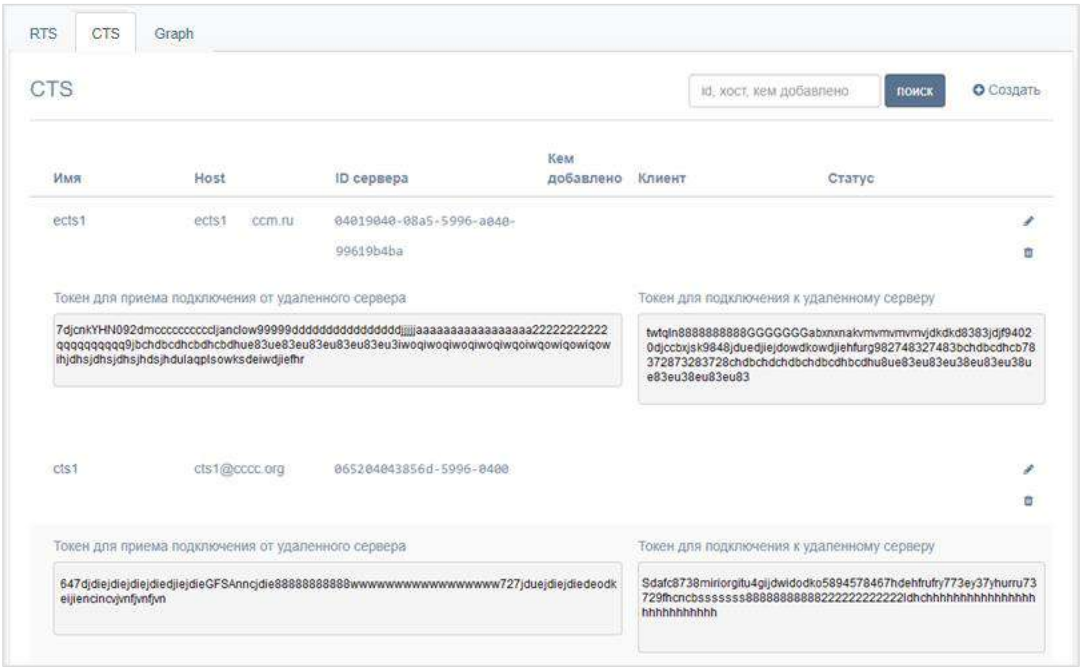


Рисунок 42

2. Проверьте статус подключения CTS с помощью цветовых маркеров рядом с именами серверов.
   - зеленый — сервер подключен и есть связь;
   - фиолетовый — сервер заблокирован;
   - красный — сервер подключен и нет связи;
   - пустое место — сервер подключен к другому RTS.

   Подключение ETS к RTS выполняется в консоли RTS, см. стр.50.
3. Подключите CTS.

Для подключения CTS:

1. В разделе «Серверы» откройте закладку «CTS».
1. Нажмите кнопку «Создать» в правом верхнем углу в секции «CTS».

   Откроется окно (Рисунок 43).

Рисунок 43

2. Заполните поля:
   - в поле «ID» укажите идентификатор сервера, с которым будет установлено подключение (идентификатор CTS хранится в разделе «Сервер» административной консоли этого CTS);
   - в поле «Имя» внесите краткое обозначение для создаваемого канала связи;
   - в поле «Host» укажите реальный адрес подключения к серверу (URL), который будет отображаться в клиентском приложении;
   - в полях «Токен для подключения от удаленного сервера» и «Токен для подключения к удаленному серверу» укажите токены;
   - в поле «Статус» выберите значение «включено» или «выключено»;
   - в полях «Клиент», «Кто установил», «Контакт на стороне eXpress», «Контакт на стороне клиента», «Партнер», «Ссылка на документацию», «Ссылка на конфиг», «Описание проблем и их решений» введите соответствующие данные;
   - в выпадающем списке «Ответственный за обновления» выберите «eXpress»/«Клиент»/«Партнер»;
   - при необходимости подключите опцию «Позволять отправлять письма с этого CTS» (если подключаете CTS).
3. Нажмите на кнопку «Сохранить».

Для просмотра графической схемы маршрутизации подключений откройте вкладку «Graph» (Рисунок 44).

Рисунок 44

Серверы обозначены на схеме цветными кругами, в зависимости от типа:

- RTS — зеленым;
- ETS — фиолетовым;
- CTS — синими.

Для удобства просмотра элементы схемы можно перетаскивать с помощью мыши.

Для просмотра информации о подключении к серверу на схеме:

1. На вкладке «Graph» нажмите на круг, которым обозначен данный сервер.

   В правом верхнем углу экрана отобразится адрес выбранного сервера и количество чатов, созданных на нем (Рисунок 45).

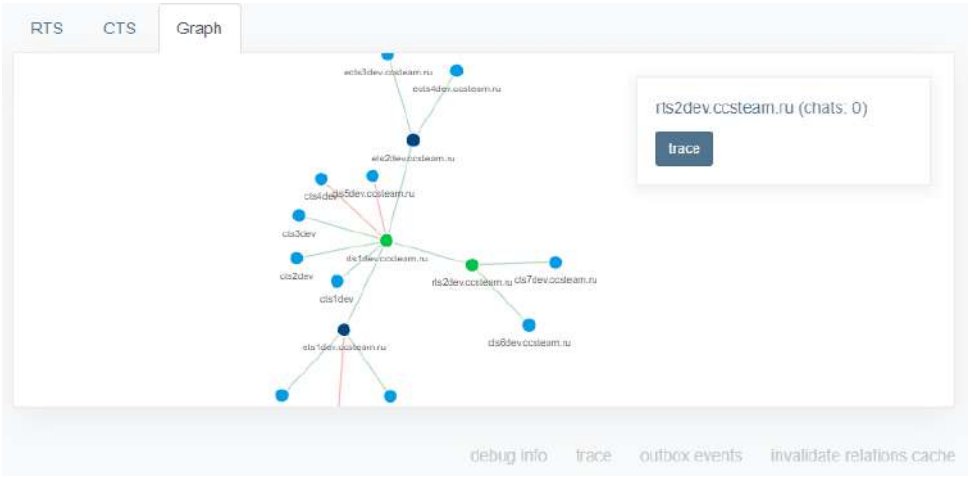


Рисунок 45

2. Нажмите на название сервера в правом верхнем углу экрана.

   Откроется окно с информацией об RTS/ETS/TTS, через который происходит обмен данными с текущим сервером (Рисунок 46 и Рисунок 47)

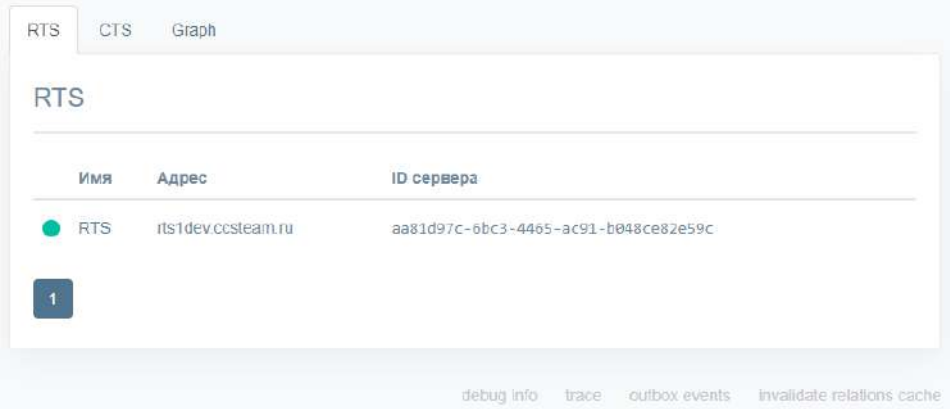


Рисунок 46

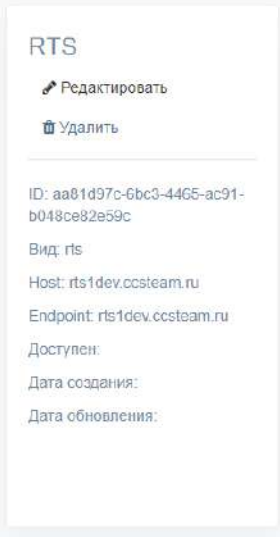


Рисунок 47

УСТАНОВКА ВЕБ-КЛИЕНТА

Внимание! Веб-клиент устанавливается на сервер после установки docker-ce и docker-compose.

Веб-клиент устанавливается только совместно с ETS-сервером!

Для установки веб-клиента:

1. Запустите командную строку.
2. Подключитесь к репозиторию разработчика в Docker для скачивания контейнеров.

```
docker login -u Login -p Password registry.public.express
```

Примечание. В качестве логина и пароля используются Login и Password, которые выдаются разработчиком.

В случае установки сертифицированной версии подключите твердотельный накопитель с программным обеспечением к платформе, на которой происходит установка, и распакуйте архивный файл cts_X.XX.X.zip.

3. Создайте рабочий каталог веб-клиента.

```
mkdir -p /opt/web_client
cd /opt/web_client
dpl --init web
```

После выполнения команды dpl --init web создается файл settings.

4. Установите цепочки сертификатов и ключа SSL.

- при использовании собственного сертификата создайте директорию для сертификатов.

Важно! Имя файла сертификата и имя ключа должны соответствовать примеру ниже:

```
mkdir -p nginx/certs
cp /somewhere/my-certificate-chain.crt nginx/certs/nginx.crt
cp /somewhere/my-unencrypted-key.key nginx/certs/nginx.key
```

Конструкции /somewhere/my-certificate-chain.crt и /somewhere/my-unencrypted-key.key индивидуальны для каждого конкретного случая.

Конструкции nginx/certs/nginx.crt и nginx/certs/nginx.key являются обязательными.

Требования к сертификатам изложены на стр. 20.

- при использовании сертификата от Let's Encrypt в файл settings добавьте параметр le_email: admin@company-mail.ru

Проверка подключения сертификатов после инсталляции описана на стр.41.

Сгенерируйте файл dhparam с помощью команды:

```
openssl dhparam -out /opt/express/web_client/nginx/dhparam.pem
2048
```

5. Созданный по умолчанию файл конфигурации имеет следующий вид и требует редактирования:

```
project_type: web
ccs_host: somehost.somedomain.sometld
web_client_config: ''
```

Пример заполнения конфигурации:

```
project_type: web
ccs_host: example.com
le_email: test@example.com
web_client_enabled: true
web_client_config:
  regions:
    ru:
      host: rts1dev.ccsteam.ru
      prefix: 7
    ae:
      host: rts2dev.ccsteam.ru
      prefix: 971
  sentryDSN: https://sentryToken@sentry.ccsteam.ru/58
  ccsHost: corp.express
  ctsWeb: false
  locales: ["en","ru","de","fr","es"]
  platformPackageId: ru.unlimitedtech.express
  gcmSenderId: senderId
  landingUrl: https://express.ms/mobile-corp-express
  allowCtsLogin: true
  allowDebugInfo: true
  gmapsApiKey: apiKeyapiKeyapiKey
  environment: dev
  actionTaskFeature: true
```

```
  changelogUrl: https://dl.express.ms/changelog/changelog-{}.md
images:
  web_client: registry.public.express/web_client:develop
```

6. В каталоге /opt/express/web_client выполните команду:

```
dpl -d
```

НАСТРОЙКА CTS

Настройка CTS включает в себя следующие процедуры:

- подключение TLS-сертификата (если это не было выполнено в процессе установки ETS) см. стр. 68;
- подключение Botx SSL-сертификата см. стр. 69;
- настройка видео- и голосовой связи см. стр. 70;
- подключение SMTP-сервера см. стр. 70;
- настройка регистрации по e-mail см. стр. 71;
- настройка доверительных подключений см. стр. 71.

ПОДКЛЮЧЕНИЕ TLS-СЕРТИФИКАТА И BOTX SSL-СЕРТИФИКАТА

Для применения TLS-протокола в трастовых соединениях:

1. Выберите пункт меню «Сервер».

   Откроется окно с информацией о данном CTS (Рисунок 48).

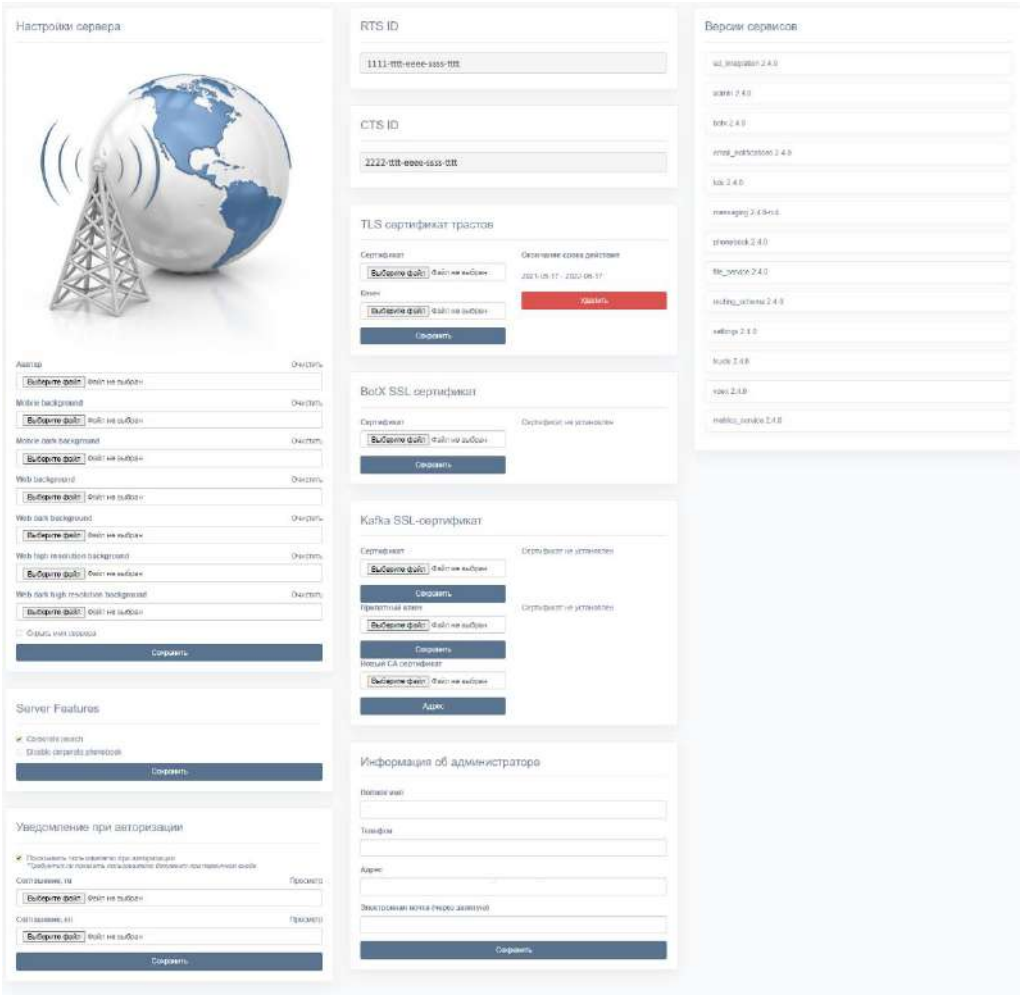


Рисунок 48

2. Внесите данные о сертификате и ключе в соответствующие поля области «TLS-сертификат трастов» (Рисунок 49).

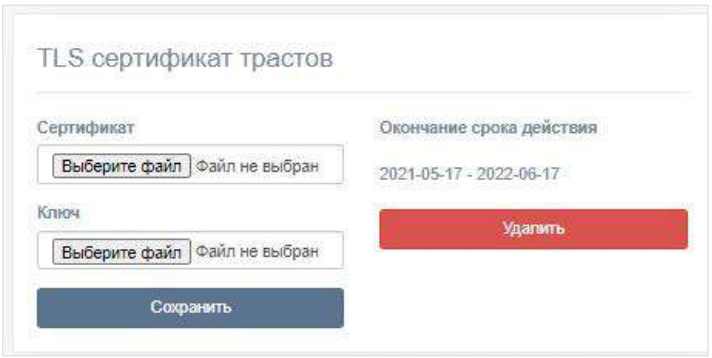


Рисунок 49

3. Нажмите кнопку «Сохранить».

Примечание. Допускается применение TLS-сертификата, использованного на этапе установки CTS.

Для подключения сертификата чат-бота в области «BotX SSL сертификат» введите данные о сертификате и нажмите кнопку «Сохранить» (Рисунок 50).

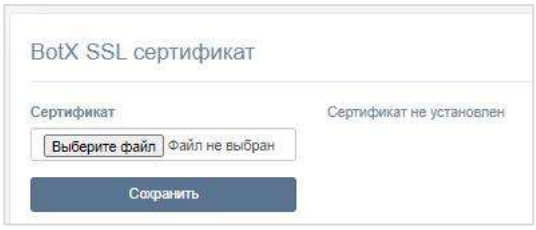


Рисунок 50

НАСТРОЙКА ВИДЕО- И ГОЛОСОВОЙ СВЯЗИ

Настройка видео- и голосовой связи выполняется после установки сервера Voex и описана на стр. 37.

ПОДКЛЮЧЕНИЕ SMTP-СЕРВЕРА

Для подключения SMTP-сервера:

1. В меню выберите пункт «E-mail» (Рисунок 51).
2. В области «Настройки e-mail» заполните поля:
   - в поле «От» укажите обратный адрес;
   - в поле «Сервер» укажите SMTP-сервер;
   - в поле «Порт» укажите номер порта для ретрансляции исходящей почты: 25, 587 или 465. Номер порта зависит от типа защищенного соединения;
   - В полях «Имя пользователя» и «Пароль» укажите данные для авторизации на SMTP-сервере.
3. Выберите тип защищенного соединения в выпадающем списке: SSL, Start/TLS или None.
4. Нажмите кнопку «Сохранить».

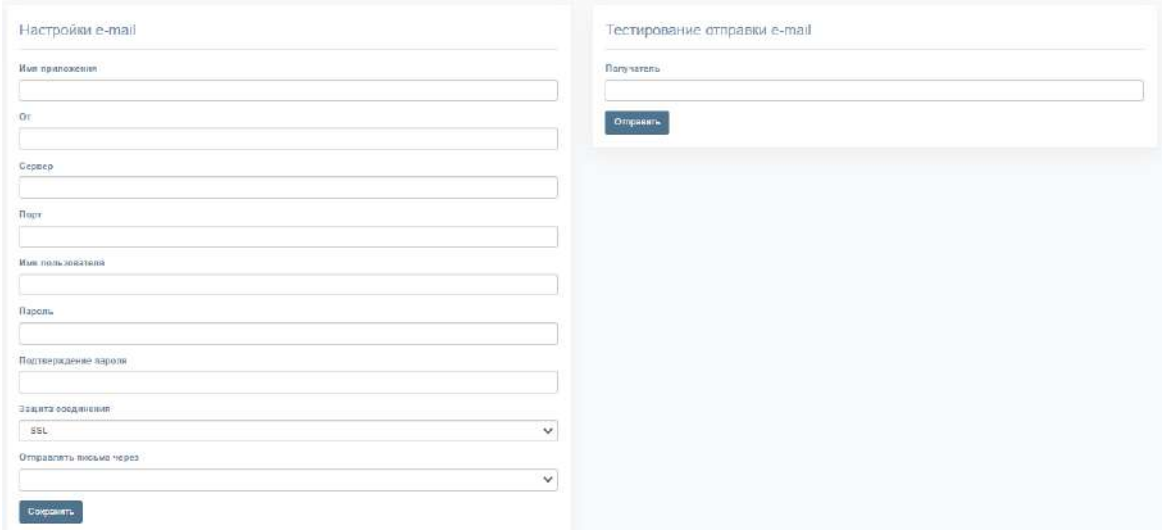


Рисунок 51

Для проверки настроек подключения воспользуйтесь областью «Тестирование отправки e-mail». Впишите в пустое поле адрес получателя и нажмите кнопку «Отправить».

НАСТРОЙКА E-MAIL

Для настройки регистрации по маске e-mail:

5. Перейдите на вкладку «Настройки регистрации» → «E-mail».

   Откроется окно «Настройки e-mail» (Рисунок 52).
6. Введите маску e-mail в поле, используя регулярное выражение (например, ^.*?@corporate.local).
7. Нажмите на кнопку «Сохранить».

Рисунок 52

После успешного сохранения изменений в верхней части экрана появится системное сообщение (Рисунок 53).

Рисунок 53

НАСТРОЙКА ДОВЕРИТЕЛЬНЫХ ПОДКЛЮЧЕНИЙ

Для создания доверительного подключения (траста):

1. Откройте пункт меню «Серверы».
2. Выберите вкладку «Trusts» (Рисунок 54).

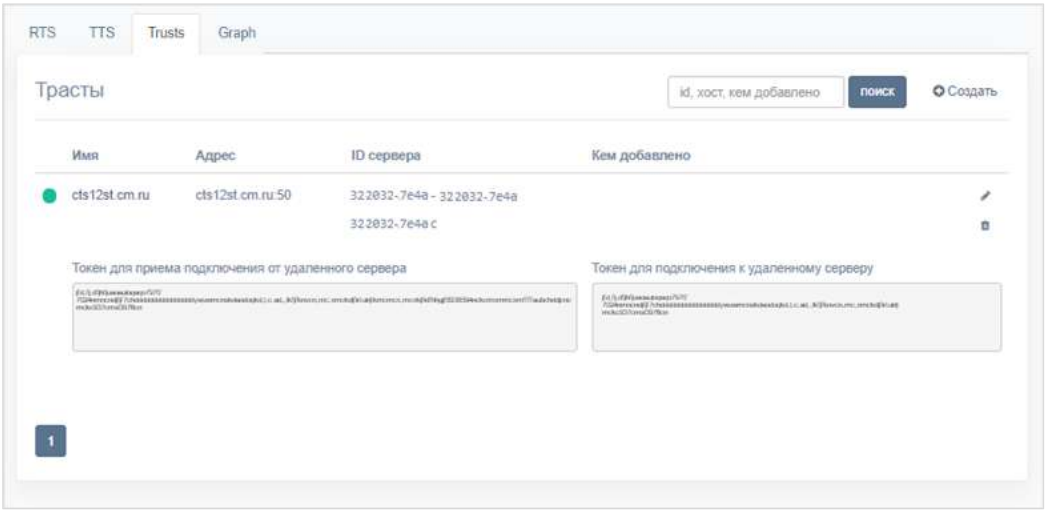


Рисунок 54

3. Нажмите кнопку «Создать» в правом верхнем углу.

Откроется окно (Рисунок 55).

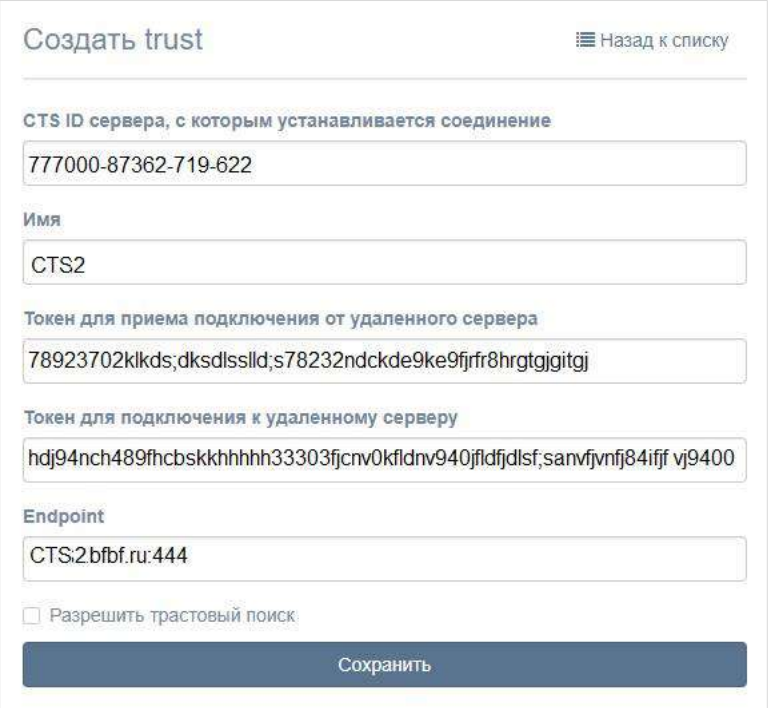


Рисунок 55

4. Заполните поля:
   - в поле CTS ID укажите идентификатор сервера CTS, с которым будет установлено соединение. Идентификатор CTS-сервера хранится в пункте меню «Сервер» административной консоли этого сервера;
   - в поле «Имя» внесите краткое обозначение для создаваемого траста;
   - в полях «Токен для приема подключения» и «Токен для подключения» укажите токены;

     Пример:
     Требуется создать траст между двумя серверами: CTS1 и CTS2. Для решения этой задачи администратор на каждом из серверов создает траст, в настройках указывая токены таким образом, чтобы токен для подключения на сервере CTS1 совпадал с токеном для приема подключения на CTS2, и наоборот.

   - в поле «Endpoint» укажите адрес подключения к серверу. В таблице с перечнем токенов данные из этого поля отображаются в столбце «Адрес»;
   - настройка «Разрешить трастовый поиск» разрешает доступ другому серверу к корпоративной книге контактов сервера, на котором создается траст. Трастовый поиск доступен в том случае, если в настройках сервера разрешен корпоративный поиск — Corporate search.
5. Нажмите на кнопку «Сохранить».

Далее зайдите в консоль администратора корпоративного сервера (в примере, приведенном на шаге 2, CTS2), с которым устанавливается соединение, и создайте траст с текущим сервером (CTS1).

НАСТРОЙКА DLP

Для формирования ключа DLP и добавления его во все чаты:

Внимание! В данном примере DLP устанавливается на Single CTS. Отличные схемы установки запрашивайте у разработчиков.

1. Выполните команду:

```
mkdir -p dlps_keys/storage && chown -R 888:888 dlps_keys
```

2. Пропишите в файле конфигурации параметр dlps_enabled: true

```
api_internal_token: S0L2U6zD0s2iQmdQ
ccs_host: 'cts_name.somedomain.sometld'
cts_id: 'aaaa-bbbb-cccc-dddd'
phoenix_secret_key_base: verystrongpassword
project_type: cts
prometheus_users: verystrongpassword
prometheus: verystrongpassword
rts_host: 'rts_name.somedomain.sometld'
rts_id: 'aaaa-bbbb-cccc-dddd'
rts_token: 'verystrongpassword'
dlps_enabled: true
```

3. Выполните команду (находясь в папке /opt/express):

```
dpl -d
```

После выполнения данной команды будет сгенерирован ключ, который будет добавляться во все чаты.

Консоль администратора будет доступа по URL https://express.mydomain.tld/dlps/. Стандартная учетная запись admin/admin.

4. В консоли администратора включите настройку DLP нажатием кнопки «Enable DLPS».

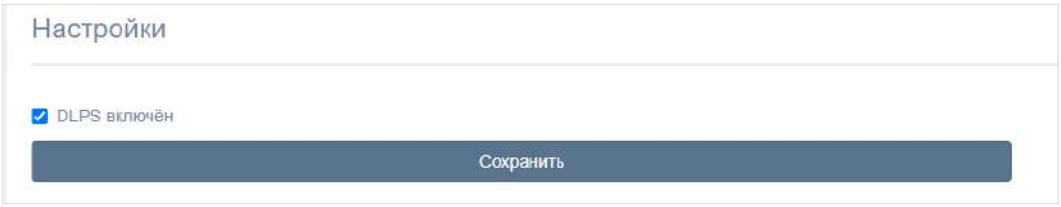


Рисунок 56

НАСТРОЙКА DLP НА ВНЕШНЕМ НОСИТЕЛЕ

Для настройки DLP на внешнем носителе:

1. Вставьте rw флэш-накопитель USB в компьютер и смонтируйте диск в нужную директорию. Директория по умолчанию — /opt/express-dlps/dlps_keys/. Файловая система на флэш-накопителе должна быть совместима с ОС RHEL
2. Пропишите в файле конфигурации настройку dlps_keys_mount_path: /PATH_TO_DIRECTORY, где PATH_TO_DIRECTORY — путь к директории, куда записываются ключи.

   Например:

```
project_type: dlps
api_internal_token: TOKEN
ccs_host: 'cts_name.somedomain.sometld'
cts_id: 'aaaa-bbbb-cccc-dddd'
dlps_icap_client_host: IP_ADDRESS
dlps_icap_client_port: PORT
```

```
dlps_icap_additional_headers: verystrongpassword
network_segment: CTS
application: PROD
client_ip: 127.0.0.1
server_ip: 127.0.0.1
kafka_host: etcd01.ru,etcd02.ru,etcd03.ru
phoenix_secret_key_base: PHOENIX_SECRET_KEY_BASE
etcd_endpoints:
http://etcd01.ru:2379,http://etcd02.ru:2379,http://etcd03.ru:2379
postgres_host: CTS.CTS.RU
postgres_user: POSTGRES_USER
postgres_password: POSTGRES_PASSWORD
dlps_keys_mount_path: /MOUNT_POINT
prometheus_users: verystrongpassword
prometheus: verystrongpassword
rts_id: 'aaaa-bbbb-cccc-dddd'
pacemaker_generate: true
pacemaker_virtual_ip: 10.0.0.1
```

3. Выполните команду:

```
mkdir -p dlps_keys/storage && chown -R 888:888 dlps_keys
```

4. Запустите DLP (если DLP уже запущен, то остановите и перезапустите).

   # dpl -d

5. Для проверки правильности установки убедитесь, что в файле /opt/express-dlps/dlps/docker-compose.yml, прописано верное значение volumes: «/PATH_TO_DIRECTORY:/app/keys».

Глава 4

ПРОЦЕДУРА ОБНОВЛЕНИЯ

РУЧНОЕ ОБНОВЛЕНИЕ

Внимание! Выполните резервное копирование перед выполнением процедуры обновления!

SINGLE CTS

Для обновления системы на версию 2.5:

Примечание: 22.07.2022 Начиная с версии 2.4 изменились минимальные требования по версии postgres. Теперь поставляется образ postgresql версии 14.4. Процедура обновления встроенной БД описана на стр. **Ошибка! Закладка не определена.**.

1. Перейдите в директорию Express cd /opt/express/.
2. Остановите сервисы из директории Express:

```
DEPLOYKA_SKIP_UPDATE=true dpl --dc stop
```

3. Выполните резервное копирование /var/lib/docker/volumes (или где они лежат в этой системе).

   При выполнении обновления сервера с версии 1.28 измените хозяина файлов для сервисов (делается один раз):

```
docker volume inspect --format '{{ .Mountpoint }}'
cts_ccs_admin_public cts_file_service_uploads cts_messaging_cache
cts_messaging_uploads cts_phonebook_uploads | xargs sudo chown -R
888:888
```

   Если предыдущая версия nginx меньше, чем 1.20.1 и используются letsencrypt сертификаты:

   - Очистите хранилище letsencrypt (один раз):

```
rm -rf cts/letsencrypt
dpl cadvinstall && dpl nxinstall
```

4. Обновите node exporter и container advisor:

```
dpl cadvinstall && dpl nxinstall
```

5. Запустите обновление:

```
dpl -d
```

   После запуска обновления требуется время на проведение внутренних процедур (ориентировочное время 10-15 минут).

6. Проверьте логи на наличие ошибок командой:

```
dpl --dc logs --tail=200 -f
```

Внимание! С версий 2.2 и 2.3 откатываться назад нельзя!

Для отката обновления поправьте файл **settings**, указав параметр, например:

```
images:
     trusts: ccs/trusts:1.28.0
```

Обновление сервера VoEx:

1. Перейдите в директорию Express cd /opt/express-voice/.
2. Остановите сервисы из директории Express:

```
DEPLOYKA_SKIP_UPDATE=true dpl --dc stop
```

3. Запустите обновление:

```
dpl -d
```

4. Проверьте логи на наличие ошибок командой:

```
dpl --dc logs --tail=200 -f
```

BACK CTS И FRONT CTS

Внимание! Перед началом процедуры обновления проверьте изменения по таблице сетевого взаимодействия!

Примечание:

- 05.03.2022 Для установок с разделением на frontend и backend нужно убедиться, что с frontend сервера доступны tcp порты 2379, 5432, 6379, 9092 на сервере backend. Также желательно закрыть доступ к этим портам отовсюду кроме frontend.
- 22.07.2022 **Начиная с версии 2.4 изменились минимальные требования по версии postgres. Теперь поставляется образ postgresql версии 14.4.** Процедура обновления встроенной БД описана на стр. **Ошибка! Закладка не определена.**.

Первым обновляется сервер Back CTS, затем сервер Front CTS.

Для обновления севера Back CTS:

1. Запустите командную строку.
2. Остановите работу приложения командой:

```
DEPLOYKA_SKIP_UPDATE=true dpl --dc stop
```

3. Выполните резервное копирование файлов /var/lib/docker/volumes (после нескольких дней эксплуатации скопированные файлы можно удалить).
4. Если версия сервера ниже 1.28, выполните:

```
docker volume inspect --format '{{ .Mountpoint }}'
cts_ccs_admin_public \ cts_file_service_uploads
cts_messaging_cache cts_messaging_uploads \ cts_phonebook_uploads
| xargs sudo chown -R 888:888
dpl cadvinstall && dpl nxinstall
```

5. Запустите обновление:

```
dpl -d
```

   После запуска обновления требуется время на проведение внутренних процедур (ориентировочное время 10-15 минут).

6. Проверьте логи на наличие ошибок командой:

```
dpl --dc logs --tail=200 -f
```

Для обновления севера Front CTS:

1. Запустите командную строку.
2. Остановите работу приложения командой:

```
DEPLOYKA_SKIP_UPDATE=true dpl --dc stop
```

3. Выполните резервное копирование файлов /var/lib/docker/volumes (после нескольких дней эксплуатации скопированные файлы можно удалить).

   Если предыдущая версия nginx меньше, чем 1.20.1 и используются letsencrypt сертификаты:

   - Очистите хранилище letsencrypt (один раз):

```
rm -rf cts/letsencrypt
```

4. Запустите обновление:

```
dpl -d
```

После запуска обновления требуется время на проведение внутренних процедур (ориентировочное время 10-15 минут).

5. Проверьте логи на наличие ошибок командой:

```
dpl --dc logs --tail=200 -f
```

Обновление сервера VoEx:

1. Перейдите в директорию Express cd /opt/express-voice/.
2. Остановите сервисы из директории Express:

```
DEPLOYKA_SKIP_UPDATE=true dpl --dc stop
```

3. Запустите обновление:

```
dpl -d
```

4. Проверьте логи на наличие ошибок командой:

```
dpl --dc logs --tail=200 -f
```

ОБНОВЛЕНИЕ С ИСПОЛЬЗОВАНИЕМ ANSIBLE-СЦЕНАРИЕВ

SINGLE CTS, BACK CTS И FRONT CTS

Для обновления сервера:

1. Запустите ansible playbook для обновления всех контейнеров:

```
ansible-playbook --ask-pass -v 05-update_cts.yaml
```

2. Введите пароль учетной записи root после ввода команды.

Для обновления ПО, установленного в контейнерах docker, на сервере Registry выполните:

Внимание! При выполнении скриптов обновления нельзя пропускать паузы, заложенные в него, т. к. их пропуск может привести к ошибкам обновления.

1. Скопируйте новые версии образов docker и скрипт загрузки образов в каталог /tmp/images и загрузите образы с помощью скрипта download.sh (скрипт доступен по ссылке):

```
cp *.tar /tmp/images/
cp /opt/deploy/script/load.sh /tmp/images/
cd /tmp/images/
./ download.sh
```

Подключитесь к консоли сервера Back и Front кластера с индексом 01 и 02, выполните команду для остановки антивируса:

```
systemctl stop kesl klnagent64
```

Примечание. В случае зависания сервера при остановке антивируса перезагрузите оба узла кластера через систему виртуализации.

2. Выполните команду:

```
pcs status
```

3. Убедитесь, что ресурсы кластера запущены согласно списку ниже:
   - dlm-clone [dlm] (back кластер) – запущен на обоих узлах кластера;
   - clvmd-clone [clvmd] (back кластер) – запущен на обоих узлах кластера;
   - clusterfs-clone [clusterfs] (back кластер) – запущен на обоих узлах кластера;
   - cluster_ip – запущен на одном узле кластера;

- dockerd – запущен на одном узле кластера;
- node_exporter (back кластер) – запущен на одном узле кластера;
- cadvisor (back кластер) – запущен на одном узле кластера;
- vmfence (back кластер) – запущен на одном узле кластера;

4. В случае если статус ресурсов кластера не соответствует перечисленным выше, выполните следующую команду, заменив *resource_name* на имя проблемного ресурса:

```
pcs resource cleanup resource_name
```

На узлах кластера Back с индексом 01 и 02 выполните команду ниже:

```
ls -la /opt/ex_data/files
```

Примечание. В случае зависание вывода списка директорий перезагрузите оба узла кластера через систему виртуализации.

5. Подключитесь к консоли сервера Back и Front кластера с индексом 01 либо 02 и выполните команду для определения текущего первичного узла, на котором запущены ресурсы кластера:

```
pcs status | grep dockerd
```

6. Подключитесь к консоли текущего первичного узла кластера Back и Front и последовательно выполните команду:

```
docker ps -a > current_version.txt
```

7. Сохраните полученный файл. Он потребуется для процедуры отката на предыдущую версию.
8. Запустите скрипт автоматического обновления всех контейнеров первичных серверов и введите пароль учетной записи root после ввода команды:

```
ansible-playbook --ask-pass -v 05-master_update_cts.yaml
```

9. После обновления первичных серверов проверьте функционирование системы, выполнив проверку логов на наличие ошибок и функции отправки сообщений.
10. Запустите скрипт автоматического обновления всех контейнеров вторичных серверов:

```
ansible-playbook --ask-pass -v 06-slave_update_cts.yaml
```

11. Введите пароль учетной записи root.

Подключитесь к консоли сервера Back и Front кластера с индексом 01 и 02, выполните команду для запуска антивируса:

```
systemctl start kesl klnagent64
```

Для отката на предыдущую версию ПО, установленного в контейнерах docker:

1. Подключитесь к консоли узлов кластера Back с индексами 01 и 02.
2. Добавьте в файл /opt/express/settings следующие строки, заменив в них версию ПО на значения из файла current_version.txt (файл получен на шаге 3 описания автоматического обновления с помощью скриптов ansible):

```
images:
  messaging: messaging:1.39.6
  settings: settings:1.39.0
  audit: audit:1.39.0
  admin: admin:1.39.1
  file_service: file_service:1.39.0
  voex: voex:1.39.0
  ad_phonebook: ad_phonebook:1.39.1
  email_notifications: email_notifications:1.39.0
```

```
  botx: botx:1.39.1
  ad_integration: ad_integration:1.39.0
  kdc: kdc:1.39.0
  routing_schema_service: routing_schema_service:1.39.0
```

3. Подключитесь к консоли узлов кластера Front с индексами 01 и 02.
4. Добавьте в файл /opt/express/settings следующие строки, заменив в них версию ПО на значения из файла current_version.txt (получен на шаге 3 описания автоматического обновления с помощью скриптов ansible):

```
images:
  trusts: trusts:1.39.0
```

Запустите скрипт автоматического обновления всех контейнеров первичных серверов и введите пароль учетной записи root после ввода команды:

```
ansible-playbook --ask-pass -v 05-master_update_cts.yaml
```

После обновления первичных серверов проверьте нормальное функционирование системы, выполнив проверку логов и функцию отправки сообщений.

Запустите скрипт автоматического обновления всех контейнеров вторичных серверов:

```
ansible-playbook --ask-pass -v 06-slave_update_cts.yaml
```

5. Введите пароль учетной записи root после ввода команды.

Для обновления ПО, установленного в контейнерах docker Web client кластера, на сервере Registry выполните:

Важно! При выполнении скриптов обновления нельзя пропускать паузы, заложенные в него, т.к. их пропуск может привести к ошибкам обновления.

1. Скопируйте новые версии образов docker и скрипт загрузки образов в каталог /tmp/images сервера Registry.
2. Загрузите образы с помощью скрипта load.sh:

```
cp *.tar /tmp/images/
cp /opt/deploy/script/load.sh /tmp/images/
cd /tmp/images/
./load.sh
```

3. С помощью команды ниже уточните новую версию образа контейнера web client:

```
docker images | grep web_client
```

Измените параметр web_client_image на актуальную версию, полученную на предыдущем шаге (параметр локализован в файле настроек group_vars/all.yaml в каталоге сценариев ANSIBLE web client (/opt/deploy/playbook-webclient)).

4. Запустите скрипт автоматического обновления всех контейнеров первичного узла кластера Web Client:

```
ansible-playbook --ask-pass -v 05-master_update_web.yaml
```

5. Введите пароль учетной записи root.
6. После обновления первичного узла кластера Web Client проверьте нормальное функционирование системы, выполнив проверку логов и функции отправки сообщений
7. Запустить скрипт автоматического обновления всех контейнеров вторичного узла кластера Web Client аналогично пп.5-6.

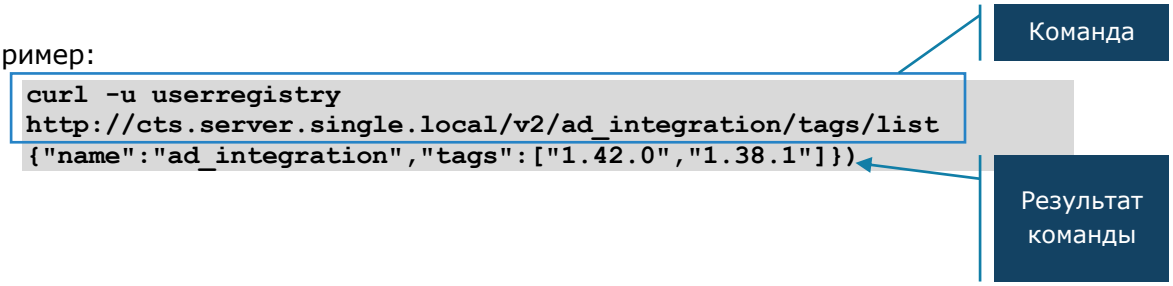
АВАРИЙНЫЕ СИТУАЦИИ ПРИ ОБНОВЛЕНИИ ИЗ ЛОКАЛЬНОГО РЕПОЗИТОРИЯ REGISTERY

Аварийные ситуации, перечисленные ниже, могут произойти в том случае, если имеется локально развернутый сервер Registery.

Ситуация 1. Отсутствия доступа к сети интернет с узла с репозиторием.

1. С узла, имеющего доступ в интернет, скачайте актуальные контейнеры с помощью скрипта по ссылке (вложение download.sh).
2. Запустите второй скрипт по ссылке (вложение upload.sh) и дождитесь окончания загрузки.
3. Сделайте тестовый запрос из консоли при помощи обращения к URL и получите версии, находящиеся в репозитории.

(Пример:



Ситуация 2. Если в п. 3 предыдущей операции результат команды – no basic auth credentials.

1. Удалите файл .docker/config.json.

   Пройдите повторную авторизацию в Docker registry.

ПРОЦЕДУРА ОБНОВЛЕНИЯ СЕРТИФИКАТА

Для обновления сертификата:

1. Подготовьте сертификат согласно требованиям на стр. 23.
2. Обновите файлы сертификатов, расположенные в папке /opt/express/nginx/certs/. Для разделенного сервера файлы обновляются на Front CTS.
3. Выполните команду в консоли:

```
cd /opt/express && dpl -d && dpl --dc restart nginx
```

Глава 5

УСТРАНЕНИЕ ТИПОВЫХ ОШИБОК

Примечание. Все работы на серверах должны проводится от имени суперпользователя.

Для получения прав суперпользователя выполните команду:

```
sudo -s
```

СК «Express» построен на базе микросерверной архитектуры с использованием контейнеризации на основе ПО Docker. Все операции обслуживания СК «Express» и устранения неполадок производятся с контейнерами Docker.

В случае неполадок в работе СК «Express» в первую очередь требуется проверить статус работы контейнеров.

Для проверки статуса контейнеров (запущен или остановлен) используйте команду:

```
docker ps -a --format "{{.Names}}: {{.Status}}"
```

Нормальное состояние контейнеров — «UP».

Если контейнеру присвоен статус «Exited», запустите его командой:

```
docker start <имя контейнера вида cts_containername_1>
```

Если проблема не решена, соберите логи системы.

Для сбора логов выполните команду:

```
cd /opt/express
dpl --dc logs -tail=1000 > logs.txt
```

Отправьте собранные логи администраторам, ответственным за СК «Express».

Если пользователь не может войти на сервер, соберите логи командой:

```
cd /opt/express
dpl --dc logs -tail=1000 ad_integration > logs.txt
```

Для перезагрузки всех контейнеров выполните команду:

```
cd /opt/express
dpl --dc restart
```

Если у пользователей нарушился порядок отображения сообщений в беседах, то проверьте время на сервере командой:

```
date
```

Если время некорректное, проверьте статус сервиса точного времени chronyd. **Для проверки статуса сервиса точного времени** выполните команду:

```
systemctl status chronyd
```

Если статус «active» имеет значение «inactive», запустите сервис командой:

```
systemctl start chronyd
```

Глава 6

ПРАВИЛА ПРИЕМКИ

ОБЩИЕ ПОЛОЖЕНИЯ.

Испытания и приемка изделия осуществляются согласно ГОСТ 15.309-98.

Для контроля и приемки изделия устанавливаются следующие категории контрольных испытаний:

- предварительные;
- приемочные;
- периодические испытания.

Испытания изделия проводятся до полного их завершения вне зависимости от результатов отдельных проверок. К началу проведения испытаний должны быть завершены мероприятия по подготовке испытаний, предусматривающие:

- полную проверку готовности мест проведения испытаний;
- полное наличие, годность и готовность средств материально-технического обеспечения, гарантирующих создание условий и режимов испытаний;
- создание необходимых условий для проведения испытаний.

Результаты испытаний считаются положительными и изделие – выдержавшим испытания, если оно испытано в полном объеме документа «Система коммуникаций «Express». Версия Е4.1. Технические условия» 05262609.62.01.29.000.001 ТУ, а результаты подтверждают соответствие испытуемых единиц продукции заданным требованиям.

Если изделие не выдерживает испытания, то осуществляется его доработка с целью устранения выявленных недостатков. После доработки изделия проводятся его повторные испытания в полном объеме.

ПРЕДВАРИТЕЛЬНЫЕ ИСПЫТАНИЯ.

Объем и последовательность предварительных испытаний изделия представлены в следующей таблице:

Наименование проверок	**Номер пункта в ТУ**[1]	
	Требования	**Методы контроля**
Проверка комплектности изделия	П. 1.4	П. 5.2
Проверка маркировки изделия	П. 1.7	П. 5.3
Проверка контрольных сумм дистрибутивного комплекта программного обеспечения изделия	П. 5.2, П. 5.3 (формуляр[2])	П. 5.4
Проверка работоспособности подсистем	П. 1.1	П. 5.5
Проверка функциональности изделия	П. 1.3	П. 5.6

[1] документ «Система коммуникаций «Express». Версия Е4.1. Технические условия» 05262609.62.01.29.000.001 ТУ
[2] документ «Система коммуникаций «Express». Версия Е4.1. Формуляр» 05262609.62.01.29.000.001 30

Предварительные испытания изделия проводят для определения его работоспособности и решения вопроса о готовности изделия к приемочным испытаниям.

Предварительные испытания следует выполнять после проведения разработчиком тестирования и отладки поставляемых программных и технических средств и представления им соответствующих документов об их готовности к испытаниям.

Изделие должно предъявляться на испытания (приемку) комплектно, согласно п. 1.5 документа «Система коммуникаций «Express». Версия Е4.1. Технические условия» 05262609.62.01.29.000.001 ТУ.

Предварительные испытания изделия проводят специалисты отдела разработки и тестирования ООО «Анлимитед Продакшен».

ПРИЕМОЧНЫЕ ИСПЫТАНИЯ.

Объем и последовательность приемочных испытаний изделия представлены в следующей таблице:

Наименование проверок	**Номер пункта ТУ**[1]	
	Требования	**Методы контроля**
Проверка комплектности изделия	П. 1.4	П. 5.2
Проверка маркировки изделия	П. 1.7	П. 5.3
Проверка контрольных сумм дистрибутивного комплекта программного обеспечения изделия	П. 5.2, п. 5.3 (формуляр[2])	П. 5.4
Проверка работоспособности подсистем	П. 1.1	П. 5.5

Приемочные испытания проводятся с целью контроля соответствия продукции требованиям документа «Система коммуникаций «Express». Версия Е4.1. Технические условия» 05262609.62.01.29.000.001 ТУ в объеме и последовательности, которые указаны в приведенной выше таблице.

Изделие предъявляют на приемку в комплекте поставки.

Объем выборки контролируемой партии изделий устанавливается согласно ГОСТ Р 50779.51–95 для нормального уровня контроля.

Приемочные испытания изделия проводятся специалистом по качеству на производстве ООО «Анлимитед Продакшен».

Программное обеспечение изделия физическому износу не подвержено, поэтому положительный результат проверки контрольных сумм дистрибутивного комплекта, полученный при проведении приемочных испытаний, подтверждает соответствие изделия функциональным требованиям документа «Система коммуникаций «Express». Версия Е4.1. Технические условия» 05262609.62.01.29.000.001 ТУ.

Если в процессе испытаний будет обнаружено несоответствие хотя бы одному требованию настоящих ТУ, изделие считается не выдержавшим испытания и возвращается для выявления причин дефектов, а также для проведения мероприя-

[1] документ «Система коммуникаций «Express». Версия Е4.1. Технические условия» 05262609.62.01.29.000.001 ТУ
[2] документ «Система коммуникаций «Express». Версия Е4.1. Формуляр» 05262609.62.01.29.000.001 30

тий по их устранению и повторного предъявления. В акте об анализе и устранении дефектов отражаются причины несоответствия требованиям документа «Система коммуникаций «Express». Версия E4.1. Технические условия» 05262609.62.01.29.000.001 ТУ.

Повторное предъявление изделия на приемочные испытания производится в порядке, установленном в документе «Система коммуникаций «Express». Версия E4.1. Технические условия» 05262609.62.01.29.000.001 ТУ.

ПЕРИОДИЧЕСКИЕ ИСПЫТАНИЯ.

Периодические испытания проводит предприятие-изготовитель для периодической проверки соответствия изделия всем требованиям, указанным в документе «Система коммуникаций «Express». Версия E4.1. Технические условия» 05262609.62.01.29.000.001 ТУ, контроля стабильности технологического процесса производства изделия, подтверждения возможности изготовления изделия по действующей конструкторской и технологической документации.

Периодические испытания проводят в соответствии с годовым графиком, но не реже одного раза в год. В графике должны быть указаны место проведения испытаний, сроки проведения испытаний, оформления документации по результатам испытаний и представления акта периодических испытаний на утверждение. График проведения периодических испытаний должен быть утвержден руководителем предприятия-изготовителя.

Объем и последовательность периодических испытаний изделия представлены в таблице ниже:

Наименование проверок	**Номер пункта ТУ**[1]	
	Требования	**Методы контроля**
Проверка комплектности изделия	П. 1.4	П. 5.2
Проверка маркировки изделия	П. 1.7	П. 5.3
Проверка контрольных сумм дистрибутивного комплекта программного обеспечения изделия	П. 5.2, П. 5.3 (формуляр[2])	П. 5.4
Проверка работоспособности подсистем	П. 1.1	П. 5.5
Проверка функциональности изделия	П. 1.3	П. 5.6

Если во время испытаний обнаружено несоответствие требованиям документа «Система коммуникаций «Express». Версия E4.1. Технические условия» 05262609.62.01.29.000.001 ТУ, то приемка очередных изделий, а также передача ранее принятых приостанавливаются до устранения обнаруженных дефектов в предъявленных к приемке и принятых, но не отгруженных изделий.

После устранения причин несоответствия требованиям изделие подвергают повторным испытаниям в полном объеме периодических испытаний.

Если при повторных испытаниях доработанных или вновь изготовленных образцов изделия обнаружено несоответствие требованиям документа «Система коммуникаций «Express». Версия E4.1. Технические условия»

[1] документ «Система коммуникаций «Express». Версия E4.1. Технические условия» 05262609.62.01.29.000.001 ТУ
[2] документ «Система коммуникаций «Express». Версия E4.1. Формуляр» 05262609.62.01.29.000.001 30

05262609.62.01.29.000.001 ТУ, то предприятие-изготовитель приостанавливает производство до выяснения причин несоответствия.

При положительных результатах повторных периодических испытаний приемку и отгрузку комплексов возобновляют. По результатам испытаний оформляют Протокол.

Изделия, подвергнутые периодическим испытаниям, используются как товарная продукция после согласования с заказчиком при сохранении гарантий предприятия-изготовителя после проверки в объеме приемо-сдаточных испытаний.

Приложение 1

СЕТЕВЫЕ ВЗАИМОДЕЙСТВИЯ SINGLE CTS

№	Источник	Получатель	Порт и протокол	Описание
1	Сервер Single CTS	Bot сервер	TCP/80	Взаимодействие Single CTS с Bot-сервером по протоколу HTTP/HTTPS
			TCP443	
	Bot сервер	Сервер Single CTS Bot сервер	TCP/80	Взаимодействие Bot-сервера с Single CTS по протоколу HTTP/HTTPS
			TCP443	
2	Внутренние ИС	Bot-сервер	TCP/80	Взаимодействие внутренних информационных систем с Bot-сервером по протоколу HTTP/HTTPS
			TCP443	
			TCP8000-8100	
	Bot сервер	Внутренние ИС	TCP/80	Взаимодействие Bot-сервера с внутренними информационными системами по протоколу HTTP/HTTPS
			TCP443	
			TCP8000-8100	
3	Сервер Single CTS	Сервер DNS	TCP/53 UDP/53	Обеспечение работы разрешения имен DNS
		Сервер NTP	UDP/123	Обеспечение работы службы точного времени NTP
		Сервер LDAP	TCP/389, 636	Обеспечение работы LDAP/LDAPS
4	Администратор	Сервер Single CTS	TCP/22	Администрирование серверов по протоколу SSH
			TCP/443	Администрирование Express через веб-интерфейс по протоколу HTTPS
5	Сервер Single CTS	Сервер SMTP	TCP/25	Обеспечение отправки писем с ПИН-кодом аутентификации по протоколу SMTP
6	Сервер Single CTS	Сервер DNS и NTP	TCP/53 UDP/53	Обеспечение работы разрешения имен DNS
			UDP/123	Обеспечение работы службы точного времени NTP
7	Внутренний пользователь	Сервер Single CTS	TCP/443	Клиентский доступ к корпоративному контуру Express с использованием протокола HTTPS
8	Внутренний пользователь	Сервер Single CTS	TCP/3478 UDP/3478	Обеспечение работы протоколов STUN/TURN
			UDP/20000-40000	Обеспечение передачи медиаданных по протоколу SRTP конференц-связи
			UDP 49152-65535	Обеспечение работы передачи медиаданных по TURN
9	Внешний пользователь	Сервер Single CTS (Внешний IP NAT)	TCP/3478 UDP/3478	Обеспечение работы протоколов STUN/TURN
			UDP/20000-40000	Обеспечение передачи медиаданных по протоколу SRTP конференц-связи
			UDP/49152-65535	Обеспечение работы передачи медиаданных по TURN
10	Внешний пользователь	Сервер Single CTS (Внешний IP NAT)	TCP/443	Клиентский доступ к корпоративному контуру Express с использованием протокола HTTPS
11	Сервер Single CTS	Сервер установки и обновлений	TCP/443	Клиентский доступ к публичному контуру Express с использованием протокола HTTPS

№	Источник	Получатель	Порт и протокол	Описание
		Registry.public.express		
12	Внешний пользователь	RTS ru.public.express	TCP/443	Обеспечение взаимодействия внешнего пользователя с RTS
13	Сервер Single CTS	RTS ru.public.express	TCP/5001	Обеспечение взаимодействия корпоративного сервера Express с RTS
14	Внутренний пользователь	RTS ru.public.express	TCP/443	Клиентский доступ к публичному контуру Express с использованием протокола HTTPS
15	Внешний пользователь	Сервер веб-клиента corp.express	TCP/443	Клиентский доступ к серверу веб-клиента в публичном контуре
16	Внутренний пользователь	Сервер веб-клиента corp.express	TCP/443	Клиентский доступ к серверу веб-клиента в публичном контуре
17	Сервер Single CTS	Сервера Let`s Encrypt (ANY)	TCP/80	При использовании бесплатного сертификата от компании Let`s Encrypt
	Сервера Let`s Encrypt (ANY)	Сервер Single CTS		
18	Сервер Single CTS	Партнерский сервер Express CTS	UDP/20000-40000 TCP/5001 TCP/80	Обеспечение прямой передачи сообщений между корпоративными серверами минуя публичный контур Обеспечение передачи медиаданных по протоколу SRTP Обеспечение передачи медиаданных по протоколу SRTP Порт TCP/80 добавляется при использовании Let's Encrypt
	Партнерский сервер Express CTS	Сервер Single CTS (Внешний IP NAT)	TCP/443 TCP/5001 UDP/20000-40000	Получение аватаров и вложений с партнерского сервера
19	RTS ru.public.express	SMS оператор	TCP/443	Отправка SMS-сообщений пользователям
20	RTS ru.public.express	Служба push-уведомлений Huawei	TCP/443	Отправка push-уведомлений пользователям Huawei
21	RTS ru.public.express	Служба push-уведомлений Apple	TCP/443	Отправка push-уведомлений пользователям iOS
22	RTS ru.public.express	Служба push-уведомлений Google	TCP/80	Отправка push-уведомлений пользователям Android

Для сервера Single CTS должен быть настроен NAT IP-to-IP и выполнена трансляция следующих портов и протоколов:

- TCP/443;
- TCP/5001;
- TCP/3478-3479;
- UDP/3478-3479;
- UDP/49152-65535;
- UDP/20000-40000.

Приложение 2

СЕТЕВЫЕ ВЗАИМОДЕЙСТВИЯ FRONT CTS И BACK CTS

В таблице ниже представлены сетевые взаимодействия разделенного сервера Express (Front CTS и Back CTS) с совмещенным сервером STUN/TURN на Front CTS.

№	Источник	Получатель	Порт и протокол	Описание
1	Сервер Back CTS	Bot сервер	TCP/80	Взаимодействие back сервера с сервером bot по протоколу HTTP либо HTTPS
			TCP443	
	Bot сервер	Сервер Back CTS	TCP/80	Взаимодействие Bot-сервера с сервером Back CTS по протоколу HTTP либо HTTPS
			TCP443	
2	Внутренние ИС	Bot сервер	TCP/80	Взаимодействие внутренних информационных систем с Bot-сервером по протоколу HTTP или HTTPS
			TCP443	
			TCP8000-8100	
	Bot сервер	Внутренние ИС	TCP/80	Взаимодействие Bot-сервера с внутренними информационными системами по протоколу HTTP либо HTTPS
			TCP443	
			TCP8000-8100	
3	Сервер Back CTS	Сервер LDAP	TCP/53 UDP/53	Обеспечение работы разрешения имен DNS
			UDP/123	Обеспечение работы службы точного времени NTP
			TCP/389 TCP/636	Обеспечение работы LDAP или LDAPS
4	Сервер Back CTS	Сервер Front CTS	TCP/80	Мониторинг работы контейнера trusts
			TCP/6379	Подключение к Redis для работы функции кеширования
			TCP/8188	Управление звонками конференц-связи
			TCP/8888	Tinyproxy локальный прокси-сервер для подключения Back CTS к репозиторию образов docker, используемых для установки и обновления изделия
5	Сервер Front CTS	Сервер Back CTS	TCP/80	Передача зашифрованных пользовательских данных без транспортной обертки TLS
			TCP/2379	Подключение к хранилищу конфигураций для получения различных настроек сервисов
			TCP/5432	Подключение контейнера trusts к базе данных для хранения информации, необходимой для работы
			TCP/9092	Подключение к программному брокеру сообщений Kafka для обмена событиями между сервисами
			TCP/6379	Подключение к Redis для работы функции кеширования
6	Администратор	Сервер Front CTS и Back CTS	TCP/22	Администрирование серверов по протоколу SSH
			TCP/443	Администрирование Express через веб-интерфейс по протоколу HTTPS

№	Источник	Получатель	Порт и протокол	Описание
7	Сервер Back CTS	Сервер SMTP	TCP/25	Обеспечение отправки писем с ПИН-кодом аутентификации по протоколу SMTP
8	Сервер Front CTS	Сервер DNS и NTP	TCP/53 UDP/53	Обеспечение работы разрешения имен DNS
			UDP/123	Обеспечение работы службы точного времени NTP
9	Внутренний пользователь	Сервер Front CTS	TCP/443	Клиентский доступ к корпоративному контуру Express с использованием протокола HTTPS
10	Внутренний пользователь	Сервер Front CTS	TCP/3478 UDP/3478	Обеспечение работы протоколов STUN/TURN
			UDP/20000-40000	Обеспечение передачи медиаданных по протоколу SRTP конференцсвязи
			UDP/49152-65535	Обеспечение передачи медиаданных по протоколу TURN голосовых вызовов
11	Внешний пользователь	Сервер Front CTS (Внешний IP NAT)	TCP/3478 UDP/3478	Обеспечение работы протоколов STUN/TURN
			UDP/20000-40000	Обеспечение передачи медиаданных по протоколу SRTP
			UDP/49152-65535	Обеспечение передачи медиаданных по протоколу TURN голосовых вызовов
12	Внешний пользователь	Сервер Front CTS (Внешний IP NAT)	TCP/443	Клиентский доступ к корпоративному контуру Express с использованием протокола HTTPS
13	Front CTS	RTS Registry.public.express	TCP/443	Доступ к репозиторию образов docker для установки и обновления ПО Express.
14	Внешний пользователь	RTS ru.public.express	TCP/443	Обеспечение взаимодействия внешнего пользователя с RTS
15	Сервер Front CTS	RTS ru.public.express	TCP/5001	Обеспечение взаимодействия корпоративного сервера Express с RTS
16	Внутренний пользователь	RTS ru.public.express	TCP/443	Клиентский доступ к публичному контуру Express с использованием протокола HTTPS
17	Внешний пользователь	Сервер веб-клиента corp.express	TCP/443	Клиентский доступ к серверу веб-клиента в публичном контуре
18	Внутренний пользователь	Сервер веб-клиента corp.express	TCP/443	Клиентский доступ к серверу голосовых коммуникаций в публичном контуре
19	Сервер Front CTS Сервер Let`s Encrypt (ANY)	Сервер Let`s Encrypt (ANY) Сервер Front CTS	TCP/443	При использовании бесплатного сертификата от компании Let`s Encrypt
			TCP/80	
20	Сервер Front CTS	Партнерский сервер Front CTS	TCP/443	Получение аватаров и вложений с партнерского сервера
			TCP/5001	Обеспечение прямой передачи сообщений между корпоративными серверами минуя публичный контур
			UDP/20000-40000	Обеспечение передачи медиаданных по протоколу SRTP
	Партнерский сервер Front CTS	Сервер Front CTS	TCP/5001	Обеспечение прямой передачи сообщений между корпоративными серверами минуя публичный контур
			UDP/20000-40000	Обеспечение передачи медиаданных по протоколу SRTP

№	Источник	Получатель	Порт и протокол	Описание
21	RTS ru.public.express	SMS оператор	TCP/443	Отправка SMS-сообщений пользователям
22	RTS ru.public.express	Служба push-уведомлений Huawei	TCP/443	Отправка push-уведомлений пользователям Huawei
23	RTS ru.public.express	Служба push-уведомлений Apple	TCP/443	Отправка push-уведомлений пользователям iOS
24	RTS ru.public.express	Служба push-уведомлений Google	TCP/443	Отправка push-уведомлений пользователям Android

Приложение 3

СЕТЕВЫЕ ВЗАИМОДЕЙСТВИЯ ETS И SINGLE CTS

№	Источник	Получатель	Порт и протокол	Описание
1	Сервер Single CTS	Сервер LDAP	TCP/53, UDP/53	Обеспечение работы разрешения имен DNS
			UDP/123	Обеспечение работы службы точного времени NTP
			TCP/389, 636	Обеспечение работы LDAP либо LDAPS
2	Сервер Single CTS	Bot сервер	TCP/80	Взаимодействие Single CTS с Bot-сервером по протоколу HTTP либо HTTPS
			TCP443	
	Bot сервер	Сервер Single CTS	TCP/80	Взаимодействие Bot-сервера с сервером Single CTS по протоколу HTTP либо HTTPS
			TCP443	
3	Внутренние ИС	Bot сервер	TCP/80	Взаимодействие внутренних информационных систем с Bot-сервером по протоколу HTTP/HTTPS
			TCP443	
			TCP8000-8100	
	Bot-сервер	Внутренние ИС	TCP/80	Взаимодействие Bot-сервера с внутренними информационными системами по протоколу HTTP/HTTPS
			TCP443	
4	Администратор	Сервер Single CTS	TCP/22	Администрирование серверов по протоколу SSH
			TCP/443	Администрирование Express через веб-интерфейс по протоколу HTTPS
5	Сервер Single CTS	Сервер SMTP	TCP/25	Обеспечение отправки писем с ПИН-кодом аутентификации по протоколу SMTP
6	Сервер ETS	Docker реестр	TCP/443	Доступ к репозиторию образов docker для установки и обновления ПО Express
7	Сервер ETS	Сервер DNS и NTP	TCP/53	Обеспечение работы разрешения имен DNS
			UDP/53	
			UDP/123	Обеспечение работы службы точного времени NTP
8	Внутренний пользователь	Сервер ETS	TCP/443	Клиентский доступ к корпоративному контуру Express с использованием протокола HTTPS
9	Сервер Single CTS	Сервер ETS	TCP/5001	Обеспечение взаимодействия корпоративного сервера Express с сервером предприятия ETS
10	Сервер Single CTS	Docker реестр	TCP/443	Доступ к репозиторию образов docker для установки и обновления ПО Express
11	Сервер Single CTS	Сервер DNS и NTP	TCP/53	Обеспечение работы разрешения имен DNS
			UDP/53	
			UDP/123	Обеспечение работы службы точного времени NTP
12	Внутренний пользователь	Сервер Single CTS	TCP/443	Клиентский доступ к корпоративному контуру Express с использованием протокола HTTPS
13	Внутренний пользователь	Сервер для веб-клиентов	TCP/443	Подключение внутренних пользователей к веб-клиенту
14	Внутренний пользователь	Сервер Single CTS	UDP/20000-40000	Обеспечение передачи медиаданных по протоколу SRTP конференцсвязи

№	Источник	Получатель	Порт и протокол	Описание
			UDP/49152-65535 TCP/3478 UDP/3478	Обеспечение передачи медиаданных по протоколу TURN голосовых вызовов. Обеспечение работы протоколов STUN/TURN
15	Сервер ETS	SMS оператор	TCP/443	Отправка SMS-сообщений пользователям
16	Сервер ETS	Служба push-уведомлений Huawei	TCP/443	Отправка push-уведомлений пользователям Huawei
17	Сервер ETS	Служба push-уведомлений Apple	TCP/443	Отправка push-уведомлений пользователям iOS
18	Сервер ETS	Служба push-уведомлений Google	TCP/443	Отправка push-уведомлений пользователям Android
19	Сервер ETS	RTS	TCP/5001	Обеспечение взаимодействия корпоративного сервера Express с RTS.
		ru.public.express		
20	Сервера Let`s Encrypt	Сервер ETS	TCP/80,443	Данное правило требуется при использовании бесплатного сертификата от компании Let`s Encrypt
		Сервер Single CTS		
	Сервер ETS	Сервера Let`s Encrypt	TCP/80,443	
	Сервер Single CTS	Сервера Let`s Encrypt	TCP/80,443	
21	Внешний пользователь	Сервер Single CTS	TCP/443	Клиентский доступ к корпоративному контуру Express с использованием протокола HTTPS
		(Внешний IP NAT)		
22	Внешний пользователь	Сервер ETS	TCP/443	Клиентский доступ к корпоративному контуру Express с использованием протокола HTTPS
23	Внешний пользователь	Сервер Single CTS	TCP/3478	Обеспечение работы протоколов STUN/TURN
		(Внешний IP NAT)	UDP/3478	
		Сервер Single CTS	UDP/20000-40000	Обеспечение передачи медиаданных по протоколу SRTP
		Сервер Single CTS	UDP/49152-65535	
24	Внешний пользователь	Сервер для веб-клиентов	TCP/443	Клиентский доступ к контуру предприятия с использованием протокола HTTPS
25	Сервер Single CTS	Партнерский сервер Express CTS	TCP/443,5001	Обеспечение прямой передачи сообщений между корпоративными серверами минуя публичный контур
	Партнерский сервер Express CTS	Сервер Single CTS		
		(Внешний IP NAT)		
	Сервер Single CTS	Партнерский сервер Express CTS	UDP/20000-40000	Обеспечение передачи медиаданных по протоколу SRTP
	Партнерский сервер Express CTS	Сервер Single CTS		
		(Внешний IP NAT)		

Приложение 4

СЕТЕВЫЕ ВЗАИМОДЕЙСТВИЯ ETS, FRONT CTS И BACK CTS

№	Источник	Получатель	Порт и протокол	Описание
1	Сервер Back CTS	Сервер LDAP	TCP/53	Обеспечение работы разрешения имен DNS
			UDP/53	
			UDP/123	Обеспечение работы службы точного времени NTP
			TCP/389	Обеспечение работы LDAP/LDAPS
			TCP/636	
2	Сервер Back CTS	Bot сервер	TCP/80	Взаимодействие Back CTS с Bot-сервером по протоколу HTTP/HTTPS
			TCP443	
	Bot сервер	Сервер Back CTS	TCP/80	Взаимодействие Bot-сервера с Back CTS по протоколу HTTP/HTTPS
			TCP443	
3	Внутренние ИС	Bot сервер	TCP/80	Взаимодействие внутренних информационных систем с сервером bot по протоколу HTTP/HTTPS
			TCP443	
			TCP8000-8100	
	Bot сервер	Внутренние ИС	TCP/80	Взаимодействие Bot-сервера с внутренними информационными системами по протоколу HTTP /HTTPS
			TCP443	
4	Сервер Back CTS	Docker реестр	TCP/443	Доступ к репозиторию образов Docker для установки и обновления ПО Express
5	Сервер Back CTS	Сервер Front CTS	TCP/80	Мониторинг работы контейнера trusts
			TCP/6379	Обеспечение аутентификации и шифрования голосовых вызовов Express
			TCP/8188	Управление звонками конференцсвязи
6	Сервер Front CTS	Сервер Back CTS	TCP/80	Передача зашифрованных пользовательских данных без транспортной обертки TLS
			TCP/2379	Подключение к хранилищу конфигураций для получения различных настроек сервисов
			TCP/5432	Подключение контейнера trusts к базе данных для хранения информации, необходимой для работы
			TCP/6379	Подключение к Redis
			TCP/9092	Подключение к программному брокеру сообщений Kafka для обмена событиями между сервисами
7	Администратор	Сервер Front CTS и Back CTS	TCP/22	Администрирование серверов по протоколу SSH
			TCP/443	Администрирование Express через веб-интерфейс по протоколу HTTPS
8	Сервер Back CTS	Сервер SMTP	TCP/25	Обеспечение отправки писем с ПИН-кодом аутентификации по протоколу SMTP
9	Сервер ETS	Docker реестр	TCP/443	Доступ к репозиторию образов Docker для установки и обновления ПО Express.

№	Источник	Получатель	Порт и протокол	Описание
10	Сервер ETS	Сервер DNS и NTP	TCP/53	Обеспечение работы разрешения имен DNS
			UDP/53	
			UDP/123	Обеспечение работы службы точного времени NTP
11	Внутренний пользователь	Сервер ETS	TCP/443	Клиентский доступ к корпоративному контуру Express с использованием протокола HTTPS
12	Сервер Front CTS	Сервер ETS	TCP/5001	Обеспечение взаимодействия корпоративного сервера Express с ETS
13	Сервер Front CTS	Docker реестр	TCP/443	Доступ к репозиторию образов Docker для установки и обновления ПО Express
14	Сервер Front CTS	Сервер DNS и NTP	TCP/53	Обеспечение работы разрешения имен DNS
			UDP/53	
			UDP/123	Обеспечение работы службы точного времени NTP
15	Внутренний пользователь	Сервер Front CTS	TCP/443	Клиентский доступ к корпоративному контуру Express с использованием протокола HTTPS
16	Внутренний пользователь	Сервер для веб-клиентов	TCP/443	Подключение внутренних пользователей к веб-клиенту
17	Внутренний пользователь	Сервер Front CTS	UDP/20000-40000 UDP/49152-65535	Обеспечение передачи медиаданных по протоколу SRTP конференцсвязи
			TCP/3478 UDP/3478	Обеспечение работы протоколов STUN/TURN
18	Сервер ETS	SMS оператор	TCP/443	Отправка SMS-сообщений пользователям
19	Сервер ETS	Служба push-уведомлений Huawei	TCP/443	Отправка push-уведомлений пользователям Huawei
20	Сервер ETS	Служба push-уведомлений Apple	TCP/443	Отправка push-уведомлений пользователям iOS
21	Сервер ETS	Служба push-уведомлений Google	TCP/443	Отправка push-уведомлений пользователям Android
22	Сервер ETS	RTS	TCP/5001	Обеспечение взаимодействия CTS с RTS
		ru.public.express		
23	Сервер Let`s Encrypt	Сервер ETS	TCP/80, 443	При использовании бесплатного сертификата от компании Let`s Encrypt
		Сервер Front CTS		
	Сервер ETS	Сервер Let`s Encrypt	TCP/80,443	
	Сервер Front CTS	Сервер Let`s Encrypt	TCP/80,443	
24	Внешний пользователь	Сервер Front CTS	TCP/443	Клиентский доступ к корпоративному контуру Express с использованием протокола HTTPS
25	Внешний пользователь	Сервер ETS	TCP/443	Клиентский доступ к корпоративному контуру Express с использованием протокола HTTPS
26	Внешний пользователь	Сервер Front CTS	TCP/3478	Обеспечение работы протоколов STUN/TURN
		(Внешний IP NAT)	UDP/3478	
			UDP/20000-40000	Обеспечение передачи медиаданных по протоколу SRTP конференцсвязи

№	Источник	Получатель	Порт и протокол	Описание
			UDP/49152-65535	Обеспечение передачи медиаданных по протоколу SRTP голосовых вызовов
27	Внешний пользователь	Сервер Front CTS	TCP/443	Клиентский доступ к корпоративному контуру Express с использованием протокола HTTPS
		(Внешний IP NAT)		
28	Сервер Front CTS	Партнерский сервер Express CTS	TCP/443,5001	Обеспечение взаимодействия CTS с RTS
	(Внешний IP NAT)		UDP/20000-40000	Обеспечение передачи медиаданных по протоколу SRTP конференцсвязи
	Партнерский сервер Express CTS	Сервер Front CTS	TCP/443,5001	Обеспечение взаимодействия CTS и RTS
		(Внешний IP NAT)	UDP/20000-40000	Обеспечение передачи медиаданных по протоколу SRTP конференцсвязи

Приложение 5

МОНИТОРИНГ EXPRESS CTS

Изделие содержит служебный модуль (docker контейнер) с ПО мониторинга Prometheus, который собирает метрики с остальных модулей.

Метрики во встроенном Prometheus хранятся 15 дней, но при необходимости метрики можно передать для длительного хранения в централизованное хранилище, совместимое с Prometheus (например, централизованный сервер Prometheus, работающий в режиме «федерации»).

Метрики условно можно разделить на группы:

- метрики состояния модулей («включен-выключен», «uptime», «время запуска» и т.п.);
- метрики производительности (cpu usage, memory usage и т.д.);
- метрики доступности и т.п.

Метрики формируются разными модулями: node_exporter, cadvisor, redis_exporter и программными средствами внутри модулей СК «Express».

Метрики состояния модулей:

Компоненты	**Модуль**	**Метрика**
Статус контейнеров в docker	Prometheus	up
Статус базы данных Posrgres	Prometheus	pg_up
Статус базы данных Redis	Prometheus	redis_up

Метрики производительности:

Компоненты	**Модуль**	**Метрика**
CPU usage	Zabbix Agent	CPU usage
Memory	Zabbix Agent	Memory usage
Networking	Zabbix Agent	rx/tx rate
SSD	Zabbix Agent	Free space
container: CPU Usage	Prometheus	container_cpu_user_seconds_total
container: Memory Usage	Prometheus	container_memory_usage_bytes
container: SSD	Prometheus	container_fs_writes_bytes_total container_fs_reads_bytes_total
container: Networking	Prometheus	container_network_transmit_bytes_total container_network_receive_bytes_total

Метрики доступности сетевых сервисов:

Компоненты	**Модуль**	**Метрика**
Front	Zabbix Server	TCP/80, 443, 3478, 6379, 8188
Front	Zabbix Server	TCP 5001
Back	Zabbix Server	TCP/80, 443, 5432, 9092

Статистическая информация о системе:

Параметр	Модуль	Метрика
Зарегистрированные пользователи	Prometheus	active_users
Подключенные пользователи к серверу в данный момент	Prometheus	online_users
Общее кол-во работающих Android клиентов	Prometheus	android_users
Общее кол-во пользователей	Prometheus	total_users
Кол-во зарегистрированных пользователей с сортировкой по названию компании	Prometheus	users_count
Общее кол-во работающих Web клиентов	Prometheus	web_users
Общее кол-во переданных сообщений	Prometheus	messages_count
Общее кол-во работающих iOS клиентов	Prometheus	ios_users
Общее кол-во работающих Descktop клиентов	Prometheus	desktop_users
Версии контейнеров Express	Prometheus	express_version
Кол-во пользователей, находящихся в данный момент в звонке	Prometheus	users_in_calls_count
Размер баз данных Postgres	Prometheus	pg_database_size
Статус федеративных подключений	Prometheus	connection_status

Для настройки добавьте в файл settings.yaml параметры:

Примечание. В случае использования раздельной установки параметры добавляются на Back CTS.

```
prometheus_options:
  command:
    - --config.file=/etc/prometheus/prometheus.yml
    - --storage.tsdb.path=/prometheus
    - --storage.tsdb.retention.time=90d
    - --web.console.libraries=/etc/prometheus/console_libraries
    - --web.console.templates=/etc/prometheus/consoles
    - --web.external-url=/system/prometheus
    - --web.route-prefix=/
```

Интерфейс для доступа к Prometheus:

- url – задается в файле settings.yaml;
- username: prometheus;
- password: генерируется в файле settings.yaml при инициализации.

Приложение 6

ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

Ниже представлен список дополнительных возможностей.

Все параметры применяются в файле settings.yaml:

- глобальный уровень логирования:

```
logger_level: warning
```

- Отключение контейнера docker_socket (отключит возможность просмотра логов из административной панели)

```
docker_socket_proxy_enabled: false
```

- Включение на Back и Front CTS межсерверного обмена по https

```
proxy_ssl_enable: true
nginx_listen_http: false
```

- Хранение данных (file_service) S3 и NFS

  Пример настройки подключения к S3 хранилищу:

```
file_service_env_override:
  ADAPTER: s3
  AWS_ACCESS_KEY_ID: access-key
  AWS_SECRET_ACCESS_KEY: secres-access-key
  AWS_S3_URI: https://storage.minio.local
  AWS_S3_BUCKET: cts-files
```

  Пример настройки подключения к NFS хранилищу:

```
ccs_admin_public_driver_opts:
  type: nfs
  o: addr=10.3.4.50,vers=3,rw
  device: ":/export/cts_ccs_admin_public"
file_service_uploads_driver_opts:
  type: nfs
  o: addr=10.3.4.50,rw
  device: ":/export/file_service_uploads"
messaging_uploads_driver_opts:
  type: nfs
  o: addr=10.3.4.50,vers=3,rw
  device: ":/export/messaging_uploads"
phonebook_uploads_driver_opts:
  type: nfs
  o: addr=10.3.4.50,rw
  device: ":/export/phonebook_uploads"
redis_data_driver_opts:
  type: nfs
  o: addr=10.3.4.50,vers=3,rw
  device: ":/export/redis_data"
```

Приложение 7

СЕТЕВАЯ СХЕМА ВЗАИМОДЕЙСТВИЯ С АТС ДЛЯ SINGLE CTS

Сетевая схема взаимодействия с АТС при развертывании Single CTS представлена на Рисунок 57.

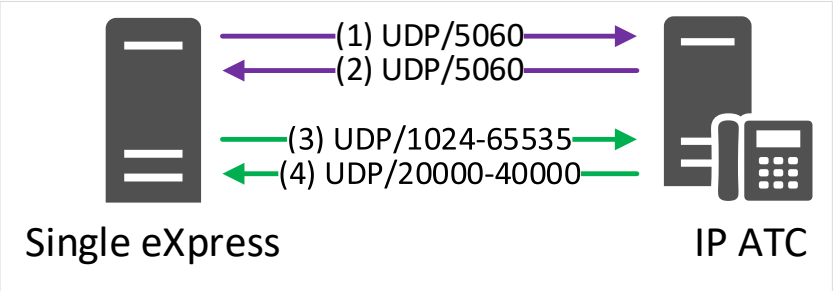


Рисунок 57

Сетевые взаимодействия для схемы развертывания Single (номера соединений в таблице соответствуют номера соединений на Рисунок 57):

Таблица 38

№	IP источника	Порт источника	IP назначения	Порт назначения	Протокол	Описание
1	IP Single eXpress	1024-65535	IP ATC	5060	UDP	SIP сигнализация вызова к IP ATC
2	IP ATC	1024-65535	IP Single eXpress	5060	UDP	SIP сигнализация вызова к eXpress
3	IP Single eXpress	20000-40000	IP ATC	1024-65535	UDP	Медиаданные вызова к IP ATC
4	IP ATC	1024-65535	IP Single eXpress	20000-40000	UDP	Медиаданные вызова к eXpress

Приложение 8

СЕТЕВАЯ СХЕМА ВЗАИМОДЕЙСТВИЯ С АТС ПРИ РАЗВЕРТЫВАНИИ FRONT CTS + VOEX И BACK CTS

Сетевая схема взаимодействия с АТС при развертывании Front CTS + VoEx и Back CTS представлена на Рисунок 58.

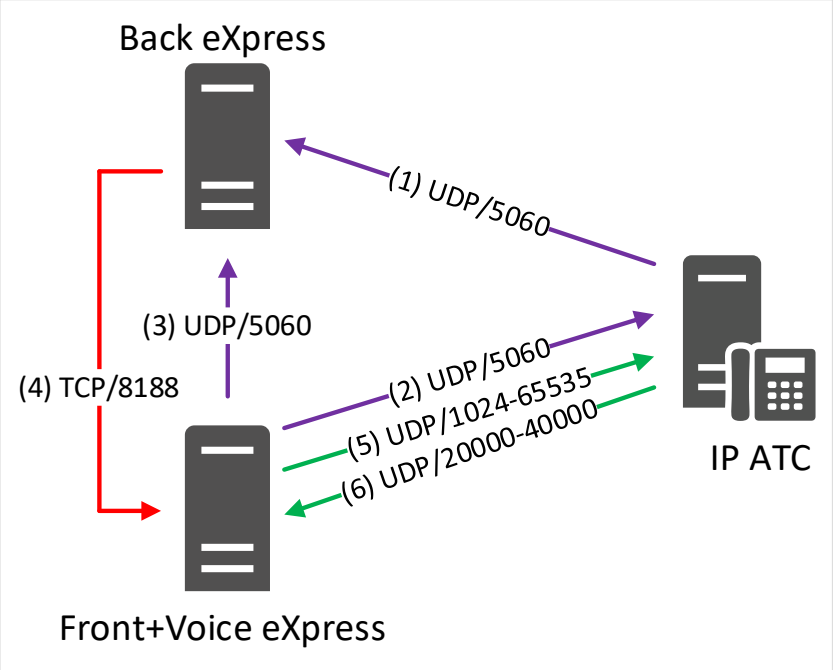


Рисунок 58

Сетевые взаимодействия для схемы развертывания Front CTS + VoEx и Back CTS номера соединений в таблице соответствуют номерам на схеме (Рисунок 58):

Таблица 39

№	IP источника	Порт источника	IP назначения	Порт назначения	Протокол	Описание
1	IP ATC	1024-65535	IP Back eXpress	5060	UDP	SIP сигнализация вызова к eXpress
2	IP Front+Voice eXpress	1024-65535	IP ATC	5060	UDP	SIP сигнализация вызова к IP ATC
3	IP Front+Voice eXpress	1024-65535	IP Back eXpress	5060	UDP	SIP сигнализация вызова к eXpress Back
4	IP Back eXpress	1024-65535	IP Front+Voice eXpress	8188	TCP	Управление работой сервера конференций
5	IP Front+Voice eXpress	20000-40000	IP ATC	1024-65535	UDP	Медиаданные вызова к IP ATC
6	IP ATC	1024-65535	IP Front+Voice eXpress	20000-40000	UDP	Медиаданные вызова к eXpress