UNLIMITED PRODUCTION

eXpress
Система коммуникаций

Руководство администратора

Установка

Сборка 3.14
03.04.2024

Почтовый адрес:	127030, г. Москва, ул. Новослободская, д. 24, стр. 1
Телефон:	+7 (499) 288-01-22
E-mail:	sales@express.ms
Web:	https://express.ms/

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ **6**
ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ **7**
ГЛАВА 1
ОБЩИЕ СВЕДЕНИЯ **8**
Назначение комплекса **8**
Основные функции **8**
Основные компоненты **8**
Доступные роли **10**
Архитектура **11**
Региональный сервер 11
Единый корпоративный сервер 13
Разделенный корпоративный сервер 14
Сервер предприятия и единый корпоративный сервер 17
Сервер предприятия и разделенный корпоративный сервер 18
Системные требования **20**
Требования к платформе 20
Требования к DNS 24
Требования к сертификату 24
Требования к корпоративному каталогу LDAP 25
Требования к серверу SMTP 25
Требования к сетевым взаимодействиям 25
Требования к серверу VoEx (STUN/TURN) 25
Требования хранению файлов записей ВКС 25
Требования к DLP 26
ГЛАВА 2
УСТАНОВКА EXPRESS **27**
Предварительная настройка **27**
ОС Ubuntu/Debian 27
ОС Centos/RHEL 29
ОС Astra Linux Орел 30
Установка сервера VoEx **32**
Предварительная настройка 32
Установка сервера VoEx 33
Установка корпоративного сервера Express **35**
Установка Single CTS 35
Установка Front CTS- и Back CTS-серверов 37
Настройка сервера VoEx **41**
Настройка сервера VoEx (STUN и TURN) 41
Настройка интеграции с модулем ВКС Vinteo: 43
Настройка IP-телефонии 43

Установка веб-клиента ... 45
Установка сервиса ссылок ... 46
Установка DLP ... 47
Установка DLP на выделенном сервере ... 47
Установка DLP на Single CTS ... 49
Установка DLP на Single CTS с хранением ключей на внешнем носителе ... 50
Установка компонентов записи звонков и конференций ... 51
Установка RTS и ETS ... 51
Проверка сертификатов ... 52
Запуск сервера ... 52

ГЛАВА 3

НАСТРОЙКА СЕРВЕРА ... 54
Настройка RTS ... 54
Подключение TLS-сертификата ... 55
Настройка видео- и голосовой связи ... 55
Подключение SMTP-сервера ... 55
Настройка push-уведомлений ... 56
Настройка CMC-сервиса ... 64
Настройка аутентификации администраторов ... 67
Настройка подключений корпоративных серверов и серверов предприятия ... 68
Настройка ETS ... 72
Подключение TLS-сертификата ... 73
Настройка видео- и голосовой связи ... 73
Подключение SMTP-сервера ... 73
Настройка push-уведомлений ... 74
Настройка CMC-сервиса ... 82
Настройка аутентификации администраторов ... 85
Настройка подключений корпоративных серверов ... 86
Настройка CTS ... 90
Подключение TLS-сертификата и Botx SSL-сертификата ... 91
Настройка видео- и голосовой связи ... 92
Подключение SMTP-сервера ... 92
Настройка аутентификации администраторов ... 93
Настройка регистрации ... 94
Настройка доверительных подключений ... 101

ГЛАВА 4
ПРОЦЕДУРА ОБНОВЛЕНИЯ 103
ГЛАВА 5
УСТРАНЕНИЕ ТИПОВЫХ ОШИБОК 104
ПРИЛОЖЕНИЕ 1
СЕТЕВЫЕ ВЗАИМОДЕЙСТВИЯ SINGLE CTS 106
ПРИЛОЖЕНИЕ 2
СЕТЕВЫЕ ВЗАИМОДЕЙСТВИЯ FRONT CTS И BACK CTS 109
ПРИЛОЖЕНИЕ 3
СЕТЕВЫЕ ВЗАИМОДЕЙСТВИЯ ETS И SINGLE CTS 111
ПРИЛОЖЕНИЕ 4
СЕТЕВЫЕ ВЗАИМОДЕЙСТВИЯ ETS, FRONT CTS И BACK CTS 113
ПРИЛОЖЕНИЕ 5
МОНИТОРИНГ EXPRESS CTS 116
ПРИЛОЖЕНИЕ 6
ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ 118
ПРИЛОЖЕНИЕ 7
НАСТРОЙКА ХОСТОВ SMARTAPPPROXY 119
ПРИЛОЖЕНИЕ 8
СЕТЕВАЯ СХЕМА ВЗАИМОДЕЙСТВИЯ С АТС ДЛЯ SINGLE CTS 120
ПРИЛОЖЕНИЕ 9
СЕТЕВАЯ СХЕМА ВЗАИМОДЕЙСТВИЯ С АТС ПРИ РАЗВЕРТЫВАНИИ FRONT CTS + VOEX И BACK CTS 121
ПРИЛОЖЕНИЕ 10
ИНТЕГРАЦИЯ CTS И KEYCLOAK 122
Этапы регистрации/авторизации 122
Сетевые взаимодействия 123
Настройка интеграции 123
Создание client scope 124
Настройка маппинга полей 125
Создание client 128
Настройка отображения формы авторизации Keycloak 129
Настройка авторизации по QR-коду 129
ИСТОРИЯ ИЗМЕНЕНИЙ 130

ВВЕДЕНИЕ

Руководство предназначено для администраторов изделия «Система коммуникаций «Express» (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/faq/.

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

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термин	Определение
AD	Active Directory — служба каталогов корпорации Microsoft для операционных систем семейства Windows Server
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
SIP	Session Initiation Protocol — протокол передачи данных, описывающий способ установки и завершения пользовательского интернет-сеанса, включающего обмен мультимедийным содержимым (IP-телефония, видео- и аудиоконференции, мгновенные сообщения)
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
АТС	Автоматическая телефонная станция компании
Виджет	Конструктивный элемент панели, отвечающий за визуальный вывод части информации, собранной системой
ВКС	Видеоконференцсвязь
Кеш	Промежуточный буфер с быстрым доступом, содержащий информацию, которая может быть запрошена с наибольшей вероятностью
КСПД	Корпоративная сеть передачи данных
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» предназначена 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

СК «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;
- обеспечение безопасного хранения и передачи конфиденциальных данных;
- создание копии данных для восстановления работоспособности подсистемы в случае ее повреждения или разрушения;
- оптимизация использования ресурсов;
- осуществление персональных и групповых аудио- и видеозвонков;
- запись звонков и видеоконференций.

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 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»; • записями из AD
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

Для интеграции с системами предотвращения утечки данных, обеспечивающих проверку сообщений пользователей на наличие запрещенного контента, используется протокол ICAP (порт TCP/1344).

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

Важно! В данном документе рассматривается неотказоустойчивая конфигурация изделия. Для получения сведений о вариантах отказоустойчивой конфигурации обратитесь к разработчику.

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);
- разделенный сервер Express (Front CTS и Back CTS).

ETS поддерживает 2 вида развертывания:

- ETS и единый сервер Express (Single CTS);
- ETS и разделенный сервер Express (Front CTS и Back CTS).

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.

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);
- conference_bot (бот для уведомлений о предстоящих конференциях; отправляет ссылку на сохраненную запись при совершении личных звонков);

- 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);
- janus (сервис для групповых звонков);
- kafka (диспетчер сообщений между сервисами);
- kdc (хранилище ключей);
- messaging (сервис обмена сообщениями, отвечает за подключение клиентов через протокол websocket);
- nginx (веб-сервер, который отвечает за маршрутизацию внутренних подключений);
- notifications_bot (бот для отправки сообщений в глобальный чат);
- phonebook (адресная книга);
- postgres (основная база данных сервисов);
- postgres_exporter (отвечает за снятие метрик с postgres);
- 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);
- redis_exporter (отвечает за снятие метрик с redis);
- 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).

ЕДИНЫЙ КОРПОРАТИВНЫЙ СЕРВЕР

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

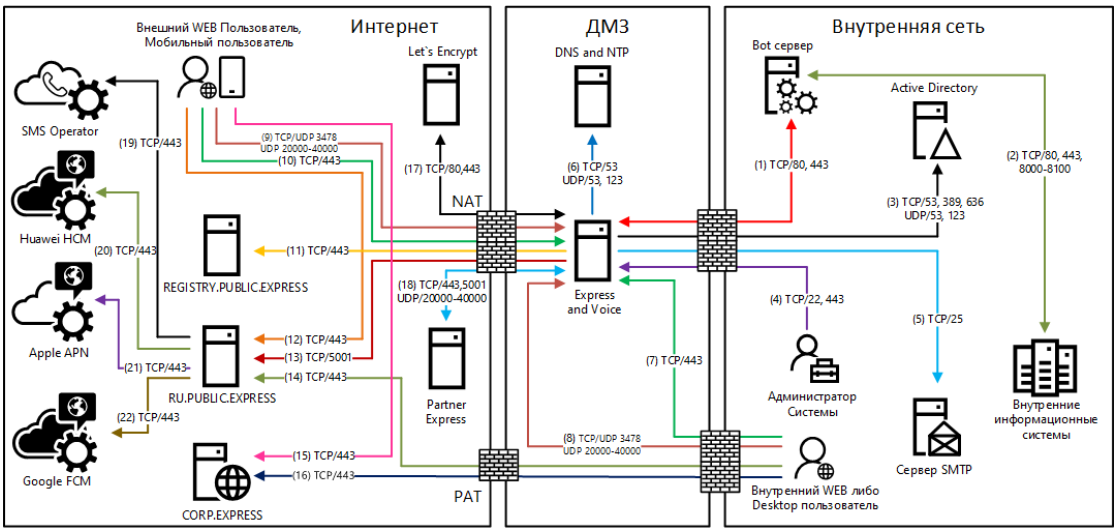

Рисунок 1. Типовая схема развертывания Single CTS

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.

Сетевая схема взаимодействия с АТС при развертывании Single CTS и сетевые взаимодействия для данной схемы развертывания представлены в Приложении 8.

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

- ad_integration (интегрируется с Active Directory и другими LDAP-сервисами, отвечает за авторизацию клиента с помощью NTLM и AD);
- admin (интерфейс администратора);
- apigw (сервис информирования пользователей о событиях в чатах);
- audit (сервис аудита подключений);
- botx (отвечает за интеграцию с ботами);
- conference_bot (бот для уведомлений о предстоящих конференциях; отправляет ссылку на сохраненную запись при совершении личных звонков);
- corporate_directory (каталог открытых ботов и чатов);
- docker_socket_proxy (отвечает за ограничения доступа к сокету Docker);
- 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);
- janus (сервис для групповых звонков);

- 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);
- phonebook (адресная книга);
- postgres (основная база данных сервисов);
- postgres_exporter (отвечает за снятие метрик с postgres);
- prometheus (отвечает за снятие, обработку и хранение метрик сервисов);
- recordings_bot (бот, который посылает ссылку на файл записи после завершения кодирования);
- redis (KV-хранилище);
- redis_exporter (отвечает за снятие метрик с redis);
- routing_schema (сервис построения схем роутинга, визуализирует схему маршрутизации в чатах);
- settings (отвечает за хранение настроек сервисов);
- smartapp_proxy (отвечает за обмен файлами между SmartApp и сервером CTS);
- traefik (отвечает за получение сертификатов от LE и терминация TLS на входе);
- transcoding (отвечает за перекодировку записи в выходной формат);
- transcoding_manager (управляет процессом кодирования);
- trusts (отвечает за обмен событиями между RTS, ETS и CTS, а также за взаимодействие с другими серверами Express);
- voex (сервис для совершения аудиовызовов).

РАЗДЕЛЕННЫЙ КОРПОРАТИВНЫЙ СЕРВЕР

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

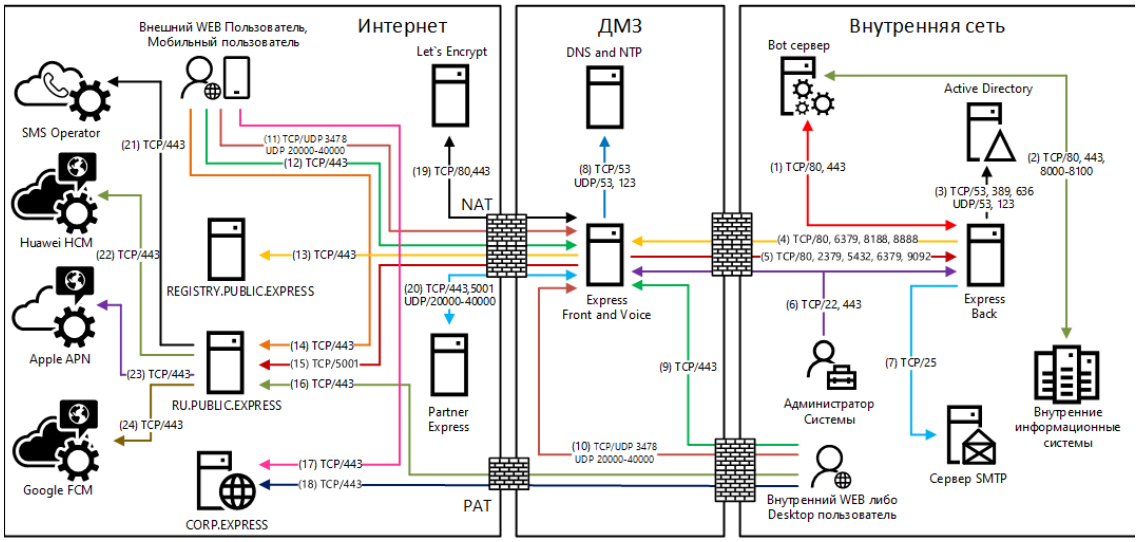

Рисунок 2. Типовая схема развертывания разделенного CTS (Front/Back)

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.

Сетевая схема взаимодействия с АТС при развертывании Front CTS + VoEx и Back CTS и сетевые взаимодействия для данной схемы развертывания представлены в Приложении 9.

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

- nginx (веб-сервер, который отвечает за маршрутизацию внутренних подключений);
- prometheus (отвечает за снятие, обработку и хранение метрик сервисов);
- traefik (отвечает за получение сертификатов от LE и терминация TLS на входе);
- transcoding (отвечает за перекодировку записи в выходной формат);
- 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);
- janus (сервис для групповых звонков).

При установке рекомендуется использовать отдельный системный Redis.

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

- ad_integration (интегрируется с Active Directory и другими LDAP-сервисами, отвечает за авторизацию клиента с помощью NTLM и AD);
- admin (интерфейс администратора);
- audit (сервис аудита подключений);
- apigw (сервис информирования пользователей о событиях в чатах);
- botx (отвечает за интеграцию с ботами);
- conference_bot (бот для уведомлений о предстоящих конференциях; отправляет ссылку на сохраненную запись при совершении личных звонков);
- corporate_directory (каталог открытых ботов и чатов);
- docker_socket_proxy (отвечает за ограничения доступа к сокету Docker);
- 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);
- phonebook (адресная книга);
- postgres (основная база данных сервисов);
- postgres_exporter (отвечает за снятие метрик с postgres);
- prometheus (отвечает за снятие, обработку и хранение метрик сервисов);
- recordings_bot (бот, который посылает ссылку на файл записи после завершения кодирования);
- redis (KV-хранилище)[1];
- redis_exporter (отвечает за снятие метрик с redis);
- routing_schema (сервис построения схем роутинга, визуализирует схему маршрутизации в чатах);
- smartapp_proxy (отвечает за обмен файлами между SmartApp и сервером CTS);
- settings (отвечает за хранение настроек сервисов);
- traefik (отвечает за получение сертификатов от LE и терминацию TLS на входе);
- transcoding_manager (управляет процессом кодирования);
- 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;
- voex (сервис для совершения аудиовызовов).

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

СЕРВЕР ПРЕДПРИЯТИЯ И ЕДИНЫЙ КОРПОРАТИВНЫЙ СЕРВЕР

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

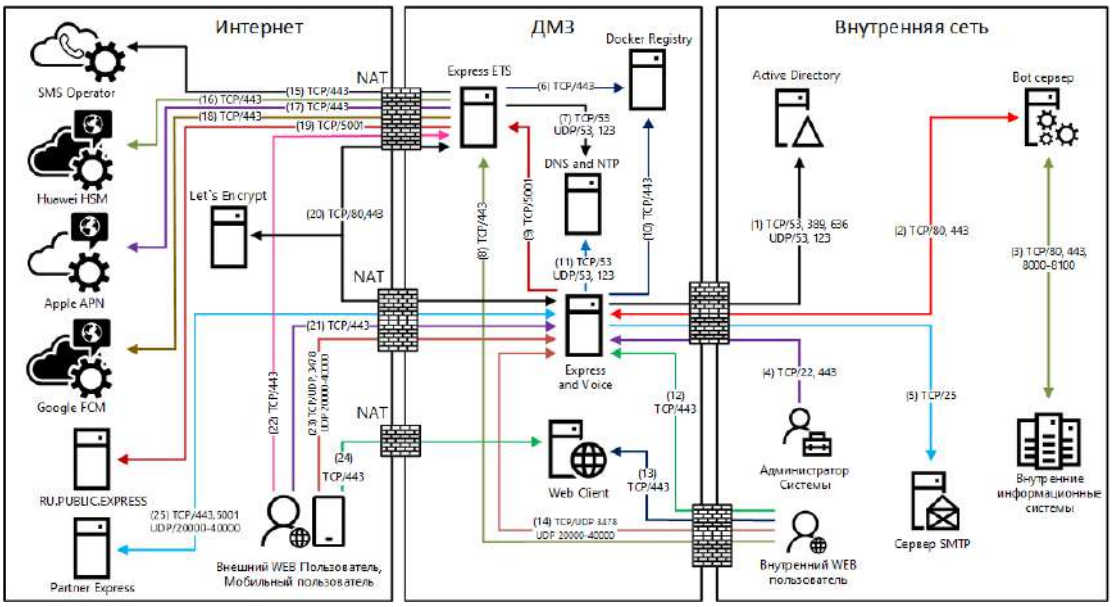

Рисунок 3. Типовая схема развертывания ETS и Single CTS

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);
- janus (сервис для групповых звонков);
- 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);
- phonebook (адресная книга);

- postgres (основная база данных сервисов);
- postgres_exporter (отвечает за снятие метрик с postgres);
- 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);
- redis_exporter (за снятие метрик с redis);
- settings (отвечает за хранение настроек сервисов);
- sms_service (сервис для отправки СМС-сообщений);
- stickers (сервис для управления стикерами);
- traefik (отвечает за получение сертификатов от LE и терминация TLS на входе);
- 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).

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 4.

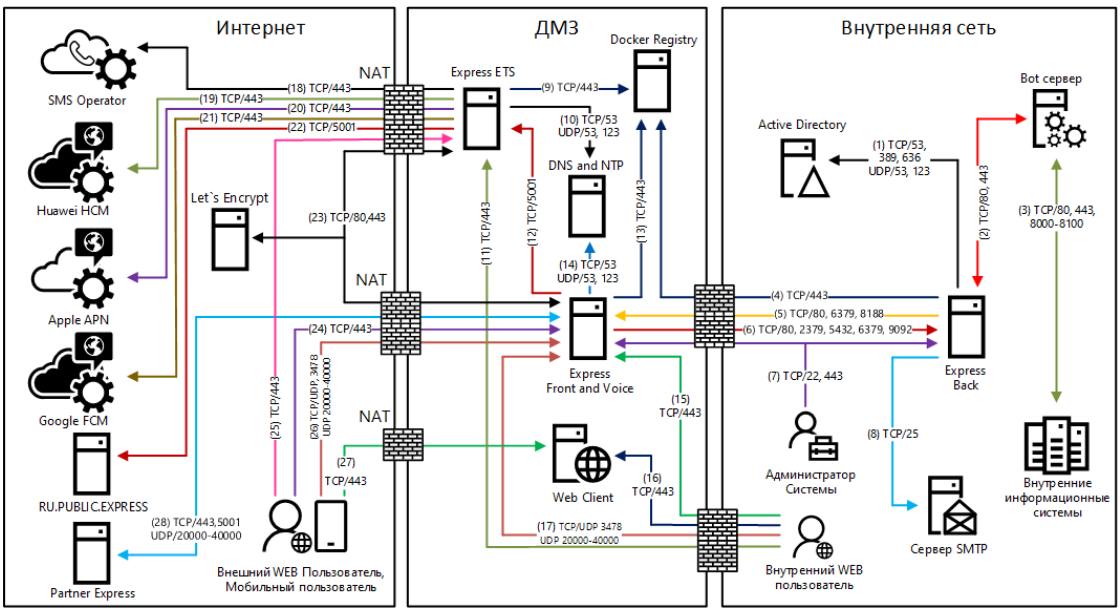

Рисунок 4. Типовая схема развертывания ETS, Front CTS и Back CTS

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 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);
- janus (сервис для групповых звонков);
- 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);
- phonebook (адресная книга);
- postgres (основная база данных сервисов);
- postgres_exporter (отвечает за снятие метрик с postgres);
- 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)**1**;
- redis_exporter (за снятие метрик с redis);
- settings (отвечает за хранение настроек сервисов);
- sms_service (сервис для отправки СМС-сообщений);
- stickers (сервис для управления стикерами);
- traefik (отвечает за получение сертификатов от LE и терминация TLS на входе);
- 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.

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

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
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
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**

Таблица 15 – Количество пользователей:5000

Роль сервера	vCPU/CPU Core	RAM Гб	SSD Гб	IOps
Front CTS	20	18	45	13
Back CTS	28	48	7389	523
Bot	10	18	1045	105
Всего	**58**	**84**	**8449**	**641**

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 (без отказоустойчивости):

Таблица 16

Элемент	Параметры
Процессор	4 ядра, частота не менее 3.60 ГГц
Оперативная память	16 Гб
Операционная система	• Ubuntu 22.04 LTS; • CentOS 7; • Centos Stream 8; • RHEL 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 и 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8; • РЕД ОС 7.2 и 7.3; • Astra Linux Special Edition 1.6 и 1.7
Жесткий диск	Не менее 500 Гб
Предустановленное ПО	• Docker-ce версии 20.10.23; • PostgreSQL версии 12 и выше; • etcd версии 3.5.x; • kafka версии 2.12-2.6.0 или 2.13-2.7.0
Сетевой адаптер	Ethernet

Минимальные системные требования к серверу ETS для установки подсистем (без отказоустойчивости):

Таблица 17

Элемент	Параметры
Процессор	4 ядра, частота не менее 3.60 ГГц
Оперативная память	16 Гб
Операционная система	• Ubuntu 22.04 LTS; • CentOS 7; • Centos Stream 8; • RHEL 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 и 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8; • РЕД ОС 7.2 и 7.3; • Astra Linux Special Edition 1.6 и 1.7
Жесткий диск	Не менее 500 Гб

Элемент	Параметры
Предустановленное ПО	• Docker-ce версии 20.10.23; • PostgreSQL версии 12 и выше; • etcd версии 3.5.x; • kafka версии 2.12-2.6.0 или 2.13-2.7.0
Сетевой адаптер	Ethernet

Минимальные системные требования к серверу RTS для установки подсистем (без отказоустойчивости):

Таблица 18

Элемент	Параметры
Процессор	4 ядра, частота не менее 3.60 ГГц
Оперативная память	16 Гб
Операционная система	• Ubuntu 22.04 LTS; • CentOS 7; • Centos Stream 8; • RHEL 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 и 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8; • РЕД ОС 7.2 и 7.3; • Astra Linux Special Edition 1.6 и 1.7
Жесткий диск	Не менее 500 Гб
Предустановленное ПО	• Docker-ce версии 20.10.23; • PostgreSQL версии 12 и выше; • Apache Cassandra версии 3.11.4; • etcd версии 3.5.x; • kafka версии 2.12-2.6.0 или 2.13-2.7.0
Сетевой адаптер	Ethernet

Требование к операционной системе: Серверы CTS, ETC, RTS поддерживают любую ОС семейства Linux, на который устанавливается Docker 20.10.23. Рекомендуется Ubuntu 20.04 LTS или Ubuntu 18.04 LTS.

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[1]).

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 19

Браузер	Версия
Google Chrome	118
Chromium	120
Yandex Browser	23
Firefox	120
Opera	100
Edge	118

[1] https://docs.docker.com/install/linux/docker-ce/ubuntu/

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).

```
-----BEGIN CERTIFICATE-----
Base64 server certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Base64 intermediate ca
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Base64 root ca
-----END CERTIFICATE-----
```

Рисунок 5

Поддерживается использование бесплатного сертификата от компании Let`s Encrypt.

ТРЕБОВАНИЯ К КОРПОРАТИВНОМУ КАТАЛОГУ LDAP

При интеграции Express с корпоративным каталогом на базе Microsoft Active Directory требуется создание учетной записи с правами «Domain Users» и контейнера «deleted objects»[1].

Стандартной практикой предоставления доступа пользователей к Express является создание группы пользователей Express в Active Directory. Тип группы — «Security», видимость группы — «Universal».

При интеграции Express с корпоративным каталогом на базе LDAP-совместимого сервера требуется создание учетной записи с правами чтения каталога.

При использовании каталога AD LDS авторизация пользователей осуществляется только по ПИН-коду на email.

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 (STUN/TURN)

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

Таблица 20

Кол-во пользователей	vCPU/CPU Core	RAM Гб	SSD 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 ХРАНЕНИЮ ФАЙЛОВ ЗАПИСЕЙ ВКС

В процессе записи конференции файлы создаются в максимально доступном качестве и затем сжимаются до расширения 1920x1080 пикселей.

Успешно созданные файлы хранятся на сервере CTS.

[1] https://docs.microsoft.com/ru-ru/troubleshoot/windows-server/identity/non-administrators-view-deleted-object-container

На сервере VoEx хранятся временные файлы, которые удаляются после завершения записи. Если запись не была завершена из-за сбоев или ошибок, файлы хранятся на сервере VoEx в течение 48 часов.

Для хранения файлов и стабильного процесса записи необходимо обеспечить соответствующий объем памяти на сервере VoEx и CTS.

Приблизительный объем файлов в зависимости от режима записи представлен в таблице ниже:

Таблица 21

Длительность записи	Описание	Объем файла
10 минут	Аудиозапись. Запись звука с микрофонов участников	9.2 Мб
10 минут	Видеотрансляция. Запись видеотрансляции и звука с микрофонов участников	16.4 Мб
10 минут	Демонстрация экрана. Запись демонстрации экрана и звука с микрофонов участников	53.7 Мб

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;
- LDAP-серверу при авторизации по LDAP;
- 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
Redis	TCP	6379
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;
2) предварительная настройка VoEx;
3) установка сервера VoEx;
4) установка корпоративного сервера;
5) настройка сервера VoEx;
6) установка регионального сервера и/или сервера предприятия;
7) запуск сервера;
8) настройка сервера:
   - RTS;
   - ETS;
   - CTS.

ПРЕДВАРИТЕЛЬНАЯ НАСТРОЙКА

Для корректной работы сервера выполните предварительную настройку.

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

Предварительная настройка зависит от ОС.

ОС UBUNTU/DEBIAN

Для предварительной настройки при использовании ОС Ubuntu/Debian:

1. Установите ОС Ubuntu 20.04 LTS или Ubuntu 18.04 LTS. Воспользуйтесь официальным источником для установки дистрибутива:

   ```
   https://ubuntu.com/download/server
   ```

   Внимание! Во время установки ОС выделите под рутовый «/» раздел 32 Гб, под SWAP раздел выделить 8 Гб, оставшееся место выделите под раздел «/var/lib/docker».

2. Удалите пакеты snapd и ufw с помощью команды:

   ```
   apt autoremove --purge snapd ufw
   ```

3. Установите программное обеспечение Docker. Для установки воспользуйтесь официальным источником:

   ```
   https://docs.docker.com/install/linux/docker-ce/ubuntu/
   ```

   Внимание! Если ПО Docker распаковано из пакета snapd, удалите его и выполните установку из официального источника.

   Пример кода для установки Docker:

   ```
   apt-get remove docker docker-engine docker.io containerd runc
   apt-get update
   apt-get install ca-certificates curl gnupg lsb-release
   curl -fsSL https://download.docker.com/linux/ubuntu/gpg | gpg --
   dearmor -o /usr/share/keyrings/docker-archive-keyring.gpg
   ```

```
echo \ "deb [arch=$(dpkg --print-architecture)
signedby=/usr/share/keyrings/docker-archive-keyring.gpg]
https://download.docker.com/linux/ubuntu \ $(lsb_release -cs)
stable" | tee /etc/apt/sources.list.d/docker.list > /dev/null
apt-get update
apt-get install docker-ce docker-ce-cli containerd.io
```

4. Установите дополнительное ПО (см. ниже).

Для установки дополнительного ПО:

1. Выполните установку NTP-сервера с помощью команды:

```
apt install chrony
```

Если имеются источники точного времени внутри компании, в файл /etc/chrony/chrony.conf внесите серверы[1] NTP в виде:

```
server ntp1.local
server ntp2.local
server ntp3.local
```

Пример кода:

```
systemctl enable chrony
systemctl restart chrony
```

Для проверки подключения к NTP-серверам используйте следующую команду:

```
chronyc sources -v
```

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
```

4. Проверьте цепочку SSL-сертификатов и убедитесь в правильном порядке набора сертификатов (см. стр. 24).
5. Проверьте правильность настроек сервера[2]:

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
Открытые порты AD сервера	389, TCP	Подключение к серверу AD для целей авторизации пользователей и получения их списка
Открытые порты AD сервера	636, TCP	TLS-подключение к серверу AD авторизации и получения списка пользователей
Открытые порты CTS	443, TCP	HTTPS-подключение мобильных клиентов к CTS

[1] Подразумеваются сервера заказчика, которые используют NTP-сервера.

[2] 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 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]	
Учетная запись Microsoft AD	Активная учетная запись с доступом к чтению выбранной группы и deleted objects	Получение списка пользователей

6. 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 – токен для приема подключения от удаленного сервера, token_for_connect – токен для подключения к удаленному серверу.

ОС CENTOS/RHEL

Для предварительной настройки при использовании ОС Centos/RHEL:

1. Установите ОС Centos/RHEL.
2. Удалите firewalld с помощью команды:

```
systemctl disable firewalld
```

   или:

```
systemctl stop firewalld
```

3. Переведите SElinux в режим Permissive, отредактировав файл /etc/selinux/config.
4. Установите программное обеспечение Docker. Для установки воспользуйтесь официальным источником[2].

[1] Могут быть предоставлены компанией разработчиком.
[2] https://docs.docker.com/engine/install/centos/

5. Установите NTP-сервер (см. ниже).

Для установки NTP-сервера:

1. Выполните установку NTP-сервера с помощью команды:

```
yum install chrony
```

2. Если имеются источники точного времени внутри компании, в файл /etc/chrony.conf внесите серверы[1] NTP в виде:

```
server ntp1.local
server ntp2.local
server ntp3.local
```

Пример кода:

```
systemctl enable chrony
systemctl start chrony
```

Для проверки подключения к NTP-серверам используйте следующую команду:

```
chronyc sources -v
```

ОС ASTRA LINUX ОРЕЛ

Для предварительной настройки при использовании ОС Astra Linux Орел:

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

```
apt install docker.io
```

3. Установите дополнительное ПО (см. ниже).

Для установки дополнительного ПО:

1. Выполните установку NTP-сервера с помощью команды:

```
apt install chrony
```

Если имеются источники точного времени внутри компании, в файл /etc/chrony/chrony.conf внесите серверы[2] NTP.

Удалите или закомментируйте строку pool и укажите свои сервера.

Пример:

```
server ntp1.local
server ntp2.local
server ntp3.local
```

2. Перезапустите службу для применения изменений:

```
systemctl restart chrony
```

Для проверки подключения к NTP-серверам используйте следующую команду:

```
chronyc sources -v
```

3. Получите права root с помощью команды:

```
sudo -s
```

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

```
{
"log-driver": "json-file",
```

[1] Подразумеваются сервера заказчика, которые используют NTP-сервера.
[2] Подразумеваются сервера заказчика, которые используют NTP-сервера.

```
 "log-opts": {
       "max-size": "1g"
 }
}
```

5. Выполните:

```
systemctl restart docker
```

6. Проверьте цепочку SSL-сертификатов и убедитесь в правильном порядке набора сертификатов (см. стр. 24).

7. Проверьте правильность настроек сервера[1]:

Таблица 26

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
Открытые порты AD сервера	389, TCP	Подключение к серверу AD для целей авторизации пользователей и получения их списка
Открытые порты AD сервера	636, TCP	TLS-подключение к серверу AD авторизации и получения списка пользователей
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[2]	
Учетная запись Microsoft AD	Активная учетная запись с доступом к чтению выбранной группы и deleted objects	Получение списка пользователей

8. Запросите у разработчика следующие индивидуальные параметры для установки (параметры предоставляются по FQDN конкретного сервера):

[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.
[2] Могут быть предоставлены компанией разработчиком.

- 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.

УСТАНОВКА СЕРВЕРА VOEX

Сервер VoEx (STUN/TURN сервер) предназначен для организации видео- и аудиосвязи между пользователями. Видео использует по умолчанию кодек VP8, битрейт 120 kbps, 360 kbps, 1080 kbps 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. 27).

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 27).

Таблица 27

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	MCU	20000-40000	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. Скачайте контейнер-инсталлятор.

```
docker run --rm registry.public.express/dpl:cts-release dpl-
install | bash
```

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
echo DPL_IMAGE_TAG=voex-release > dpl.env
dpl --init
```

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: []
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 28

Название настройки	Значение
external_interface	Наименование интерфейса с внешним IP-адресом[1]
janus_keep_private_host	Включение согласования подключения на все локальные ip-адреса сервера
janus_ws_acl	Адреса или сети серверов, на которых расположен контейнер messaging (например, 172.18.0.)
janus_ws_ip - ip	Интерфейс, который использует janus websocket для управления конференциями сервисом messaging
nat_1_1_mapping keep_private_host	При использовании NAT 1:1 указывается внешний IP-адрес и включается режим сохранения приватного IP-адреса
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: []
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
redis_userdb, redis_statsdb	Параметры подключения coturn к redis серверу (ip-адрес, порт, пароль, номер базы данных)
turnserver_external_ip	Внешний IP-адрес
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

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_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 проверьте наличие параметра permit_ip в settings.yaml:

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

11. Установите systemd unit в систему и запустите:

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

12. Выполните команду:

```
dpl -d
```

[1] IP-адрес должен быть «белым».

УСТАНОВКА КОРПОРАТИВНОГО СЕРВЕРА EXPRESS

Важно! Перед началом процедуры установки необходимо установить VoEx (см. стр. 32).

УСТАНОВКА SINGLE CTS

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

Для установки CTS:

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. Скачайте контейнер-инсталлятор.

   ```
   docker run --rm registry.public.express/dpl:cts-release dpl-install | bash
   ```

   Из репозитория на сервер скачается файл в формате YAML с контейнерами и инсталлятор.
4. Создайте рабочий каталог CTS.

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

   После выполнения команды dpl --init создается файл settings.yaml.
5. 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. 24.
   - 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. 52.
6. Выполните настройку DLP для доступа администраторов безопасности к содержимому сообщений (параметры настройки см. стр.49).
7. 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
```

8. 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:

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

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. Для предотвращения ошибок рекомендуется заменить параметры сгенерированного файла параметрами, выданными разработчиками. 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.

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

Таблица 29

Название настройки	Значение
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)

Название настройки	Значение
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

sip_trunk_enable: true	Параметр устанавливается для использования вызовов через SIP-телефонию. После добавления параметра выполните в каталоге /opt/express команду
	`- dpl -d messaging`
	`ss -stuln | grep 5060`

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. 36:

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

При первой возможности замените значение verystrongpassword на более сложное.

УСТАНОВКА FRONT CTS- И BACK CTS-СЕРВЕРОВ

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

Для установки Front CTS:

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. Скачайте контейнер-инсталлятор.

   ```
   docker run --rm registry.public.express/dpl:cts-release dpl-
   install | bash
   ```

   Из репозитория на сервер скачается файл в формате YAML с контейнерами и инсталлятор.
4. Создайте рабочий каталог Front CTS:

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

```
dpl --init
```

5. 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. 24.

   - 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. 52.

6. Откройте для редактирования конфигурационный файл settings.yaml, добавив добавьте следующие параметры:

```
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.

7. Отредактируйте конфигурационный файл settings.yaml, добавив 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. 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. Скачайте контейнер-инсталлятор.

```
docker run --rm registry.public.express/dpl:cts-release dpl-
install | bash
```

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

4. Создайте рабочий каталог Back CTS.

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

5. 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. 24.

   - 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. 52.

6. Скопируйте файл конфигурации с Front CTS (/opt/express/settings.yaml) на сервер Back CTS и разместите его в папке /opt/express.
7. 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
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
```

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.

8. При редактировании файла конфигурации удалите дополнительные настройки:

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

добавьте следующий параметр:

```
cts_backend: true
```

и отредактируйте параметры (подставив соответсвующие значения frontend_name.somedomain.sometld и backend_name.somedomain.sometld):

```
voex_redis_connection_string:
redis://frontend_name.somedomain.sometld:6379/1
janus_url: ws://frontend_name.somedomain.sometld:8188
kafka_advertised_host_name: backend_name.somedomain.sometld
```

9. 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 - apt-get install -y tinyproxy
RHEL\CentOS - yum install -y epel-release
RHEL\CentOS - 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:

```
systemctl restart tinyproxy
```

НАСТРОЙКА СЕРВЕРА VOEX

Настройка сервера VoEx включает в себя:

- настройку серверов STUN и TURN (обязательная настройка);
- настройку интеграции Vinteo (опциональная настройка);
- настройку IP-телефонии (опциональная настройка).

НАСТРОЙКА СЕРВЕРА VOEX (STUN И TURN)

Для настройки сервера VoEx (STUN и TURN):

1. Запустите сервер VoEx в командной строке командой:

```
dpl -d
```

2. Откройте консоль администратора.
3. В разделе «VoEx» (Рисунок 6) для включения функции логирования звонков установите отметку «Включить логирование звонков», введите данные в поле «Период очистки логов звонков».
4. 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»;
   - в поле «STUN Server (через запятую)» введите внешний FQDN вашего сервера и через двоеточие номер порта, например «express.firma.ru:3478».

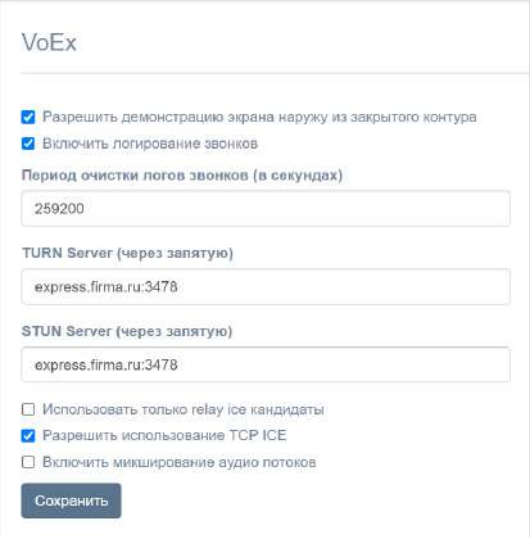

Рисунок 6

5. Поставьте следующие отметки, если это необходимо (Таблица 30):

Таблица 30

Настройка	Описание
Разрешить демонстрацию экрана наружу из закрытого контура	Возможность демонстрировать экран своих устройств другим пользователям, находящимся за пределами КСПД (RTS-пользователям, пользователям трастовых серверов, пользователям, покинувшим зону КСПД)
Использовать только relay ice кандидаты	Принудительное использование TURN сервера
Разрешить использование TCP ICE	Запрещает использование TCP в TURN сервере
Включить микширование аудио потоков	Объединяет аудиопотоки звонков, направленные от пользователей к серверу, в один поток

Примечание. Рекомендуется поставить отметки «Разрешить демонстрацию экрана наружу из закрытого контура», «Включить логирование звонков» и «Включить микширование аудио потоков».

6. Нажмите кнопку «Сохранить».

Для запуска сервера VoEx выполните команды, аналогичные командам запуска сервера CTS на стр. 52. Команды установки сервера VoEx выполняются из директории /opt/express-voice/.

НАСТРОЙКА ИНТЕГРАЦИИ С МОДУЛЕМ ВКС VINTEO:

Для настройки интеграции с модулем ВКС Vinteo:

1. В секции «Vinteo» установите флаг «Интеграция с Vinteo включена» (Рисунок 7).

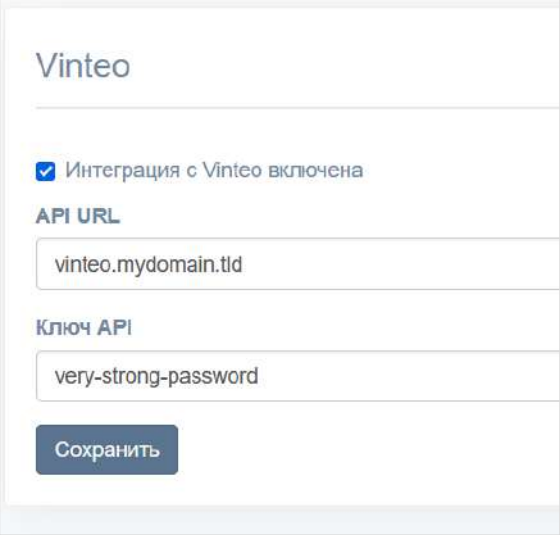

Рисунок 7

2. Заполните поля:

Таблица 31

Поле	Назначение
API URL	Путь к API модуля ВКС Vinteo
Ключ API	API ключ, сгенерированный в ВКС Vinteo

3. Нажмите на кнопку «Сохранить».

НАСТРОЙКА IP-ТЕЛЕФОНИИ

Для настройки IP-телефонии:

1. В секции «SIP» установите флаг «SIP включен» (Рисунок 8).

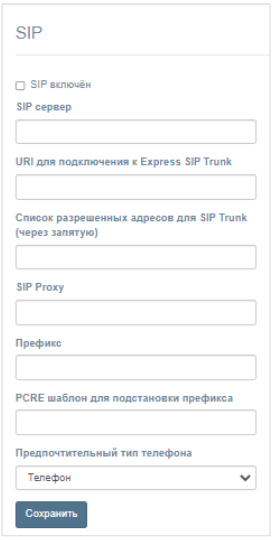

Рисунок 8

2. Заполните поля:

Таблица 32

Поле	Назначение
SIP сервер	Доменное имя или IP-адрес АТС (SIP-транк). Если порт отличается от UDP/5060, укажите его через двоеточие
URI для подключения к SIP Trunk	Адрес Back CTS, на котором установлен контейнер messaging. Заполняется для развертывания Front CTS + VoEx и Back CTS. Формат записи: sip:<IP или DNS-имя>:<port>
Список разрешенных адресов SIP Trunk	IP-адреса, с которых будут приниматься вызовы SIP-транком СК «Express». Укажите минимум два IP-адреса: • IP-адрес АТС; • адрес, на котором установлен контейнер janus (SIP-шлюз устанавливаемый вместе с СК «Express»). Все IP или сети указываются с маской, например – 10.10.10.1/32 для одиночного IP, 192.168.12.0/24 для сети. Для развертывания Single CTS укажите IP-адрес самого сервера СК «Express» (10.10.10.1/32) и внутренний IP интерфейса docker сети (172.18.0.1/32) и АТС. Для развертывания Front CTS + VoEx и Back CTS укажите IP Front+VoEx и АТС
SIP Proxy	Адрес прокси-сервера SIP-телефонии или адрес АТС. Формат записи SIP: <IP или DNS-имя >:<port>. Не обязательно указывать порт, если он не отличается от стандартного UDP/5060
Префикс	Строка, подставляемая к началу набираемого номера при передаче номера на АТС и номера, принимаемого с АТС, в случае, если АТС отправляет номер без префикса
PCRE шаблон для подстановки префикса	регулярное выражение по совпадению структуры номера, к которому при исходящем вызове с СК «Express» будет подставляться префикс. Для того, чтобы префикс не подставлялся к номерам, введите выражение - ^[0-9](1)
Предпочтительный тип телефона	Тип телефона, с которого будут осуществляться звонки. Возможные варианты: телефон, IP-телефон, телефон (другой), IP-телефон (другой). Сопоставление параметров объекта пользователя с данными типами телефонов осуществляется в разделе «Active Directory» интерфейса администрирования.

3. Нажмите кнопку «Сохранить».

Далее выполняется настройки клиентского АТС SIP-транка.

Внимание! Для всех схем развертывания, обязательным условием является отключение проверки состояния SIP-транка.

Для корректной работы при схеме развертывания Single CTS[1] настройте в АТС SIP-транк:

1. Для вызовов с АТС в Систему укажите IP назначения Single;
2. Для вызовов с Системы в АТС укажите IP назначения Single.

Для корректной работы при схеме развертывания Front CTS + VoEx и Back[2] настройте в АТС 2 SIP-транк:

1. Для вызовов с АТС в Систему укажите IP назначения Back;
2. Для вызовов с Системы в АТС укажите IP назначения Front.

[1] Сетевая схема взаимодействия с АТС при развертывании Single CTS и сетевые взаимодействия для данной схемы развертывания представлены в Приложении 8.

[2] Сетевая схема взаимодействия с АТС при развертывании Front CTS + VoEx и Back CTS и сетевые взаимодействия для данной схемы развертывания представлены в Приложении 9.

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
echo DPL_IMAGE_TAG=web-release > dpl.env
dpl --init
```

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

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 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. 24.

   - 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. 52.

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

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

Пример заполнения конфигурации:

```
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
  ets: true
  gmapsApiKey: apiKeyapiKeyapiKey
  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
```

УСТАНОВКА СЕРВИСА ССЫЛОК

Для установки сервиса ссылок:

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.

3. Создайте рабочий каталог веб-клиента^

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

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

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 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. 24.

   - 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. 52.

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

```
ccs_host: somehost.somedomain.sometld
```

Пример заполнения конфигурации:

```
ccs_host: xlnk.example.com
le_email: test@example.com
home_address: www.example.com
android_app_link:
'https://play.google.com/store/apps/details?id=ru.unlimitedtech.express'
ios_app_link: 'https://apps.apple.com/ru/app/express-enterprise-messaging/id1225251588?l=en'
ets_id: 00000000-0000-000-000-000000000000
api_gw_url: 'http://link:4000'
web_host_default: 'web.example.com'
```

5. В каталоге /opt/express/xlnk выполните команду:

```
dpl -d
```

Для изменения файла конфигурации воспользуйтесь любым текстовым редактором и внесите исправления в файл (Таблица 33):

Таблица 33

Название настройки	Значение
ccs_host	Полное имя домена данного сервера, прописанное в DNS и соответствующее имени, на которое приобретался сертификат
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
home_address	Полное имя домена основного сайта компании, на который будут перенаправляться пользователи при обращении без ссылки на чат/конференцию
ets_id	Идентификатор сервера ETS, необходимый для определения ссылок, созданных на серверах предприятия. Включает отображение ссылок на мобильные приложения компании
android_app_link ios_app_link	Ссылки на мобильные приложения в магазинах приложений Apple, Play Market
android_app_name ios_app_name	Название ссылки на мобильные приложения, по умолчанию имеют значение Android Custom App, iOS Custom App. Отображается при переходе с мобильных устройств по ссылке
api_gw_url	Путь до сервиса xlink для доступа
web_host_default	Полное имя домена сервера web-клиента для чата/конференции

УСТАНОВКА DLP

УСТАНОВКА DLP НА ВЫДЕЛЕННОМ СЕРВЕРЕ

Для формирования ключа DLP и добавления его во все чаты:

Внимание! В данном примере DLP устанавливается на отдельном от CTS сервере.

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.

3. Скачайте контейнер-инсталлятор.

```
docker run --rm registry.public.express/dpl:dlps-release dpl-install | bash
```

4. Создайте рабочий каталог веб-клиента.

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

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

5. 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. 24.

- 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. 52.

6. Выполните команду:

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

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

```
api_internal_token: token
ccs_host: somehost.somedomain.sometld
cts_id: ''
dlps_host: ''
dlps_icap_client_host: ''
dlps_icap_additional_headers: {}
etcd_endpoints: http://etcd:2379
kafka_host: kafka
phoenix_secret_key_base: token
postgres_endpoints: ''
postgres_user: ''
postgres_password: ''
redis_connection_string: ''
rts_id: ''dlps_enabled: true
```

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

```
dpl -d
```

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

Для изменения файла конфигурации воспользуйтесь любым текстовым редактором и внесите исправления в файл (Таблица 34):

Таблица 34

Название настройки	Значение
ccs_host	Полное имя домена сервера CTS, прописанное в DNS и соответствующее имени, на которое приобретался сертификат
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
cts_id	Идентификатор установленного сервера
rts_id	Идентификатор сервера RTS (предоставляется разработчиком)
etcd_endpoints	Адрес подключения к ETCD-серверу
kafka_host	Адрес подключения к Kafka-серверу
redis_connection_string	Параметры подключения к базе данных REDIS
postgres_endpoints postgres_user postgres_password	Параметры подключения к базе данных PostgreSQL
dlps_postgres_endpoints dlps_postgres_user dlps_postgres_password	В случае использования отдельной базы для dlps-модуля указывается дополнительно

УСТАНОВКА DLP НА SINGLE CTS

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
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 && dpl --dc restart nginx
```

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».

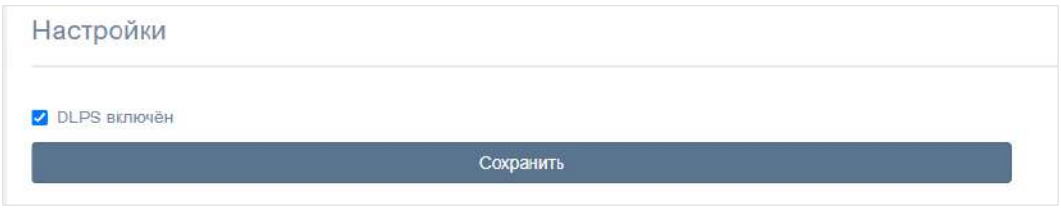

Рисунок 9

УСТАНОВКА DLP НА SINGLE CTS С ХРАНЕНИЕМ КЛЮЧЕЙ НА ВНЕШНЕМ НОСИТЕЛЕ

Для настройки DLP на внешнем носителе:

1. Вставьте rw флеш-накопитель USB в компьютер и смонтируйте диск в нужную директорию. Директория по умолчанию — /opt/express-dlps/dlps_keys/. Файловая система на флеш-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:

```
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».

УСТАНОВКА КОМПОНЕНТОВ ЗАПИСИ ЗВОНКОВ И КОНФЕРЕНЦИЙ

Примечания:

- перед установкой необходимо обновить версию сервера CTS до версии 3.10 и выше[1];
- перед установкой компонентов рекомендуется ознакомиться с архитектурой;
- если janus установлен отдельно от CTS, операции в пунктах 3-5 выполняются на сервере VoEx;
- если сервер VoEx расположен отдельно от Front CTS, необходимо открыть сетевой доступ к CTS Back по порту 80 или 443 (в зависимости от конфигурации).

Для установки компонентов:

1. На Back CTS или Single CTS добавьте в /opt/express/settings.yaml:

```
transcoding_enabled: true
```

2. На сервере Back CTS или Single CTS выполните команду:

```
cd /opt/express/ && dpl -p && dpl -d transcoding_manager
recordings_bot admin && dpl --dc restart nginx
```

3. В зависимости от архитектурного решения на одном из следующих серверов — VoEx, Front CTS или Single CTS — добавьте в /opt/express-voice/settings.yaml:

   Важно! Значения ccs_host, api_internal_token скопируйте из /opt/express/settings.yaml, расположенного на Back CTS или Single CTS.

```
transcoding_hosts:
  cts:
    ccs_host: cts.corp.express
    api_internal_token: token-cts
```

   Если сервер записи и janus используется несколькими CTS, перечислить несколько хостов:

```
transcoding_hosts:
 cts1:
  ccs_host:
  cts1.corp.express
  api_internal_token: token-cts1
 cts2:
  ccs_host: cts2.corp.express
  api_internal_token: token-cts2
```

4. В зависимости от архитектурного решения, на одном из следующих серверов — VoEx, Front CTS или Single CTS — выполните команду:

```
cd /opt/express-voice/ && dpl -p && dpl -d
```

5. В зависимости от архитектурного решения, на одном из следующих серверов — VoEx, Front CTS или Single CTS — выполните команду:

```
 chown -R 888:888 /var/lib/docker/volumes/voex_transcoding/_data
```

УСТАНОВКА RTS И ETS

Установка сервера RTS выполняется по аналогии с установкой сервера Single CTS:

- при редактировании файла конфигурации задайте следующие параметры:

```
cassandra_host: 10.0.0.1
```

[1] Настройка записи звонков и конференций описана в одноименном разделе в документе «Руководство администратора. Эксплуатация».

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

Установка сервера ETS выполняется по аналогии с установкой сервера Single CTS:

- при редактировании файла конфигурации задайте следующие параметры:

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

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 сначала 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. Команда должна производиться на Back CTS.

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

Примечание. Требования к паролю администратора:

- минимальная длина пароля – 8 символов;
- пароль должен содержать как минимум один специальный символ #!?&@$%^&*(), одну строчную и одну прописную букву.

Если консоль администратора не установилась, то произошла ошибка несовпадения по политике паролей. В этом случае, а также в случае возникновения других ошибок выполните проверку.

Для проверки на наличие ошибок в появившихся логах найдите наиболее частое упоминание с ошибками и перезапустите контейнер, выдающий ошибку, с помощью команды:

```
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;
- ETS;
- CTS.

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 10):

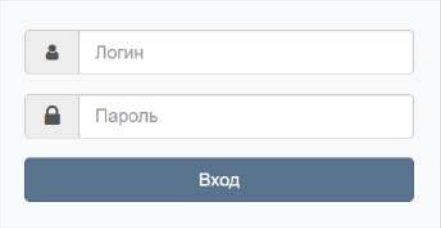

Рисунок 10

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);
- настройка видео- и голосовой связи;
- подключение SMTP-сервера;
- настройка push-уведомлений;
- подключение администраторов данного RTS из AD;
- настройка подключений ETS и CTS.

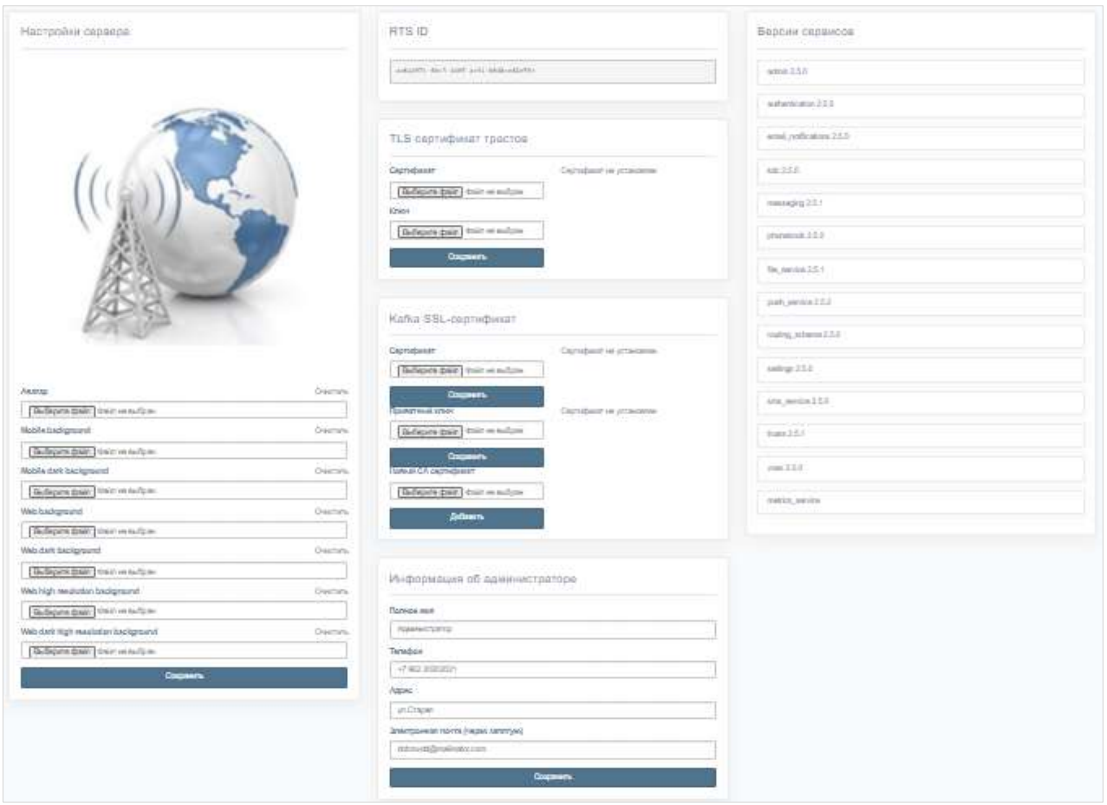

Рисунок 11

ПОДКЛЮЧЕНИЕ TLS-СЕРТИФИКАТА

Для настройки TLS-сертификата:

- в консоли администратора выберите пункт меню «Сервер».

  Откроется окно с информацией о данном RTS сервере (Рисунок 11).

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. 41.

ПОДКЛЮЧЕНИЕ SMTP-СЕРВЕРА

Для подключения SMTP-сервера:

1. В меню выберите пункт «E-mail» (Рисунок 12).
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».

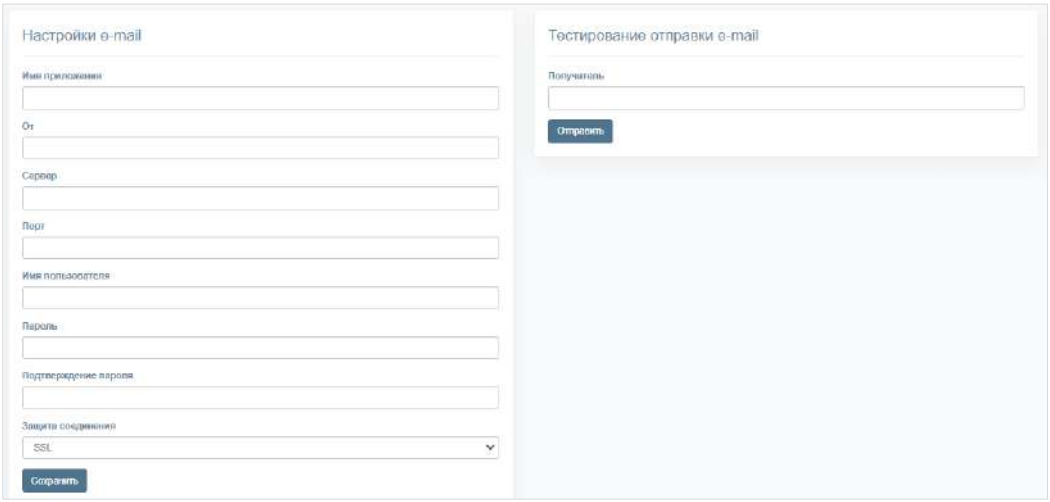

Рисунок 12

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 13).

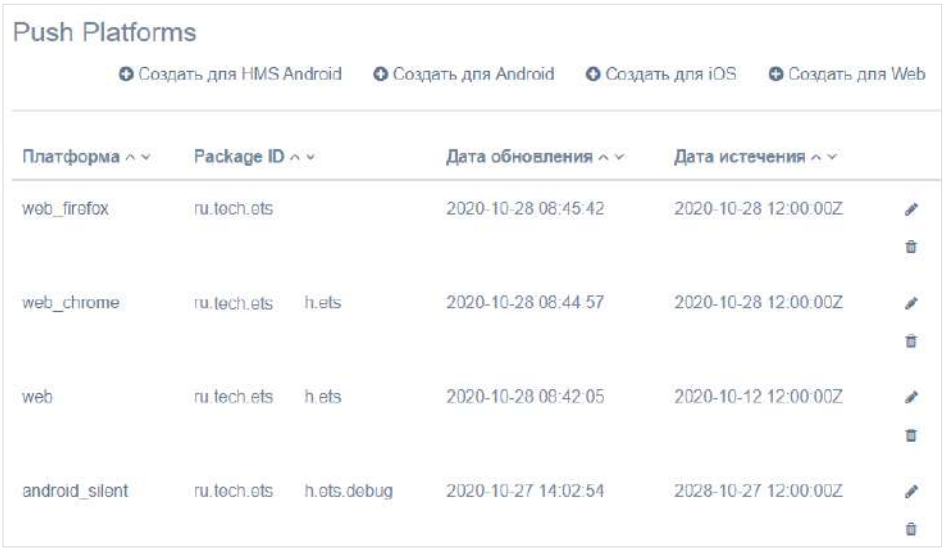

Рисунок 13

Таблица содержит следующую информацию:

Таблица 35

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 RuStore – через RuStore, для iOS — через APNS.

Примечание. Для корректной работы необходим доступ к APN Push сервисам:

- Apple APN — api.push.apple.com
- Google FCM — fcm.googleapis.com
- Huawei HSM — push-api.cloud.huawei.com, oauth-login.cloud.huawei.com

Для создания подключения на Android RuStore:

1. Войдите в консоль RuStore.
2. Создайте новое приложение (если еще не создано), нажав на кнопку + Добавить приложение в правом верхнем углу страницы
3. Войдите в созданное приложение создайте новый проект в разделе «Push-уведомления -> Проекты» (Рисунок 14).

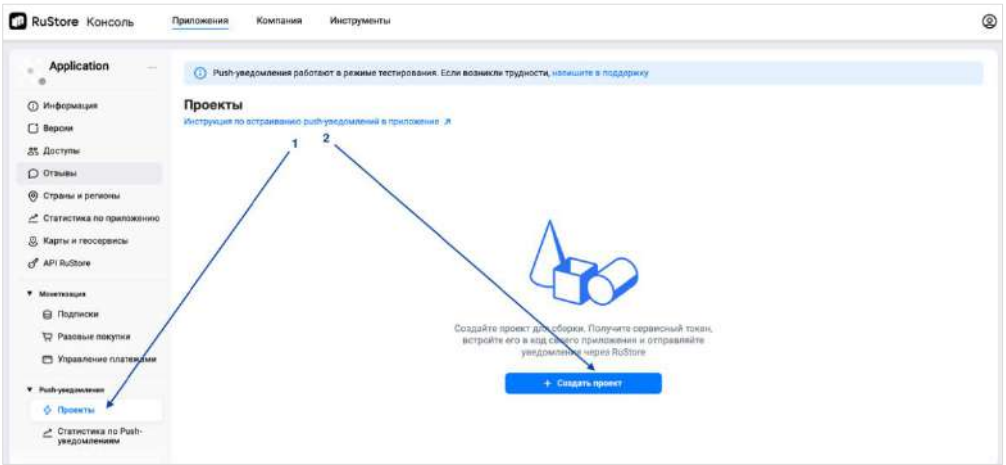

Рисунок 14

4. Заполните поля нового проекта (Рисунок 15, Таблица 36) и нажмите кнопку «Создать».

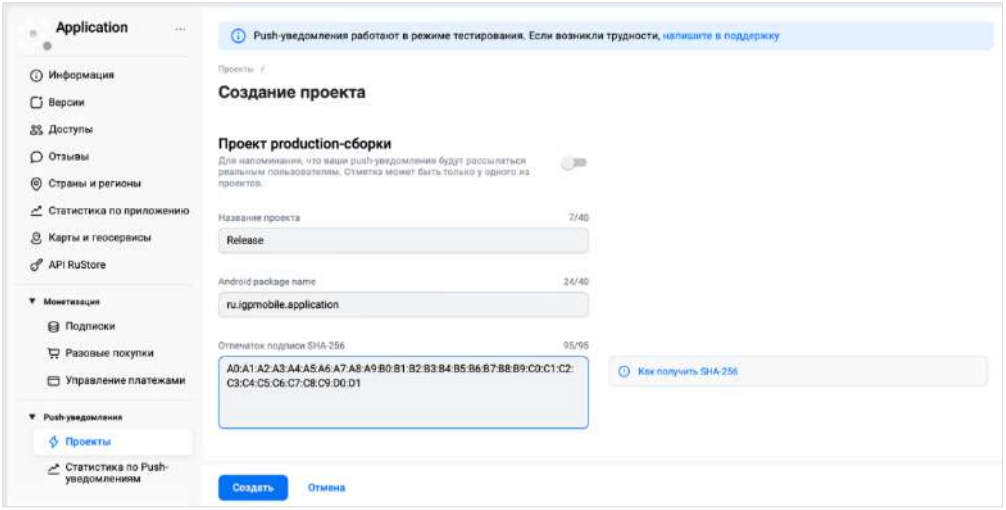

Рисунок 15

Таблица 36

Параметр	Описание	Значение
Название проекта	Название проекта. Может быть произвольным.	Например: Release
Android Package Name	Это корректное наименование пакета вашего приложения	Например: com.app.packageid
Отпечаток подписи SHA-256	Для получения отпечатка подписи SHA-256 воспользуйтесь инструкцией по ссылке на странице	

5. Создайте сервисный токен (Рисунок 16).

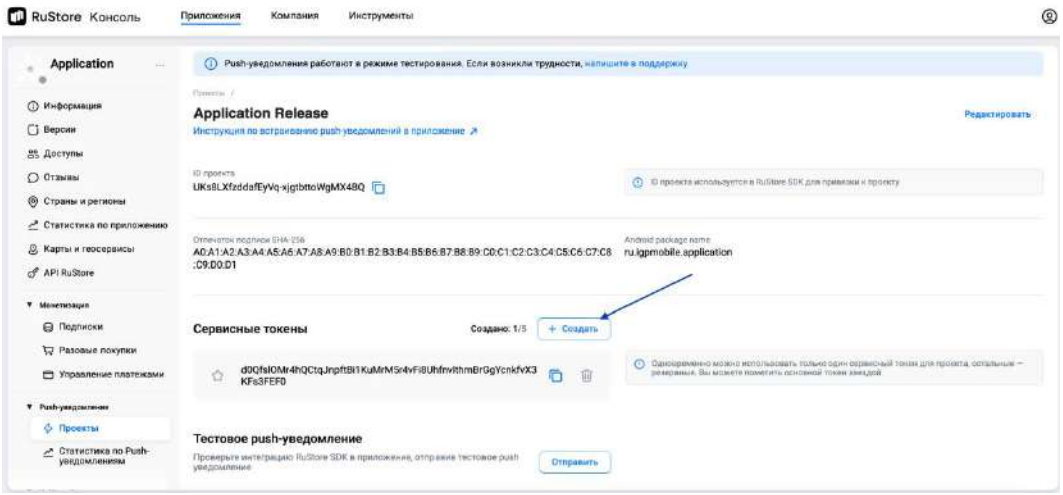

Рисунок 16

6. В консоли администратора СК Express в разделе Push Service нажмите кнопку «Создать для Android RuStore».

   Откроется окно создания подключения для платформы RuStore (Рисунок 17):

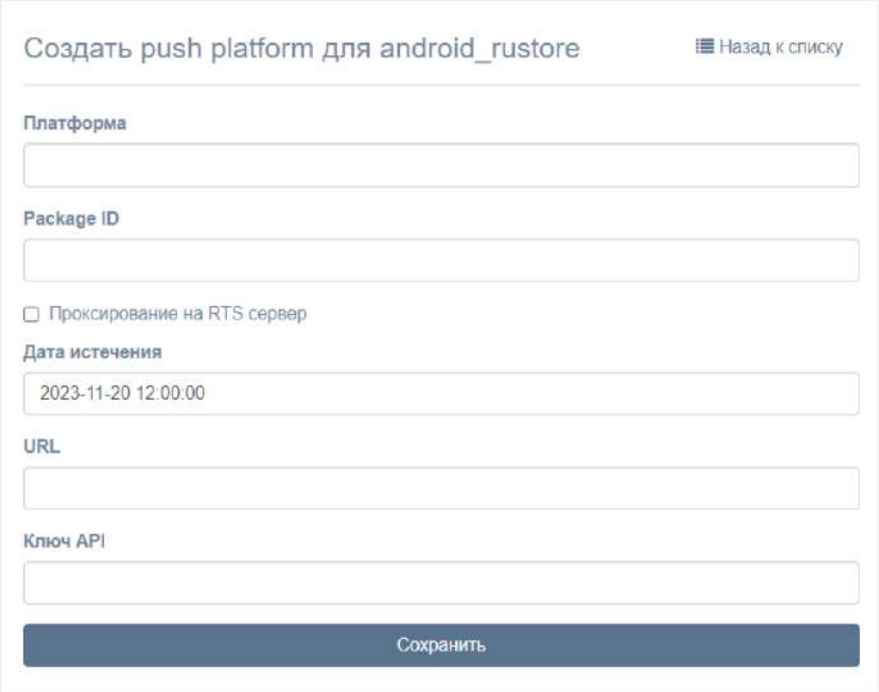

Рисунок 17

7. Заполните поля формы (Таблица 37):

Таблица 37

Параметр	Описание	Значение
Платформа	Платформа, на которой подключены push-уведомления	android_rustore
Package ID	Название сборки приложения Express	com.app.packageid
Дата истечения	Дата истечения поступления push-уведомлений	
URL	Адрес проекта вcRuStore (https://vkpns.rustore.ru/v1/projects/<project_id>/messages:send, где /<project_id> – это id проекта)	Например: https://vkpns.rustore.ru/v1/projects UKs8LXfzddafEyVq-xjgtbttoWgMX4BQ /messages:send
API Key	Ключ API, выдаваемый в консоли администратора RuStore	См. Рисунок 18

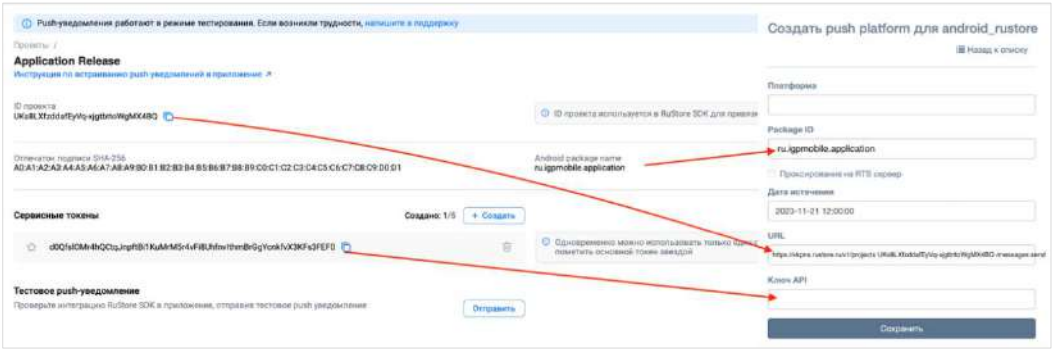

Рисунок 18

8. Для включения проксирования на RTS-сервер поставьте отметку в чек-боксе рядом с соответствующим полем.
9. Нажмите кнопку «Сохранить».

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 19).

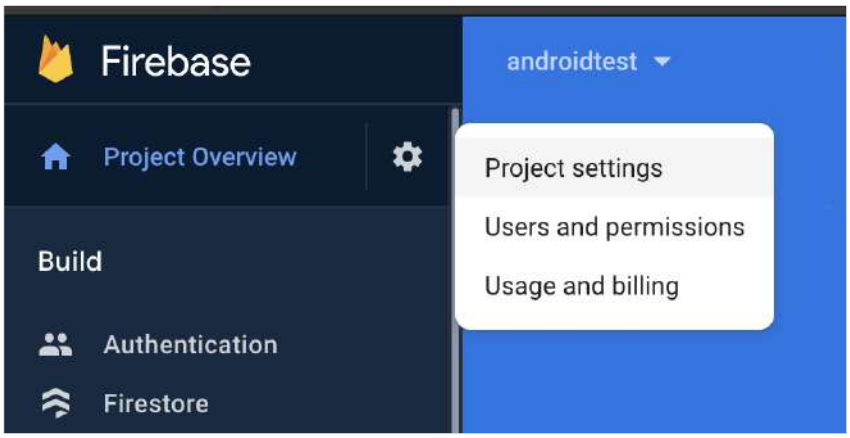

Рисунок 19

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 20).

Рисунок 20

4. Заполните поля формы (Таблица 38):

Таблица 38

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 21

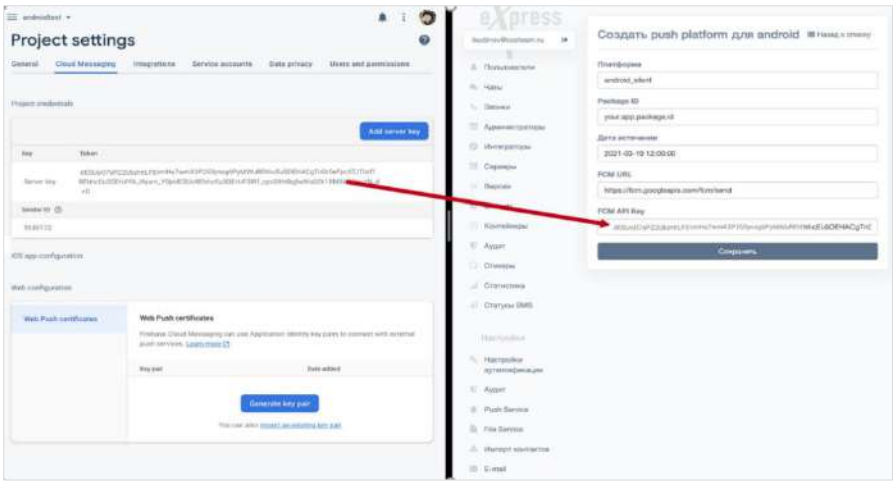

Рисунок 21

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 22).

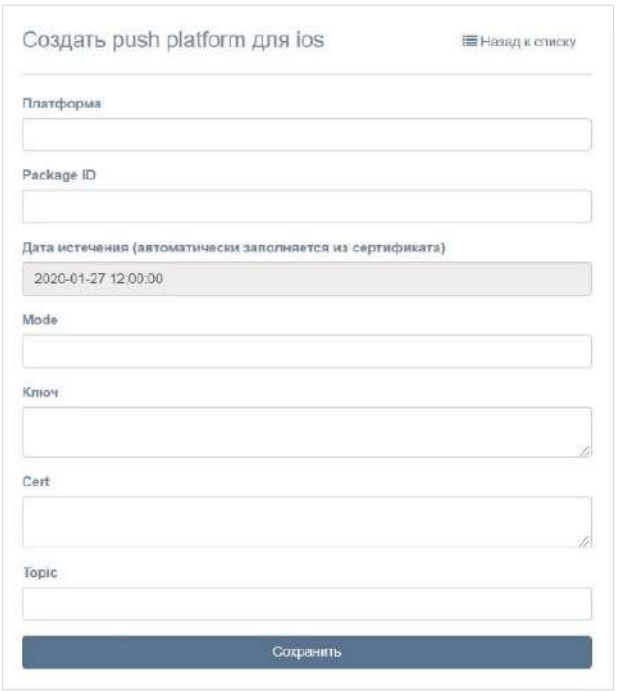

Рисунок 22

2. Заполните поля формы (Таблица 39):

Таблица 39

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	

Параметр	Описание	Значение
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 23).

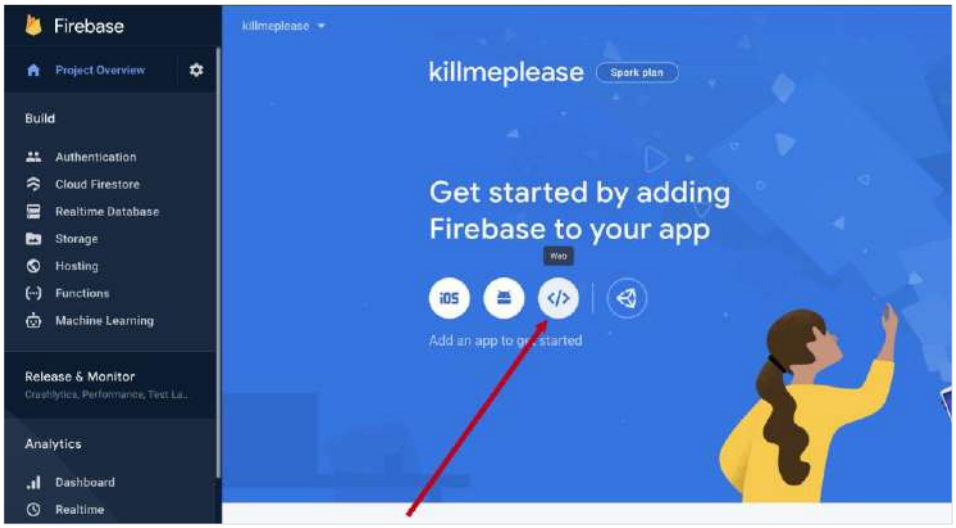

Рисунок 23

3. В открывшемся окне нажмите кнопку «Generate key pairs» (Рисунок 24).

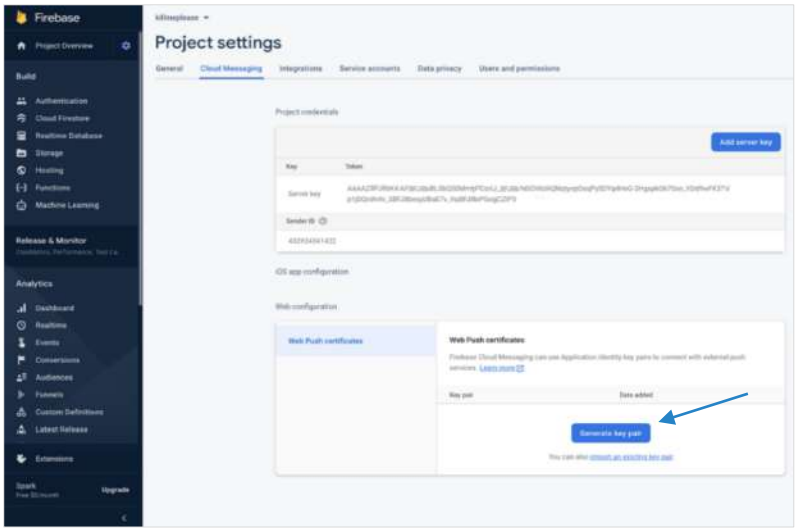

Рисунок 24

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 25).

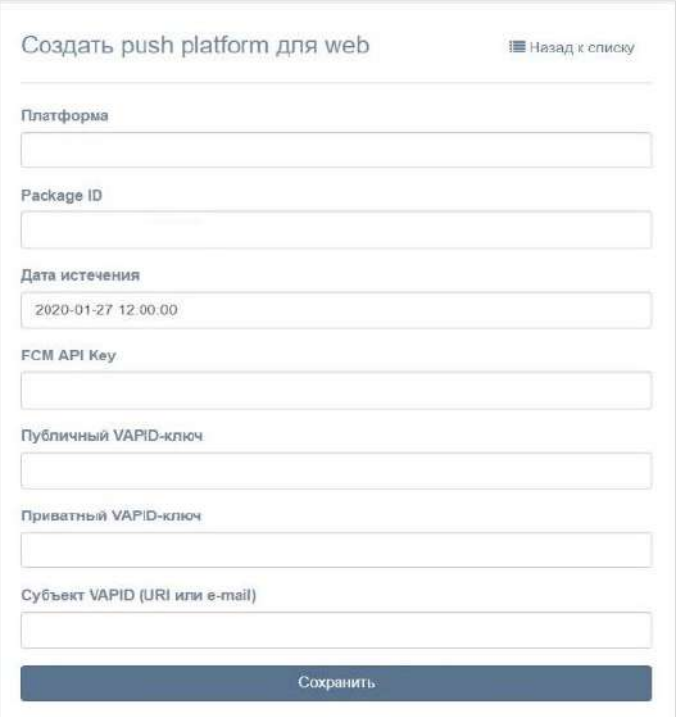

Рисунок 25

5. Заполните поля формы (Таблица 40).

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

Таблица 40

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 26
Публичный VAPID-ключ	Публичный ключ API, сгенерированный в консоли администратора Firebase	См. Рисунок 26
Приватный VAPID-ключ	Приватный ключ API, сгенерированный в консоли администратора Firebase	См. Рисунок 26
Субъект VAPID (URI или e-mail)	Адрес электронной почты пользователя в firebase	mailto:<email аккаунта firebase>

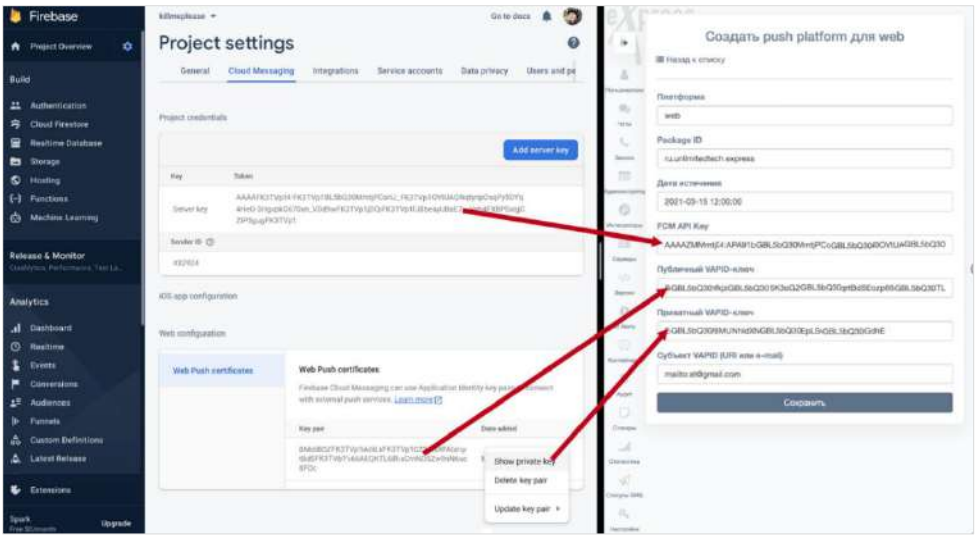

Рисунок 26

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 27).

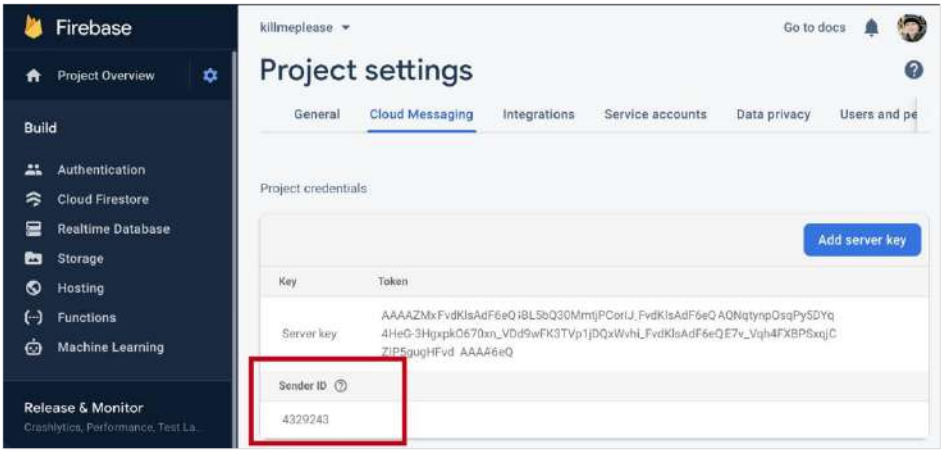

Рисунок 27

НАСТРОЙКА СМС-СЕРВИСА

В разделе «SMS» администратор может настраивать интеграцию с провайдером, который будет отправлять пользователям СМС-сообщения с кодом авторизации, и параметры безопасности.

НАСТРОЙКА ТЕКСТА СМС-СООБЩЕНИЯ

Для настройки текста СМС-сообщения:

1. Выберите в меню раздел «SMS».

   Откроется окно «Настройки SMS».
2. В поле «Провайдер» выберите провайдера. Например, Beeline (Рисунок 28).

Рисунок 28

3. В поле «Текст SMS сообщения» введите текст СМС-сообщения, которое будет отправляться вместе с кодом авторизации, и нажмите на кнопку «Сохранить» (Рисунок 29).

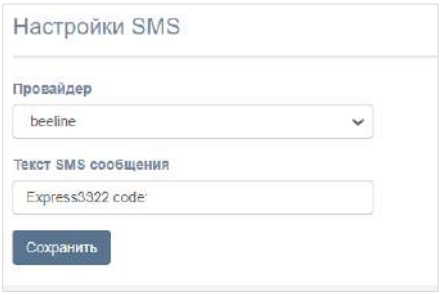

Рисунок 29

НАСТРОЙКА ИНТЕГРАЦИИ С ПРОВАЙДЕРОМ

Для настройки интеграции с провайдером:

1. Перейдите в подраздел «Адаптеры».
2. Установите параметры выбранного провайдера в соответствующей секции, и нажмите на кнопку «Сохранить».

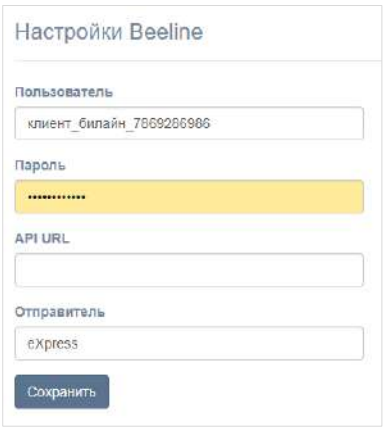

Рисунок 30

Настраиваемые параметры зависят от провайдера. Примеры настроек для провайдеров представлены ниже (Таблица 41):

Таблица 41

Параметр	Назначение	Провайдер
Ключ API	Ключ для отправки СМС-сообщений. Предоставляется провайдером	Clickatell
API URL	Адрес API СМС-сервиса	Clickatell, QTelecom, Beeline, SMSTraffic
Пользователь	Имя пользователя СМС-сервиса провайдера	QTelecom, Beeline, SMSTraffic, Stream Telecom
Логин	Логин по льзователя СМС-сервиса провайдера	SMSC, Tele2
Пароль	Пароль пользователя СМС-сервиса провайдера	QTelecom, Beeline, SMSC, Tele2, SMSTraffic, Stream Telecom
Отправитель	Имя отправителя СМС (например, eXpress)	QTelecom, Beeline, SMSC, SMSTraffic
Отправитель для MTS	Имя отправителя СМС (например, eXpress)	QTelecom,
Shortcode	Предоставляется провайдером	Tele2
SID	Предоставляется провайдером	Twilio
Токен	Предоставляется провайдером	Twilio
От	Имя отправителя СМС-сообщения	Stream Telecom
Validity	Время жизни сообщения	Stream Telecom
Callback URL	Адрес скрипта, на который возвращаются POST данные о статусе доставки СМС	Stream Telecom
Пользователь	Цифровой идентификатор клиента, который возвращается на адрес, указанный в параметре Callback_url	Stream Telecom
Name deliver	Название рассылки, присваиваемое для удобства поиска в статистике	Stream Telecom

НАСТРОЙКА ПАРАМЕТРОВ БЕЗОПАСНОСТИ

В Express предусмотрены следующие параметры безопасности:

- ограничение количества запросов для определенного IP-адреса;
- фильтр по User-Agent;
- фильтр по DEF-коду;
- фильтр по номеру телефона;
- ограничение количества запросов на определенный телефонный номер.

Для настройки параметров безопасности:

1. Перейдите в подраздел «Безопасность».
2. Введите значения в соответствующие поля и нажмите «Сохранить» (Рисунок 31 - Рисунок 35).

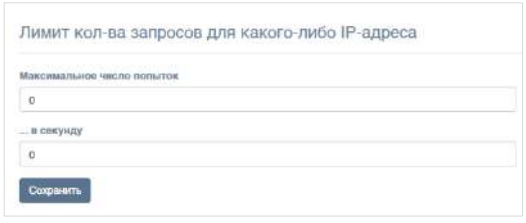

Рисунок 31

Рисунок 32

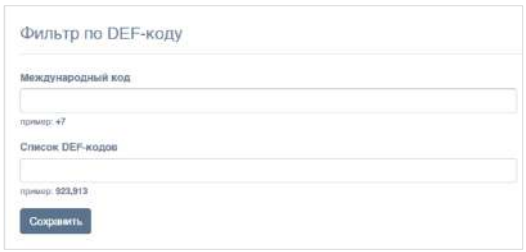

Рисунок 33

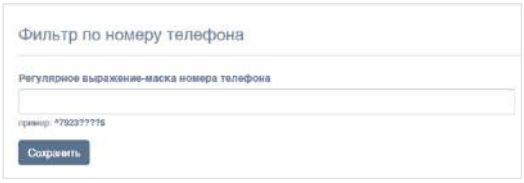

Рисунок 34

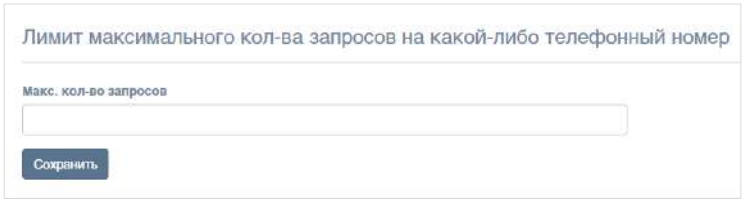

Рисунок 35

НАСТРОЙКА АУТЕНТИФИКАЦИИ АДМИНИСТРАТОРОВ

Для настройки загрузки учетных записей администратора из AD:

1. Перейдите в раздел «Аутентификация администраторов».
   Откроется окно (Рисунок 36):

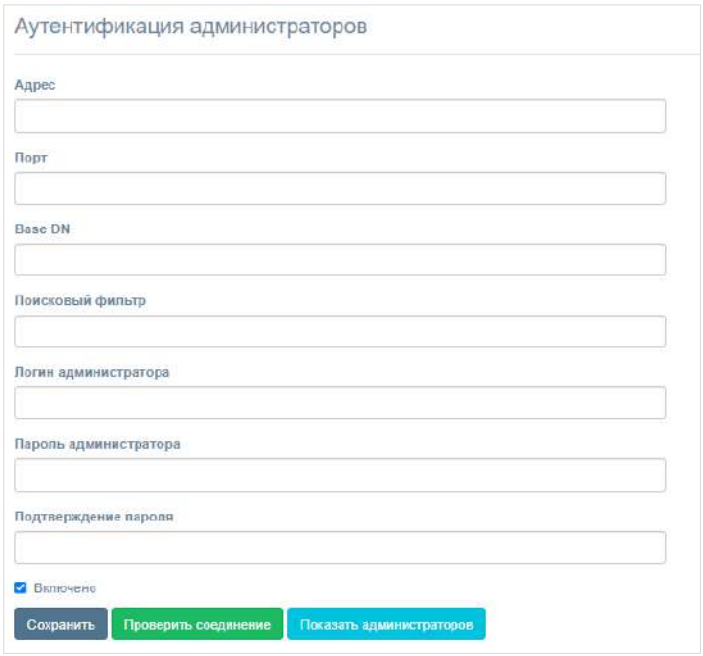

Рисунок 36

2. Настройте параметры, представленные в таблице ниже (Таблица 42).
   Значения параметров предоставляет администратор Active Directory.

Таблица 42

Параметр	Описание
Адрес	Адрес Active Directory
Порт	Порт подключения к AD
Base DN	Объект каталога, начиная с которого производится поиск

Поисковый фильтр	Фильтр для поиска в Active Directory
Логин администратора	Логин пользователя, имеющего доступ к чтению списка пользователей по указанному DN
Пароль администратора	Пароль пользователя, имеющего доступ к чтению списка пользователей по указанному DN
Подтверждение пароля	Подтверждение пароля пользователя, имеющего доступ к чтению списка пользователей по указанному DN

Для включения/отключения аутентификации администраторов Active Directory установите/снимите флаг «Включено».

Для проверки соединения с Active Directory нажмите кнопку «Проверить соединение».

После нажатия кнопки «Показать администраторов» выводится список администраторов Active Directory.

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 37, Рисунок 38, Рисунок 39).

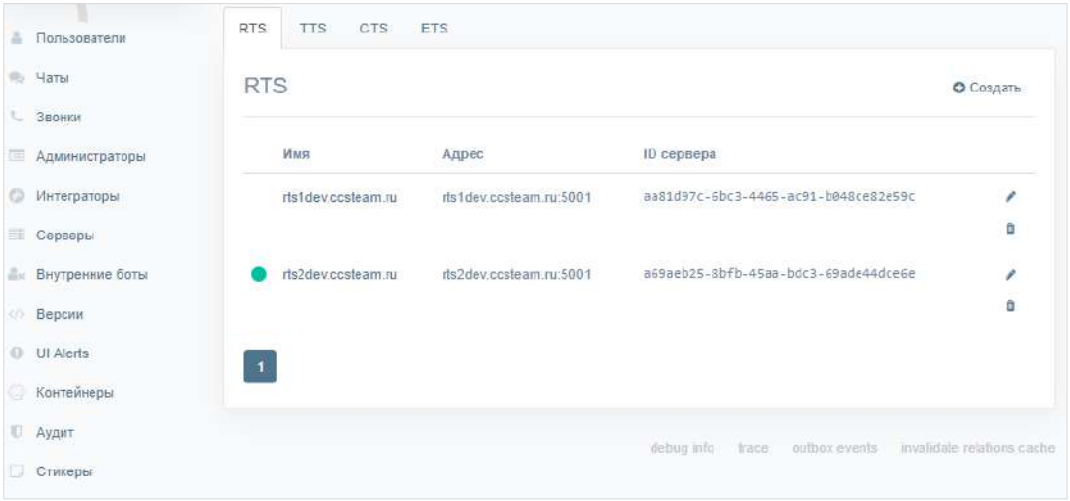

Рисунок 37

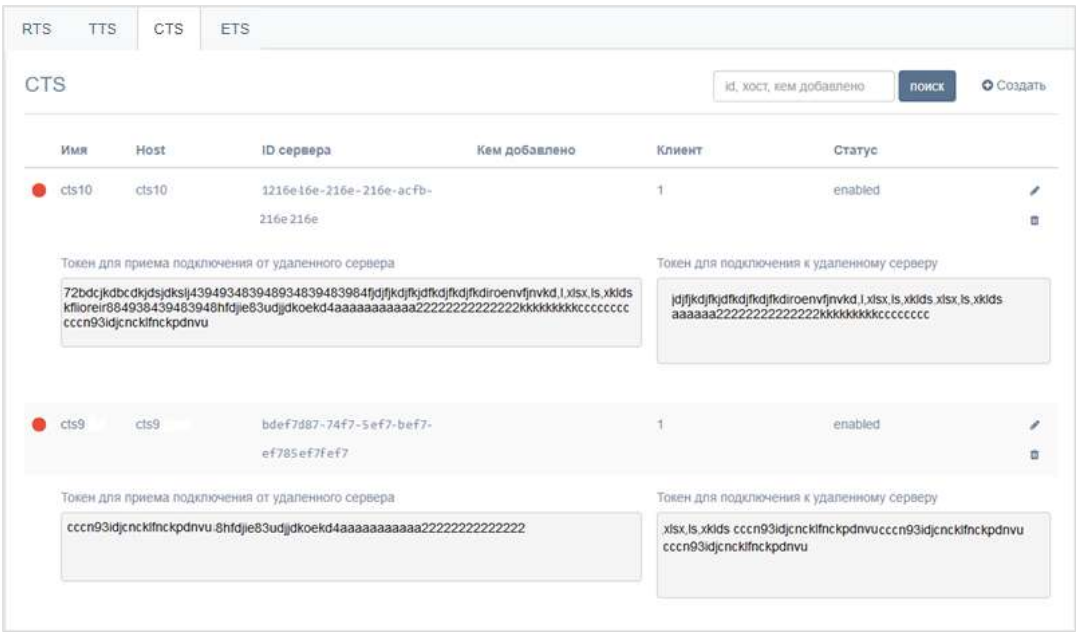

Рисунок 38

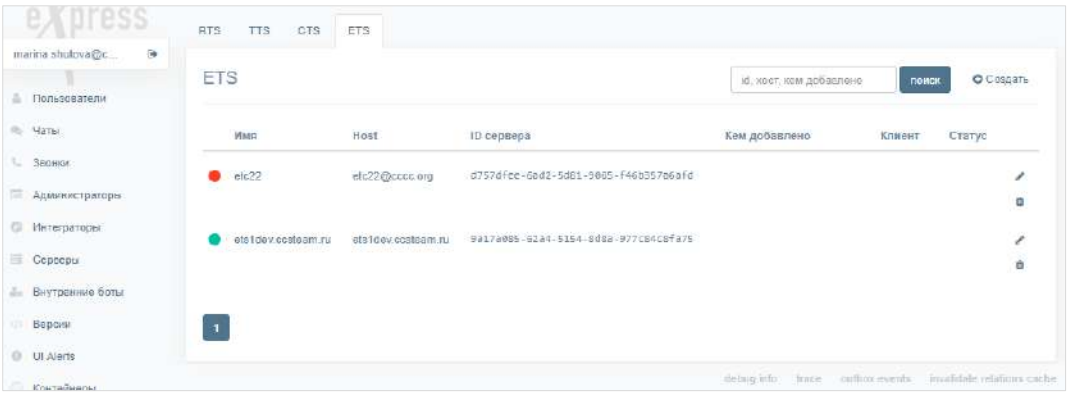

Рисунок 39

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 40 и Рисунок 41).

Рисунок 40

Рисунок 41

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 42).

Рисунок 42

2. Нажмите на имя TTS.

   Откроется окно (Рисунок 43):

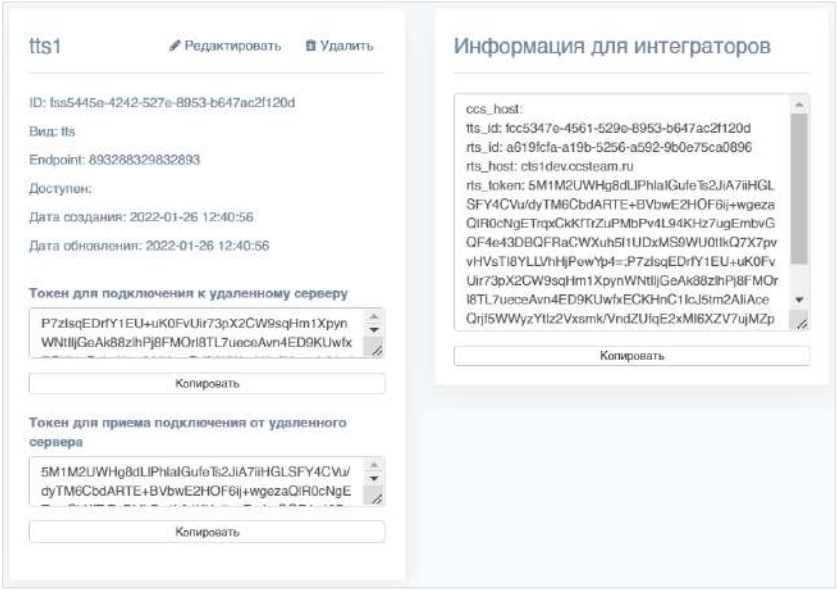

Рисунок 43

В открывшемся окне содержится следующая информация (Таблица 43):

Таблица 43

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 44).

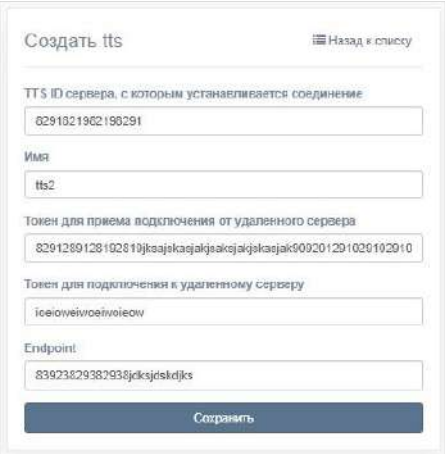

Рисунок 44

НАСТРОЙКА ETS

Настройка ETS включает в себя следующие процедуры:

- подключение TLS-сертификата (если это не было выполнено в процессе установки ETS);
- настройка видео- и голосовой связи;
- подключение SMTP-сервера;
- настройка push-уведомлений;
- подключение администраторов данного ETS из AD;
- настройка подключений CTS;
- установка веб-клиента.

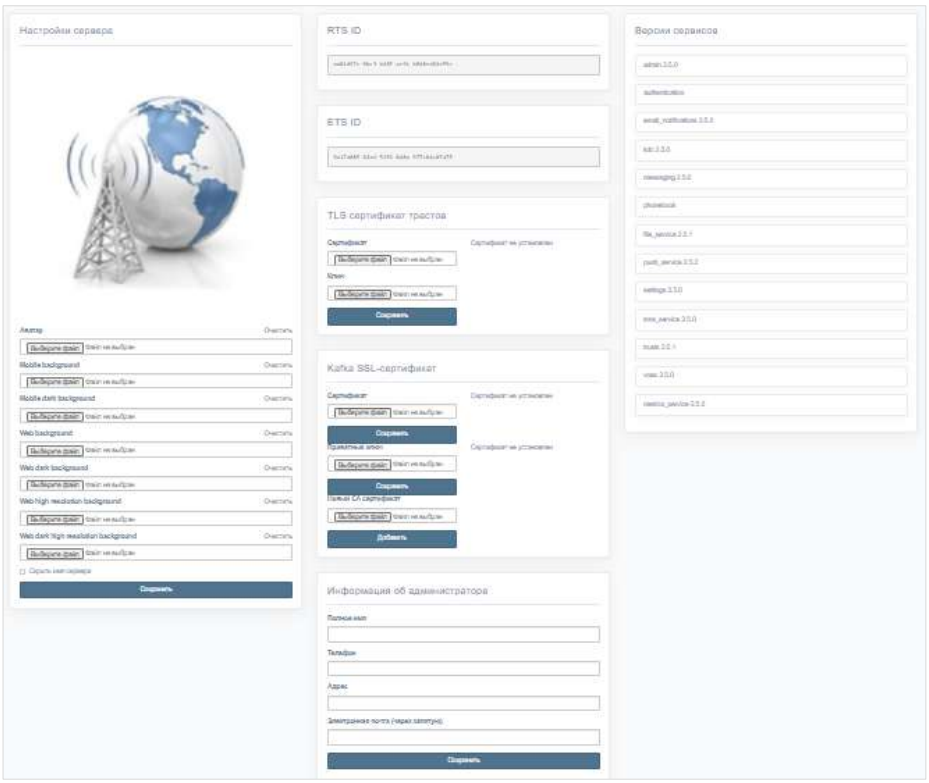

Рисунок 45

ПОДКЛЮЧЕНИЕ TLS-СЕРТИФИКАТА

Для настройки TLS-сертификата:

- в консоли администратора выберите пункт меню «Сервер».

  Откроется окно с информацией о данном RTS-сервере (Рисунок 45).

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. 41.

ПОДКЛЮЧЕНИЕ SMTP-СЕРВЕРА

Для подключения SMTP-сервера:

1. В меню выберите пункт «E-mail» (Рисунок 46).
2. В области «Настройки e-mail» заполните поля:
   - в поле «Имя приложения» укажите название приложения, от которого будут отправляться письма;
   - 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».

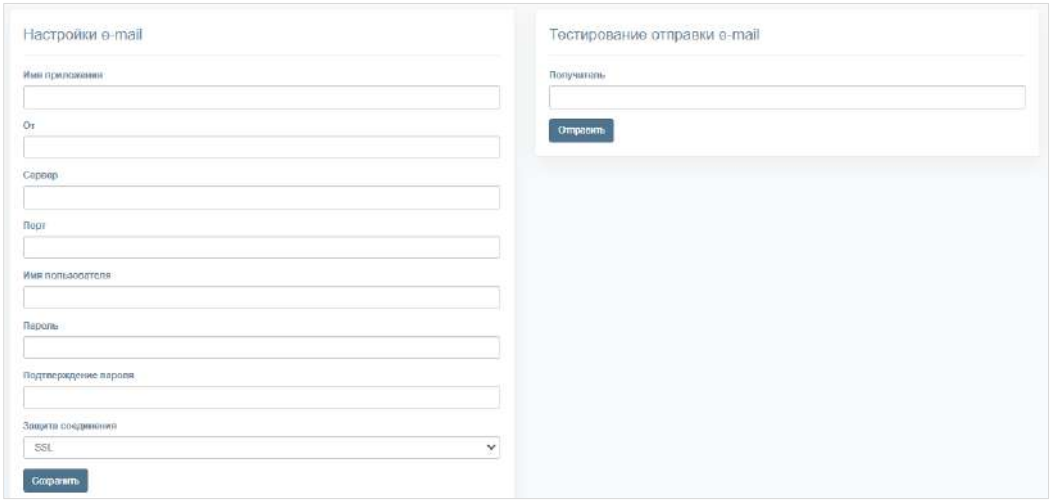

Рисунок 46

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 47).

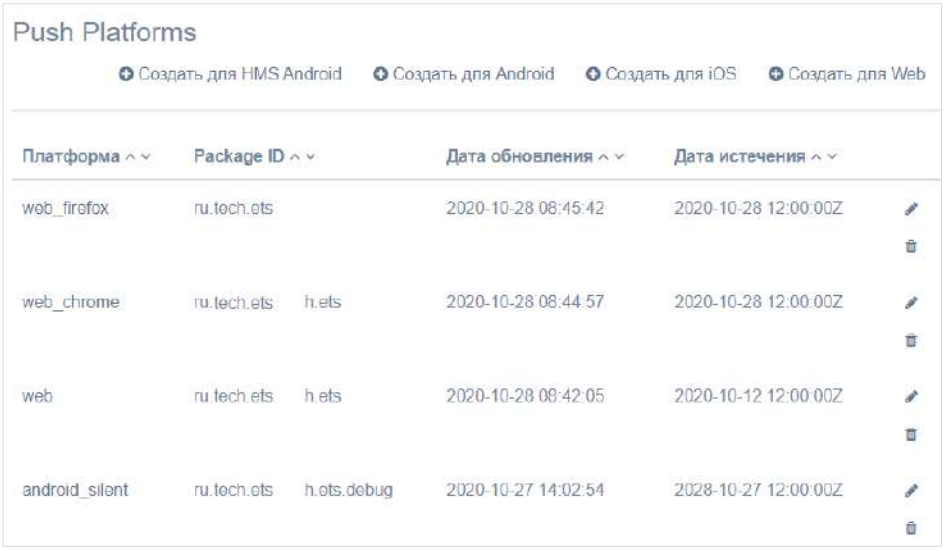

Рисунок 47

Таблица содержит следующую информацию (Таблица 44):

Таблица 44

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 RuStore – через RuStore, для iOS — через APNS.

Примечание. Для корректной работы необходим доступ к APN Push-сервисам:

- Apple APN — api.push.apple.com;
- Google FCM — fcm.googleapis.com;
- Huawei HSM — push-api.cloud.huawei.com, oauth-login.cloud.huawei.com.

Для создания подключения на Android RuStore:

1. Войдите в консоль RuStore.
2. Создайте новое приложение (если еще не создано), нажав на кнопку + Добавить приложение в правом верхнем углу страницы .
3. Войдите в созданное приложение создайте новый проект в разделе «Push-уведомления -> Проекты» (Рисунок 48).

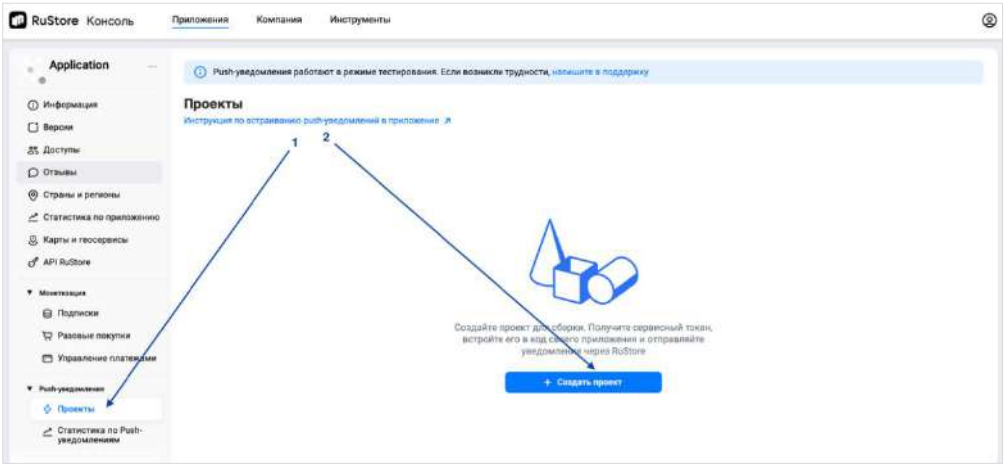

Рисунок 48

4. Заполните поля нового проекта (Рисунок 49, Таблица 45) и нажмите кнопку «Создать».

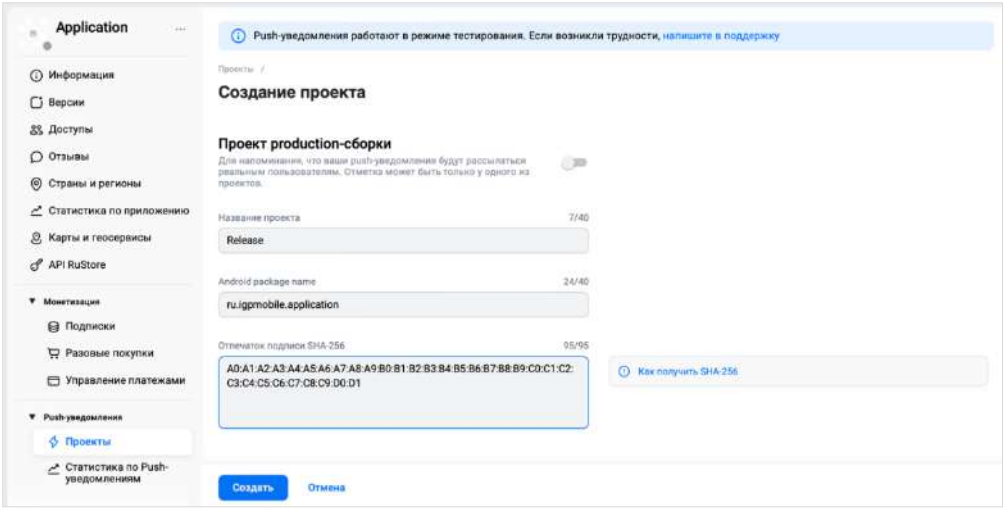

Рисунок 49

Таблица 45

Параметр	Описание	Значение
Название проекта	Название проекта. Может быть произвольным.	Например: Release
Android Package Name	Это корректное наименование пакета вашего приложения	Например: com.app.packageid
Отпечаток подписи SHA-256	Для получения отпечатка подписи SHA-256 воспользуйтесь инструкцией по ссылке на странице	

5. Создайте сервисный токен (Рисунок 50).

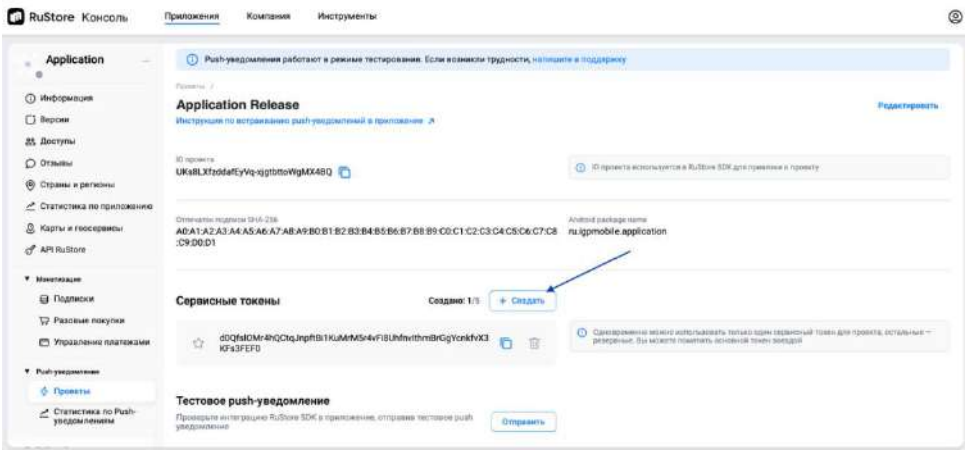

Рисунок 50

6. В консоли администратора СК Express в разделе Push Service нажмите кнопку «Создать для Android RuStore».

   Откроется окно создания подключения для платформы RuStore (Рисунок 51).

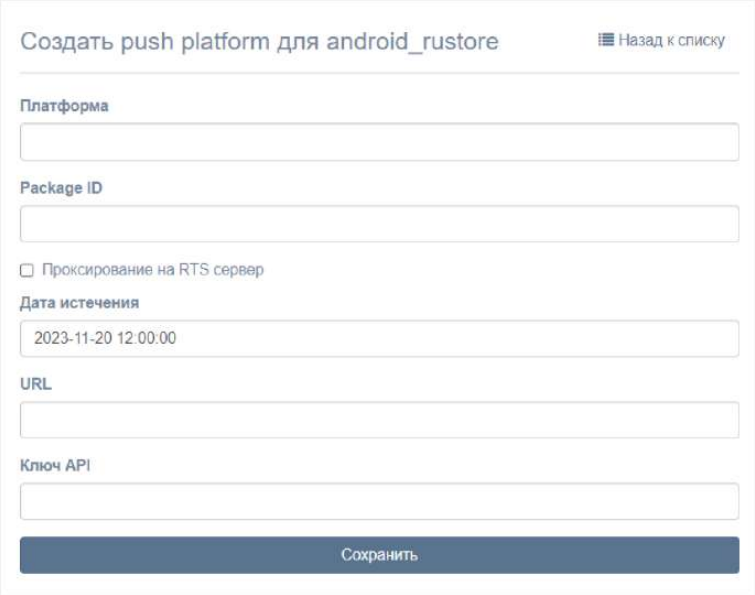

Рисунок 51

7. Заполните поля формы (Таблица 46):

Таблица 46

Параметр	Описание	Значение
Платформа	Платформа, на которой подключены push-уведомления	android_rustore
Package ID	Название сборки приложения Express	com.app.packageid
Дата истечения	Дата истечения поступления push-уведомлений	
URL	Адрес проекта вcRuStore (https://vkpns.rustore.ru/v1/projects/<project_id>/messages:send, где /<project_id> – это id проекта)	Например: https://vkpns.rustore.ru/v1/projects UKs8LXfzddafEyVq-xjgtbttoWgMX4BQ /messages:send
API Key	Ключ API, выдаваемый в консоли администратора RuStore	См. Рисунок 52

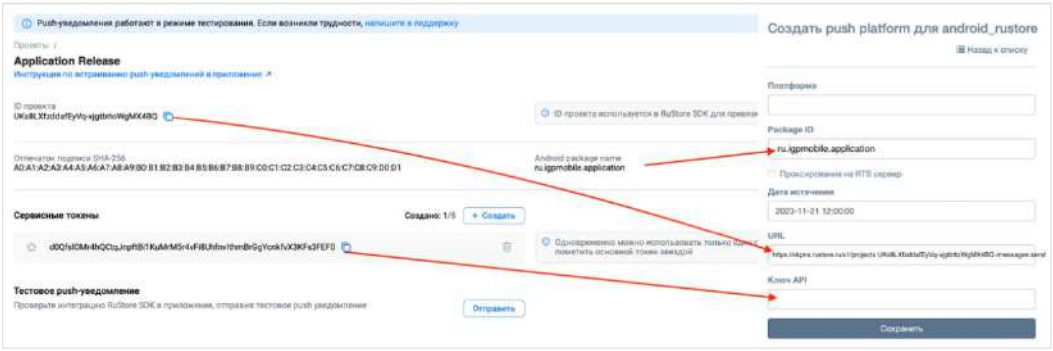

Рисунок 52

8. Для включения проксирования на RTS-сервер поставьте отметку в чек-боксе рядом с соответствующим полем.
9. Нажмите кнопку «Сохранить».

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 53).

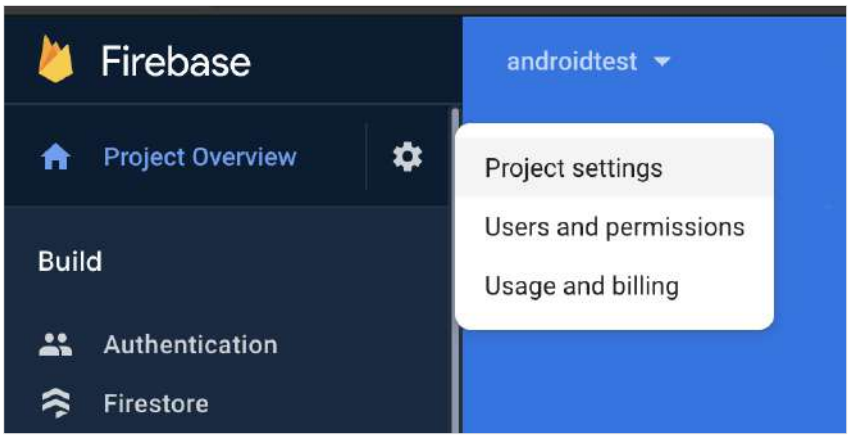

Рисунок 53

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 54).

Рисунок 54

4. Заполните поля формы (Таблица 47):

Таблица 47

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 55

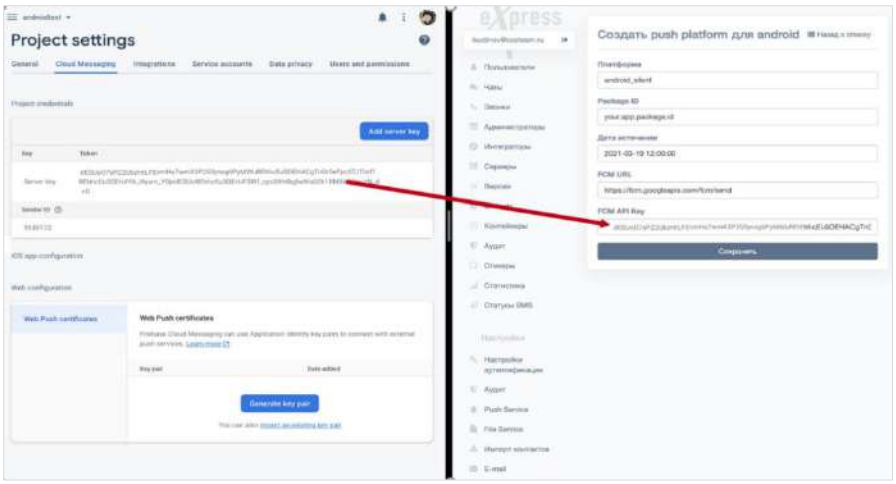

Рисунок 55

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 56).

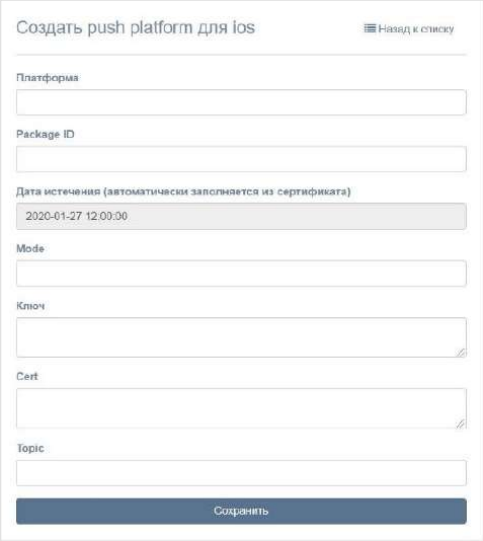

Рисунок 56

2. Заполните поля формы (Таблица 48):

Таблица 48

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	

Параметр	Описание	Значение
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 57).

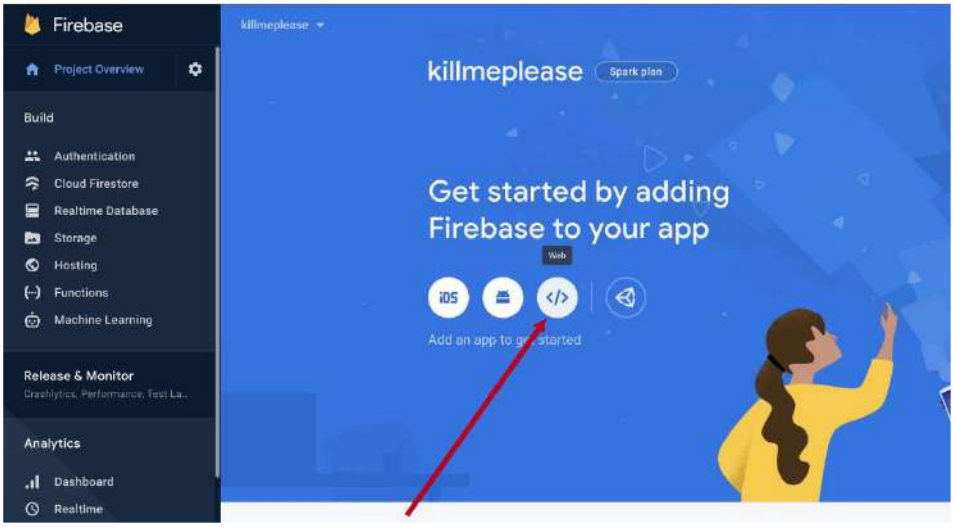

Рисунок 57

3. В открывшемся окне нажмите кнопку «Generate key pairs» (Рисунок 58).

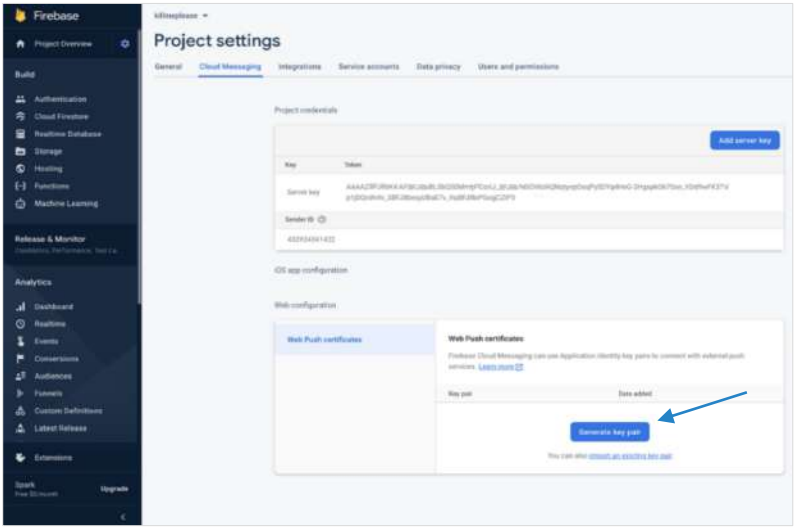

Рисунок 58

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 59).

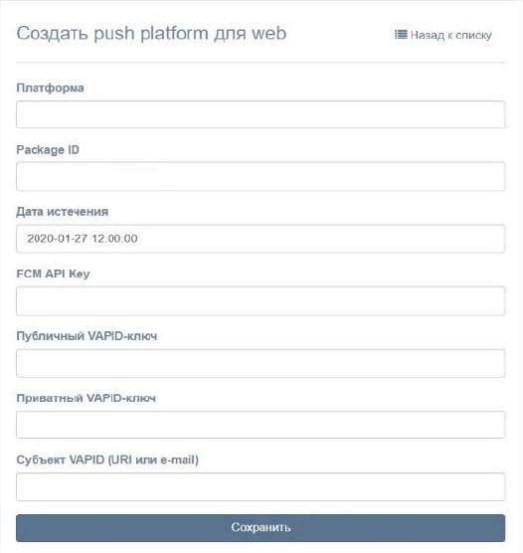

Рисунок 59

5. Заполните поля формы (Таблица 49).

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

Таблица 49

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 60
Публичный VAPID-ключ	Публичный ключ API, сгенерированный в консоли администратора Firebase	См. Рисунок 60
Приватный VAPID-ключ	Приватный ключ API, сгенерированный в консоли администратора Firebase	См. Рисунок 60
Субъект VAPID (URI или e-mail)	Адрес электронной почты пользователя в firebase	mailto:<email аккаунта firebase>

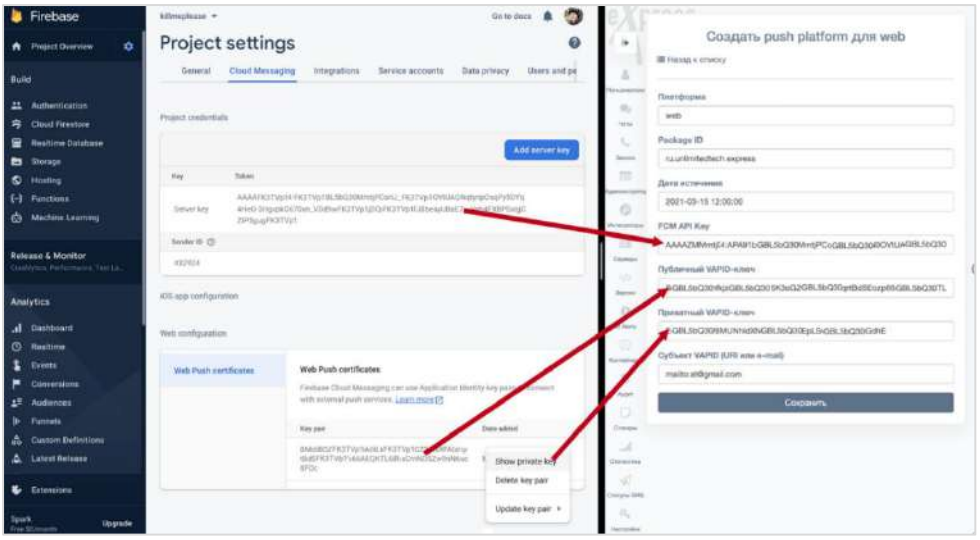

Рисунок 60

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 61).

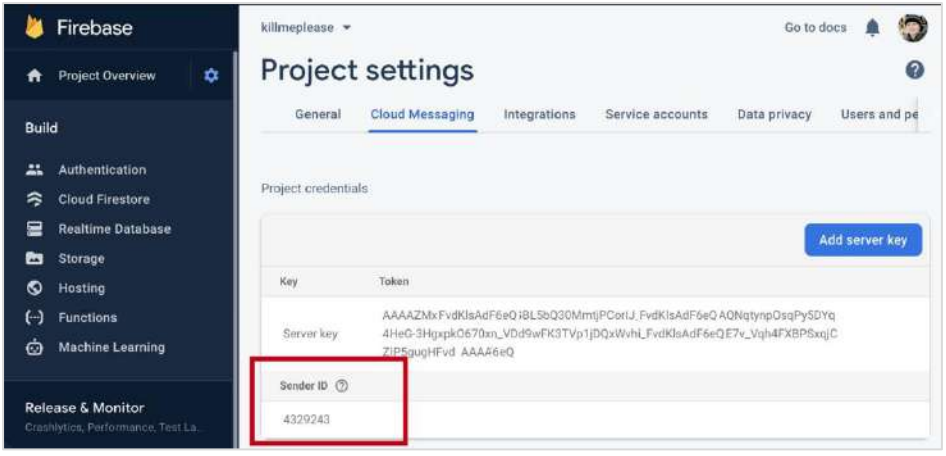

Рисунок 61

НАСТРОЙКА СМС-СЕРВИСА

В разделе «SMS» администратор может настраивать интеграцию с провайдером, который будет отправлять пользователям СМС-сообщения с кодом авторизации, и параметры безопасности.

НАСТРОЙКА ТЕКСТА СМС-СООБЩЕНИЯ

Для настройки текста СМС-сообщения:

1. Выберите в меню раздел «SMS».

   Откроется окно «Настройки SMS».
2. В поле «Провайдер» выберите провайдера. Например, Beeline (Рисунок 62).

Рисунок 62

3. В поле «Текст SMS сообщения» введите текст СМС-сообщения, которое будет отправляться вместе с кодом авторизации, и нажмите на кнопку «Сохранить» (Рисунок 63).

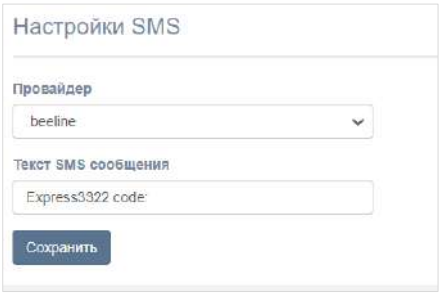

Рисунок 63

НАСТРОЙКА ИНТЕГРАЦИИ С ПРОВАЙДЕРОМ

Для настройки интеграции с провайдером:

1. Перейдите в подраздел «Адаптеры».
2. Установите параметры выбранного провайдера в соответствующей секции, и нажмите на кнопку «Сохранить» (Рисунок 64).

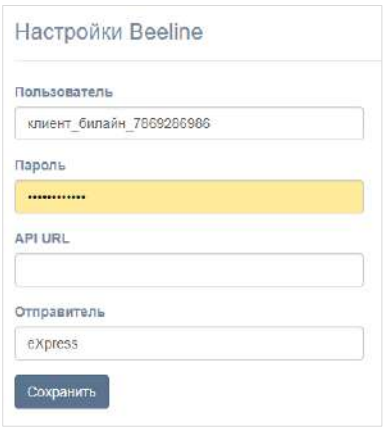

Рисунок 64

Настраиваемые параметры зависят от провайдера. Примеры настроек для провайдеров представлены ниже (Таблица 50):

Таблица 50

Параметр	Назначение	Провайдер
Ключ API	Ключ для отправки СМС-сообщений. Предоставляется провайдером	Clickatell
API URL	Адрес API СМС-сервиса	Clickatell, QTelecom, Beeline, SMSTraffic
Пользователь	Имя пользователя СМС-сервиса провайдера	QTelecom, Beeline, SMSTraffic, Stream Telecom
Логин	Логин пользователя СМС-сервиса провайдера	SMSC, Tele2
Пароль	Пароль пользователя СМС-сервиса провайдера	QTelecom, Beeline, SMSC, Tele2, SMSTraffic, Stream Telecom
Отправитель	Имя отправителя СМС (например, eXpress)	QTelecom, Beeline, SMSC, SMSTraffic
Отправитель для MTS	Имя отправителя СМС (например, eXpress)	QTelecom
Shortcode	Предоставляется провайдером	Tele2
SID	Предоставляется провайдером	Twilio
Токен	Предоставляется провайдером	Twilio
От	Имя отправителя СМС-сообщения	Stream Telecom
Validity	Время жизни сообщения	Stream Telecom
Callback URL	Адрес скрипта, на который возвращаются POST данные о статусе доставки СМС	Stream Telecom
Пользователь	Цифровой идентификатор клиента, который возвращается на адрес, указанный в параметре Callback_url	Stream Telecom
Name deliver	Название рассылки, присваиваемое для удобства поиска в статистике	Stream Telecom

НАСТРОЙКА ПАРАМЕТРОВ БЕЗОПАСНОСТИ

В Express предусмотрены следующие параметры безопасности:

- ограничение количества запросов для определенного IP-адреса;
- фильтр по User-Agent;
- фильтр по DEF-коду;
- фильтр по номеру телефона;
- ограничение количества запросов на определенный телефонный номер.

Для настройки параметров безопасности:

1. Перейдите в подраздел «Безопасность».
2. Введите значения в соответствующие поля и нажмите «Сохранить» (Рисунок 65 - Рисунок 69).

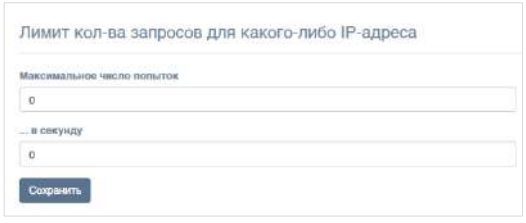

Рисунок 65

Рисунок 66

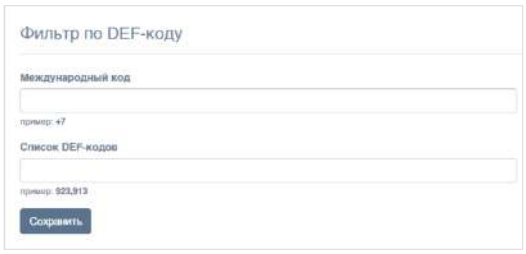

Рисунок 67

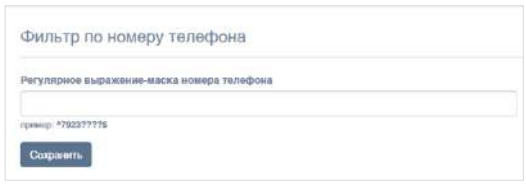

Рисунок 68

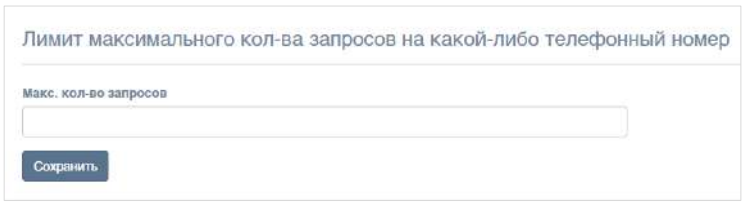

Рисунок 69

НАСТРОЙКА АУТЕНТИФИКАЦИИ АДМИНИСТРАТОРОВ

Для настройки загрузки учетных записей администратора из AD:

1. Перейдите в раздел «Аутентификация администраторов».
   Откроется окно (Рисунок 70):

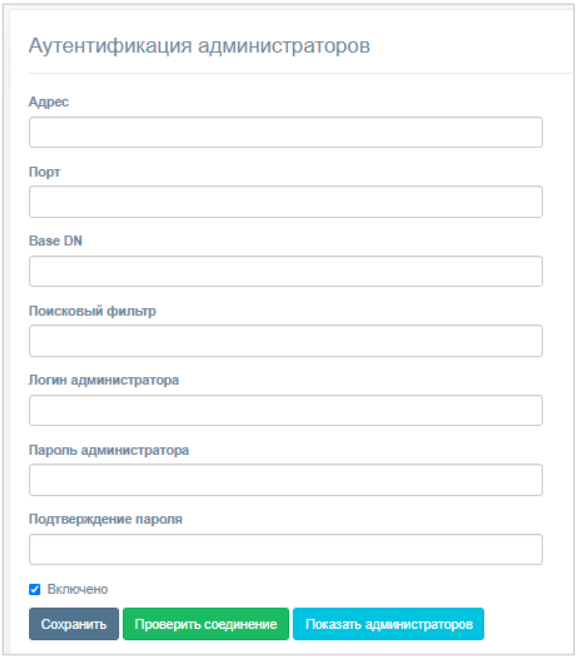

Рисунок 70

2. Настройте параметры, представленные ниже (Таблица 51).
   Значения параметров предоставляет администратор Active Directory.

Таблица 51

Параметр	Описание
Адрес	Адрес Active Directory
Порт	Порт подключения к AD
Base DN	Объект каталога, начиная с которого производится поиск

Поисковый фильтр	Фильтр для поиска LDAP. Должен обеспечивать фильтрацию активных пользователей, которым разрешено подключение к данному серверу. Рекомендуемая конструкция запроса: «**(&(objectClass=person)(objectClass=user)(memberOf:1.2.840.113556.1.4.1941:=cn=express,ou=Groups,dc=firma,dc=local))**» где «**cn= express,ou=Groups,dc=firma,dc=local**» DN группы, члены которой будут пользователями Express. При использовании кроссдоменных структур укажите домен **DC=ru** в параметрах подключения. Пример настройки синхронизации административных пользователей с фильтром: **(|(memberOf=adm,OU=Groups,DC=example,DC=local)(memberOf=CN=adm_bot,OU=Groups,DC=example,DC=local)(memberOf=adm_ib,OU=Groups,DC=example,DC=local))**
Логин администратора	Логин пользователя, имеющего доступ к чтению списка пользователей по указанному DN
Пароль администратора	Пароль пользователя, имеющего доступ к чтению списка пользователей по указанному DN
Подтверждение пароля	Подтверждение пароля пользователя, имеющего доступ к чтению списка пользователей по указанному DN

Для включения/отключения аутентификации администраторов Active Directory установите/снимите флаг «Включено».

Для проверки соединения с Active Directory нажмите кнопку «Проверить соединение».

После нажатия кнопки «Показать администраторов» выводится список администраторов Active Directory.

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 71), и CTS, подключенных к данному ETS (Рисунок 72).

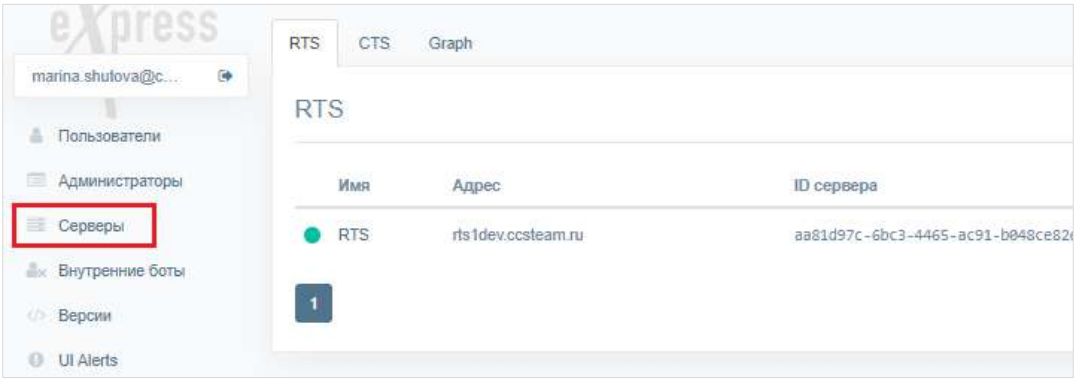

Рисунок 71

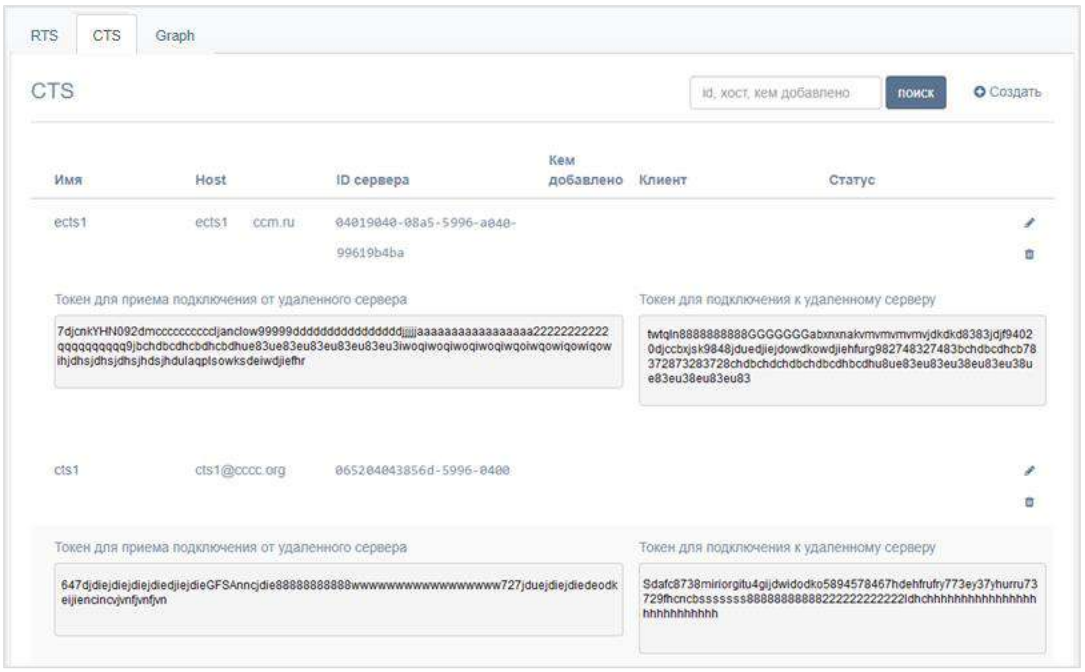

Рисунок 72

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.68.
3. Подключите CTS.

Для подключения CTS:

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

   Откроется окно (Рисунок 73):

Рисунок 73

3. 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. Обозначение должно отражать его корпоративную принадлежность, например «МСК-ETS-01», «express vip»;
   - 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).
4. Нажмите на кнопку «Сохранить».

Для просмотра графической схемы маршрутизации подключений откройте вкладку «Graph» (Рисунок 74).

Рисунок 74

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 75).

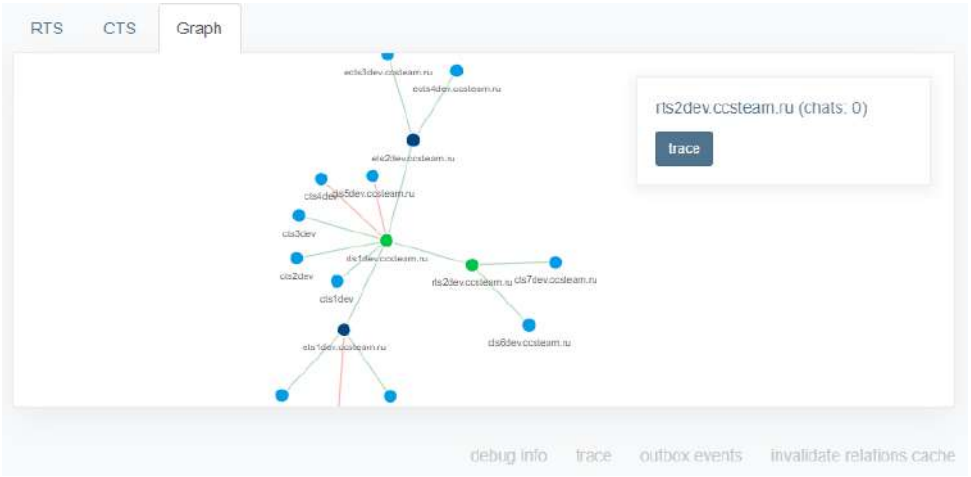

Рисунок 75

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 76 и Рисунок 77)

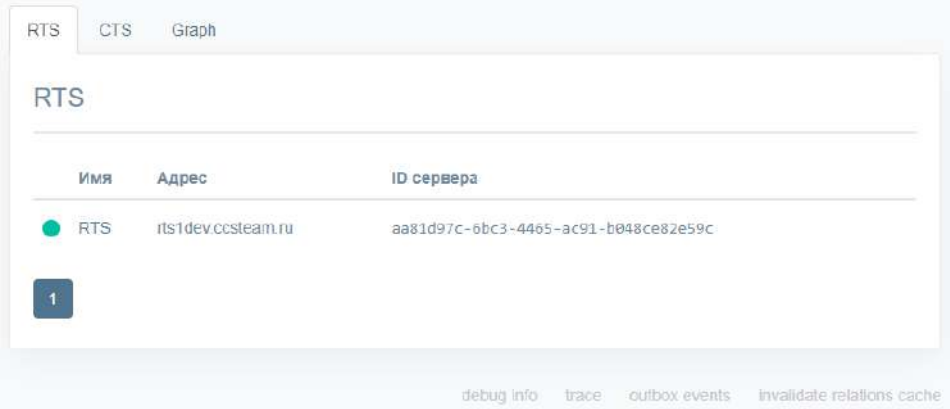

Рисунок 76

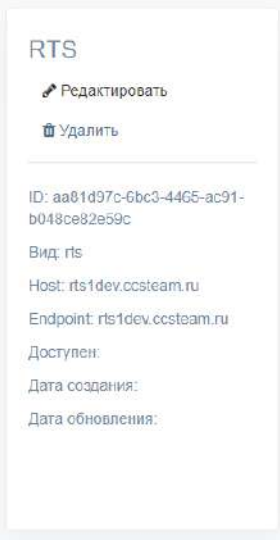

Рисунок 77

НАСТРОЙКА CTS

Настройка CTS включает в себя следующие процедуры:

- подключение TLS-сертификата (если это не было выполнено в процессе установки ETS);
- подключение Botx SSL-сертификата;
- настройка видео- и голосовой связи;
- подключение SMTP-сервера;
- подключение администраторов данного CTS из AD;
- настройка интеграции с Active Directory;
- настройка доверительных подключений.

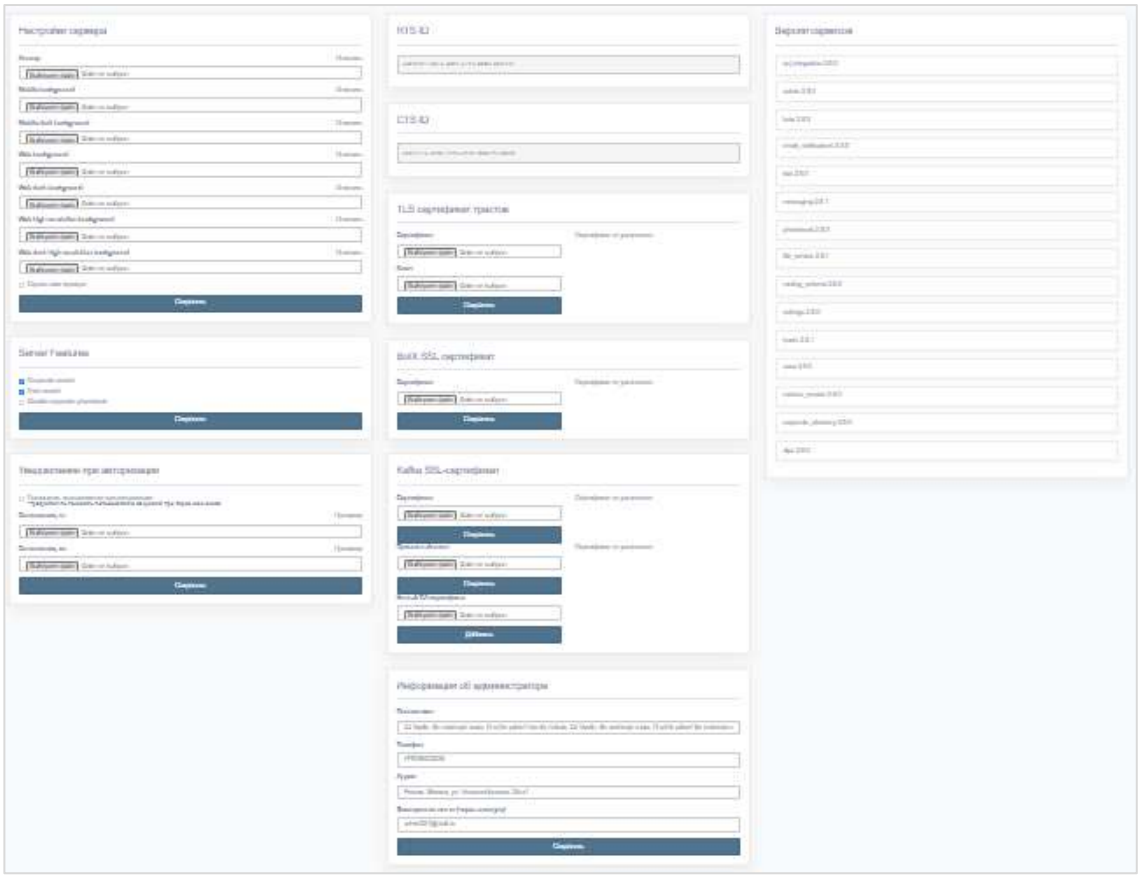

Рисунок 78

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 78).

2. Внесите данные о сертификате и ключе в соответствующие поля области «TLS-сертификат трастов» (Рисунок 79).

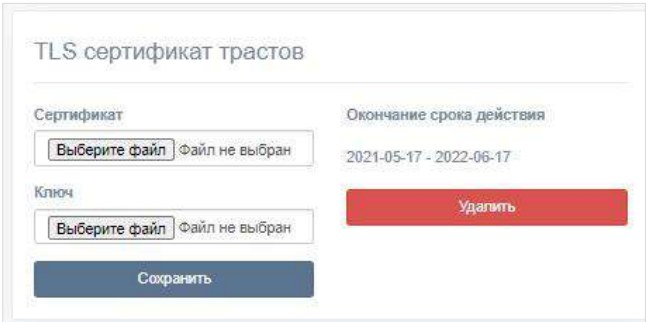

Рисунок 79

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 80).

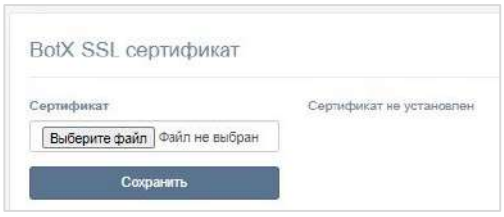

Рисунок 80

НАСТРОЙКА ВИДЕО- И ГОЛОСОВОЙ СВЯЗИ

Настройка видео- и голосовой связи выполняется после установки сервера VoEx и описана на стр. 41.

ПОДКЛЮЧЕНИЕ SMTP-СЕРВЕРА

Для подключения SMTP-сервера:

1. В меню выберите пункт «E-mail» (Рисунок 81).
2. В области «Настройки e-mail» заполните поля:
   - в поле «Имя приложения» укажите название приложения, от которого будут отправляться письма;
   - 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;
   - в поле «Отправлять письма через» укажите сервер, с которого будут отправляться письма (при выборе «Локальные настройки» в выпадающем списке, письма будут отправляться через сервер, настроенный в данном окне, при выборе «RTS» — письма будут отправляться через RTS).
3. Выберите тип защищенного соединения в выпадающем списке: SSL, Start/TLS или None.
4. Нажмите кнопку «Сохранить».

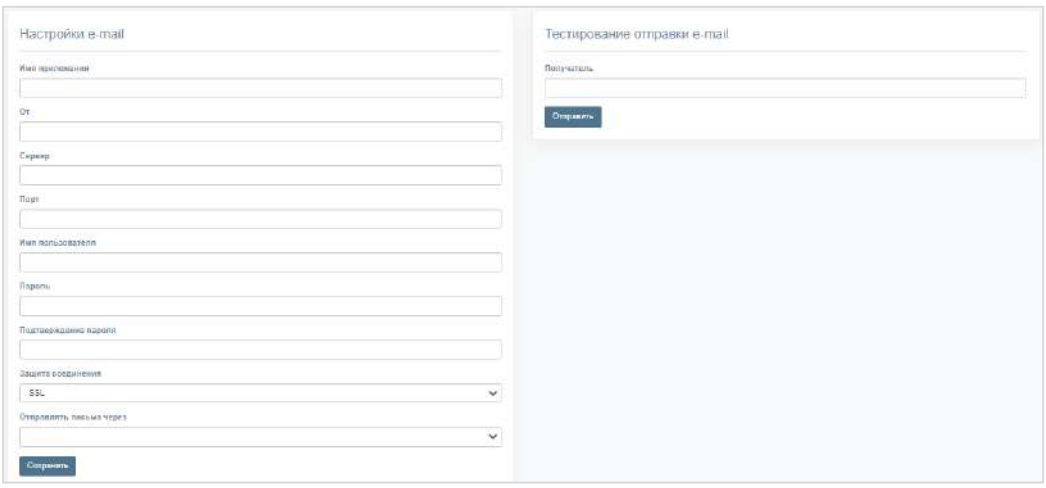

Рисунок 81

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

НАСТРОЙКА АУТЕНТИФИКАЦИИ АДМИНИСТРАТОРОВ

Раздел предназначен для подключения администраторов с помощью AD.

Для настройки загрузки учетных записей администратора из AD:

1. Перейдите в раздел «Аутентификация администраторов» (Рисунок 82).

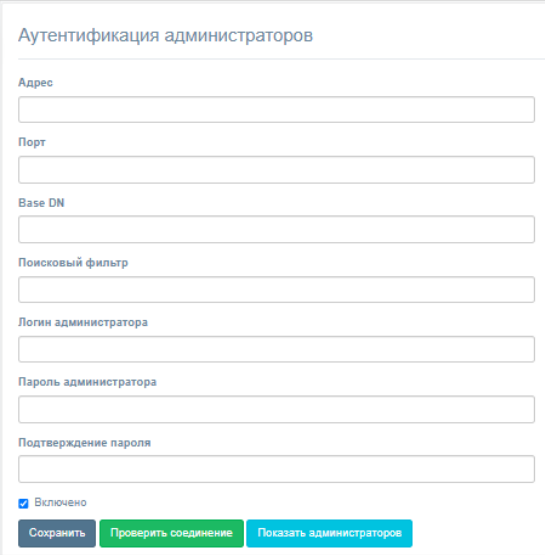

Рисунок 82

2. Настройте параметры, представленные ниже (Таблица 52).

   Значения параметров предоставляет администратор Active Directory.

Таблица 52

Параметр	Описание
Адрес	Адрес Active Directory
Порт	Порт подключения к AD
Base DN	Объект каталога, начиная с которого производится поиск
Поисковый фильтр	Фильтр для поиска LDAP. Должен обеспечивать фильтрацию активных пользователей, которым разрешено подключение к данному серверу. Рекомендуемая конструкция запроса: «`(&(objectClass=person)(objectClass=user)(memberOf:1.2.840.113556.1.4.1941:=cn= express,ou=Groups,dc=firma,dc=local))`» где «`cn= express,ou=Groups,dc=firma,dc=local`» DN группы, члены которой будут пользователями Express. При использовании кроссдоменных структур укажите домен `DC=ru` в параметрах подключения. Пример настройки синхронизации административных пользователей с фильтром: `(|(memberOf=adm,OU=Groups,DC=example,DC=local)(memberOf=CN=adm_bot,OU=Groups,DC=example,DC=local)(memberOf=adm_ib,OU=Groups,DC=example,DC=local))`
Логин администратора	Логин пользователя, имеющего доступ к чтению списка пользователей по указанному DN
Пароль администратора	Пароль пользователя, имеющего доступ к чтению списка пользователей по указанному DN
Подтверждение пароля	Подтверждение пароля пользователя, имеющего доступ к чтению списка пользователей по указанному DN

Для включения/отключения аутентификации администраторов Active Directory установите/снимите флаг «Включено».

Для проверки соединения с Active Directory нажмите кнопку «Проверить соединение».

НАСТРОЙКА РЕГИСТРАЦИИ

После нажатия кнопки «Показать администраторов» выводится список администраторов Active Directory.

Администратору доступны следующие способы для настройки регистрации/авторизации пользователей в системе:

- Active Directory (NTLM);
- E-mail;
- OpenID.

Для выбора способа регистрации:

1. Перейдите в раздел «Настройка регистрации» (Рисунок 83).
2. Выберите метод регистрации.
3. Укажите количество неудачных попыток при подтверждении регистрации пользователем.
4. Нажмите «Сохранить».

Примечание. Если пользователь превысил максимальное количество попыток ввода пароля, отправьте повторный запрос на регистрацию.

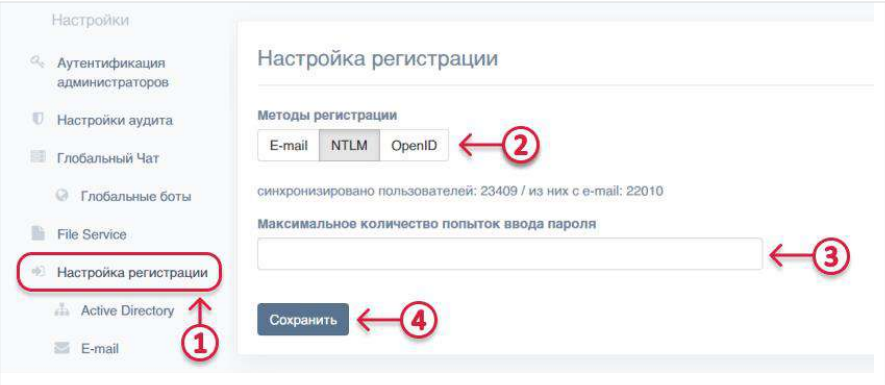

Рисунок 83

Выбранный метод регистрации будет сохранен. В верхней части экрана появится соответствующее системное сообщение.

Для завершения настройки задайте параметры для указанного способа в соответствующей вкладке: E-mail, NTML или OpenID.

НАСТРОЙКА ИНТЕГРАЦИИ С ACTIVE DIRECTORY

Для интеграции с AD подключитесь к AD и загрузите контакты на сервер.

При интеграции Express с корпоративным каталогом на базе Microsoft Active Directory создайте учетную запись с правами «Domain Users» и чтение контейнера «deleted objects» (https://support.microsoft.com/en-us/help/892806/how-to-let-non-administrators-view-the-active-directory-deleted-object).

Для подключения к Active Directory:

Примечание. Для корректной настройки системы под домен заказчика рекомендуется привлечь администратора Active Directory.

1. Перейдите в раздел «Active Directory».

   Откроется окно (Рисунок 84):

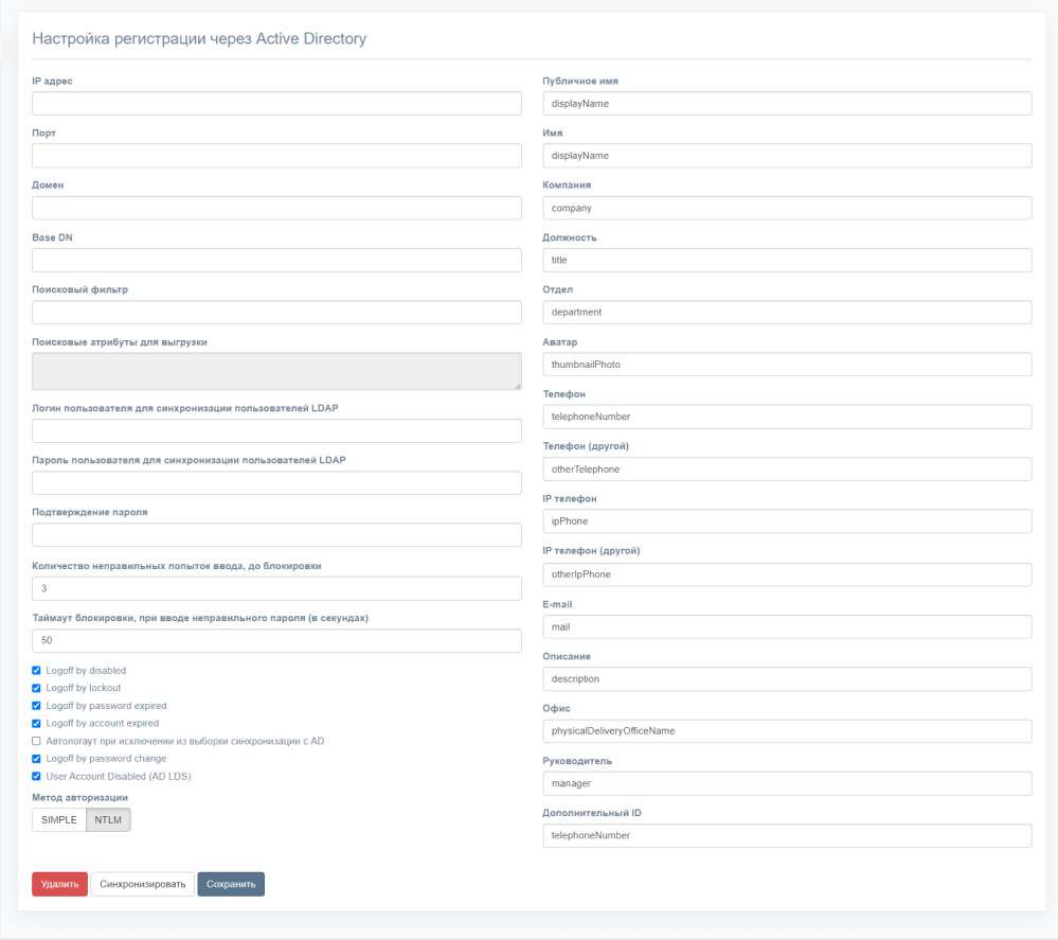

Рисунок 84

2. Заполните поля (Таблица 53):

Таблица 53

Название поля	Комментарий
IP-адрес	FQDN имя вашего домена или IP-адрес контроллера домена, например «**firma.local**». Если требуется подключение по протоколу LDAPS, то перед именем домена или IP-адреса введите «**ldaps://**», например «**ldaps://firma.local**»
Порт	Порт подключения к LDAP. Для протокола ldap введите значение «**389**», для протокола ldaps — значение «**636**»
Домен	Введите FQDN домена AD, например «**firma.local**»
Base DN	Введите точку начала просмотра каталога LDAP, например «**dc=firma,dc=local**». При реализации сложной доменной структуры (forest + несколько доменов) укажите «**dc=local**»
Поисковый фильтр	Фильтр для поиска LDAP. Должен обеспечивать фильтрацию активных пользователей, которым разрешено подключение к данному серверу.

Название поля	Комментарий
	Рекомендуемая конструкция запроса: «**(&(objectClass=person)(objectClass=user)(memberOf:1.2.840.113556.1.4.1941:=cn= express,ou=Groups,dc=firma,dc=local))**» где «**cn= express,ou=Groups,dc=firma,dc=local**» DN группы, члены которой будут пользователями Express. При использовании кроссдоменных структур укажите домен **DC=ru** в параметрах подключения. Пример настройки синхронизации административных пользователей с фильтром: **(&(objectClass=person)(objectClass=user)(CN=M-Express-Users,OU=Remote Users,OU=Groups,DC=oteko,DC=ru))**
Логин пользователя для синхронизации пользователей LDAP	Пользователь, которому разрешено чтение информации по вышеуказанному фильтру. Введите имя пользователя Active Directory в виде: «**net_bios_domain_name\user_name**» под которым будет осуществляться чтение каталога Active Directory, например «**firma\user_.name**»
Пароль пользователя для синхронизации пользователей LDAP	Пароль пользователя, которому разрешено чтение информации
Количество неправильных попыток ввода до блокировки	Введите количество попыток входа на одну попытку меньше, чем в аналогичном параметре групповой политики домена
Таймаут блокировки при вводе неправильного пароля (в секундах)	Введите время в секундах, равное времени сброса таймера неудачных попыток входа в групповой политики домена
Имя	Переменная должна соответствовать значению в AD
Компания	Переменная должна соответствовать значению в AD
Должность	Переменная должна соответствовать значению в AD
Отделение	Переменная должна соответствовать значению в AD
Аватар	Переменная должна соответствовать значению в AD. Файл для загрузки в должен соответствовать требованиям: • формат JPG; • объем не более 100 кб; • размер изображения должен вписываться в квадрат 500×500 пикселей
Телефон	Переменная должна соответствовать значению в AD
E-mail	Переменная должна соответствовать значению в AD
Описание	Переменная должна соответствовать значению в AD
Офис	Переменная должна соответствовать значению в AD
Руководитель	Переменная должна соответствовать значению в AD

3. Укажите события в Active Directory, при которых у пользователя Express будет повторно запрашиваться аутентификация на корпоративном сервере Express:
   - logoff by disabled — создает запрос на отключение пользователя от CTS. Данный запрос требует подтверждения в разделе "Logout list", после подтверждения пользователь будет автоматически отключен от CTS;
   - logoff by lockout — после блокировки профиля пользователя в AD из-за неправильно введенного пароля создается запрос на отключение пользователя от CTS. Данный запрос требует подтверждения в разделе "Logout list", после подтверждения пользователь будет автоматически отключен от CTS;
   - logoff by password expired — если срок действия пароля пользователя в AD истек, создается запрос на отключение пользователя от CTS. Данный запрос требует подтверждения в разделе "Logout list", после подтверждения пользователь будет автоматически отключен от CTS;
   - logoff by account expired — если срок действия учетной записи пользователя в AD истек, создается запрос на отключение пользователя от CTS.

Данный запрос требует подтверждения в разделе "Logout list", после подтверждения пользователь будет автоматически отключен от CTS;

- автологаут при исключении из выборки синхронизации с AD — если учетная запись исключена из группы, пользователь будет автоматически отключен от CTS;
- logoff by password change — если пароль от учетной записи пользователя в AD изменен, пользователь будет автоматически отключен от CTS;
- User Account Disabled — если профиль пользователя заблокирован.

4. Выберите метод аутентификации в Active Directory по логину и паролю пользователей Express, рекомендуемое значение «NTLM».
5. Нажмите кнопки «Сохранить» и «Синхронизировать».

   Если все настройки указаны правильно, в течение 3-х часов список пользователей появится в разделе «Пользователи».

В случае возникновения проблем при синхронизации проверьте корректность полученных данных из AD с помощью команды ldapsearch (красным цветом выделены параметры, которые требуется заменить в соответствии с настройками подключения к AD):

```
$ ldapsearch -v -h myhost.mydomain.mytld -p 389 -D 'mydomain\myuser'
-W -b "cn=Users,dc=mydomain,dc=mytld" -s sub
"(&(objectCategory=person)(objectClass=user)(memberOf:1.2.840.113556.
1.4.1941:=CN=ExpressUsers,CN=Users,DC=mydomain,DC=mytld))" -x
```

Примечание. Для OS Ubuntu версии 19 и выше, а также при возникновении ошибки на других OS, выполните следующую команду:

```
$ ldapsearch -v -H myhost.mydomain.mytld -p 389 -D 'mydomain\myuser' -W -b
"cn=Users,dc=mydomain,dc=mytld" -s sub "(&(objectCategory=person)(ob-
jectClass=user)(memberOf:1.2.840.113556.1.4.1941:=CN=ExpressUsers,CN=Us-
ers,DC=mydomain,DC=mytld))" -x
```

Для предоставления доступа пользователей к Express создайте группы пользователей Express в Active Directory. Тип группы — «Security», видимость группы — «Universal».

При интеграции Express с корпоративным каталогом на базе LDAP-совместимого сервера создайте учетную запись с правами чтения каталога.

Для настройки видимости полей профиля:

1. Перейдите в раздел «Настройки видимости полей».

   Откроется окно «Видимость полей профиля»:

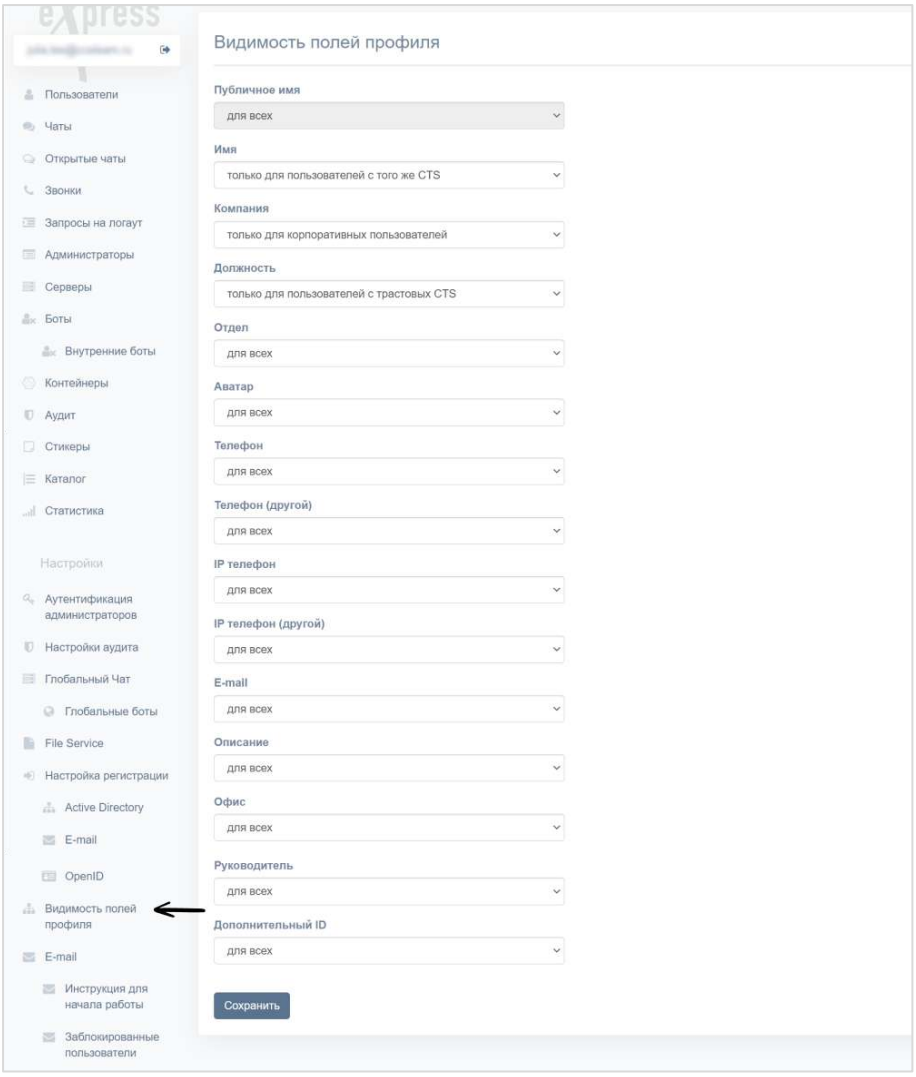

Рисунок 85

2. Установите значения корпоративных переменных профиля в полях доступа.

   Корпоративные переменные профиля автоматически заполняются значениями из базы AD и доступны для просмотра в приложении в карточке чата. Уровень доступа к данным принимает следующие значения (Таблица 54):

Таблица 54

Название поля	Комментарий
Только для пользователей с того же CTS	Значение данного поля доступно для просмотра в приложении только пользователям, зарегистрированным на данном корпоративном сервере
Только для пользователей с трастовых CTS	Значение данного поля доступно для просмотра в приложении только пользователям, зарегистрированным на: • данном корпоративном сервере; • серверах, с которыми установлено трастовое соединение
Только для корпоративных пользователей	Значение данного поля доступно для просмотра в приложении всем пользователям, зарегистрированным в корпоративном контуре
Для всех	Значение данного поля доступно для просмотра в приложении всем пользователям

НАСТРОЙКА E-MAIL

Для настройки регистрации по маске e-mail:

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

   Откроется окно «Настройки e-mail» (Рисунок 86).
2. Введите маску e-mail в поле, используя регулярное выражение (например, ^.*?@corporate.local).
3. Нажмите на кнопку «Сохранить».

Рисунок 86

После успешного сохранения изменений в верхней части экрана появится системное сообщение (Рисунок 87).

Рисунок 87

НАСТРОЙКА OPENID

Примечание. Перед настройкой OpenID необходимо настроить интеграцию CTS и Keycloak. См. «Интеграция CTS и Keycloak».

Для настройки OpenID:

1. Перейдите в раздел «Настройка регистрации» → «OpenID».

   Откроется окно настройки параметров регистрации через OpenID (Рисунок 88).

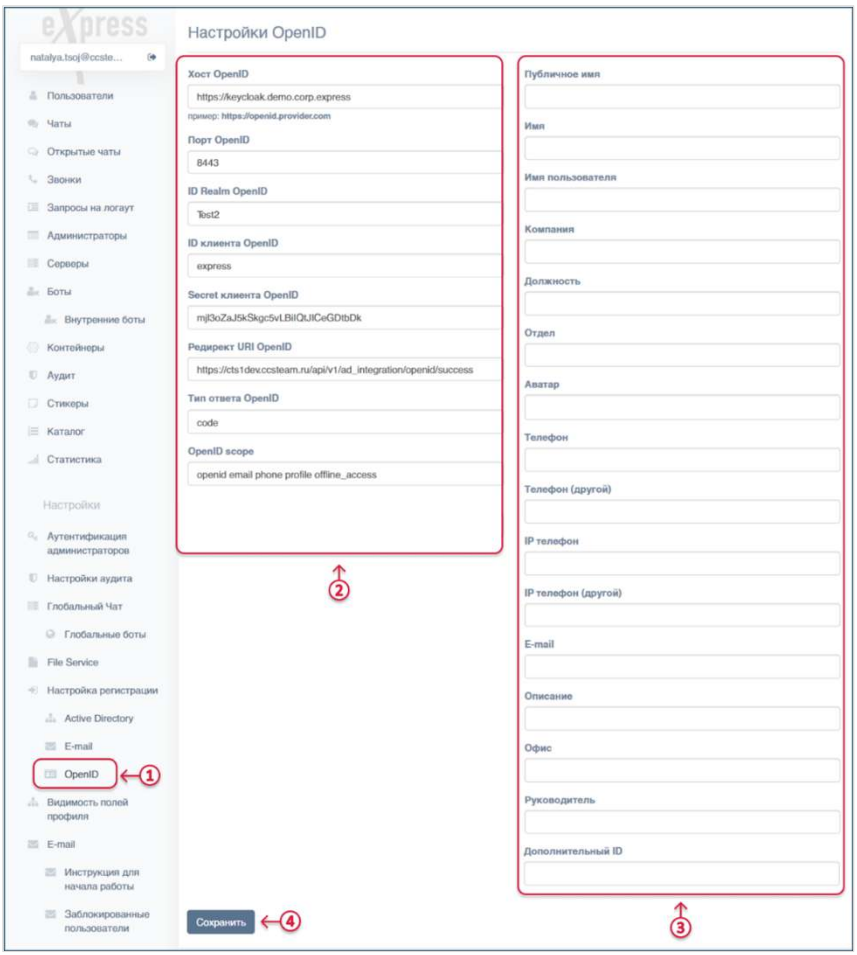

Рисунок 88

2. В полях левой колонки укажите значения параметров.

   Примечание. В поле «OpenID scope» рекомендуется указать значение из строки «scope» консоли администратора Keycloak. Это необходимо для получения списка передаваемого «scope».

   Для этого откройте консоль администратора Keycloak, перейдите в раздел «Clients» →Client scopes→Client ID→Evaluate→Generated acsess token→строка «scope» и скопируйте значение (Рисунок 89).

3. В полях правой колонки укажите атрибуты, которые будут отображаться в карточке пользователя.

   Для настройки уровней доступа к атрибутам.

4. Нажмите кнопку «Сохранить».
5. В файл settings.yaml сервера CTS Back добавьте:

```
openid_enabled: true
```

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

```
dpl -d ad_integration
```

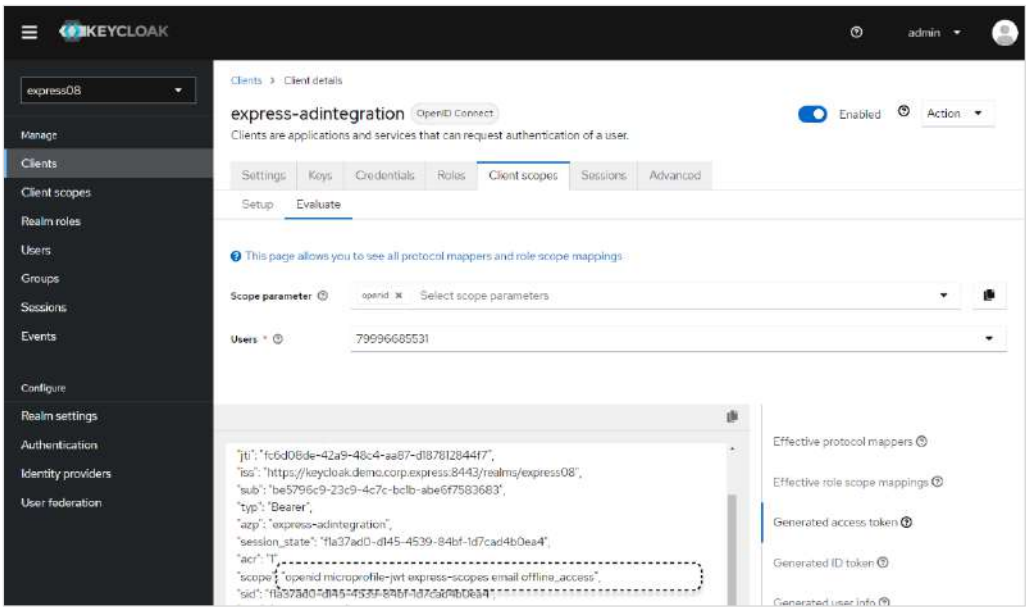

Рисунок 89

НАСТРОЙКА ДОВЕРИТЕЛЬНЫХ ПОДКЛЮЧЕНИЙ

Для создания доверительного подключения (траста):

1. Откройте пункт меню «Серверы».
2. Выберите вкладку «Trusts» (Рисунок 90).

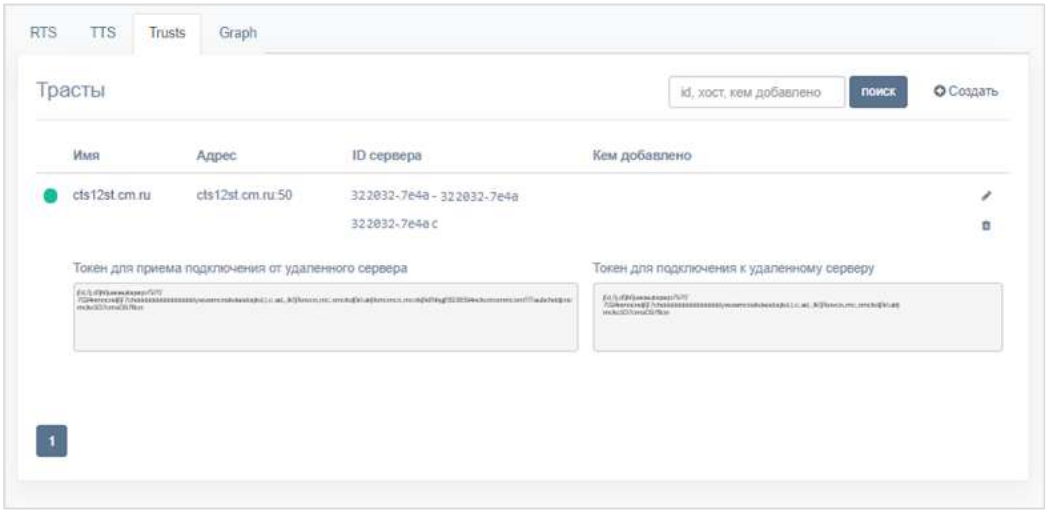

Рисунок 90

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

Откроется окно (Рисунок 91):

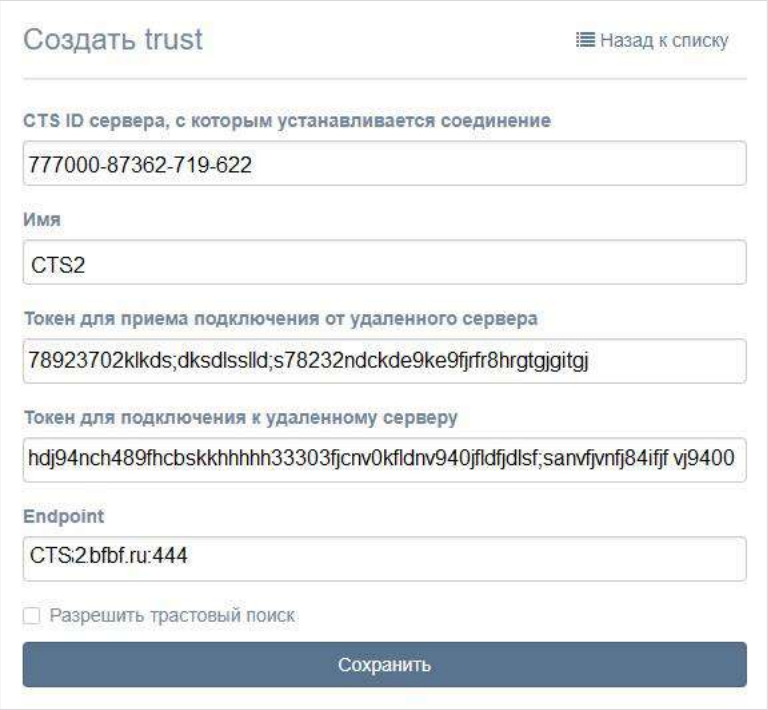

Рисунок 91

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).

Глава 4

ПРОЦЕДУРА ОБНОВЛЕНИЯ

Полностью процедура обновления системы, её компонентов и дополнительного ПО описана в документе «Руководство администратора. Обновление».

Процедура обновления системы включает:

- обновление ОС;
- ручное обновление серверов,
- обновление серверов с использованием Ansible-сценариев;
- обновление отказоустойчивой конфигурации.

Процедура обновления дополнительных компонентов системы и интеграционного ПО включает:

- обновление десктоп-версии;
- обновление сертификата;
- обновление Kafka;
- обновление PostgreSQL.

Документ «Руководство администратора. Обновление» содержит описание процедуры обновления СК «Express» до версии 3.0 и процесса миграции больших баз данных.

Также в документе приведено описание возможных аварийных ситуаций при обновлении из локального репозитория Registery.

Глава 5

УСТРАНЕНИЕ ТИПОВЫХ ОШИБОК

Примечание. Все работы на серверах должны проводиться 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
```

Ошибка авторизации

Данная ошибка может появиться в том случае, если аккаунт пользователя появился в системе после синхронизации с AD:

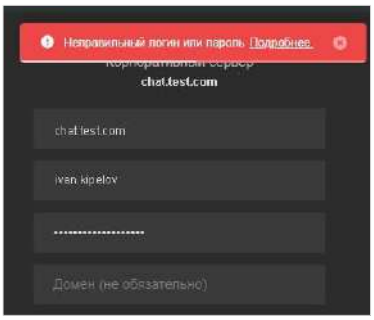

Рисунок 92. Ошибка авторизации

Возникновение данной ошибки происходит в том случае, если в AD зарегистрированы пользователи с разными User logon name и в настройках AD указан другой домен.

Для решения проблемы при авторизации пользователь должен дополнить свой логин доменом через @, например user9@it-company.local.

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 конференцсвязи
			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
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 Registry.public.express	TCP/443	Клиентский доступ к публичному контуру Express с использованием протокола HTTPS

№	Источник	Получатель	Порт и протокол	Описание
12	Внешний пользователь	RTS ru.public.express	TCP/443	Обеспечение взаимодействия внешнего пользователя с RTS
13	Внешний пользователь	xlnk.ms	TCP/443	Обеспечение работы ссылок на чаты и звонки, если заказчик не указывает собственный сервер для подобных ссылок. Подробнее см. в ссылки на чаты/звонки в документе «Руководство администратора. Эксплуатация», раздел «Ссылки на чаты и звонки»
14	Внутренний пользователь	xlnk.ms	TCP/443	Обеспечение работы ссылок на чаты и звонки, если заказчик не указывает собственный сервер для подобных ссылок. Подробнее см. в ссылки на чаты/звонки в документе «Руководство администратора. Эксплуатация», раздел «Ссылки на чаты и звонки»
15	Внешний пользователь	updates.express.ms	TCP/443	Сервер для поиска и скачивания обновления декстоп-версии приложения
16	Внутренний пользователь	updates.express.ms	TCP/443	Сервер для поиска и скачивания обновления декстоп-версии приложения
17	Внешний пользователь	m-ru.public.express (89.108.82.35)	TCP/UDP/3478	Обеспечение проведения звонков с внешними пользователями
18	Внешний пользователь	storage.yandexcloud.net	TCP/443	Обеспечение доступа к хранилищу с файлами внешних пользователей
19	Сервер Single CTS	RTS ru.public.express	TCP/5001	Обеспечение взаимодействия корпоративного сервера Express с RTS
20	Внутренний пользователь	RTS ru.public.express	TCP/443	Клиентский доступ к публичному контуру Express с использованием протокола HTTPS
21	Внешний пользователь	Сервер веб-клиента corp.express	TCP/443	Клиентский доступ к серверу веб-клиента в публичном контуре
22	Внутренний пользователь	Сервер веб-клиента corp.express	TCP/443	Клиентский доступ к серверу веб-клиента в публичном контуре
23	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		
24	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
25	RTS ru.public.express	SMS оператор	TCP/443	Отправка SMS-сообщений пользователям

№	Источник	Получатель	Порт и протокол	Описание
26	RTS ru.public.express	Служба push-уведомлений Huawei	TCP/443	Отправка push-уведомлений пользователям Huawei
27	RTS ru.public.express	Служба push-уведомлений Apple	TCP/443	Отправка push-уведомлений пользователям iOS
28	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;
- UDP/3478;
- DP/49152-65535;
- UDP/20000-40000.

Порт TCP/80 добавляется при использовании Let's Encrypt.

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
7	Сервер Back CTS	Сервер SMTP	TCP/25	Обеспечение отправки писем с ПИН-кодом аутентификации по протоколу SMTP

№	Источник	Получатель	Порт и протокол	Описание
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
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
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
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 конференц-связи

№	Источник	Получатель	Порт и протокол	Описание
			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 ru.public.express	TCP/5001	Обеспечение взаимодействия корпоративного сервера Express с RTS
20	Сервера Let`s Encrypt	Сервер ETS Сервер Single CTS	TCP/80,443	Данное правило требуется при использовании бесплатного сертификата от компании Let`s Encrypt
	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 (Внешний IP NAT)	TCP/443	Клиентский доступ к корпоративному контуру Express с использованием протокола HTTPS
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
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 конференц-связи
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.
10	Сервер ETS		TCP/53	

№	Источник	Получатель	Порт и протокол	Описание
		Сервер DNS и NTP	UDP/53	Обеспечение работы разрешения имен DNS
			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	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
27	Внешний пользователь	Сервер Front CTS (Внешний IP NAT)	TCP/443	Клиентский доступ к корпоративному контуру Express с использованием протокола HTTPS
28	Сервер Front CTS (Внешний IP NAT)	Партнерский сервер Express CTS	TCP/443,5001	Обеспечение взаимодействия CTS с RTS
			UDP/20000-40000	Обеспечение передачи медиаданных по протоколу SRTP конференцсвязи
	Партнерский сервер Express CTS	Сервер Front CTS (Внешний IP NAT)	TCP/443,5001	Обеспечение взаимодействия CTS и RTS
			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

НАСТРОЙКА ХОСТОВ SMARTAPPPROXY

Если файл из КСПД должен стать частью веб-страницы SmartApp Frontend (например, видео в плеере), передача файлов через сервис «File Service» не работает. Для этой задачи существует вариант передачи файлов через smartapp_proxy.

Примечание.

- данный функционал доступен только в SmartApp без кеширования и с проксированием;
- данная инструкция актуальна для сборки сервера CTS 3.4 или выше.

Для настройки хостов SmartAppProxy на Single CTS:

1. Добавьте в файл settings.yaml сервера CTS:

```
smartapp_proxy_enabled: true
smartapp_proxy_env_override:
  COOKIE_KEY: _file_service_key
  COOKIE_SIGNING_SALT: <salt из file_service или vm5ponDZ вшитый дефолт>
```

2. Выполните деплой:

```
dpl -p
dpl -d smartapp_proxy admin
```

3. Завершите настройку в консоли администратора сервера CTS (см. «Руководство администратора. Эксплуатация», раздел «Настройка хостов SmartAppProxy»).

Для настройки хостов SmartAppProxy на разделенном корпоративном сервере (Front CTS+Back CTS):

1. Добавьте в файл settings.yaml сервера Back CTS:

```
smartapp_proxy_enabled: true
smartapp_proxy_env_override:
  COOKIE_KEY: _file_service_key
  COOKIE_SIGNING_SALT: <salt из file_service или vm5ponDZ вшитый дефолт>
```

2. Выполнить деплой:

```
dpl -p
dpl -d smartapp_proxy admin
```

3. Завершите настройку в консоли администратора сервера CTS (см. «Руководство администратора. Эксплуатация», раздел «Настройка хостов SmartAppProxy»).

Приложение 8

СЕТЕВАЯ СХЕМА ВЗАИМОДЕЙСТВИЯ С АТС ДЛЯ SINGLE CTS

Сетевая схема взаимодействия с АТС при развертывании Single CTS представлена на Рисунок 93.

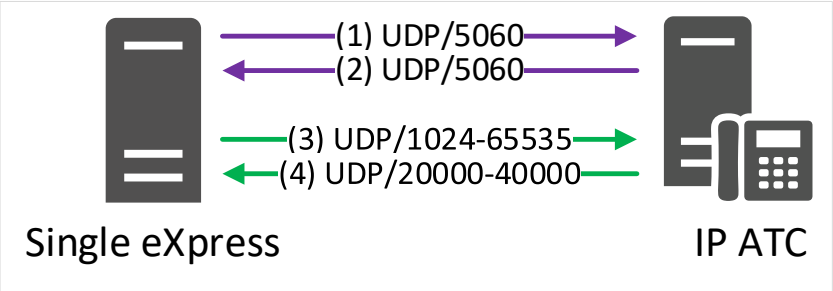

Рисунок 93

Сетевые взаимодействия для схемы развертывания Single (номера соединений в таблице соответствуют номерам соединений на Рисунок 93):

Таблица 55

№	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 9

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 94.

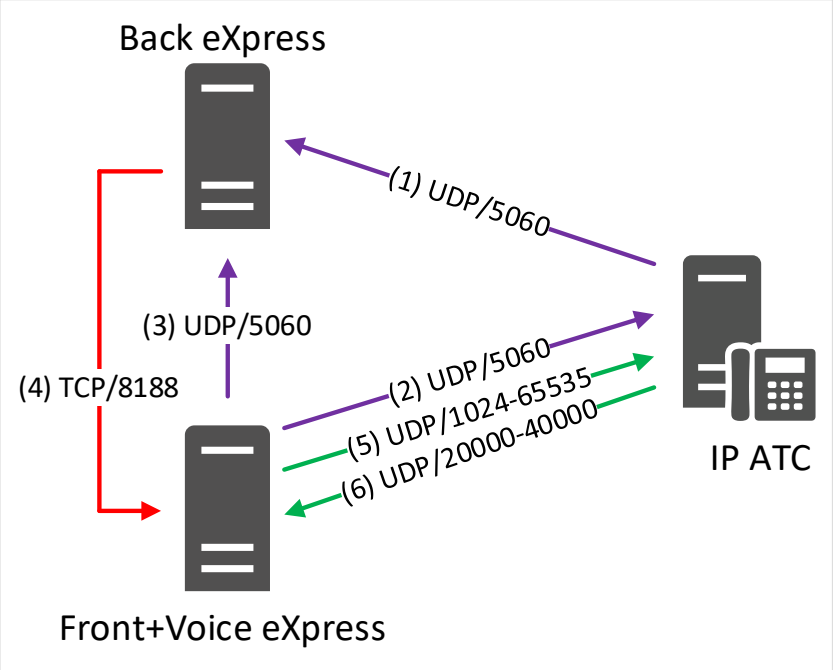

Рисунок 94

Сетевые взаимодействия для схемы развертывания Front CTS + VoEx и Back CTS (номера соединений в таблице соответствуют номерам на Рисунок 94):

Таблица 56

№	IP источника	Порт источника	IP назначения	Порт назначения	Протокол	Описание
1	IP АТС	1024-65535	IP Back eXpress	5060	UDP	SIP сигнализация вызова к eXpress
2	IP Front+Voice eXpress	1024-65535	IP АТС	5060	UDP	SIP сигнализация вызова к IP АТС
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 АТС	1024-65535	UDP	Медиаданные вызова к IP АТС
6	IP АТС	1024-65535	IP Front+Voice eXpress	20000-40000	UDP	Медиаданные вызова к eXpress

Приложение 10

ИНТЕГРАЦИЯ CTS И KEYCLOAK

Keycloak — это продукт с открытым исходным кодом для реализации единого входа. Данное программное обеспечение позволяет управлять идентификацией и доступом к сервисам и приложениям. Лицензия ПО — Apache License 2.0, разработано RedHat, Inc.

Основные функции Keycloak:

- управление пользователями, группами и ролями;
- аутентификация клиентских приложений по протоколам OpenID Connect и SAML;
- единый вход (single sign-on);
- поддержка как реляционных СУБД, так и NoSQL (MongoDB);
- кластеризация;
- ограниченная поддержка аутентификации по OTP (с помощью Google Authenticator);
- интеграция с внешними директориями LDAP и Active Directory;
- интеграция с социальными сервисами (Facebook, Twitter, GitHub, StackExchange etc.)
- расширение функциональности через разработку собственных SPI.

ЭТАПЫ РЕГИСТРАЦИИ/АВТОРИЗАЦИИ

Основные этапы регистрации/авторизации пользователя на CTS с помощью Keycloak показаны на схеме ниже (Рисунок 95):

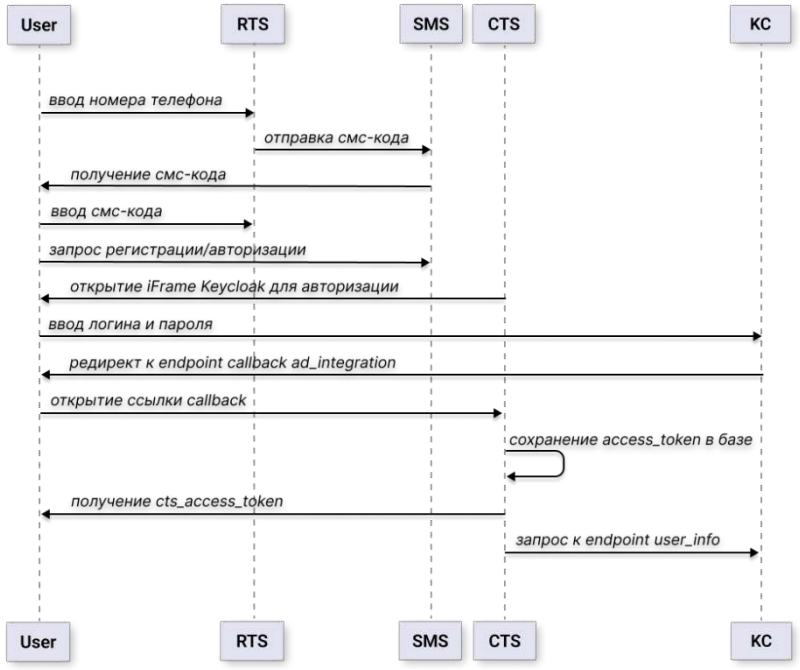

Рисунок 95

СЕТЕВЫЕ ВЗАИМОДЕЙСТВИЯ

Существуют следующие варианты сетевых взаимодействий:

- пользовательский доступ к интерфейсу Keycloak;
- пользовательский доступ к интерфейсу Keycloak через revers proxy.

Схема пользовательского доступа к интерфейсу Keycloak показана на рисунке ниже (Рисунок 96):

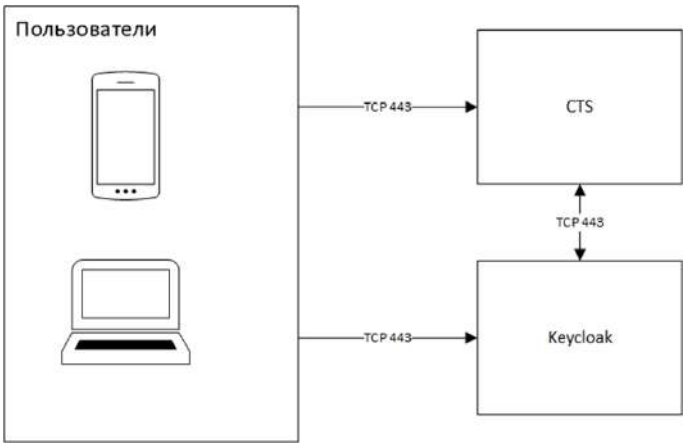

Рисунок 96

Схема пользовательского доступа к интерфейсу Keycloak через revers proxy показана на рисунке ниже (Рисунок 97):

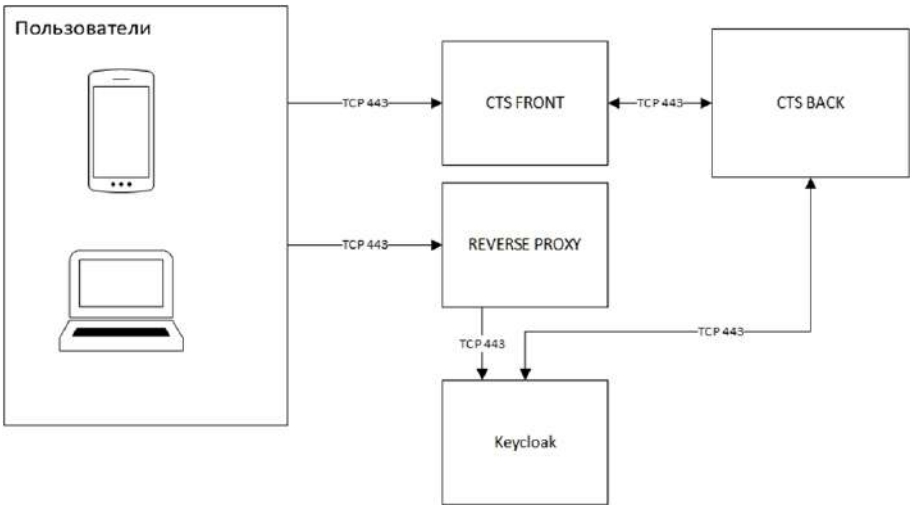

Рисунок 97

НАСТРОЙКА ИНТЕГРАЦИИ

Примечание. Данное описание настройки интеграции составлено на примере интерфейса консоли администратора Keycloak версии 21.1.2.

Настройка интеграции CTS и Keycloack включает в себя следующие процедуры:

- создание client scope;
- настройка маппинга полей;
- создание client;

- настройка отображение формы авторизации Keycloak;
- настройка авторизацию по QR-коду.

СОЗДАНИЕ CLIENT SCOPE

Для интеграции CTS и Keycloak, необходимо сначала создать client scope и настроить маппинг полей:

- username — обязательный параметр (в консоли администратора CTS указать соответствие «Имя пользователя» — «preferred_username»);
- user ID — обязательный параметр;
- domain — обязательный параметр (в консоли администратора CTS указать соответствие «Домен» — «domain»)
- name — необязательный параметр;
- public name — необязательный параметр;
- company — необязательный параметр.

Дополнительные мапперы создаются опционально с типом «User Attribute» и привязываются к конечной точке «user-info».

Для создания client scope:

1. В консоли администратора Keycloak перейдите в раздел «Client scopes».
2. Нажмите на кнопку «Create client scope» и задайте следующие значения (Рисунок 98):

Параметр	Значение
Name	Название client scope. Например, **express-scopes**
Description	Оставить незаполненным
Type	None
Display on consent screen	On
Consent screen text	Оставить незаполненным
Include in token scope	On
Display Order	Оставить незаполненным

3. Нажмите «Save».

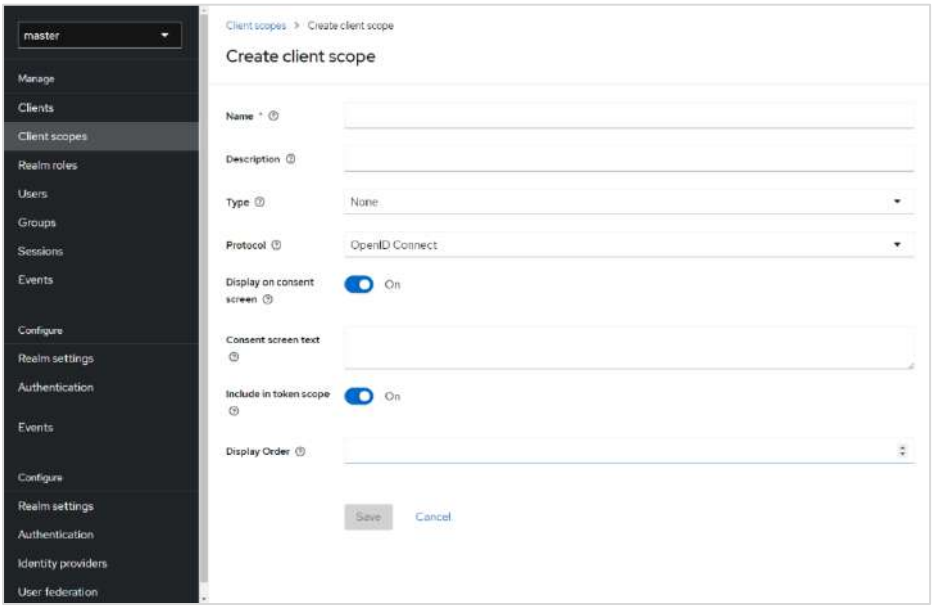

Рисунок 98

Для добавления маппинга полей типа «User property»:

1. В созданном client scope «express-scopes» выберите вкладку «Mappers».
2. Нажмите на кнопку «Configure a new mapper» (Рисунок 99).

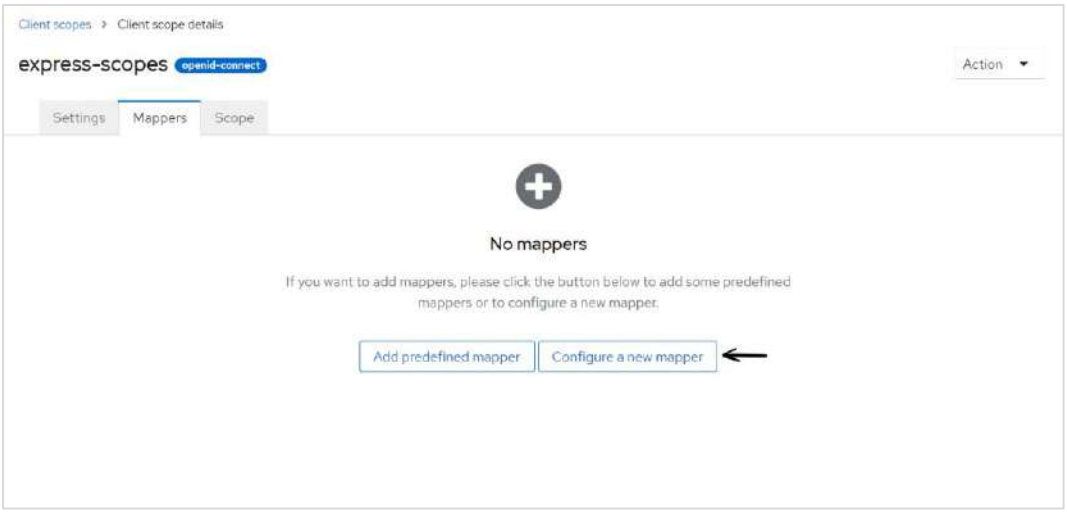

Рисунок 99

3. В окне «Configure a new mapper» выберите «User Property».
4. В отобразившемся окне задайте следующие значения (Рисунок 100).
   - для атрибута «Username»

Поле/переключатель	Значение
Mapper type	User Property
Name	username
Property	username
Token Claim Name	preferred_username
Claim JSON Type	String
Add to ID token	On
Add to access token	On
Add to userinfo	On

   - для атрибута «User ID»

Поле/переключатель	Значение
Mapper type	User Property
Name	User ID
Property	id
Token Claim Name	user_id
Claim JSON Type	String
Add to ID token	On
Add to access token	On
Add to userinfo	On

5. Нажмите «Save».

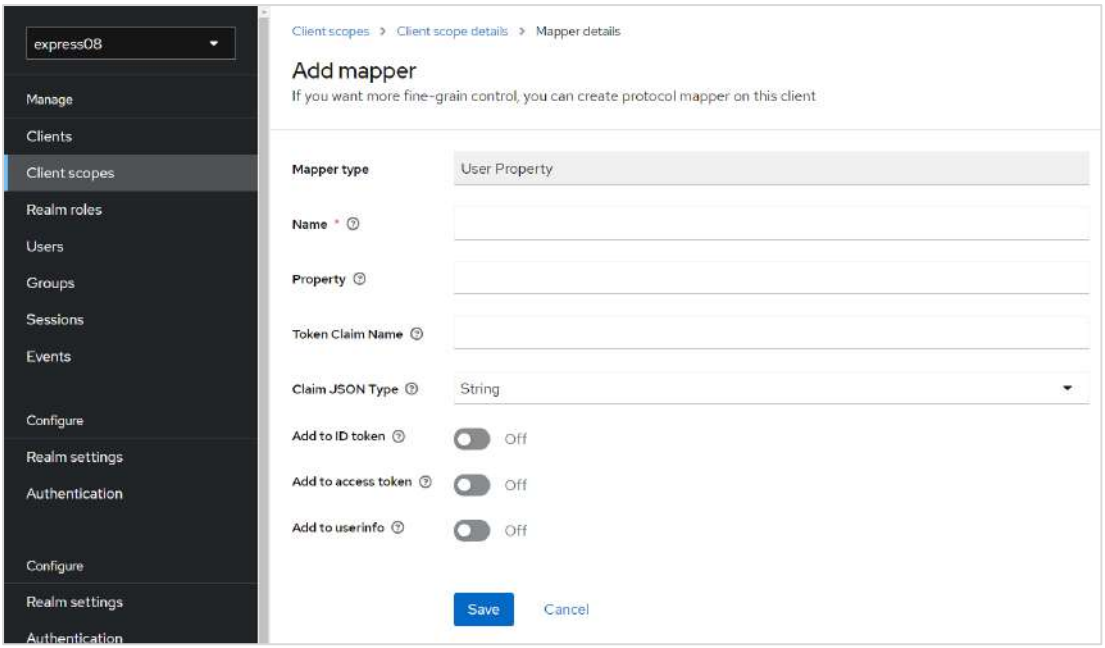

Рисунок 100

Для добавления маппинга полей типа «User attribute»:

1. В созданном client scope «express-scopes» выберите вкладку «Mappers».
2. Нажмите на кнопку «Configure a new mapper» (Рисунок 99).
3. В окне «Configure a new mapper» выберите пункт «User Attribute»
4. В отобразившемся окне задайте следующие значения (Рисунок 101):
   - для атрибута «Domain» (обязательный атрибут)

Поле/переключатель	Значение
Mapper type	User Attribute
Name	Domain
User Attribute	domain
Token Claim Name	domain
Claim JSON Type	String
Add to ID token	Off
Add to access token	Off
Add to userinfo	On
Multivalued	Off
Aggregate attribute values	Off

   - для атрибута «Name» (опциональный атрибут)

Поле/переключатель	Значение
Mapper type	User Attribute
Name	Name
User Attribute:	name
Token Claim Name	name
Claim JSON Type	String
Add to ID token	Off
Add to access token	Off
Add to userinfo	On
Multivalued	Off
Aggregate attribute values	Off

- для атрибута «Public name» (опциональный атрибут)

Поле/переключатель	Значение
Mapper type	User Attribute
Name	Public name
User Attribute:	public_name
Token Claim Name	public_name
Claim JSON Type	String
Add to ID token	Off
Add to access token	Off
Add to userinfo	On
Multivalued	Off
Aggregate attribute values	Off

- для атрибута «Company» (опциональный атрибут)

Поле/переключатель	Значение
Mapper type	User Attribute
Name	Company
User Attribute:	company
Token Claim Name	company
Claim JSON Type	String
Add to ID token	Off
Add to access token	Off
Add to userinfo	On
Multivalued	Off
Aggregate attribute values	Off

5. Нажмите «Save».

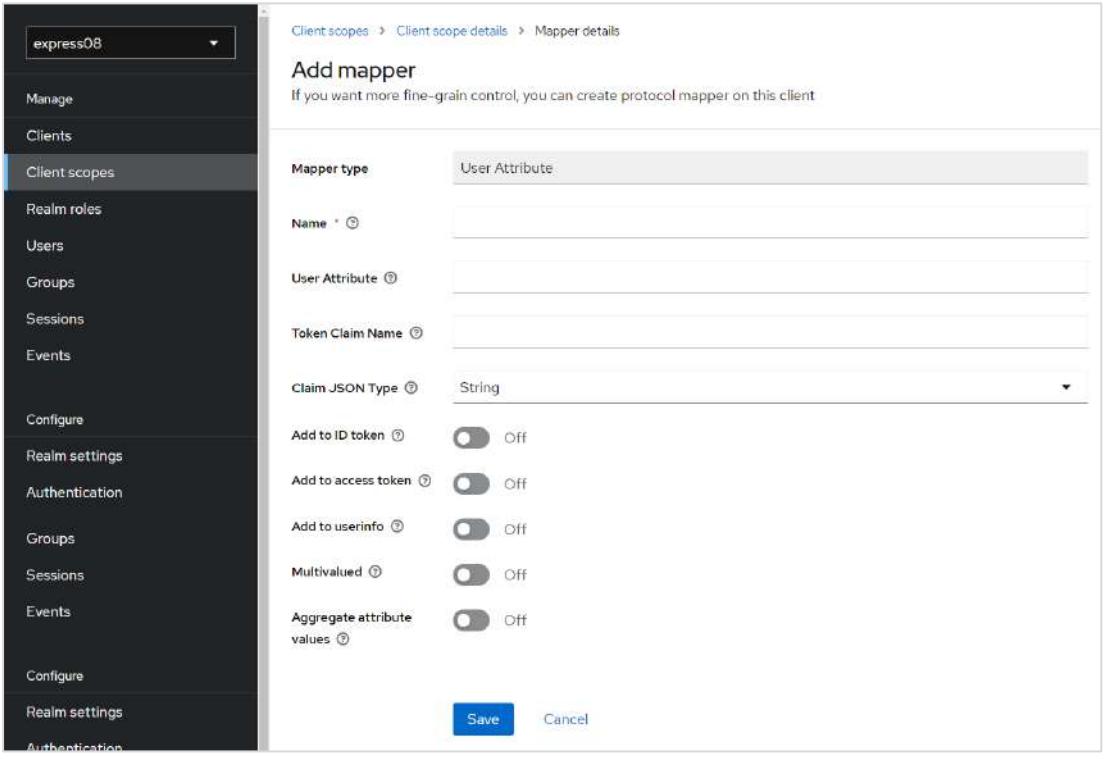

Рисунок 101

СОЗДАНИЕ CLIENT

Для создания Client:

1. В консоли администратора Keycloak перейдите в раздел «Clients».
2. Нажмите на кнопку «Create client».
3. В открывшемся окне задайте следующие значения (Рисунок 102):

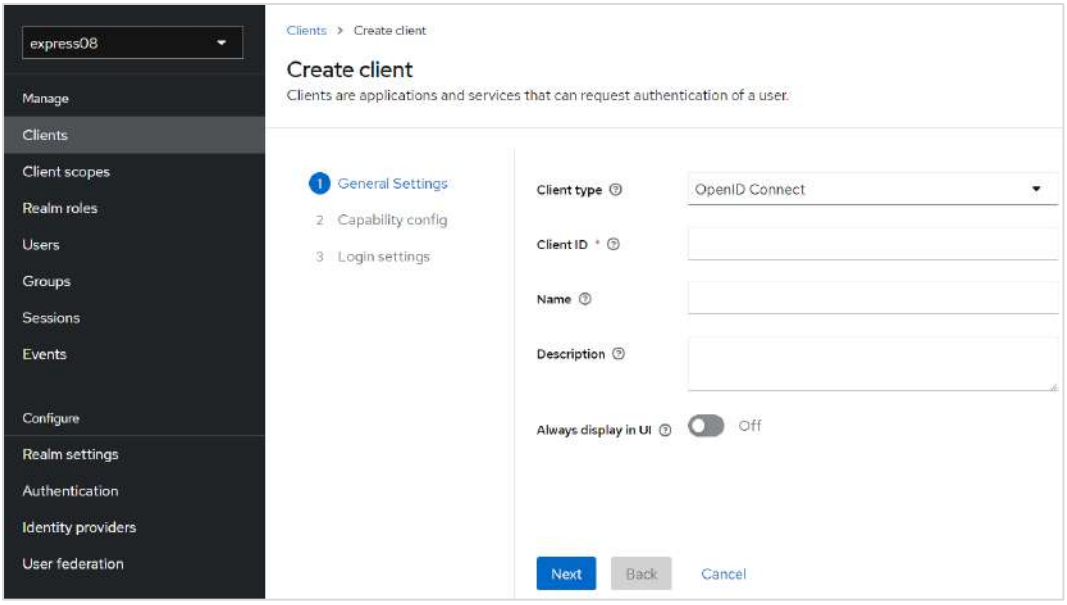

Рисунок 102

Параметр	Значение
Client type	OpenID Connect
Client ID	Идентификационный номер клиента, например **«express-adintegration»**
Name	CTS integration
Description	Оставить незаполненым
Always display in UI	Off

4. Нажмите на кнопку «Next».
5. В открывшемся окне задайте следующие значения:

Параметр	Значение
Client authentication	On
Authorization	Оставить незаполненым
Authentication flow	Установите флаги: • «Standard flow»; • «Direct access grants»; • «Service accounts roles»; • «OIDC CIBA Grant»

6. Нажмите на кнопку «Next».

Параметр	Значение
Root URL	Оставить незаполненым
Home URL	Оставить незаполненым
Valid redirect URIs	https://cts.company.local/api/v1/ad_integration/openid/success* (адрес cts.company.local необходимо заменить на адрес своего CTS / CTS BACK)

Параметр	Значение
Root URL	Оставить незаполненым
Valid post logout redirect URIs	+
Web origins	+

7. Нажмите на кнопку «Save».
8. В консоли администратора Keycloak перейдите в раздел «Clients».
9. Нажмите кнопку «Add client scope».
10. Выберите созданный ранее client scope «express-scopes».
11. Нажмите на меню «Add» и выберите «Default».
12. Далее в окне «Client details» для scope «offline_access» установите значение «Default».

НАСТРОЙКА ОТОБРАЖЕНИЯ ФОРМЫ АВТОРИЗАЦИИ KEYCLOAK

Для отображения формы авторизации Keycloak:

1. В консоли администратора Keycloak перейдите в раздел «Realm settings».
2. Выберите вкладку «Security defenses».
3. В поле «Content-Security-Policy» укажите:

```
frame-src 'self'; frame-ancestors 'self' https://web.company.local file:; object-src 'none';
```

4. Нажмите на кнопку «Save».

НАСТРОЙКА АВТОРИЗАЦИИ ПО QR-КОДУ

Для включения авторизации на CTS-сервере по QR-коду в командной строке в строке запуска сервера Keycloak добавить:

```
--spi-ciba-auth-channel-ciba-http-auth-channel-http-authentication-channel-uri=https://ru.public.express
/api/v1/authentication/openid/ciba/callback
```

Для включения авторизации на ETS-сервер по QR-коду в командной строке запуска в строке сервера Keycloak добавить:

```
--spi-ciba-auth-channel-ciba-http-auth-channel-http-authentication-channel-uri=https://ets.corp.lan
/api/v1/authentication/openid/ciba/callback
```

ИСТОРИЯ ИЗМЕНЕНИЙ

Раздел «История изменений» содержит список изменений в документе, связанных с изменениями/доработками СК «Express».

Сборка 2.5.7

№	Раздел	Изменение	Сервер	Ссылка
1.	Настройка интеграции с Active Directory	Дополнены требования к аватарам пользователей		стр. 94
2.	Установка корпоративного сервера eXpress	Исправлено примечание		стр. 35
3.	Настройка push-уведомлений	Добавлено примечание с указанием APN Push сервисов	RTS	стр. 56
			ETS	стр. 74
4.	Приложение 6	Добавлено		стр. 118
5.	Настройка сервера VOEX	Актуализирован Рисунок 6 и Рисунок 8	CTS	стр. 41
6.	Подключение SMTP-сервера	Дополнена информация в списке «Настройки e-mail»	CTS	стр. 92
7.	Настройка аутентификации администраторов	В тексте переименован пункт меню	CTS	стр. 93
8.	Термины и определения	Добавлены АТС и SIP	CTS	стр. 7
9.	Основные компоненты	Добавлена информация о SIP	CTS	стр. 8
10.	Единый корпоративный сервер	Добавлена информация о SIP	CTS	стр. 13
11.	Разделенный корпоративный сервер	Добавлена информация о SIP	CTS	стр. 14
12.	Установка Single CTS	Добавлен параметр SIP	CTS	стр. 35
13.	Настройка сервера VoEx	Добавлена Таблица 32	CTS	стр. 41
14.	Настройки АТС SIP-транк	Добавлено	CTS	стр. 43
15.	Приложение 7	Добавлено	CTS	стр. 120
16.	Приложение 8	Добавлено	CTS	стр. 121
17.	Приложение 9	Добавлено	CTS	стр. 121

Сборка 2.6.0

№	Раздел	Изменение	Сервер	Ссылка
1.	Основные компоненты	Добавлена информация о модуле SIP		стр. 8
2.	Архитектура. Единый корпоративный сервер	Добавлена информация о подключении АТС, архитектурные схемы, сетевые схемы взаимодействия, убрали компонент ZooKeeper		стр. 13
3.	Архитектура. Разделенный корпоративный сервер			стр. 14
4.	Приложение 7			стр. 120
5.	Приложение 8			стр. 121
6.	Архитектура. Сервер предприятия и единый корпоративный сервер	Убрали компонент ZooKeeper		стр. 17

7.	Архитектура. Сервер предприятия и разделенный корпоративный сервер	Убрали компонент ZooKeeper		стр. 18
8.	Установка Single CTS	В таблицу с доступными параметрами конфигурации добавлен параметр для подключения SIP		стр. 37
9.	Настройка сервера VoEx	Добавлены изменения в настройку сервера VoEx и SIP	CTS, ETS, RTS	стр. 41
10.	Настройка АТС SIP-транк	Добавлен раздел о настройке SIP-транк в зависимости от архитектуры развертывания		стр. 43

Сборка 2.7.0

№	Раздел	Изменение	Сервер	Ссылка
1.	Архитектура	Добавление поясняющие примечания об особенностях конфигурации, добавлено описание Bot-сервера		стр. 11
2.	Системные требования	Актуализированы системные требования к платформе		стр. 20
3.	Единый корпоративный сервер	Актуализирована типовая схема развертывания	CTS	стр. 13
4.	Разделенный корпоративный сервер	Актуализирована типовая схема развертывания	CTS	стр. 14
5.	Сервер предприятия и единый корпоративный сервер	Актуализирована типовая схема развертывания	ETS, CTS	стр. 17
6.	Сервер предприятия и разделенный корпоративный сервер	Актуализирована типовая схема развертывания	ETS, CTS	стр. 18
7.	Приложение 1	Актуализирована таблица сетевых взаимодействий	CTS	стр. 106
8.	Приложение 2	Актуализирована таблица сетевых взаимодействий	CTS	стр. 109
9.	Приложение 3	Актуализирована таблица сетевых взаимодействий	ETS, CTS	стр. 111
10.	Приложение 4	Актуализирована таблица сетевых взаимодействий	ETS, CTS	стр. 113

Сборка 2.9.0

№	Раздел	Изменение	Сервер	Ссылка
1.	Настройка подключений корпоративных серверов	Актуализирована информация о заполнении поля «Имя»	ETS	стр. 86
2.	Установка Веб-клиента	Перенесен раздел	ETS	стр. 45
			RTS	стр. 45
3.	Настройка сервера VoEx	Изменена структура раздела		стр. 41
4.	Настройка интеграции с Active Directory	Актуализирован пункт о настройке видимости полей профиля	CTS	стр. 94
5.	Настройка СМС-сервиса	Добавлено	ETS	стр. 82
			RTS	стр. 64

Сборка 2.10.0

№	Раздел	Изменение	Сервер	Ссылка
1.	Требования к DNS	Добавлена информация об использовании технологии Split DNS, описаны особенности её применения	CTS	стр. 24

Сборка 2.11.0

№	Раздел	Изменение	Сервер	Ссылка
1.	Запуск сервера	Добавлено примечание о создании учетной записи администратора сервера на Back CTS	CTS	стр. 52

Сборка 2.12.0

№	Раздел	Изменение	Сервер	Ссылка
1.	Архитектура	Добавлено примечание о Partner Express		стр. 11

Сборка 3.0.0

№	Раздел	Изменение	Сервер	Ссылка
1.	Архитектура	Из списка контейнеров удалены контейнеры «logstash» и «elasticsearch»		стр. 13, 14
2.	Архитектура	В список контейнеров добавлен контейнер «metrics_service»		стр. 13, 14, 17, 18
3.	Устранение уязвимостей	Добавлен пункт в примечание		
5.	Настройка IP-телефонии	Добавлены ссылки на Приложения 7 и 8		стр. 43
6.	Процедура обновления	Добавлен подраздел «Обновление ОС»		стр. 103
7.	Процедура установки	Актуализирована процедура установки корпоративных серверов	CTS	стр. 35
8.	Требования к DLP	Актуализированы требования к DLP		стр. 25
9.	Требования к платформе	Актуализированы требования к платформе		стр. 20
10	Обновление Deployka	По всему документу исправлена операция DEPLOYKA_SKIP_UPDATE=true на DPL_PULL_POLICY=never		
11	Актуализированы сетевые взаимодействия	Актуализированы сетевые взаимодействия в приложениях	CTS ETS	стр. 106 стр. 109 стр. 111 стр. 113

Сборка 3.1.0

№	Раздел	Изменение	Сервер	Ссылка
1.	Требования к платформе	Добавлена версия ОС 22.04 LTS		стр. 20

Сборка 3.3.0

№	Раздел	Изменение	Сервер	Ссылка
1.	Установка сервера VoEx	Обновлен		стр. 32
2.	Настройка регистрации	Добавлен	CTS	стр. 94

Сборка 3.4

№	Раздел	Изменение	Сервер	Ссылка
1.	Системные требования	Обновлены в части использования SSD вместо HDD		стр. 20

Сборка 3.5

№	Раздел	Изменение	Сервер	Ссылка
1.	Архитектура	Обновлен		стр. 11

Сборка 3.6

№	Раздел	Изменение	Сервер	Ссылка
1.	Архитектура	Добавлен контейнер «smartapp_proxy»		стр. 11
2.	Настройка хостов SamerAppProxy	Добавлен раздел		стр. 119
4	Глава 6. Устранение уязвимостей	Удалено		
6.	Настройка DLP	Обновлена команда в шаге 3		стр. 49
7.	Установка сервера VoeX	Адрес в шаге 11 изменен		стр. 32

Сборка 3.7

№	Раздел	Изменение	Сервер	Ссылка
			ETS	стр. 45
2.	Настройка интеграции с Active Directory	Дополнено описание событий в Active Directory, при которых у пользователя Express будет повторно запрашиваться аутентификация на корпоративном сервере Express	CTS	стр. 96
3.	Настройка push-уведомлений	Добавлено описание подключения к Android RuStore	RTS	стр. 56
			ETS	стр. 74

Сборка 3.8

№	Раздел	Изменение	Сервер	Ссылка
1.	Настройка OpenID	Актуализирован	CTS	стр. 99
2.	Интеграция CTS и Keycloak	Создан		стр. 122
4.	Требования к платформе	Добавлена таблица «Количество пользователей: 5000»		стр. 20
5.	Основные компоненты	Добавлено «Для интеграции с системами предотвращения утечки данных, обеспечивающих проверку сообщений пользователей на наличие запрещенного контента, используется протокол ICAP (порт TCP/1344)»		стр. 8

6.	Настройка сервера VoEx (STUN и TURN)	Актуализирован		стр. 41

Сборка 3.9

№	Раздел	Изменение	Сервер	Ссылка
1.	Разделенный корпоративный сервер	Добавлен контейнер prometheus в перечень компонентов сервера Front CTS	CTS	стр. 14
2.	Запуск сервера	Добавлены требования к паролю администратора. Вынесена отдельной операцией проверка на наличие ошибок	CTS	стр. 52
3.	Настройка интеграции с Active Directory	Добавлена команда для OS Ubuntu версии 19 и выше и других систем в случае ошибки	CTS	стр. 94

Сборка 3.10

№	Раздел	Изменение	Сервер	Ссылка
1.	Требования к хранению файлов записей ВКС	Добавлена информация о требованиях к хранению файлов записей ВКС	CTS	стр. 25
2.	Установка компонентов записи звонков и конференций	Добавлен	CTS	стр. 47
3.	Настройка маппинга полей	Добавлен Рисунок 99, дополнено описание шагов		стр. 125
4.	Процедура обновления	В разделе перечислены необходимые обновления, убраны подразделы, дана ссылка на отдельный документ по процедуре обновления.		стр. 103

Сборка 3.11

№	Раздел	Изменение	Сервер	Ссылка
1.	Требования к платформе	Удалены требования к ОС персональных компьютеров пользователей		стр. 20
2.	Установка компонентов записи звонков и конференций	Добавлено требование об обновлении версии сервера CTS перед установкой компонентов, актуализирован шаг два	CTS	стр. 47

Сборка 3.12

№	Раздел	Изменение	Сервер	Ссылка
1.	Единый корпоративный сервер	Исправлено имя докер-контейнера docker_socket_proxy в перечне докер-контейнеров Single CTS-сервера	CTS	стр. 13
2.	Разделенный корпоративный сервер	Исправлено имя докер-контейнера docker_socket_proxy в перечне докер-контейнеров Back CTS-сервера	CTS	стр. 14
3.	Разделенный корпоративный сервер	Из перечня докер-контейнеров Back CTS-сервера удален janus	CTS	стр. 14
4.	Устранение типовых ошибок	Исправлены имена докер-контейнеров: cts-containername_1; --tail		стр. 104
5.	Приложение 1	Актуализирована таблица «Сетевые взаимодействия Single CTS». Пункты 13–19	CTS	стр. 106
6.	Единый корпоративный сервер	Добавлены контейнеры transcoding, transcoding_manager и recordings_bot в перечень компонентов сервера CTS	CTS	стр. 13

7.	Разделенный корпоративный сервер	Добавлен контейнер transcoding в перечень компонентов сервера Front CTS	CTS	стр. 14
8.	Разделенный корпоративный сервер	Добавлены контейнеры transcoding_manager и recordings_bot в перечень компонентов сервера Back CTS	CTS	стр. 14

Сборка 3.13

№	Раздел	Изменение	Сервер	Ссылка
1.	Установка Front CTS- и Back CTS-серверов	Актуализирован порядок установки Front CTS-сервера (пп. 6; 7) и Back CTS-сервера (пп. 7; 8)	CTS	стр. 37
2.	Установка сервера ссылок	Добавлен раздел, описывающий установку сервера ссылок	CTS	стр. 46
3.	Установка веб-клиента	Раздел перенесен в главу 2 «Установка Express»	Для всех серверов	стр. 45
4.	Установка DLP	Добавлен отдельный раздел, описывающий установку DLP. Ранее содержавшаяся информация по установке DLP перенесена в данный раздел	CTS	стр. 47

Сборка 3.14

№	Раздел	Изменение	Сервер	Ссылка
1.	Установка Front CTS- и Back CTS-серверов	Актуализированы команды шагов 8 и 9 установки Back CTS	CTS	стр. 37
2.	Установка сервера VoEx. Предварительная настройка	Актуализирована Таблица 27	CTS	стр. 32
3.	Установка DLP на выделенном сервере	Добавлен шаг 3 установки выделенного DLP-сервера	CTS	стр. 47
4.	Установка сервера VoEx	Актуализировано название шага 3	CTS	стр. 33
5.	Установка сервера VoEx	Актуализирована Таблица 28	CTS	стр. 33
6.	Установка Single CTS	Актуализировано название шага 3	CTS	стр. 35
7.	Установка Front CTS- и Back CTS-серверов	Актуализировано название шага 3	CTS	стр. 37, стр. 39