UNLIMITED PRODUCTION

eXpress Communication System

Administrator's Guide

Volume 3. Operation of the ETS Server

Build 3.36
03/17/2025

© Unlimited Production, 2025. All rights reserved.

All copyrights to the operating documentation are protected.

This document is included in the product delivery package. It is subject to all terms and conditions of the license agreement. Neither this document, nor any part thereof, whether printed or electronic, may be copied or transmitted to third parties for commercial purposes without the express written permission of Unlimited Production.

The information contained in this document may be changed by the developer without special notice, which does not constitute a breach of obligations to the user by Unlimited Productions.

The server addresses, configuration file values, and user account data specified in the document are provided for example and are for informational purposes only. User data, including biometric data, are fictitious and do not contain personal data.

The provided components of eXpress CS as part of the delivery are intended exclusively for demonstration of functionality and are not intended for operation in a productive environment. For the correct functioning of eXpress CS, it is necessary to develop an architectural scheme of the installation taking into account the specifics of the infrastructure for productive operation.

Mailing address:	127030, Moscow, 24/1 Novoslobodskaya Street
Phone:	+7 (499) 288-01-22
E-mail:	sales@express.ms
Web:	https://express.ms/

TABLE OF CONTENTS

INTRODUCTION

This manual is intended for administrators of the product eXpress Communication System (hereinafter referred to as eXpress CS, eXpress, system). This volume contains general information about the system, as well as information necessary for operating an enterprise server.

Product Support Service You can contact the product support service by e-mail support@express.ms. The page of the product support service on the Unlimited Production website is available at https://express.ms/faq/.

Website. Information on the product by Unlimited Production can be found on the website https://express.ms/.

List of volumes of the Administrator's Guide:

- Volume 1. "Administrator's Guide. Installation.
- Volume 2. "Administrator's Guide. Operation of the CTS Server.
- Volume 3. "Administrator's Guide. Operation of the ETS Server.
- Volume 4. "Administrator's Guide. Installation and Operation of the RTS Server (available upon request).

TERMS AND DEFINITIONS

Term	Definition
AD	Active Directory is Microsoft Corporation's directory service for the Windows Server operating systems
API	Application programming interface — the interface enabling communication between software programs and applications
APNS	Apple Push Notification Service
botX	A platform for chatbot development
CTS	Corporate Transport Server
ETS	Enterprise Transport Server
FCM	Firebase Cloud Messaging is a service that simplifies messaging between mobile apps and server apps
JSON	JavaScript-based text-based data interchange format
NTLM	Network Authentication Protocol developed by Microsoft for Windows NT
RTS	Regional Transport Server
SIEM	Security information and event management
Single CTS	Single Corporate Server
SMTP	A network protocol designed for e-mail transmission in TCP/IP networks
SSL	Cryptographic protocol for secure communication
STUN	A network protocol for discovering an external IP address, used to establish a UDP connection between two hosts when they are both behind a NAT router.
TLS	Transport Layer Security Protocol
TTS	Transport Transfer Server. A server designed to transmit messages between corporate servers instead of the RTS server, including between the CTS servers that do not have a trusted connection with each other (non-trusted CTS servers)
TURN	A protocol for receiving incoming data over TCP or UDP connections
VAPID keys	Voluntary Application Server Identification involves a pair of keys: a public one and a private one. The private key is kept secret by the server whereas the public key is passed to the client. The keys allow the push notification service to know which application server signed the user and to be sure that it is the same server that sends notifications to a particular user.
Widget	A structural element of the panel responsible for visual display of a part of information collected by the system.
Videoconferencing	Multicast videoconferencing
CTN	Corporate data transmission network
Cache	A fast-access intermediate buffer containing information that is most likely to be queried
TSP	Trusted Services Platform
PC	Personal Computer
Decoupled CTS	Decoupled Corporate Server (Front CTS and Back CTS)
Routing	The contour, in which a chat exists (corporate, public, mixed)
Trust	A service for data transmission between the CTS and RTS and other services within their contour

Chapter 1

GENERAL INFORMATION

PURPOSE OF THE SYSTEM

eXpress CS is designed to provide high-quality continuous communication between the company's employees and to reduce the risk of information leaks by moving the exchange channels from the Internet into the perimeter of the Company's local computer networks.

MAIN FUNCTIONS

eXpress CS performs the following main functions:

- enabling fast exchange of text messages and files by users with the help of mobile devices and the web client on PCs within personal and group chats;
- making personal and group audio and video calls;
- ensuring secure storage and transmission of confidential data;
- creating copies of data to restore the subsystem's functionality when it is damaged or destroyed;
- streamlining the use of resources.

MAIN COMPONENTS

eXpress CS envisages three user interaction contours (which can be supplied in three versions):

- public (external);
- enterprise contour (company's internal contour, which combines several internal servers);
- corporate (internal).

The public (external) user interaction contour is used for:

- initial user registration;
- sending push notifications;
- exchanging messages and files with users who are not connected to any internal contour;
- making calls by users not connected to any internal contour;
- routing messages and files between internal contours that have no direct trusted connections.

The enterprise contour (company's internal contour) is used for:

- registering users;
- sending push notifications;
- routing messages and files between corporate contours that have no direct trusted connections.

The corporate (internal) user interaction contour is used for:

- registering corporate users;
- exchanging messages, files and making calls to corporate users;
- providing a corporate address book;
- routing messages and files between the company's corporate contour and corporate contours of partners, with whom trusted connections are established.

eXpress CS incorporates the following separately installed components:

- regional eXpress server (hereinafter referred to as the "RTS server");
- enterprise server (hereinafter referred to as the "ETS server");
- corporate eXpress server (hereinafter referred to as the "CTS server");
- Media server;
- Bot Server;
- Mobile app;
- Desktop app;
- Web app.

Attention! **For all the described functions to work properly, the application and server versions must match.**

The RTS, ETS and CTS servers are the main elements in the system architecture.

The RTS brings together and maintains computer networks within one region and is responsible for the operation of the public interaction contour.

The ETS server brings together and maintains computer networks and corporate servers within one large company and is responsible for the operation of the enterprise contour.

A customized application is released for the ETS server, which is managed by the company operating the ETS. CTS users connected to the ETS server receive text messages (SMS) and push notifications from this ETS.

The CTS server connects and maintains client devices within the organization, connects to the ETS server or the RTS server and acts as an intermediary between the client device and the ETS/RTS server. The CTS server is responsible for the operation of the enterprise contour. Once the ETS server has been installed, information exchange between the corporate servers takes place within the enterprise, data from the CTS server is transmitted to the ETS server, and the ETS server performs information exchange with the external contour (for more details, see the document "Administrator's Guide. Volume 2. Operation of the CTS Server").

The client device can connect to both the CTS server and the ETS server or the RTS server directly. For each server, a user registers their profile. Depending on the active profile, the user has access to their resources in the form of chats, contacts and messaging history. The client can connect to the CTS server once a connection to the RTS or ETS server has been established. All messages transmitted between corporate users are stored on the CTS server and are not accessible to server administrators.

A separate Media server is used to support voice and video calls.

If the number of users is 100 or more, the Transcoding server is detached from the Media server to a separate server.

For the deployment of chatbots and SmartApps, a separate server (Bot Server) is used.

The system is managed via administrator web interface, which makes it possible to configure eXpress and control the operation of the application.

PROTECTION MECHANISMS

The security of transmission of confidential data is ensured by the following protective mechanisms implemented by eXpress CS:

- role-based access control method;
- multi-level method of authentication and identification of users, including the use of additional authentication tools;
- use of cryptographic means to protect communication channels outside the controlled area;
- a set of solutions for backup and recovery of system data.

Additional mechanisms have been implemented for working in unstable networks or in networks with low quality:

- local access to data on the device when there is no network connection;
- access to local copies of previously sent and received data in the event of no connection to the server, including:
  - viewing the local contact list;
  - viewing downloaded chat history cache;
  - full-text search through the correspondence history;
  - viewing previously received and sent files, a copy of which is contained on the client device.

AVAILABLE ROLES

The system is managed by the organization's employees with administrator rights. The administrative rights in the system are assigned hierarchically.

For the safe and successful operation, when installing eXpress CS, the following roles are established (see Table 1):

Table 1

Role	Rights	Account type
Administrator	• role assignment; • viewing security log; • managing chats; • managing user accounts; • connecting chatbots; • managing system settings	Internal User
Corporate User	• sending messages; • creating a chat; • viewing the server address book; • connecting to chatbots	Internal User
Regional User	• sending messages; • creating a chat	External user
Security Administrator[1]	• viewing messages in the DLP console; • viewing logs in the DLP console	Internal User

[1] for CTS server users only (for more details, see the document "Administrator's Guide. Volume 2. Operation of the CTS Server").

The specific assignment of administrator access rights is determined by the policy of the company using eXpress CS.

The type of account depends on the position of the server on which the user is authorized. If there is a RTS server within the protected contour, a regional user becomes an internal user.

eXpress CS envisages the creation of administrators with limited rights for specific tasks.

Administrators' tasks:

- installation and management of updates of system-wide and application software;
- configuration, maintenance and monitoring of server equipment;
- backup management and data recovery;
- centralized configuration of the Mobile app;
- managing user accounts.

On the CTS server, within the framework of the role model for individual user groups, the administrator can set restrictions for users with regard to operations with attachments:

- prohibition of sending/forwarding attachments to chats;
- prohibition of downloading/viewing attachments in chats;
- prohibition of the ability to forward/share/save attachments to the device's memory.

First, the administrator creates user groups in the User Groups section to which the restrictions will apply, and then, in the Role Model section, sets the rules that the restrictions will be subject to.

Restrictions can be configured for specific users or specific groups based on server affiliation (for more information, see the document "Administrator's Guide. Volume 2. CTS server operation").

CONTACTS MANAGEMENT

The administrator manages user accounts (contacts). The administrator can:

- add a new user to the corporate and enterprise contours if authorization via e-mail is configured;
- manage the connection of users to the corporate contour;
- connect the CTS/ETS server to the RTS server;
- connect the CTS server to the ETS/RTS server;
- establish and configure trusts between the CTS servers;
- delete user accounts on the CTS servers if e-mail authentication is configured;
- manage user accounts (create, edit, delete) and manage administrator access rights.

The following methods are available to the administrator for setting up user registration/authorization in the system:

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

ETS server administrators can only настройка configure simplified user authorization via E-mail.

eXpress CS can operate in conjunction with the Active Directory directory service (hereinafter referred to as the "AD"). Changes made to user accounts in AD are reflected in the corresponding accounts in eXpress.

When using OpenID as the registration/authorization method, eXpress CS uses CTS server integration with Keycloak. The KeyCloak directory service is a set of general-purpose or special-purpose software tools that provide management of the creation and use of user accounts.

User registration/authorization in the system via e-mail does not require additional integration and is provided by eXpress's own tools.

Chapter 2

OPERATION OF THE ENTERPRISE SERVER

This chapter describes the main sections and procedures for working in the Enterprise Server (ETS) administrator web interface.

AUTHORIZATION IN THE ADMINISTRATOR WEB INTERFACE

To authorize in the administrator web interface:

1. In the address bar of your browser, enter the address of the administrator web interface https://ets_host/admin.

   An authorization window will open (see Figure 1.):

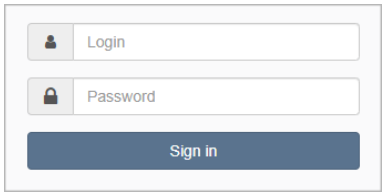

Figure 1.

2. Enter the account name and password in the appropriate fields.
3. Click "Login".

   Authorization will be performed (see Figure 2.).

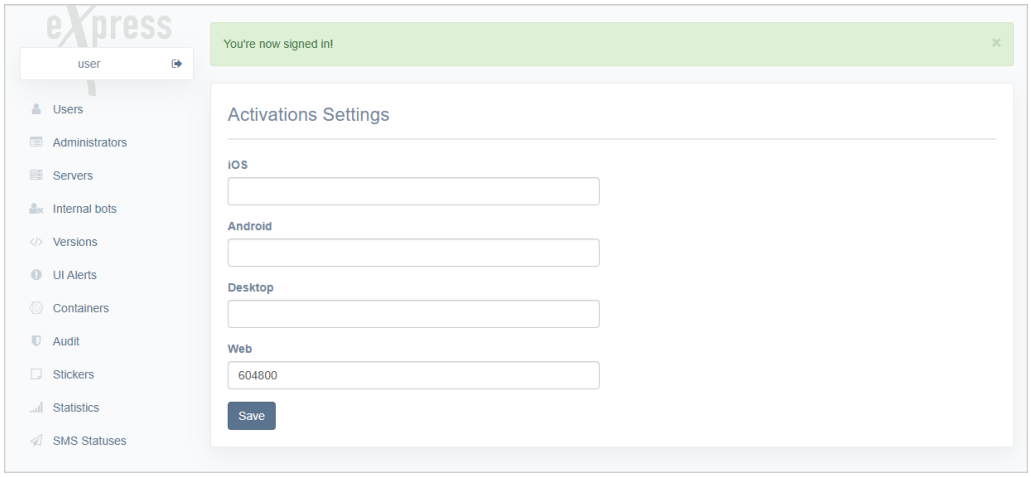

Figure 2.

To exit the administrator web interface, click in the upper left part of the window. An authorization window will open with the corresponding message (see Figure 3.).

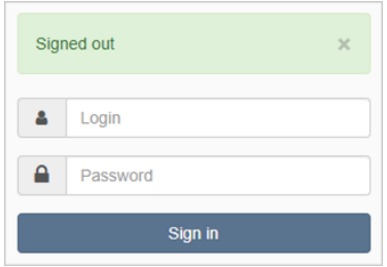

Figure 3.

DESCRIPTION OF ADMINISTRATOR WEB INTERFACE

This subsection describes the administrator web interface using the “Users” section interface as an example (see Figure 4.).

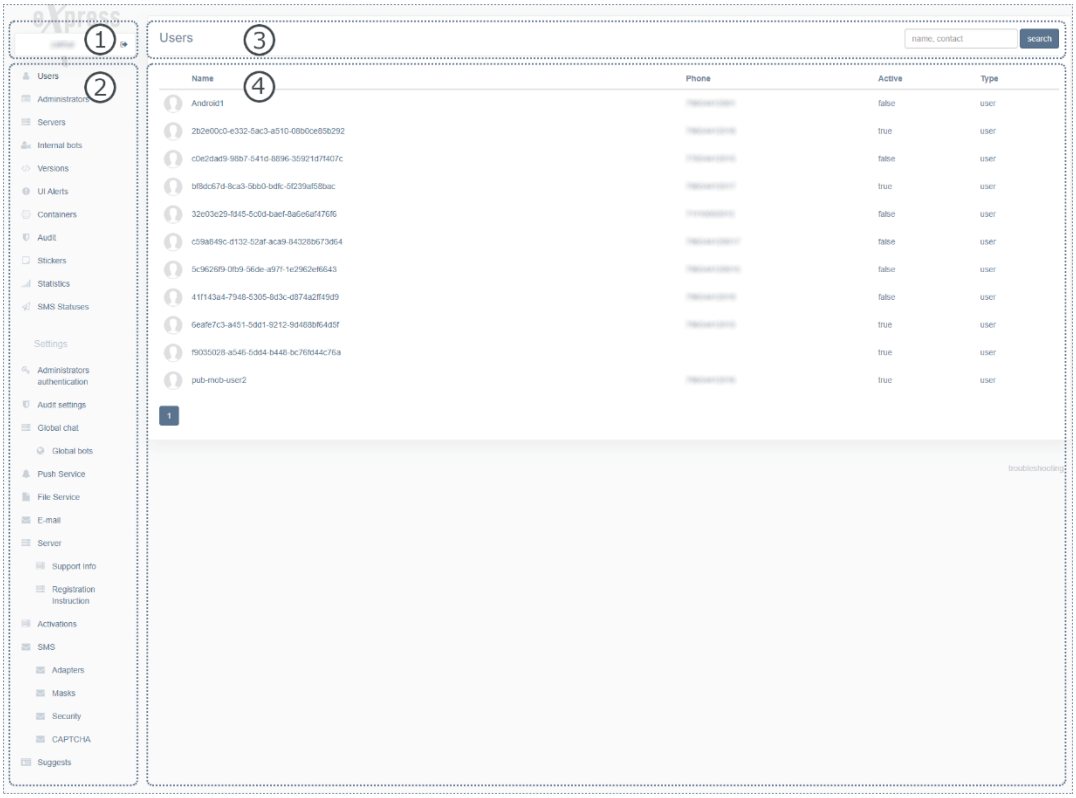

Figure 4.

Interface of the administrator web interface consists of the following blocks:

1. Current user login, logout and edit buttons in the top left corner.
2. A menu for navigating through sections of the administrator console, located on the left side of the window.
3. Window header. Contains the name of the current section (menu item), and may also contain controls and a search bar.
4. The working area that occupies the main area of the window.

In sections designed for storing and processing large amounts of data, the work area is presented in the form of a table.

To sort data in forward and reverse order, use the ^ and v buttons in the column header.

To search for data, enter the corresponding value, in whole or in part, in the search bar in the upper right corner of the window and click “Search”.

The menu consists of items that allow the system administrator to perform the operations listed in the table below (see Table 2).

Table 2

Document section	Menu item	Purpose	Description in the document
	Servers	Viewing and setting up CTS connections	page 16

Document section	Menu item	Purpose	Description in the document
Server Management	Server	• setting up the appearance of the application; • setting up the TLS certificate; • viewing the identifier of the current ETS and RTS server it is connected to; • viewing versions of installed services	page 21
	Versions	Viewing the names of connected cts servers and their versions	page 23
Managing User Accounts	Users	Viewing account information	page 25
User Authentication and Authorization	E-mail	Setting up the SMTP server and e-mail from which e-mails are sent from the server to recipients	page 24
	SMS Statuses	Viewing information about SMS codes that were used to authenticate users in the system	page 29
	Simplified Connection via E-mail	Assigning domains and e-mail addresses of corporate users to specific CTS servers	page 29
User Notification	SMS	Setting Up the Text of SMS Messages	page 30
	Adapters	Choosing a mobile service provider	page 31
	Masks	Service provider mask	page 31
	Security	Setting Up Security Settings	page 33
	Captcha	Additional user verification when logging into the app	page 34
	UI Alerts	Setting up user notifications about updates	page 36
	Push Service	Setting Up Push Notifications	page 36
Setting up user session activity time	Activations	Setting up user session activity time	page 41
Managing administrator user accounts	Administrators	View information about administrators and administrator groups	page 42
		Creating administrator accounts	page 43
		Setting up administrator accounts	page 44
		Creating, deleting, setting Up administrator groups	page 52
	Setting Up Administrator Authentication	Setting up administrator connections from Active Directory	page 44
Global Chat	Global Chat	• enabling and disabling global chat; • setting up global chat settings	page 52

Document section	Menu item	Purpose	Description in the document
Managing Bots	Internal Bots	• changing and setting up internal bots; • adding the administrator for bots	page 53
	Global Bots	• adding global bots to the global chat; • removing global bots from global chat	page 55
Managing File Service	File Service	• setting up storage and deletion periods for files; • proxying	page 56
Logs	Containers	View Docker containers list and logs	page 57
	Audit Settings	• Activating and deactivating tracking of user connections; • Setting up sending of information about security events to the SIEM of the information system into which eXpress is integrated	page 58
	Audit	Audit of administrator and user actions	page 60
Application Performance Statistics	Statistics	Viewing application performance statistics	page 63
Managing Stickers	Stickers	• viewing sticker packs and their elements; • adding and removing sticker packs and their elements; • customizing sticker packs	page 66

SERVER MANAGEMENT

This section describes the following administrator web interface menu items:

- Servers;
- Server;
- Support Contact Management;
- Versions;
- Connecting the SMTP Server.

The "Servers" section provides information the RTS server to which the ETS server is connected, and the CTS servers connected to this ETS server (seeFigure 5. and Figure 6.). The "Servers" section allows the user to create, edit, and delete connections to the CTS server, as well as view information about the servers with which connection is established and an interactive connection routing diagram.

The Server section contains information about the ETS server and parameters for setting up its operation.

In the "Support Contacts Management" section, you can configure the methods by which the user can contact eXpress Customer Support, as well as download a file with frequently asked questions to the user's device.

The Versions section provides information about all CTS servers connected to the ETS server and the versions of microservices installed on them.

The "Connecting the SMTP Server" section provides information on the procedure for connecting an SMTP server, which is necessary for user authorization using e-mail.

SERVERS

By default, this section is available in the "RTS" tab. It contains information about the connection of this ETS server to the RTS/CTS servers (see Figure 5.).

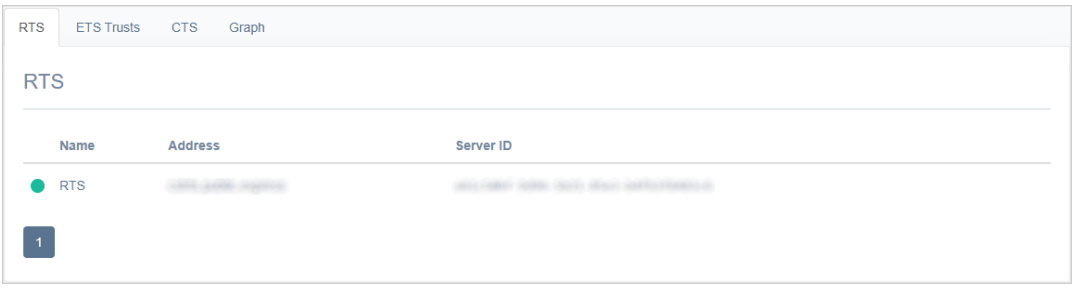

Figure 5.

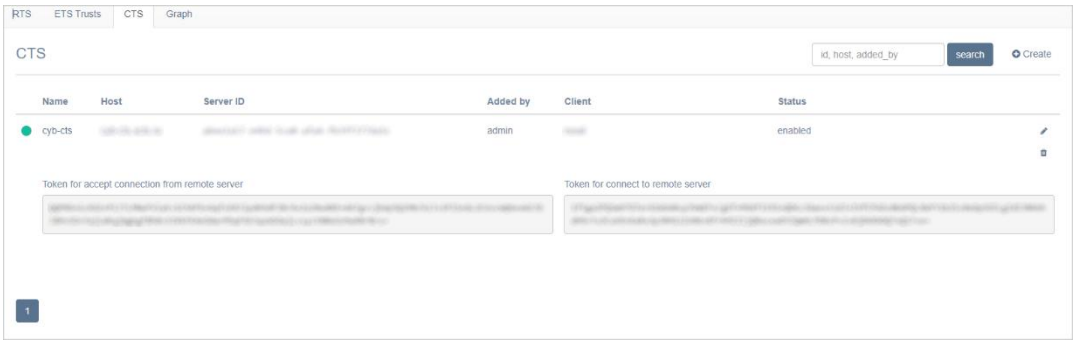

Figure 6.

Authentication when connecting between servers is performed with the use of tokens. A token is a sequence of characters that allows you to accurately identify an object and determine its privilege level. It is generated by the system when creating trust connections and is linked to a specific connection.

Note. Tokens for connecting to the ETS server are provided by the developer company and are entered into the Settings installation file when installing the server.

The following functionality is available to the administrator:

- connecting the CTS server to the ETS server;
- editing connections to the CTS server;
- deleting connections to the CTS server;
- viewing information about the RTS/CTS servers with which a connection has been established;
- viewing the interactive graphical connection routing diagram.

ESTABLISHING CONNECTION TO CORPORATE SERVER

To connect the CTS:

1. In the "Servers" section, open the "CTS" tab (see Figure 6.)
2. Click "Create" in the upper right corner of the or "CTS" section.

   A window will open (see Figure 7.):

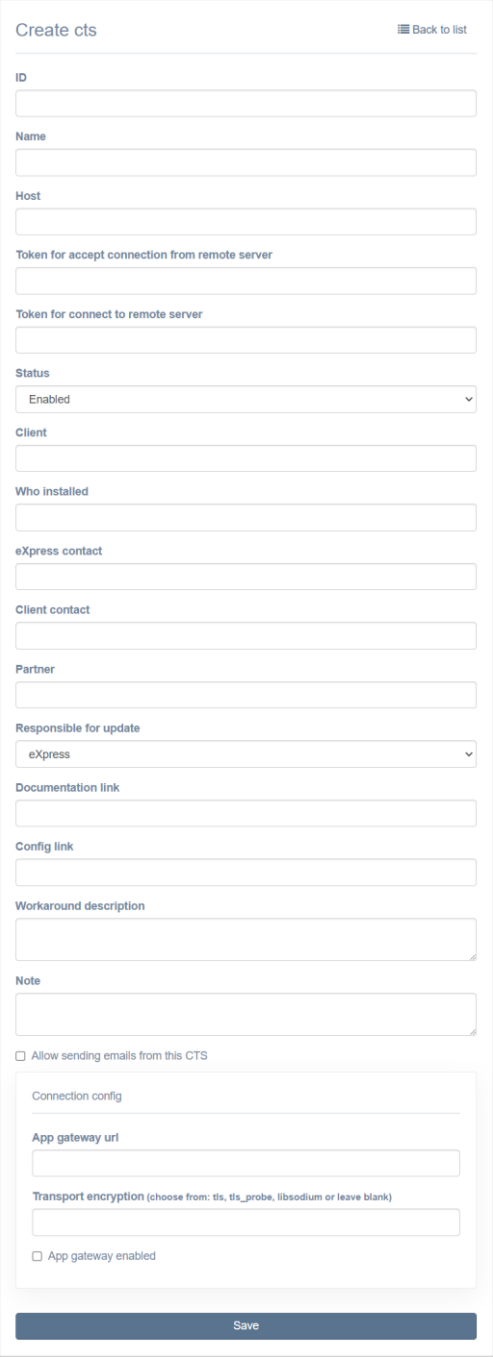

Figure 7.

The window that opens contains the following information (see Table 3):

Table 3

Parameter	Description
ID	Identifier of the server with which the connection will be established (the CTS ID is stored in the "Server" section of the Admin Console of the relevant CTS server)
Name	Short designation for the communication channel being created
Host	Real server connection address (URL), which will be displayed in the client app
Token for connection from a remote server	Token for accepting connection
Token for connection to a remote server	Connection token

Status	Connection status: • enabled • disabled
Client	Relevant data
Who installed	Relevant data
Contact on the eXpress side	Relevant data
Contact on the Client side	Relevant data
Partner	Relevant data
Link to documentation	Relevant data
Link to configuration files	Relevant data
Description of problems and their solutions	Relevant data
Who is responsible for updates	• eXpress; • Client; • Partner
Allow sending e-mails from this CTS	Enable this option (if you are connecting a CTS server)

3. Click "Save".

To edit a connection, click and make changes in the window that opens.

To delete the connection, click .

VIEWING INFORMATION ABOUT THE SERVER

To view information about the server with which a connection has been established, select the desired tab and the server in the "Name" column. A window will open (see Figure 8.):

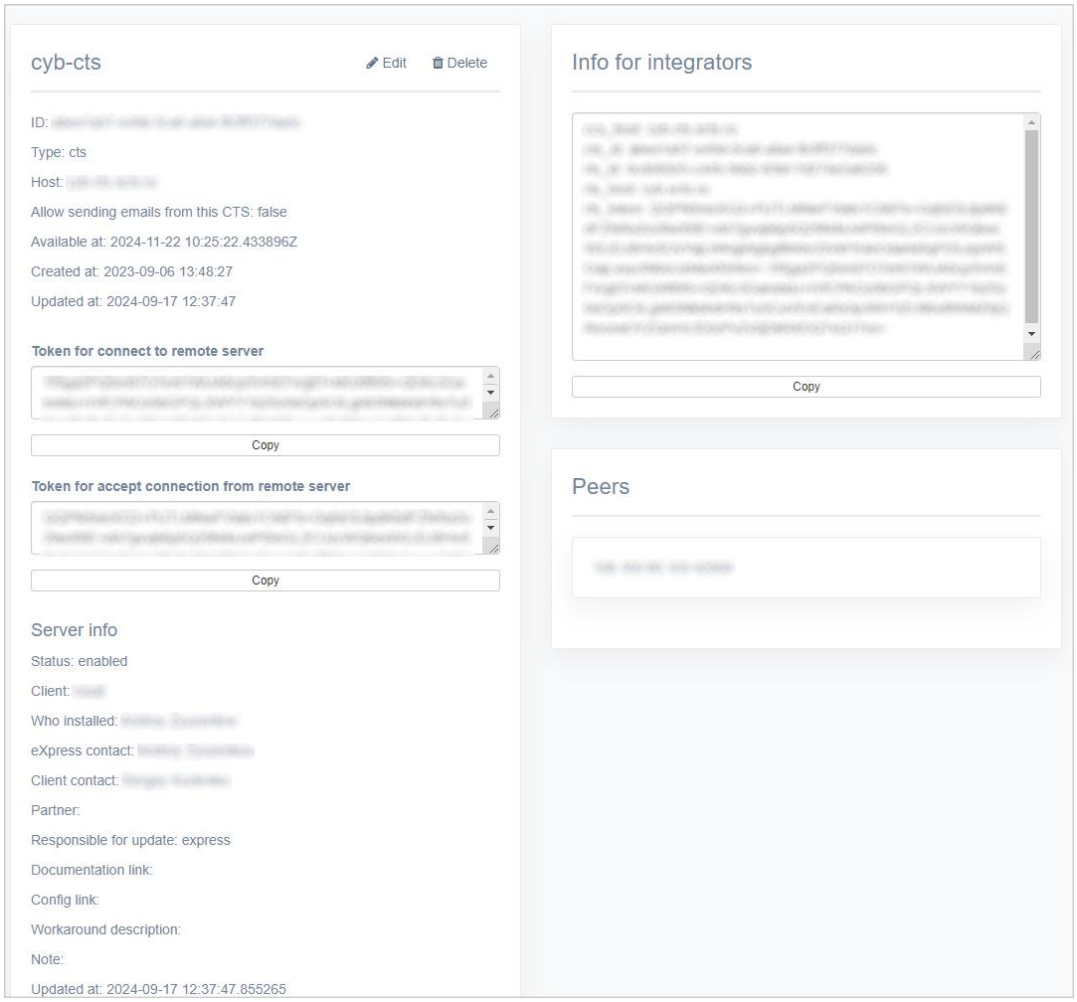

Figure 8.

The "Information for Integrators" section contains the data, which is required for server integration.

The "Peers" section displays the IP addresses of servers connected to this server.

GRAPHICAL CONNECTION ROUTING DIAGRAM

The following functionality is available to the administrator on this tab:

- viewing the graphical connection routing diagram;
- viewing information about a specific server.

To view the graphical connection routing diagram, open the "Graph" tab (see Figure 9.):

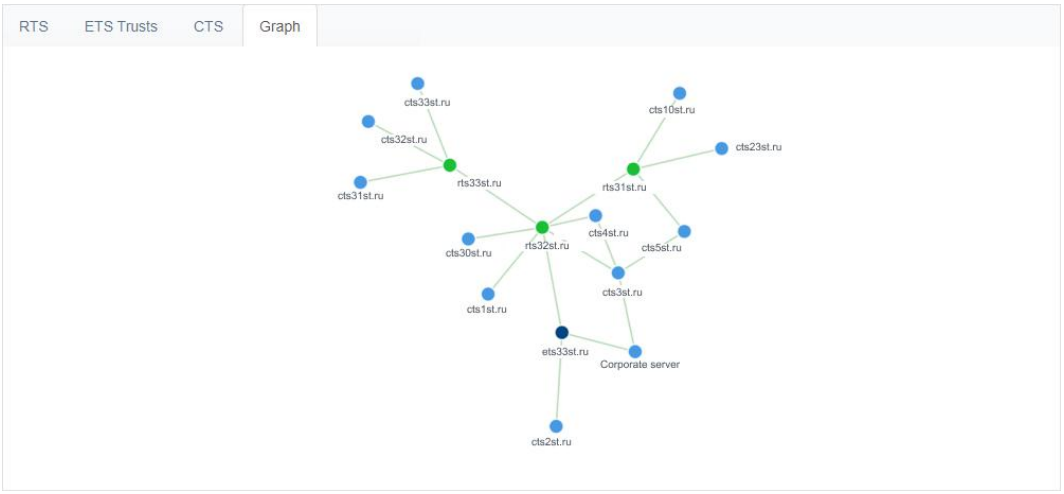

Figure 9.

Servers are indicated in the diagram with colored circles, depending on the type:

- RTS — green;
- ETS — purple;
- CTS — blue.

For ease of viewing, diagram elements can be dragged with the mouse.

To view information about a specific server in the diagram:

1. In the "Graph" tab, click on the circle that represents the respective server.

   The address of the selected server and the number of chats created on it will be displayed in the upper right corner of the screen (see Figure 10.).

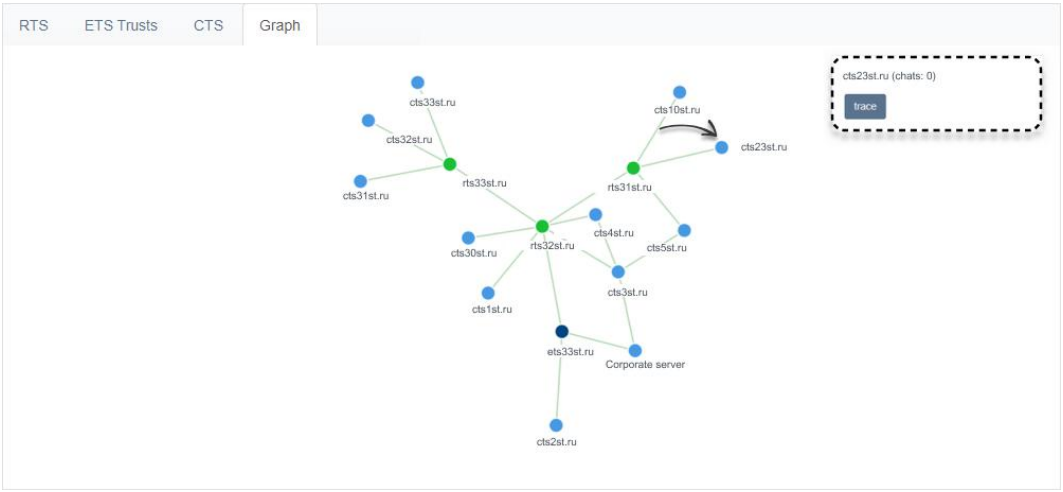

Figure 10.

2. Click on the server name in the upper right corner of the screen.

   A window will open with information about the RTS/CTS server through which data is exchanged with the current server (see Figure 11.).

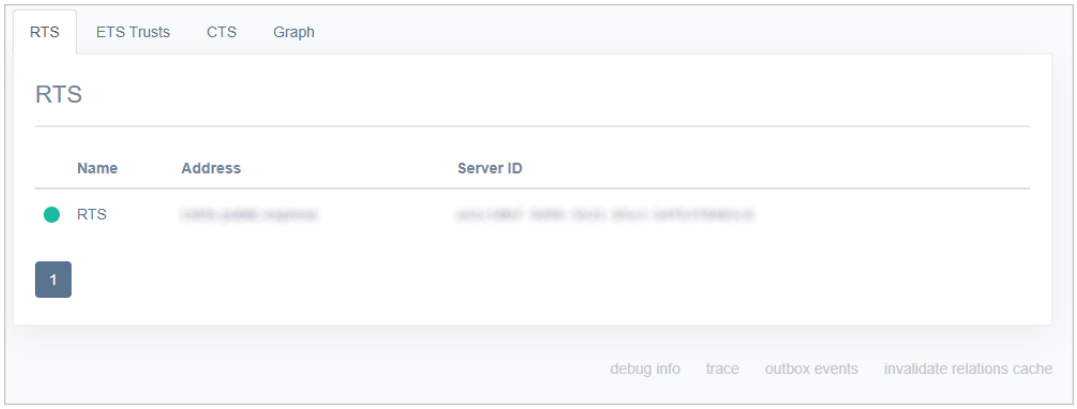

Figure 11.

SERVER

The “Server” section consists of several sections that provide information about this CTS server (see Figure 12.), as well as the parameters for setting up its operation.

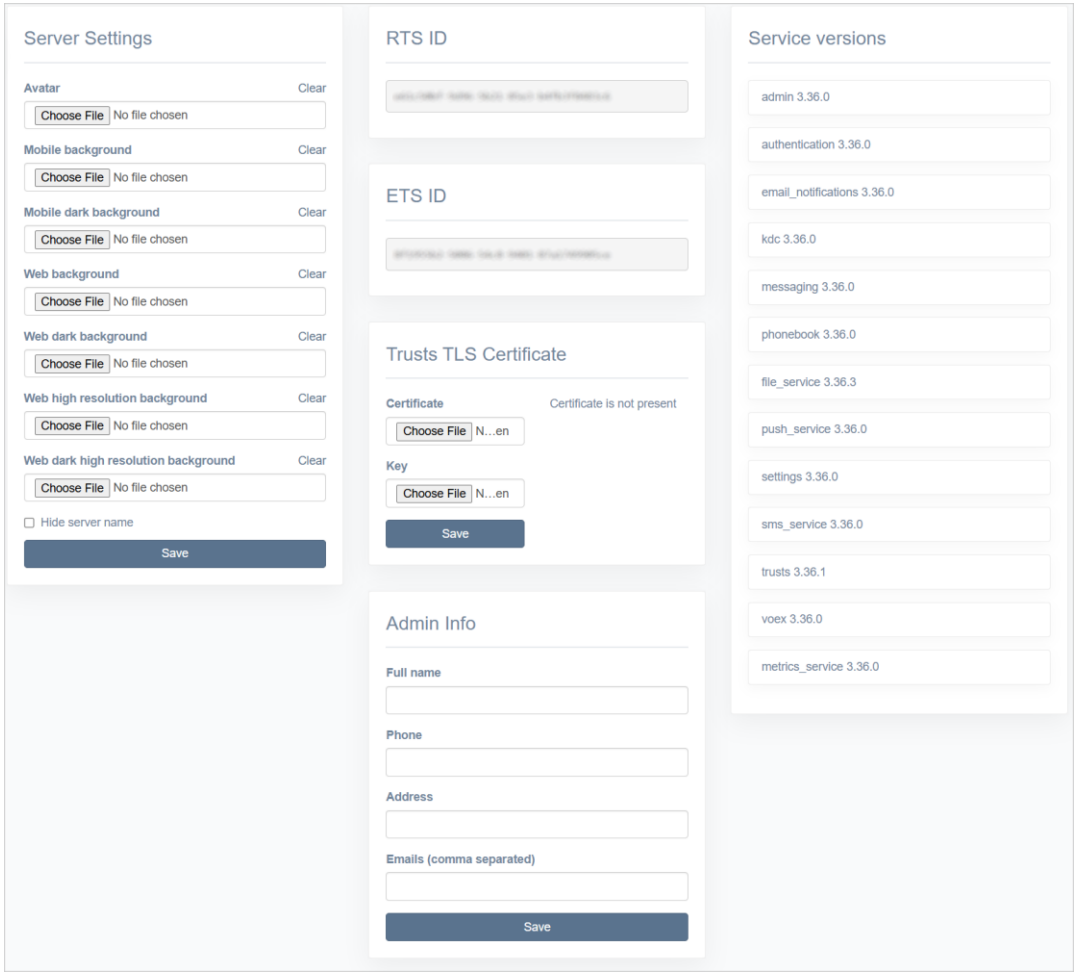

Figure 12.

The following functionality is available to the administrator:

- setting up display of server information and loading of application backgrounds on user devices;
- viewing information about the CTS server identifiers;
- setting up parameters for using the TLS protocol in trust connections;
- entering administrator contact information;
- viewing the list of services installed on the CTS server and their versions.

SERVER SETTINGS

In the "Server Settings" section, the administrator sets the corporate style and wallpaper in chats:

- ETS avatar;
- Mobile app background;
- Web app background;
- dark Web app background;
- high resolution Web app background;
- dark high resolution Web app background,

and also sets up the option to display/hide server name by checking the "Hide server name" box.

Note. The background must be a raster square seamless image with a resolution of 600x600 px up to 50 KB.

To save your settings, click "Save".

RTS ID AND ETS ID

The "RTS ID" and "ETS ID" sections show the identifiers of the ETS server on which the administrator web interface is opened and the RTS server to which the ETS server is connected. The identifier is used when setting up trust servers to transfer data between CTS and ETS and other services included in their circuit (for more information about trusts and setting up their connection, see the document "Administrator's Guide. Volume 2. Operation of the CTS Server").

TRUST TLS CERTIFICATE

In the "Trust TLS Certificate" section, enter data for using the TLS protocol in trust connections.

To enter data:

1. Upload files with information about the certificate and the key in the appropriate fields in the "Trust TLS Certificate" section.
2. Click "Save".

Note. It is allowed to use the TLS certificate used during the server installation stage.

ADMINISTRATOR INFORMATION

In the "Administrator Information" section, enter the administrator information.

This information is displayed in user apps when an error occurs during registration.

SERVICE VERSIONS

The “Service Versions” section contains a list of services installed on the ETS server and their versions.

SUPPORT CONTACTS MANAGEMENT

In this section, you can configure the methods by which the user can contact eXpress Customer Support, as well as download a file with frequently asked questions to the user's device.

To set up support contacts:

1. Check/uncheck the box “Display eXpress support contacts”.
2. Fill in the fields of the form (see Figure 13.).

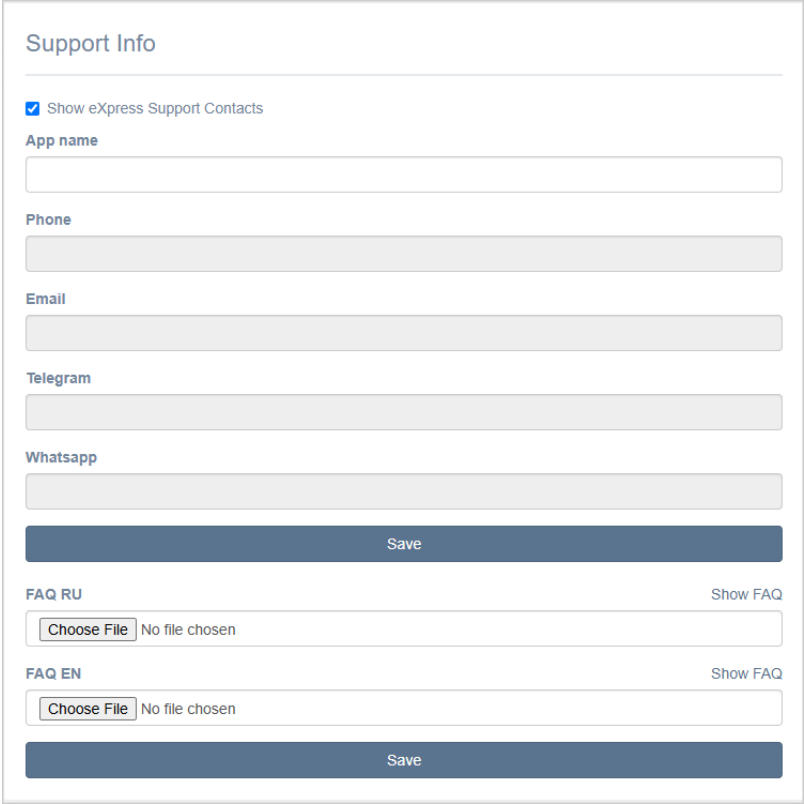

Figure 13.

3. Click “Save”.

To upload a file with instructions:

1. Click “Select file” (in Russian or English).
2. Select a .html file from your file system.
3. Click “Save”.

To view the text of the instructions, click “View FAQ”.

VERSIONS

The “Versions” section provides information about all CTS servers connected to the ETS server and the versions of microservices installed on them. As versions age, their color will change from green to red (see Figure 14.).

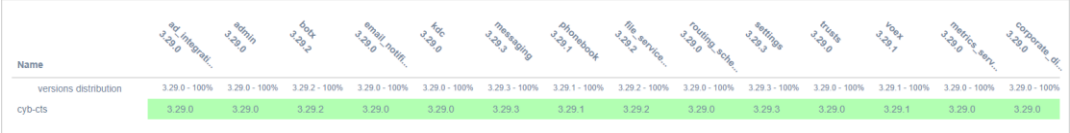

Figure 14.

CONNECTING THE SMTP SERVER

This operation is mandatory when choosing the user authorization method using e-mail.

The SMTP server is used to send user device authentication PIN codes to e-mail. First, create an account on the mail server under which the letter with the code will be sent.

Note. The ETS server can send PIN codes for authentication of the user's device to e-mail only if the “Allow sending e-mails from this CTS” field is checked (“Servers” section → “CTS” tab → Edit CTS → “Allow sending e-mails from this CTS” field).

If not checked, PIN codes for user device authentication will be sent to the e-mail from the CTS server.

To connect the SMTP Server:

1. Select “E-mail” from the menu.

   The "E-mail Settings" window will open for entering parameters (see Figure 15.).

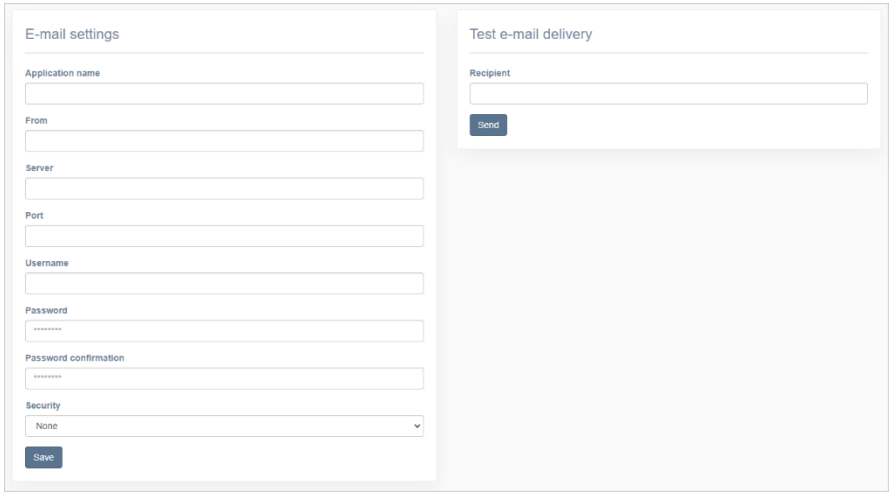

Figure 15.

2. In the “E-mail Settings” window, fill in the fields as follows (see Table 4):

Table 4

Field	Description
App name	The name of the app from which e-mails will be sent
From	Return address
Server	SMTP server
Port	Port number for retransmission of outgoing mail: 25, 587 or 465. The port number depends on the type of secure connection
User name	Data for authorization on the SMTP server
Password	Data for authorization on the SMTP server
Connection protection	Type of secure connection (drop-down list: SSL, Start/TLS or empty value)

3. Click “Save”.

To check connection settings, use the “Test E-mail Sending” area. Enter the recipient's address in the empty field and click “Send”.

MANAGING USER ACCOUNTS

This section describes the following administrator web interface menu items:

- Users;
- Registration Instructions.

USERS

The section is a table that lists the user accounts registered in the application (see Figure 16.).

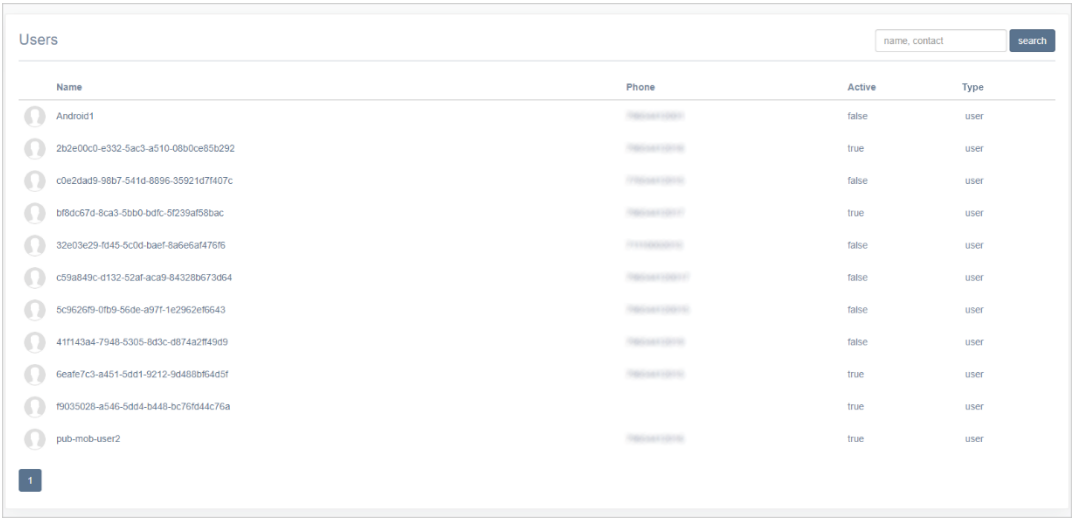

Figure 16.

The table consists of the following columns (see Table 5):

Table 5

Column name	Information
Name	User name
Phone	The phone number, which was used for registration
Active	Account status: activated (true) and not activated (false)
Type	Account type (user)

OPERATIONS WITH USER ACCOUNTS

The following functionality is available to the administrator:

- viewing account information;
- personalized operations with a specific account.

VIEWING ACCOUNT INFORMATION

Each account has a card containing full information about the account (see Figure 17.).

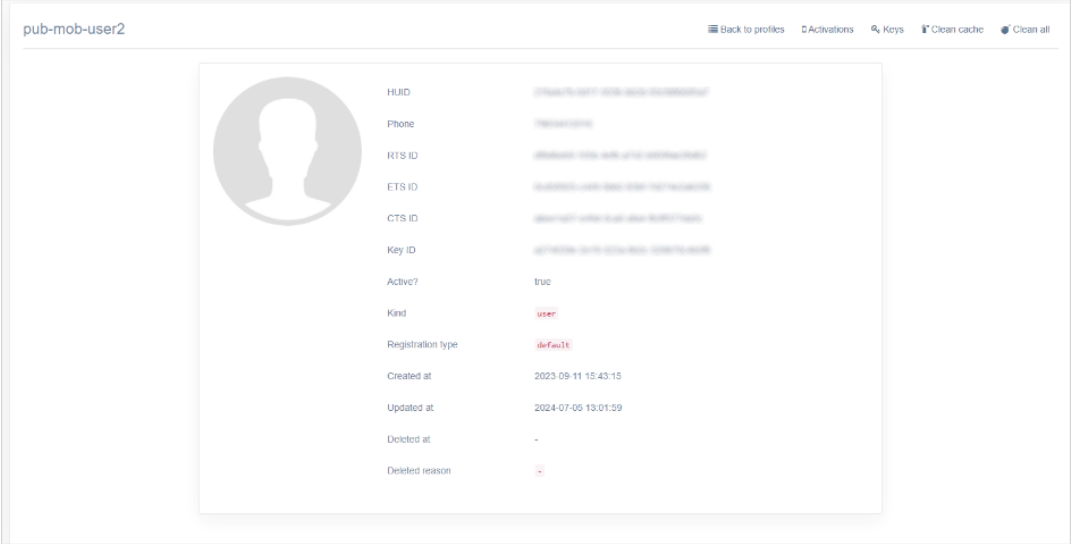

Figure 17.

Information in the user card is for reference only and cannot be edited.

OPERATIONS WITH A SPECIFIC USER ACCOUNT

To perform operations with a specific user account, use the buttons on the toolbar (see Figure 18.):

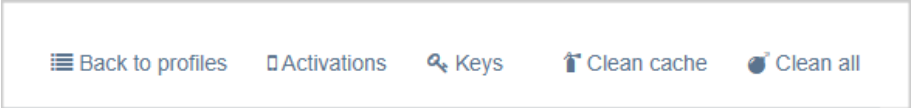

Figure 18.

The list of available operations:

- return to the "Users" section;
- list of open sessions (activations);
- keys;
- clear cache;
- clear all.

To return to the "Users" page, click "Back to profiles".

To view information about open sessions **of the registered corporate user**, click "Activation". Each session is represented by an information card (see Figure 19.).

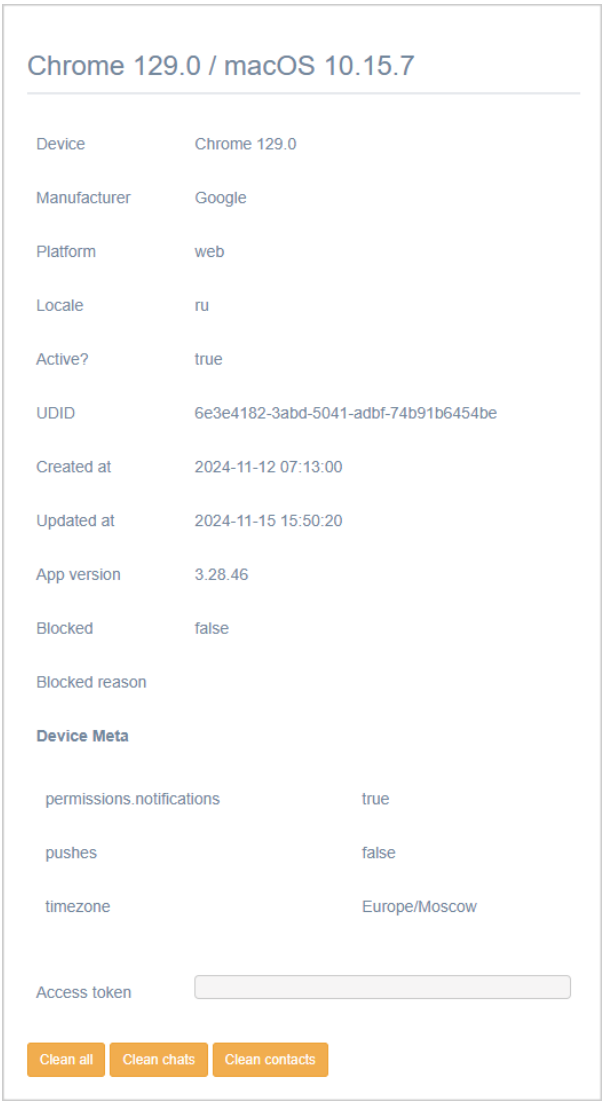

Figure 19.

To view all information cards, scroll down the page.

The user's active and terminated sessions are displayed in the cards. Each session is identified by UDID and contains information about the user's device, browser version, application version, whether the session was terminated (locked) for any reason, permissions on the device (Device Meta), and time zone Access. The "Device hostname" field displays the DNS Hostname.

Device Meta parameters:

- Permissions.microphone — is microphone use allowed;
- Permissions.notifications — are notifications allowed in the browser or in the operating system;
- Pushes — whether notifications are enabled in the desktop app (web app notifications are managed by the browser) or in the mobile app (iOS app notifications are managed by the operating system);
- Permissions.contacts — is access to contacts allowed;
- Permissions.storage — is access to device storage allowed.

To view reference information about the keys assigned to the user, click "Keys". A window with help information will opne (see Figure 20.).

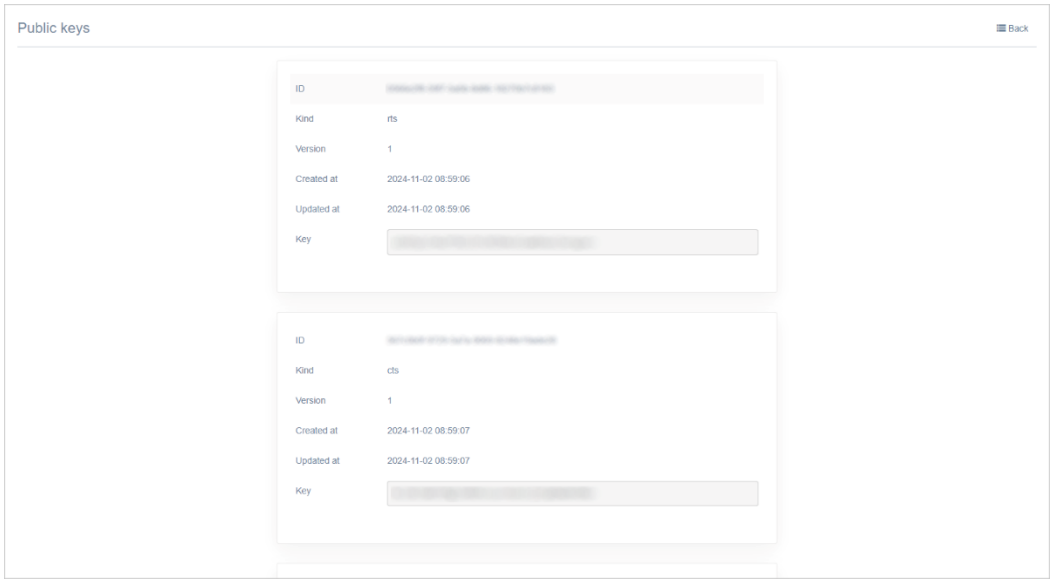

Figure 20.

To clear the cache on all user devices, click "Clear Cache". This method is used when the user cannot clear the device cache on their own or performing the operation on their part does not solve the problems that have arisen.

The "Clear all" button performs similar function – deletes the cache and forcibly returns the user to the authorization window. To enter the application, the user must log in again.

REGISTRATION INSTRUCTIONS

In this section, you can upload a file with instructions for registering with eXpress CS.

To set up support contacts:

1. Check/uncheck the box "Show to users" (see Figure 21.).

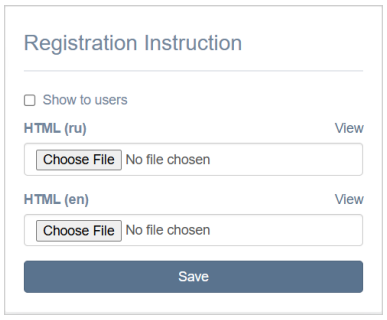

Figure 21.

2. Click "Select file" (in Russian or English).
3. Select a .html file from your file system.
4. Click "Save".

To view the text of the instructions, click "View".

USER AUTHENTICATION AND AUTHORIZATION

This section describes the following:

- methods of user device authentication;
- verification status;

- setting up simplified authorization.

METHODS OF USER DEVICE AUTHENTICATION

When a user logs into the app, their device is authenticated. The user is sent a verification SMS message or a PIN code via e-mail.

If authentication occurs by checking the delivery status of an SMS message, this status is displayed in the SMS Statuses section.

SMS STATUSES

The "SMS Statuses" section provides information about SMS codes that were used to authenticate users in the system (see Figure 22.).

Figure 22.

The table contains the following information (see Table 6):

Table 6

Column name	Information
SMS ID	Identifier of SMS messages, which have been sent
Phone	The phone number to which the code was sent
Provider	Online services for sending SMS-mailings
Status	Sending status: • failed; • delivered
Status code	Status program code
Error code	Program error code
Sending time	Date and time of sending the SMS message

You can select the provider and set up security parameters in the "SMS" section, for more details see page 30.

SETTING UP SIMPLIFIED AUTHORIZATION

eXpress CS allows the administrator to associate domains or e-mail addresses of corporate users with specific CTS servers. When a client app sends a user's domain/e-mail address during login, the system knows which CTS it belongs to. In this case, the user does not have to specify the CTS address; it is entered automatically. This process is called "simplified authorization" and is configured in the "Simplified connection via e-mail" section (see Figure 23.).

Note. If simplified connection is not configured, when a user attempts to log in using a corporate e-mail address, login will not be possible and the user will receive the message "Corporate e-mail not found."

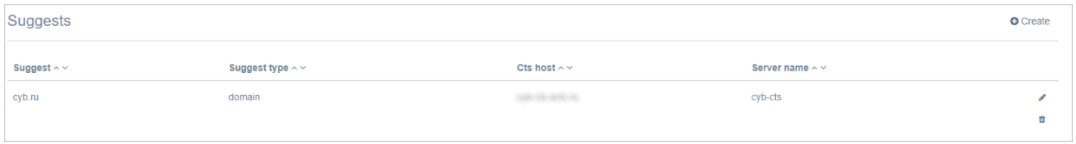

Figure 23.

The “Simplified connection via e-mail” section allows the administrator to perform the following functions:

- view a list of domains and e-mail addresses linked to corporate servers;
- enable simplified authorization (link domains or e-mail addresses of corporate users to specific CTS servers);
- disable simplified authorization;
- configure the matching type: by e-mail address or by domain.

The data in the “Simplified connection via e-mail” section is presented in the form of a table, which contains the following information (see Table 7):

Table 7

Column name	Information
Template	The user's domain or corporate e-mail address
Type	Matching type. Possible values: • e-mail — by e-mail address; • domain — by e-mail domain
CTS host	The address of the corporate server to which the domain or e-mail address is linked
Server name	CTS server to which the e-mail address is linked

To set up simplified authorization:

1. Click “Create ” in the upper right corner.
2. In the window that opens, fill in the fields (see Table 7).
3. Click “Submit”.

To return to the “Simplified connection via e-mail” table, click “Back to list”.

To disable simplified connection, delete the entry from the table by clicking and confirm the action by clicking the “Yes” button.

To edit an entry, click , make changes and click “Submit”.

USER NOTIFICATION

This section describes the following administrator web interface menu items:

- SMS;
- Adapters;
- UI Alerts;
- Push Service.

SETTING UP SMS SERVICE

In the “SMS” section, the administrator can configure the following:

- message text;

- integration with a service provider that will send users SMS messages with the authorization code;
- SMS service provider gateway routing;
- security parameters.

SETTING UP THE TEXT OF SMS MESSAGES

To set up the text of SMS messages:

1. Select the "SMS" section in the menu.

   The "SMS Settings" window will open.
2. In the "Provider" field, select a provider. For example, Beeline.
3. In the "Text of SMS message" field, enter the text that will be sent along with the authorization code, and click "Save" (see Figure 24.).

Figure 24.

SETTING UP INTEGRATION WITH PROVIDER

Integration with the service provider is configured in the "Adapters" subsection.

Setting up integration with provider:

1. Go to the "SMS" section and select the "Adapters" subsection.
2. Configure the parameters of the selected provider in the appropriate section, and click "Save" (see Figure 25.).

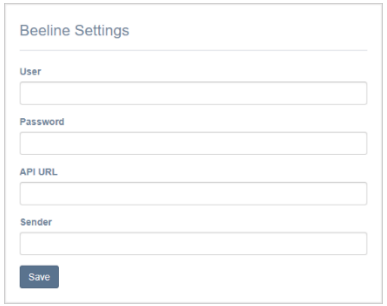

Figure 25.

The settings you can configure vary by provider. Examples of settings for providers are provided in the table below (see Table 8):

Table 8

Provider	Field name	Value
Clickatell	API key	Key for sending SMS messages. Provided by provider
	API URL	SMS service API address
QTelecom	User	Username of the provider's SMS service
	Password	Provider's SMS service user password
	API URL	SMS service API address
	Sender	SMS sender name (e.g. eXpress)

Provider	Field name	Value
	Sender for MTS	SMS sender name (e.g. eXpress)
Beeline	User	Username of the provider's SMS service
	Password	Provider's SMS service user password
	API URL	SMS service API address
	Sender	SMS sender name (e.g. eXpress)
SMSC	Login	User login of the provider's SMS service
	Password	Provider's SMS service user password
	Sender	SMS sender name (e.g. eXpress)
Tele2	Login	User login of the provider's SMS service
	Password	Provider's SMS service user password
	Shortcode	Provided by provider
Twilio	SID	Provided by provider
	Token	Provided by provider
	Sender	SMS sender name (e.g. eXpress)
SMSTraffic	User	Username of the provider's SMS service
	Password	Provider's SMS service user password
	API URL	SMS service API address
	Sender	SMS sender name (e.g. eXpress)
Stream Telecom	User	Username of the provider's SMS service
	Password	Provider's SMS service user password
	From	SMS sender name
	Validity	Message validity period
	Callback URL	Address of the script to which POST data about the SMS delivery status is returned
	Name deliver	Mailing name assigned for ease of searching in statistics
SMSCountry	API URL	SMS service API address
	Sender	SMS sender name (e.g. eXpress)
	Auth Key	Provided by provider
	Auth Token	Provided by provider

SETTING UP THE SMS PROVIDER MASK

The “Masks” subsection in the “SMS” section allows you to configure the routing of the provider's SMS gateway using a phone number mask (see Figure 26.).

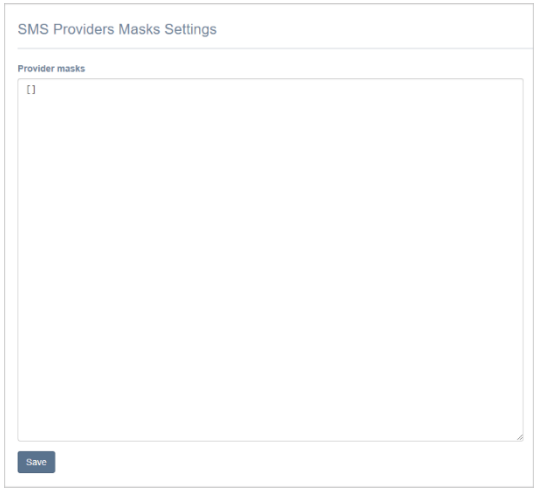

Figure 26.

To set up an SMS gateway, go to the “Masks” subsection, add the required configuration in the window that opens and click “Save” (see Figure 27.):

Figure 27.

SETTING UP SECURITY SETTINGS

The following security parameters are available in eXpress:

- a limit of the number of requests for a specific IP address;
- filter by User-Agent;
- filter by DEF code;
- filter by phone number;
- a limit on the number of requests to a specific phone number.

To set up security settings:

1. Go to the “SMS” section and select the “Security” subsection.
2. Enter the values in the appropriate fields and click “Save” (see Figure 28.).

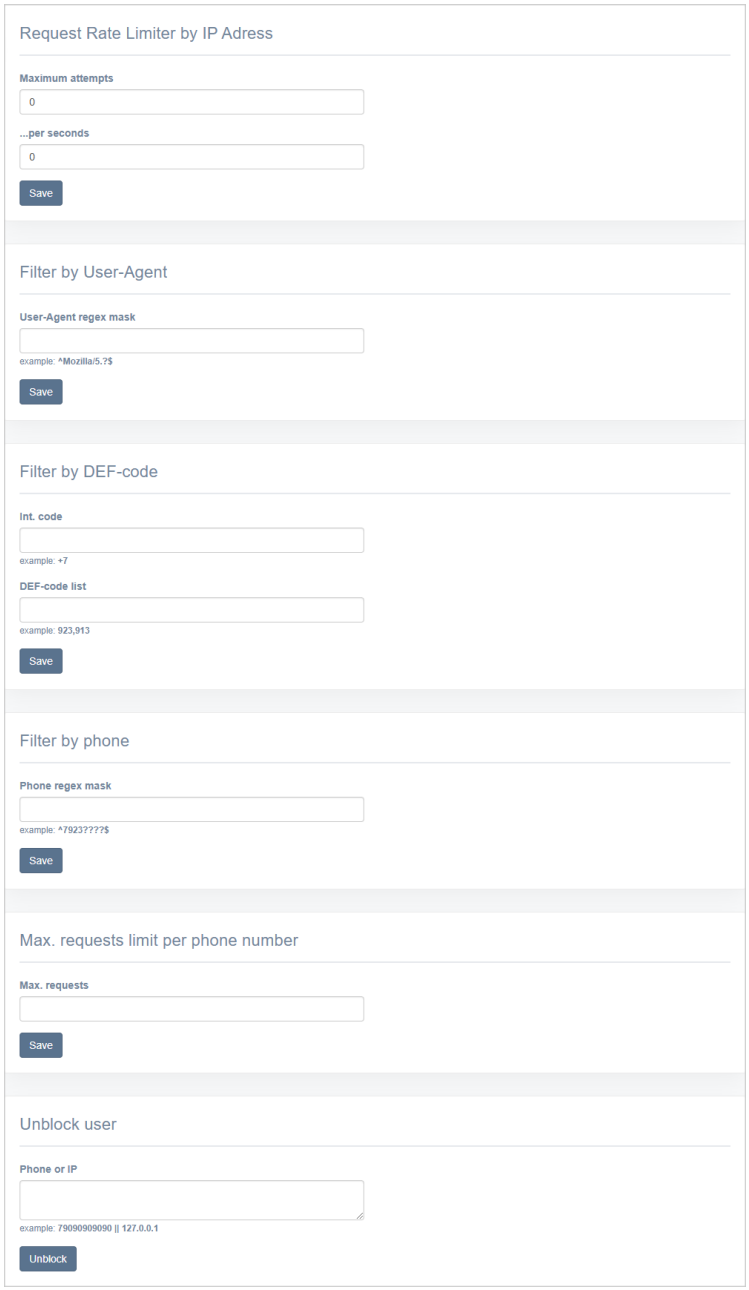

Figure 28.

SMS CAPTCHA

Captcha is used to protect against automated attacks.

To set up captcha activation:

1. Go to the "SMS" section and select the "Captcha" subsection.

   The "SMS Captcha Settings" window will open with fields for activating verification and entering parameters (see Figure 29.).

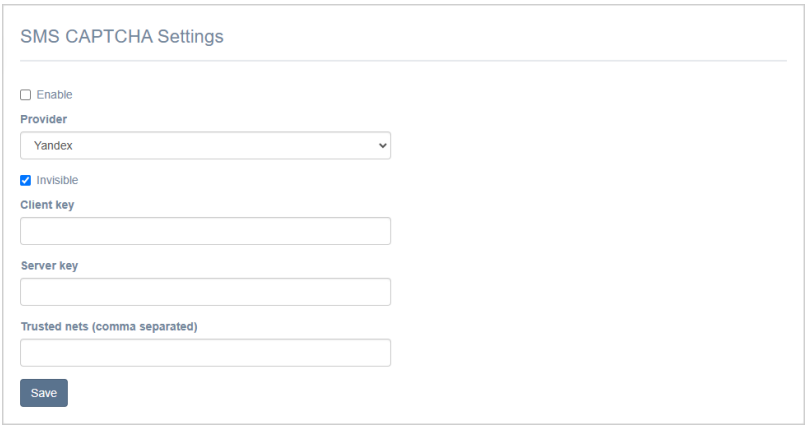

Figure 29.

2. Enable/disable verification by checking the box next to "Verification enabled".
3. Select a service provider from the list (Yandex is currently used by default).
4. Enable/disable the use of invisible captcha by checking the box next to "Invisible captcha" (for more details, follow this link).
5. Specify client and server tokens.
6. Enter a list of trusted IP addresses from which the captcha will not be displayed to the user when requested.
7. Click "Save".

UNBLOCKING A USER ACCOUNT

In the "SMS" section, you can unblock a user account that has been blocked for the following reasons:

- the request limit has been exceeded for the phone number;
- the request limit has been exceeded for the IP address.

Note. You can determine why a user account is blocked by looking at the error in the authentication logs:

- blocked_by_max_requests — blocked by phone number;
- blocked_by_rate_limit — blocked by IP.

Figure 30.

To unblock an account that is blocked due to exceeding the phone number request limit:

1. Go to the "Security" subsection.
2. In the "Unblock User" section, in the "Phone" field, enter the phone number from which the authorization attempts were made. For example, 79090909090 (see Figure 30.).
3. Click "Unblock".

   The request counter will be reset.

To unblock an account that is blocked due to exceeding the IP address request limit:

1. Go to the "Security" subsection.
2. In the "Unblock User" section, in the "Phone" field, enter the IP address from which the user logged in. For example, 127.0.0.1 (see Figure 30.).
3. Click "Unblock".

   The request counter will be reset.

SETTING UP PUSH NOTIFICATIONS

To connect and configure push notifications, go to the"Push Service" section.

The interface is designed to connect push notifications (see Figure 31.).

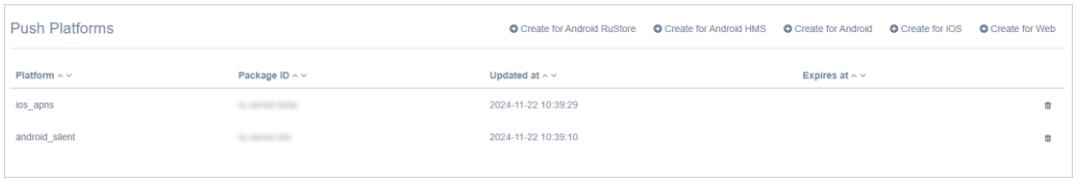

Figure 31.

The table contains the following information (see Table 9):

Table 9

Column name	Information
Platform	The platform on which push notifications are enabled
Package ID	eXpress app build package name
Update date	Date when push notifications settings were last changed
Expiration Date	Push notification expiration date

The mechanism for enabling push notifications varies depending on the platform. Push notifications are connected as follows:

- for Android — via FCM;
- for Huawei — via Push Kit;
- for iOS — via APNS;
- for web apps — via FCM.

Note. For correct operation, access to APN Push services is required:

- Apple APN – api.push.apple.com;
- Google FCM — fcm.googleapis.com; www.googleapis.com;
- Huawei HMS — push-api.cloud.huawei.com, oauth-login.cloud.huawei.com;
- RuStore — vkpns.rustore.ru.

To create a connection in Android:

1. Open the Firebase console.
2. In the project (menu "Project Overview"), where the keys for Android are configured, select "Project settings".
3. In eXpress administrator console, in the "Push Service" section, click "Create for Android" in the upper right corner.

A window for creating a connection for the Android platform will open (see Figure 32.).

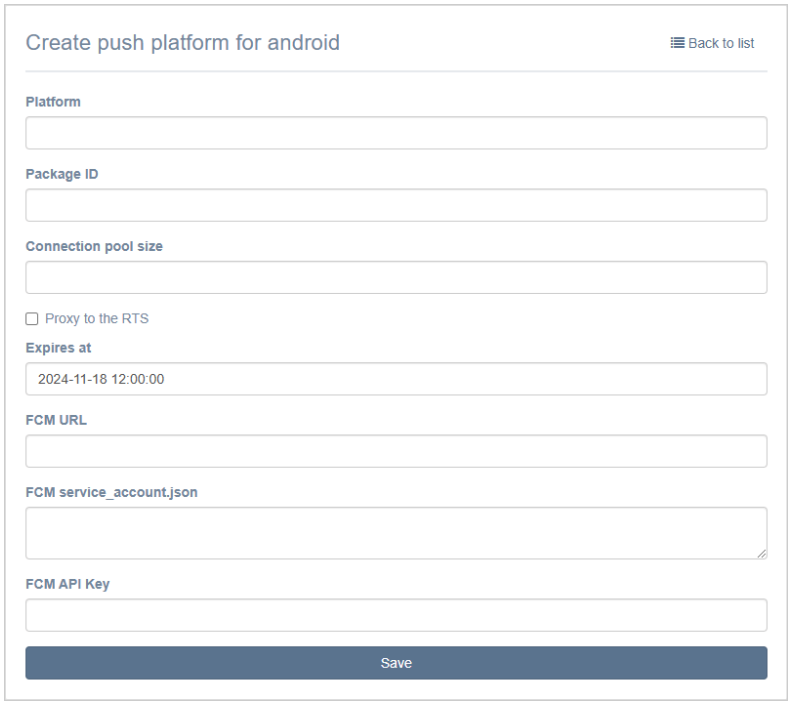

Figure 32.

4. Fill in the fields of the form (see Table 10):

Table 10

Parameter	Description	Value
Platform	The platform on which push notifications are enabled	android_silent
Package ID	eXpress app build package name	
Maximum number of platform connections	Push platform connection pool size	If you leave the field blank, the default pool size will be set to 10.
Expiration Date	Push notification expiration date	
FCM URL	Firebase Cloud Messaging Server Address	https://fcm.googleapis.com/v1/projects/{fcmProjectID}/messages:send The ProjectID value is taken from the Firebase console (Project Settings → General)
FCM service_account.json	Service account JSON file	The file can be downloaded from the Firebase console (Project Settings → Service Account)
FCM API Key	The key is not provided or required on the latest version of the Firebase Cloud Messaging API (HTTP v1)	

5. Click “Save”.

To create a connection on HMS Android:

1. Click “Create for HMS Android”.

   A window for creating a connection for the Huawei platform will open (see Figure 33.).

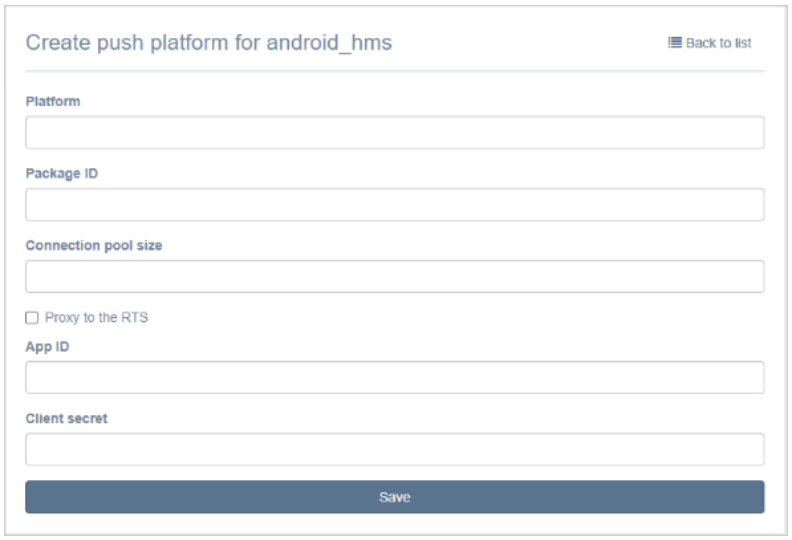

Figure 33.

2. Fill in the fields of the form (see Table 11):

Table 11

Parameter	Description	Value
Platform	The platform on which push notifications are enabled	android_hms
Package ID	eXpress app build package name	
Maximum number of platform connections	Push platform connection pool size	If you leave the field blank, the default pool size will be 10.
App ID	App ID in the Push Kit console	
Client secret key	Key in the Push Kit console	

3. Click “Save”.

To create a connection in iOS:

1. Click “Create for iOS” in the upper right corner.

   A window for creating a connection for the iOS platform will open (see Figure 34.).

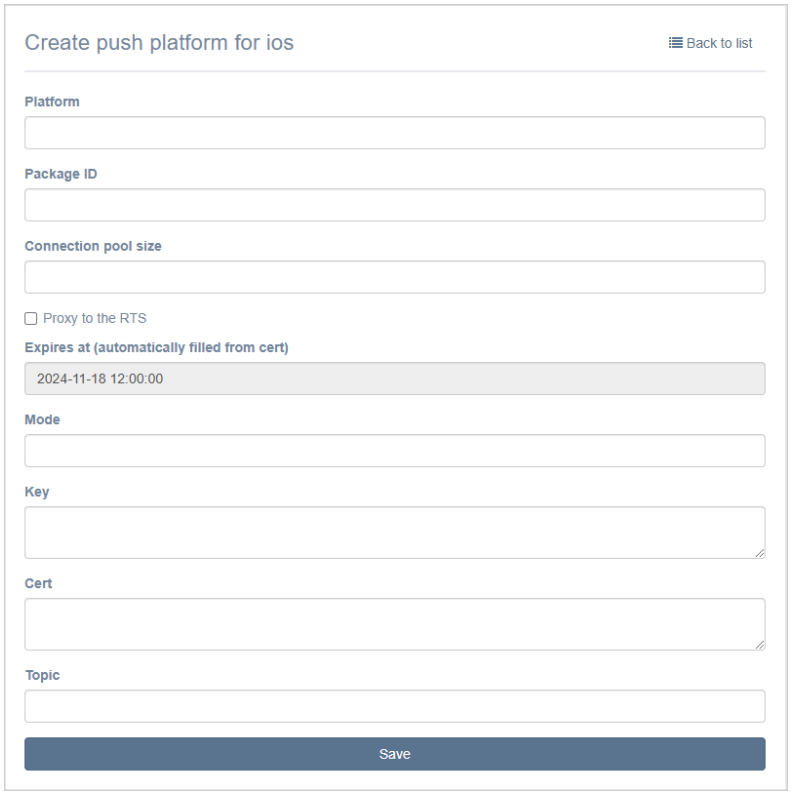

Figure 34.

2. Fill in the fields of the form (see Table 12):

Table 12

Parameter	Description	Value
Platform	The platform on which push notifications are enabled	• ios_apns (for alert push with apns certificate); • ios_voex (for push notifications calls with voip certificate)
Package ID	eXpress app build package name	
Maximum number of platform connections	Push platform connection pool size	If you leave the field blank, the default pool size will be 10.
Expiration Date	Push notification expiration date	
Mode	Push notification operating mode. Possible values for prod/dev	• dev (for beta build); • prod (for release/prerelease)
Key	Private key	
Cert	Certificate	
Topic	eXpress app build name	Package ID (for ios_apns); Empty value (for ios_voex)

3. Click “Save”.

To create a connection in the Web app:

1. Open the Firebase console.
2. In the Firebase console, create a project for the web interface.
3. In the window that opens, click “Generate key pairs”.
4. In the administrator console, in the “Push Service” section, click “Create for Web” in the upper right corner.

   A window for creating a connection for the Web app will open (see Figure 35.).

Figure 35.

5. Fill in the fields of the form (see Table 13).

Note. In the "Platform" field, enter the value "web".

Table 13

Parameter	Description	Value
Platform	The platform on which push notifications are enabled	• web; • web_chrome; • web_firefox
Package ID	eXpress app build package name	
Expiration Date	Push notification expiration date	
FCM API Key	API key issued in the Firebase administrator console	
Public VAPID key	Public API key generated in the Firebase administrator console	
Private VAPID key	Private API key generated in the Firebase administrator console	
VAPID subject (URI or e-mail)	User E-mail address in Firebase	mailto:<e-mail of the Firebase account>

6. Click "Save".
7. Repeat steps 1 to -6 for Chrome, and specify the "web_chrome" value in the "Platform" field.

   Two entries will appear in the "Push Service" section (for two browsers).
8. In the Docker image configuration file (WEB_CLIENT_CONFIG), change the gcmSenderId parameter to the value from Firebase.

To edit a connection, select it from the list, click and make changes in the window that opens.

To remove a connection, select it from the list and click .

UI ALERTS

The interface is used for the creation of UI Alerts. UI Alert is a special trigger that blocks the app until the user fulfills certain requirements (updates the app to a specific version, clears data).

To forcibly lockout the app:

1. Open the "UI Alerts" section.
2. Click "Create".

   A window will open (see Figure 36.):

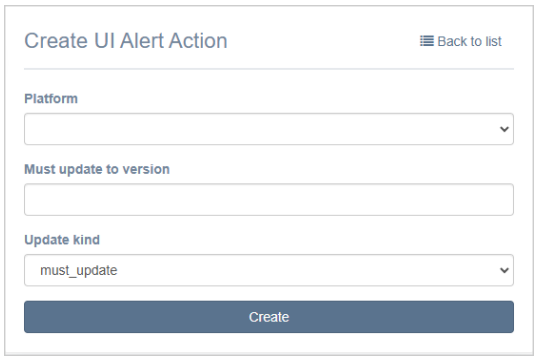

Figure 36.

3. Fill in the fields of the form that opens (see Table 14):

Table 14

Parameter	Purpose
Platform	Determines what client platform is the UI Alert intended for
Must update to version	Minimum required client version for the platform selected above (in the format X.X.X, for example, 3.9.1)
Update kind	What actions will be required from the user: • must_update — update the client app to the current version; • must_clear_data — re-enter session to clear local cache; • must_update_and_clear_data – update the client app to the current version and re-enter the session to clear the local cache

4. Click "Create".

   A lockout message will be sent to the user's phone with a requirement to perform the specified actions to restore access to the app.

SETTING UP USER SESSION ACTIVITY TIME

In the "Activations" section, you can set the time in seconds after which the user session in iOS, Android, Web or Desktop app is closed and you are returned to the authorization window.

To set up the user session activity time:

1. Go to the "Activations" section.

   The "Activation Settings" window will open with fields for entering parameters (see Figure 37.).
2. Specify the session duration in seconds (to disable automatic closing of the user session, leave the field blank).
3. Click "Save".

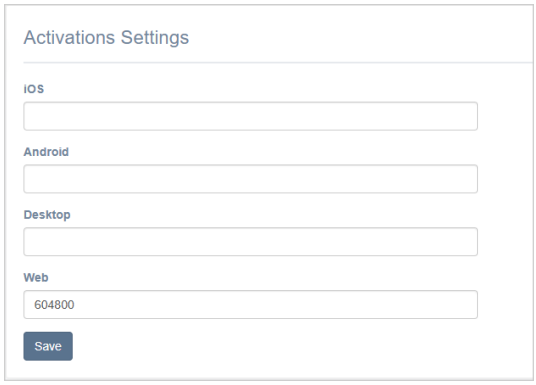

Figure 37.

4. Click “Save”.

MANAGING ADMINISTRATOR USER ACCOUNTS

Administrator accounts are managed in the “Administrators” section. This section allows you to:

- create administrator accounts;
- edit administrator accounts;
- delete administrator accounts;
- lockout/unblock administrator accounts;
- configure access rights for groups of administrators;
- connect administrator accounts using A.

A complete list of administrators is provided in the “Administrators” menu item (see Figure 38.).

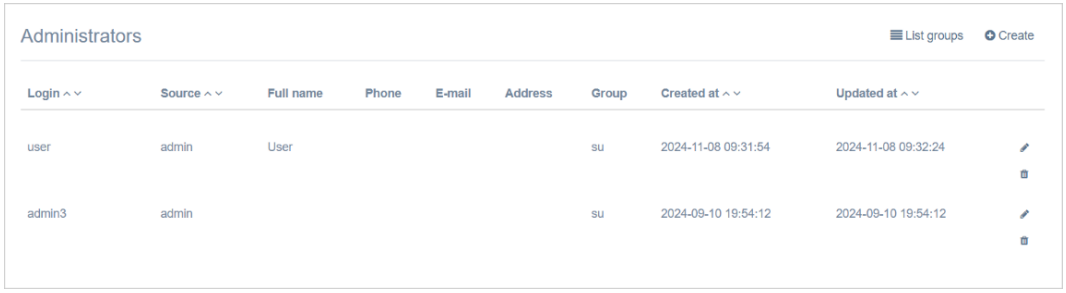

Figure 38.

The table with the list of administrators contains the following information (see Table 15):

Table 15

Column name	Information
Login	The identification name of the account in Active Directory. Used when authorizing a user
Source	Account source: • ad — loaded from Active Directory; • admin — created in the administrator console
Full name	Administrator's full name
Phone	Administrator's contact phone number
E-mail	Administrator's contact e-mail address
Address	Administrator's physical address

Column name	Information
Group	The group to which the administrator belongs
Creation date	Account creation date
Update date	Date the account was last updated

CREATING ADMINISTRATOR ACCOUNTS

The administrator console implements two methods for creating administrator accounts: loading a generated group of accounts from AD and creating them using the web interface.

To create an administrator account:

1. Select the "Administrators" menu item.
2. In the upper right corner, click "Create".

   A window will open (see Figure 39.):

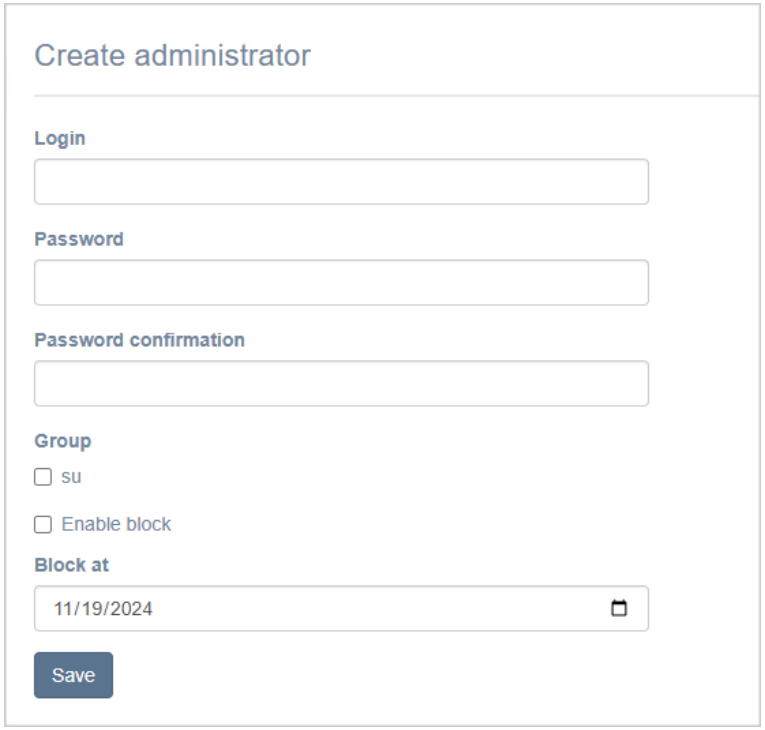

Figure 39.

3. Fill in the fields of the form.

   In the "Group" field, select the groups that the created administrator account will belong to.

   The "Enable lockout" setting allows you to lock out the administrator account on a specific day.

   To set up the administrator account lockout settings, Select a date in the "Lockout on" field.
4. Click "Save".

   The message "Administrator account saved" will be displayed at the top of the window.
5. Fill in/edit the form fields in the next window and click "Save" (see Figure 40.):

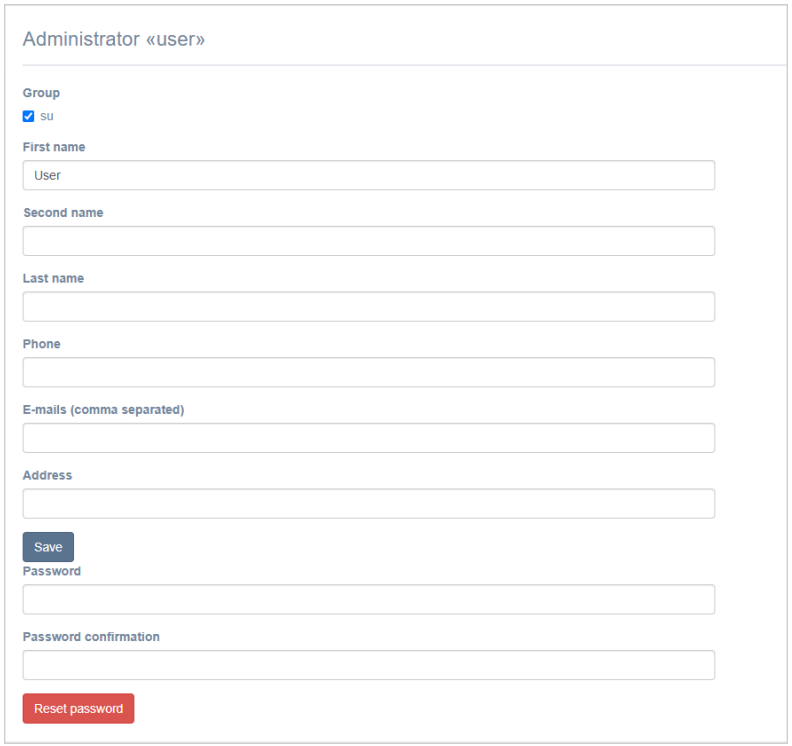

Figure 40.

6. Click “Save”.

   The created account will be displayed in the table.

SETTING UP ADMINISTRATOR AUTHENTICATION

This section is intended for connecting administrators using AD.

To set up loading of administrator accounts from AD:

1. Go to the “Administrator Authentication” section (see Figure 41.):

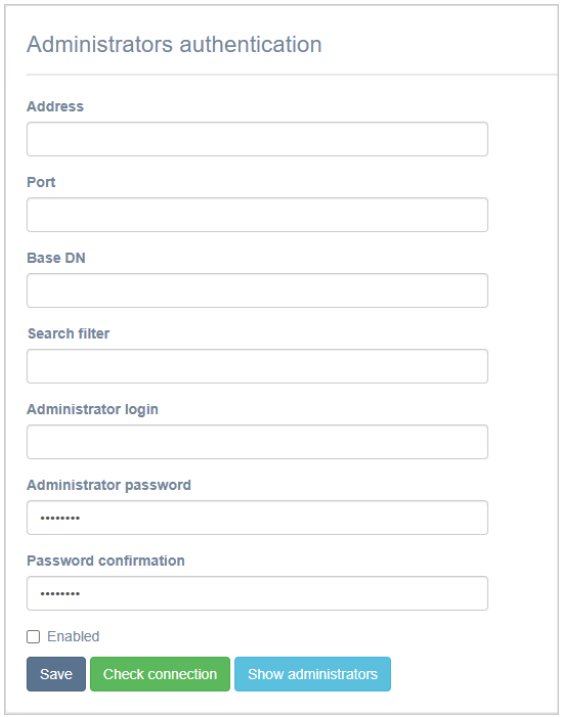

Figure 41.

2. Configure the settings shown in the table below (see Table 16).

   The parameter values are provided by the Active Directory administrator.

Table 16

Parameter	Description
Address	Active Directory address
Port	AD connection port
Base DN	Directory object from which the search is performed
Search filter	Filter for LDAP search. It shall ensure filtering of active users who are allowed to connect to this server. Recommended query construct: "(&(objectClass=person)(objectClass=user)(memberOf:1.2.840.113556.1.4.1941:=cn= express,ou=Groups,dc=firma,dc=local))" where "cn= express,ou=Groups,dc=firma,dc=local" is the DN of the group, whose members will be eXpress users. When using cross-domain structures, specify the domain DC=ru in the connection parameters. An example of setting up synchronization of administrative users with a filter: (|(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))
Administrator login	Login of the user who has read access to the list of users at the specified DN
Administrator password	Password of the user who has read access to the list of users at the specified DN
Password confirmation	Confirmation of the password of the user who has read access to the list of users at the specified DN

To enable/disable authentication of Active Directory administrators, check/uncheck "Enabled".

To test the connection to Active Directory, click "Test Connection".

After clicking on the "Show administrators" button, a list of Active Directory administrators is displayed.

SETTING UP ADMINISTRATOR ACCESS RIGHTS

Role-based division of rights in eXpress CS is implemented by combining administrators into different groups. Each group of administrators has its own set of rights.

To create a group:

1. Select the “Administrators” menu item.
2. In the upper right corner, click “Show Groups”.

   A window will open with a list of groups and their rights – “Groups” (see Figure 42.).

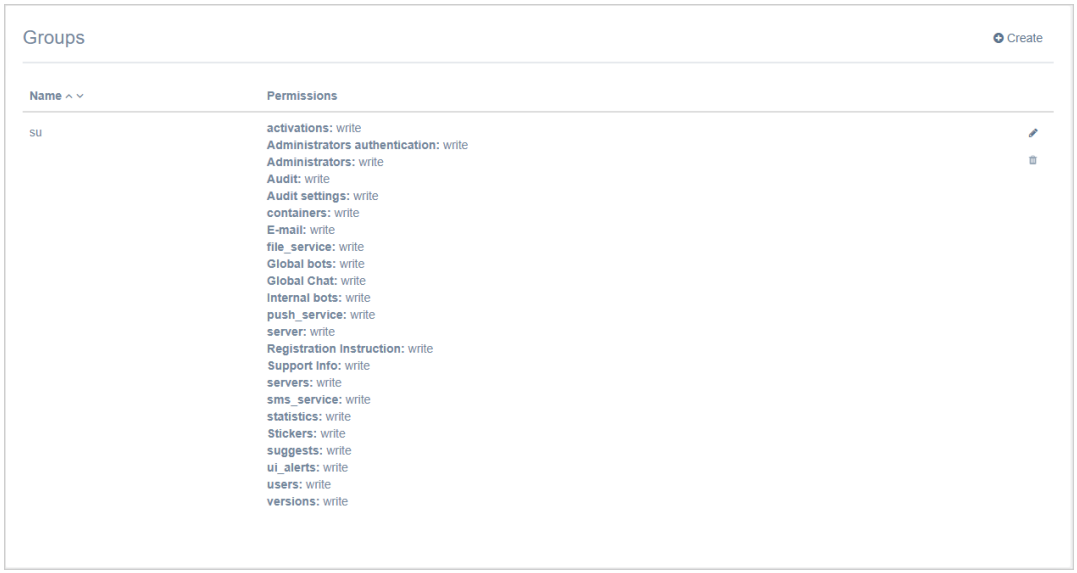

Figure 42.

3. In the upper right corner, click “Create”.

   A window for creating a group and setting its rights will open (see Figure 43.).

   The rights buttons have the following meanings, see the tale below (see Table 17):

   - No — the administrator does not have access rights to the menu item;
   - read — the administrator can only view the information in the menu item;
   - Write — the administrator can view the information in the menu item and make changes to it.

4. In the “Name” field, enter the name of the group.
5. In the “LDAP Group” field, the name of the administrator group in AD can be specified.

   If the administrators of the group being created or edited are members of the specified group in Active Directory, they will receive the rights of the corresponding AD group.

6. In the “Rights” section, set access rights for the group.
7. Click “Save”.

   The created group will be displayed in the “Groups” window.

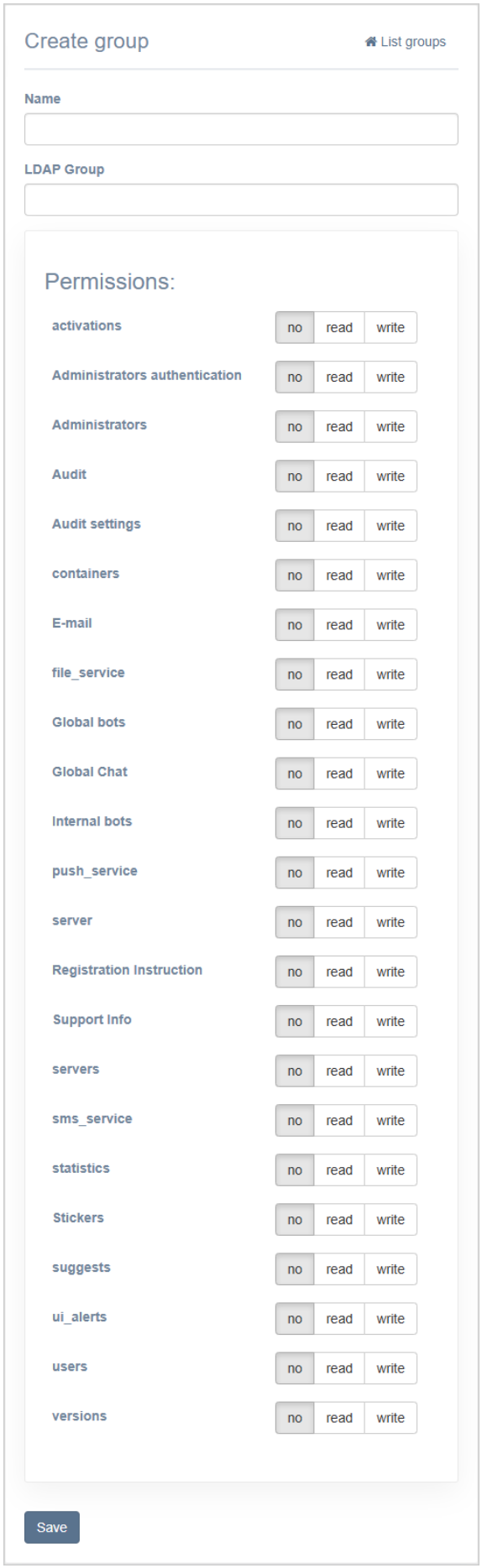
Create group
List groups
Name
LDAP Group
Permissions:
activations no read write
Administrators authentication no read write
Administrators no read write
Audit no read write
Audit settings no read write
containers no read write
E-mail no read write
file_service no read write
Global bots no read write
Global Chat no read write
Internal bots no read write
push_service no read write
server no read write
Registration Instruction no read write
Support Info no read write
servers no read write
sms_service no read write
statistics no read write
Stickers no read write
suggests no read write
ui_alerts no read write
users no read write
versions no read write
Save

Figure 43.

The list of administrator rights is presented in the table below (see Table 17).

Table 17

Menu item name	Rights		
	NO	**READ**	**WRITE**
Activations	No access to the section	Viewing user session active time settings	Changing user session active time settings
Authentication of Administrators	No access to the section	Viewing administrator authentication settings	Changing administrator authentication settings
Administrators	No access to the section	Viewing: • list of administrators; • administrator groups	Creating, editing and deleting administrators. Setting Up Administrator Rights
Change of their password by the administrators	No access to the section	View of their profile by the administrator	Change of their profile by the administrator
Audit	No access to the section	Viewing audit events	Viewing audit events
Audit Settings	No access to the section	Viewing security event information transmission settings	Enable/disable sending of information about security events to the SIEM of the information system into which eXpress is integrated
Containers	No access to the section	Viewing Docker containers lists and logs	Viewing Docker containers lists and logs
E-mail	No access to the section	Viewing: • mail server settings; • test recipient e-mail addresses	Changing: • mail server settings; • test recipient e-mail address. Testing e-mail sending
File Service	No access to the section	Viewing settings: • network contour on the CTS server; • deletion of files on the hard drive	Changing settings: • network contour on the CTS server; • deletion of files on the hard drive
Global Bots	No access to the section	Viewing the list of global bots	Adding global bots to the global chat. Removing global bots from global chat
Global Chat	No access to the section	Viewing global chat settings	Enabling and disabling global chat. Setting Up Global Chat Settings
Internal Bots	No access to the section	Viewing the list of internal bots	Changing and setting up internal bot Adding a bot administrator
Push Service	No access to the section	Viewing settings of push notifications	Setting Up Push Notifications
Server	No access to the section	Viewing settings: • corporate server; • Authorization notifications. Viewing the corporate address book search enable/disable indicator. Viewing validity periods: • TLS certificates of trusts; • SSL certificates of chatbots platform. Viewing service versions	Changing settings: • corporate server; • Authorization notifications. Enabling/disabling corporate address book search Addition and removal: • TLS certificates of trusts; • SSL certificates of chatbots platform. Viewing service versions

Menu item name	Rights		
	NO	READ	WRITE
Registration Instructions	No access to the section	Viewing attached files	Viewing and editing attached files
Support Contacts	No access to the section	View completed fields and marks placed	Viewing, editing data, saving changes
Servers	No access to the section	Viewing configured trusts	Connecting and changing trust settings
SMS Statuses	No access to the section	Viewing information about SMS codes that were used to authenticate users in the system	Choosing an SMS service provider
Statistics	No access to the section	Viewing application performance statistics	Viewing application performance statistics
Stickers	No access to the section	Viewing stickers	Uploading and deleting stickers
Simplified Connection via E-mail	No access to the section	Viewing the list of users with simplified authorization	SETTING UP SIMPLIFIED AUTHORIZATION
UI Alerts	No access to the section	View forced lockouts	Creating and deleting forced lockouts
Users	No access to the section	Viewing: • user list; • account settings; • open user sessions; • user lockouts; • public keys; • chats in which the users are participants	Clearing the user account cache
Versions	No access to the section	Viewing the versions of CTS and services installed on this ETS	Viewing the versions of CTS and services installed on this ETS

To edit a group, click . Make changes in the window that opens and click "Save".

To delete a group, click . The button will be unavailable, if the group contains at least one administrator account.

EDITING ADMINISTRATOR ACCOUNTS;

There are two ways to edit the administrator account.

FIRST METHOD

To edit the administrator account:

1. Open the "Administrators" menu item and select the required account.
2. Click .

   A window will open (see Figure 44.):

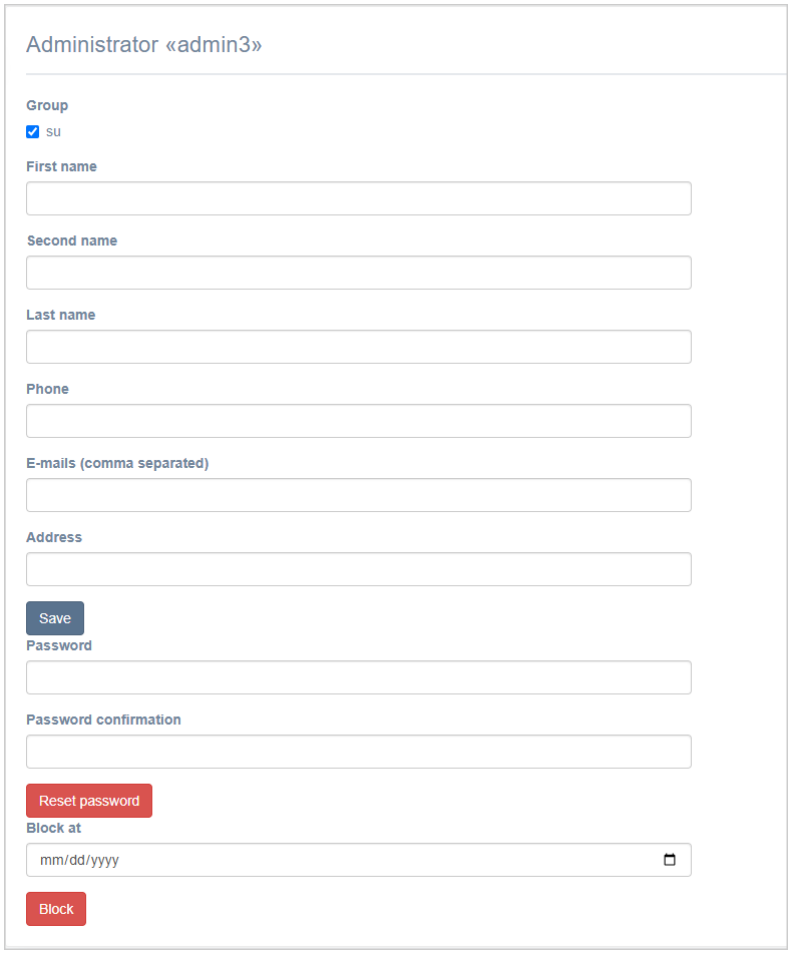

Figure 44.

3. Make the necessary changes to the fields.

Note. The administrator can be a member of several groups. To select groups, check the appropriate options in the "Groups" field.

4. Click "Save".

SECOND METHOD.

To edit the administrator account:

1. Tap on  in the upper left part of the window (Figure 45.).

Figure 45.

If "write" is set in the "Administrators" item of the administrator rights settings, the window with the administrator profile settings (Figure 44.) will open.

If "no" or "read" is set in the "Administrators" menu item, but "write" is set in the "Change of their password by the administrator" item, the window with administrator password and data settings will open (Figure 46.).

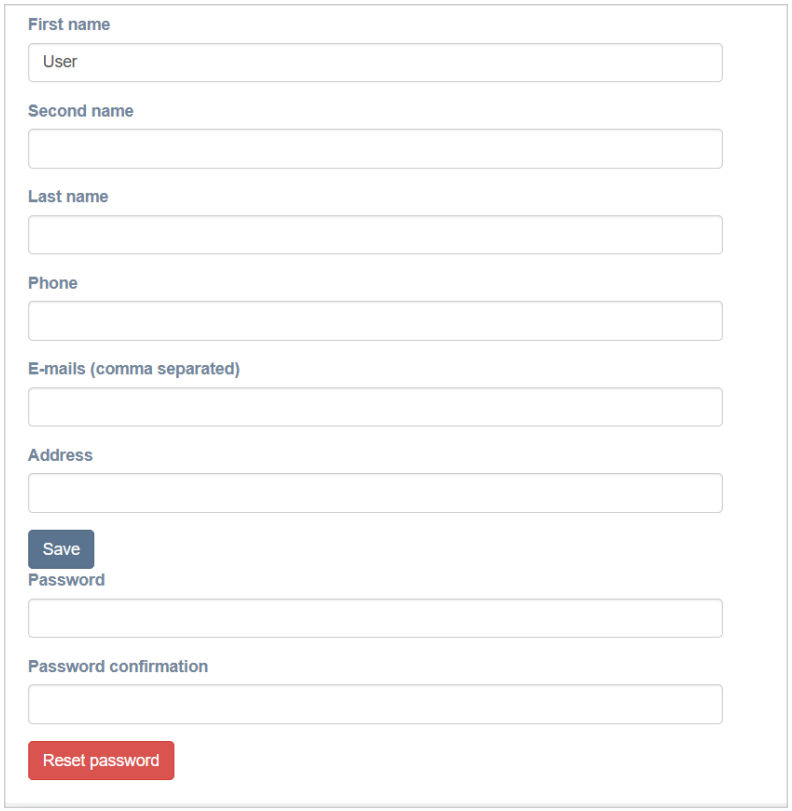

Figure 46.

2. Make the necessary changes to the fields.
3. Click “Save”.

LOCKING OUT ADMINISTRATOR ACCOUNTS

To lockout an administrator account:

1. Open the “Administrators” menu item and select the required account.
2. Click .
3. In the form that opens, click the calendar button in the “Lockout on” field.
4. Select the lockout date from the calendar (see Figure 47.).

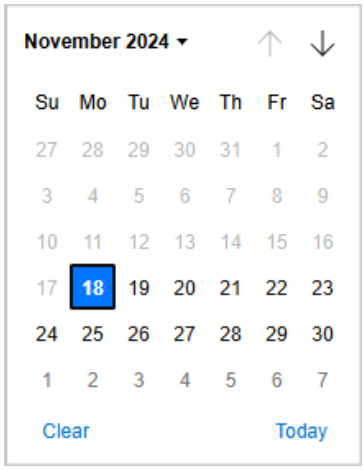

Figure 47.

5. Click “Lockout”.

6. Confirm the action in the modal window that opens.

   The administrator account will be locked out on the set date.

To change the administrator account lockout settings select a date in the "Lockout on" field, click "Lockout" and confirm the action in the modal window that opens.

To unblock an administrator account click "Cancel lockout" and confirm the action in the modal window that opens by clicking "Yes".

To unblock a locked out administrator account, click "Unblock" (see Figure 48.) and, confirm the action in the modal window that opens by clicking "Yes".

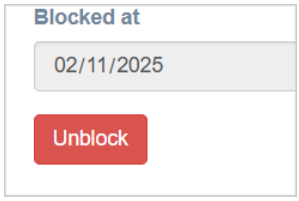

Figure 48.

DELETING ADMINISTRATOR ACCOUNTS

To remove the administrator account:

1. Open the "Administrators" menu item and select the required account.
2. Click to the right of the corresponding account.
3. Confirm the action in the pop-up window by clicking the "OK" button.

   The message "Administrator removed" will be displayed at the top of the window.

GLOBAL CHAT

Global chat (see Figure 49.) is a system chat that allows you to send messages that are relevant to all users, for example:

- information about app updates;
- maintenance notifications.

Global chat is created on all types of servers (CTS, ETS, RTS). There can only be one global chat per server. To send messages to the global chat, you need to connect Notifications Bot (see page 55).

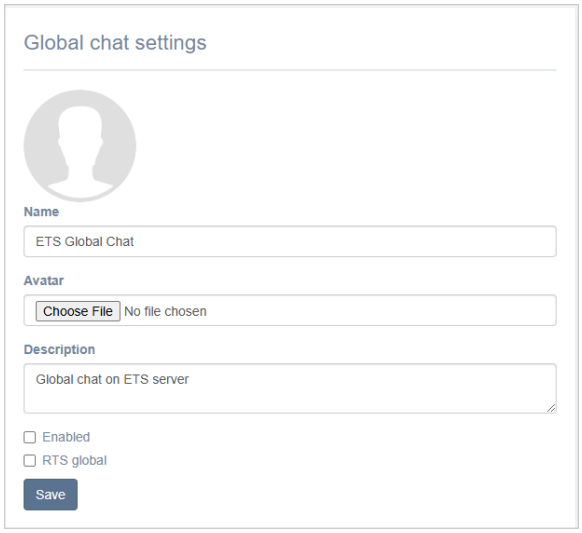

Figure 49.

The “Global Chat” section consists of two blocks:

- Global Chat;
- Global Bots.

GLOBAL CHAT SETTINGS

To set up global chat:

1. Select the “Global Chat” section in the administrator panel.
2. In the window that opens, specify the chat parameters.
3. Enable/disable the “Global Chat” functionality by checking/unchecking the box next to the “Enabled” field (global chat is disabled by default).
4. Click “Save”.

MANAGING BOTS

This section describes the following administrator web interface menu items:

- Internal Bots;
- Global Bots.

INTERNAL BOTS

Information about internal bots is provided in the “Internal Bots” subsection of the administrator console (see Figure 50.).

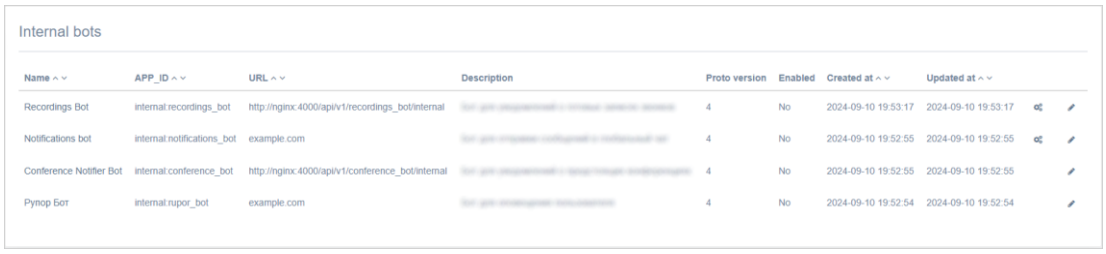

Figure 50.

Internal bots are created automatically after the system is deployed.

The table contains the following information (see Table 18):

Table 18

Column name	Information
Name	Bot name
APP_ID	Bot ID
URL	Bot address
Description	Bot purpose
Protocol version	Version of the protocol for working with botx
Enabled	Bot operation status
Creation date	Bot creation date and time
Update date	Time of last change of bot parameters

To view internal bot parameters, select the desired bot from the list. The bot editing window will open (see Figure 51.).

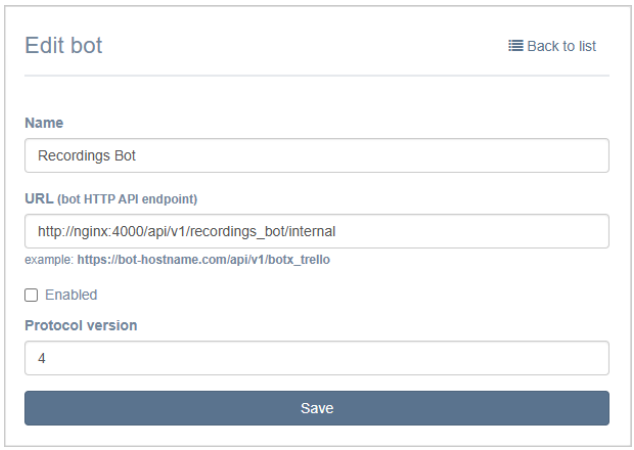

Figure 51.

To return to the general list of internal bots, click "Back to List".

To edit internal bot parameters:

1. Select a bot from the list.

   The bot editing window will open.
2. If necessary, change the bot name or URL.
3. If necessary, change the bot's operating status by checking the "Enabled" field.
4. Click "Save".

   The editing window will close and the changes will be displayed in the general list of internal bots.

DESCRIPTION OF CONFERENCE BOT

Conference Bot is designed to notify users about upcoming conferences.

The bot informs the user:

- about the creation of a new conference with his participation;
- about upcoming conferences;
- about changes in the parameters of the upcoming conference.

When a conference is canceled, information about it disappears from the user's chat window.

When a scheduled conference with the user's participation is created, the user receives a notification in the chat with the bot. All bot functions are available (disabling notifications, setting reminders, setting time zone, search).

The conference announcement includes:

- information about the creation of a conference or changes to its parameters;
- date and time of conference creation;
- name of the organizer of the conference;
- link to join the conference;
- the "Show Members" button.

DESCRIPTION OF NOTIFICATIONS BOT

Notifications Bot is designed to send messages to the Global Chat. Users with administrator rights can send messages to the Global Chat.

To add an administrator to Notifications Bot:

1. Go to the "Internal Bots" tab (see Figure 52.) and click .

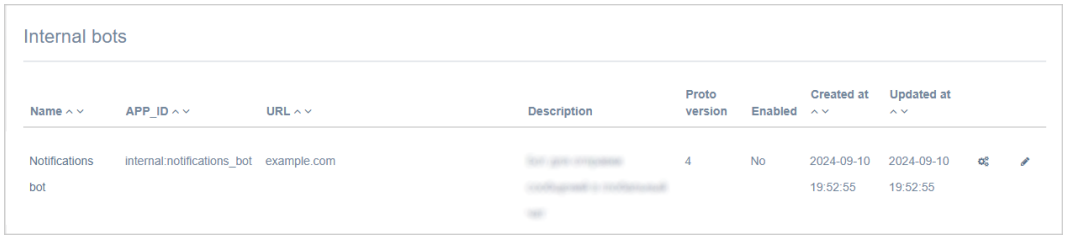

Figure 52.

   The list of administrators will be displayed in the window that opens.
2. Click "Add Bot Administrator".
3. In the list that opens, select the user who should receive administrator rights and click +.

   The message "Administrator added" will be displayed at the top of the screen.

GLOBAL BOTS

Global bots are bots that can be added to the global chat.

The section is a table with information about bots (see Figure 53.).

Figure 53.

The table contains the following information (see Table 19):

Table 19

Column name	Information
Name	Bot name
Description	Bot purpose
Enabled	Bot operation status

To add a bot to the global chat:

1. Click "Add bot to global chat".
2. In the window that opens, select the desired bot.

   Note. For successful addition, the bot must first be enabled.

3. Click "+" to the left of the bot's name.

   A list of global bots will open, and the message "Bot added to global chat" will be displayed at the top of the screen.

To remove a bot from the global chat, select the desired bot and click 🗑. The bot will be removed from the list, and the message "Bot removed from global chat" will be displayed at the top of the screen.

MANAGING FILE SERVICE

In the "File Service" section, the administrator can configure the following:

- file storage periods;
- proxying when delivering static content.

SETTING UP FILE STORAGE PERIODS

To set up file cleaning:

1. Go to the "File Service" section (see Figure 54.)

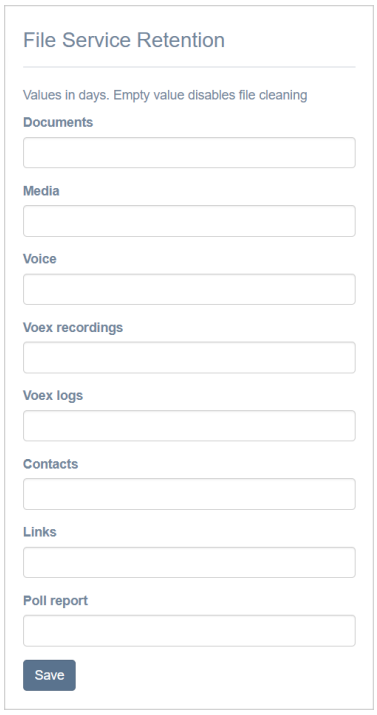

Figure 54.

2. Specify the number of days during which documents, media, and voice files shall be stored. An empty value will disable the file cleaning function.
3. Click "Save".

Proxying when Delivering Static Content

To enable/disable proxy settings:

1. Go to the "File Service" section.

   The "Proxying" window will open (see Figure 55.).

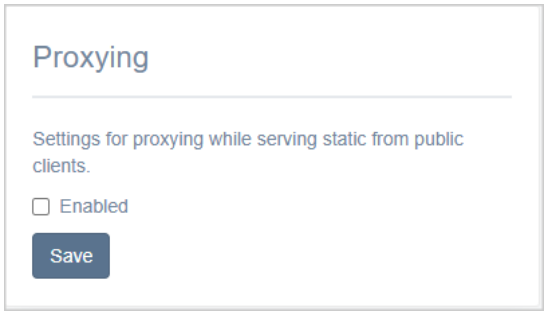

Figure 55.

2. Check/uncheck the "Enabled" field.
3. Click "Save".

LOGS

This section describes the following administrator web interface menu items:

- Containers;
- Audit Settings;
- Audit.

VIEWING LOGS

eXpress CS does not provide a single source for viewing logs of all product events. Each container has its own event log.

To view the list of Docker containers, select the "Containers" section (see Figure 56.).

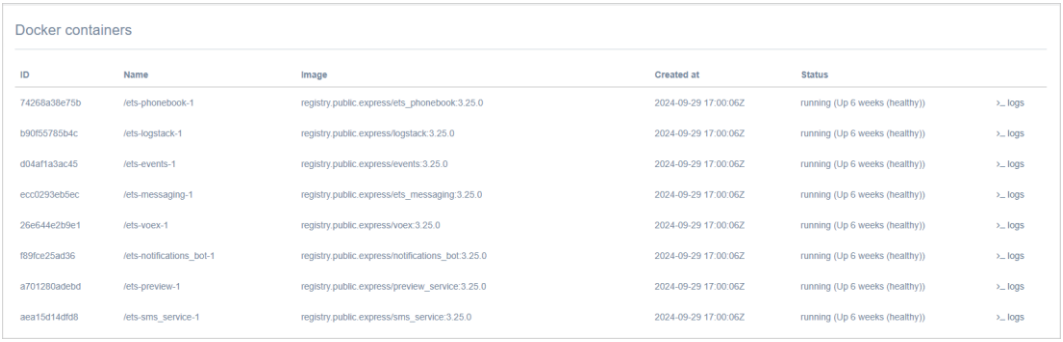

Figure 56.

The table with the list of installed Docker containers contains the following information (see Table 20):

Table 20

Column name	Information
ID	Container ID
Name	Container name in the "server_container" format

Column name	Information
Image	The directory where the container image is stored
Creation date	Container creation date
Status	Container status, which takes the following values: • Created; • Restarting; • Running; • Removing; • Paused; • Exited; • Dead
Logs	Hyperlink to container log

To view a container log:

1. Click on the "Logs" hyperlink next to the Docker container.

   A window will open (see Figure 57.):

Figure 57.

2. In the "Date" field, specify the time period for which you want to display records on the screen.

   Note. If the "Date" field is left blank, all log entries for the day or the latest entries will be displayed on a black screen, according to the number of lines specified in the "Tail" field.

3. Enter the number of lines in the "Tail" field.
4. Check the "Follow" box to receive real-time event notifications.

   Note. The log will be updated with new entries regardless of whether the "Follow" field is checked or not. If the box is checked, eXpress CS will return the administrator to the end of the list to the new event record.

5. Click "Show".

   The container log lines will be displayed on a black screen.

When the clipboard is full, new events in the log will overwrite the oldest ones. When updating a container to a new version, old logs are completely erased.

SETTING UP EVENT INFORMATION TRANSMISSION

eXpress CS has a function for enabling/disabling sending information about security events to the SIEM of the information system into which eXpress CS is integrated.

Work with SIEM occurs via the TCP protocol in syslog format. When transmitting security event information, only audit data is sent.

To set up the transmission of security information to SIEM:

1. Go to the "Audit Settings" section (see Figure 58.).

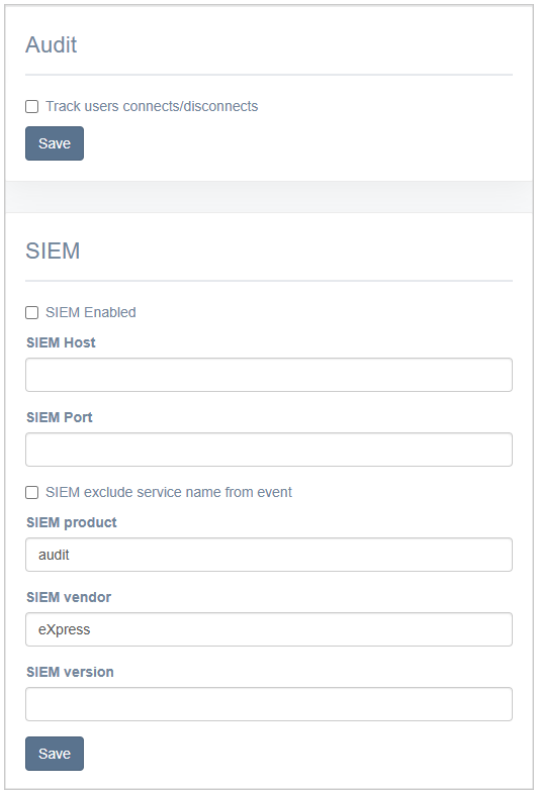

Figure 58.

2. Enable/disable the “Track user connections/disconnections” setting in the “Audit” section.
3. Click “Save”.

To set up the transmission of security information to SIEM:

1. Enable/disable the “SIEM Enabled” setting.
2. In the “SIEM Host” field, enter the address of the SIEM host.
3. In the “SIEM Port” field, specify the SIEM port number.
4. Enable/disable the setting “SIEM exclude service name from event generation arguments”.
5. In the “SIEM Product” field, enter the required service name.
6. In the “SIEM Vendor” field, enter the vendor name.
7. In the “SIEM version” field, specify the version that is sent to the SIEM (if left blank, the backend version will be used).
8. Click “Save”.

AUDIT OF ADMINISTRATOR AND USER ACTIONS

A special interface has been implemented in eXpress CS for the performance of audit of the actions of administrators and users.

To view the events table, select the "Audit" item (see Figure 59.).

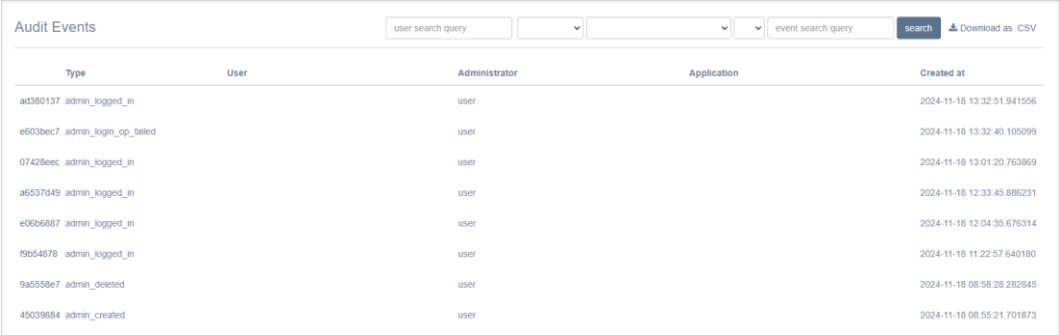

Figure 59.

The parameters of the events recorded in the audit log are shown in the table below (see Table 21):

Table 21

Column name	Information
View	Event ID as a hyperlink and its type. Clicking the hyperlink opens the event's program code
User	User name
Administrator	Name of the administrator
Application	The platform on which the event occurred
Creation date	Event registration date

The following events are logged in the audit log (see Table 22):

Table 22

Event	Description
account_deleted	Account has been deleted
activations_platform_lifetimes_settings_updated	Activation lifetime settings for platforms have been updated
admin_added	An administrator has been added using the CLI method
admin_authentication_updated	System administrator authorization settings have been updated
admin_block_canceled	Administrator account lockout has been canceled
admin_block_date_set	Administrator account lockout date has been set
admin_blocked	Administrator account has been locked out
admin_created	An administrator account has been created
admin_deferred_block_canceled	Delayed administrator account lockout has been canceled
admin_deferred_block_set	Delayed administrator account lockout has been configured
admin_deleted	An administrator account has been deleted
admin_group_created	An administrator group has been created
admin_group_deleted	An administrator group has been deleted
admin_group_updated	The name of the administrator group has been updated
admin_info_updated	Administrator information has been updated
admin_logged_in	Administrator has logged in
admin_logged_out	Administrator has logged out

Event	Description
admin_login_backoff_timeout	The number of unsuccessful administrator login attempts over a certain period (by default — 1 hour) has exceeded the maximum allowed value (by default — 3)
admin_login_op_disabled	The number of unsuccessful administrator login attempts has exceeded the maximum allowed value (by default — 10)
admin_login_op_failed	Unsuccessful administrator authorization attempt without exceeding the allowed values
admin_unblocked	Administrator account has been unblocked
admin_updated_parameters	Administrator account settings have been updated
admin_updated_password	Administrator account password has been updated
audit_settings_updated	Audit settings have been updated
background_wallpaper_settings_updated	Chat background settings for clients have been updated
bot_updated	Chatbot has been updated (only applies to internal bots)
captcha_settings_changed	CAPTCHA settings changed
chat_member_added	Chat member has been added
chat_member_become_admin	Chat member has become chat administrator
chat_member_become_nonadmin	Chat participant has been deprived of chat administrator rights
chat_member_deleted	Chat member has been deleted from chat
clean	Chat history has been cleared
devops_token_created	DevOps token has been created
e2e_encryption_disabled	End-to-end encryption has been disabled in ordinary chat
e2e_encryption_enabled	End-to-end encryption has been enabled in ordinary chat
email_settinds_changed	Mail server settings changed
email_settings_changed	SMTP server settings have been set using the CLI method
faq_updated	FAQ have been updated
file_service_settings_changed	File storage settings changed
file_settings_have_been_set	File storage settings have been set using the CLI method
files_retired	File storage has been cleared
global_chat_enabled	Global chat has been enabled
global_chat_settings_changed	Global chat settings have been changed
hide_name_settings_updated	Hide server name settings have been updated
push_platform_created	Push notifications for the platform have been created
push_platform_deleted	Push notifications for the platform have been deleted
push_platform_updated	Configuration of push notifications for the platform has been deleted
registration_instruction_updated	New user registration instruction has been updated
server_avatar_updated	Server avatar has been updated
sms_filter_max_requests_settings_changed	SMS security settings have been changed (“Maximum number of requests per phone number”)
sms_filter_phone_settings_changed	SMS security settings have been changed (“Filter by phone number”)
sms_ip_rate_limit_settings_changed	SMS security settings have been changed (“Maximum number of requests per IP address)
sms_filter_user_agent_settings_changed	SMS security settings have been changed (“Filter by User-Agent”)
sms_filter_def_settings_changed	SMS security settings have been changed (“Filter by DEF code”)
sms_settings_changed	SMS settings have been changed

Event	Description
sticker_pack_created	Sticker pack has been created
sticker_pack_deleted	Sticker pack has been deleted
sticker_pack_saved	Information about sticker pack has been saved
sticker_pack_updated	Sticker pack has been updated
sticker_saved	Sticker has been saved
suggest_created	CTS suggest for simplified connection has been created
suggest_deleted	CTS suggest for simplified connection has been deleted
suggest_updated	CTS suggest for simplified connection has been updated
support_info_updated	technical support contacts have been changed
trusts_certificate_deleted	Trust TLS-certificate has been deleted
trusts_certificate_updated	Trust TLS-certificate has been updated
trusts_server_created	Trust connection to another server has been created
trusts_server_deleted	Trust connection to another server has been deleted
trusts_settings_changed	Trust settings changed
user_connected	User has logged in to the application (with an indication of the platform)
user_disconnected	User has logged out of the application (with an indication of the platform)
user_unblocked	User has been unblocked (by IP or phone after exceeding the number of login attempts)
<имя провайдера>_sms_settings_changed	Settings of a specific SMS provider have been changed
account_deleted	Account has been deleted
activations_platform_lifetimes_settings_updated	Activation lifetime settings for platforms have been updated
admin_added	An administrator has been added using the CLI method
admin_authentication_updated	System administrator authorization settings have been updated
admin_block_canceled	Administrator account lockout has been canceled
admin_block_date_set	Administrator account lockout date has been set
admin_blocked	Administrator account has been locked out
admin_created	An administrator account has been created
admin_deferred_block_canceled	Delayed administrator account lockout has been canceled
admin_deferred_block_set	Delayed administrator account lockout has been configured

To search for events in the table, fields at the top of the window are used (see Figure 60.):

- search by user — search is performed by user name in the system;
- in the drop-down lists, you can select the administrator name, event type, and platform;
- search by events — full-text search for events is performed in program code.

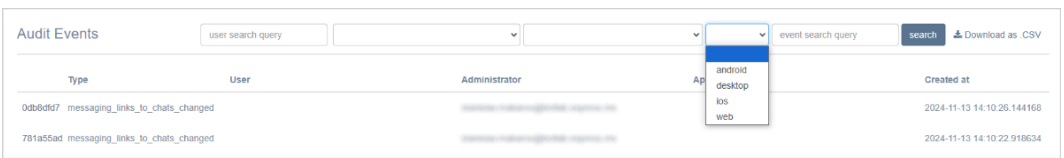

Figure 60.

To download the data displayed on the screen as a single data file, click Download as .CSV.

Note. If the file content is not displayed correctly, check the encoding and change it to UTF-8, if necessary.

APPLICATION PERFORMANCE STATISTICS

eXpress CS collects statistical information about the number of users, chats, messages and group calls per unit of time and presents it in a visual form — a widget.

The "Statistics" section contains a set of widgets in the form of graphs and pie charts (see Figure 61.).

Widget parameters are set by default, the administrator cannot add a new widget or edit an existing one.

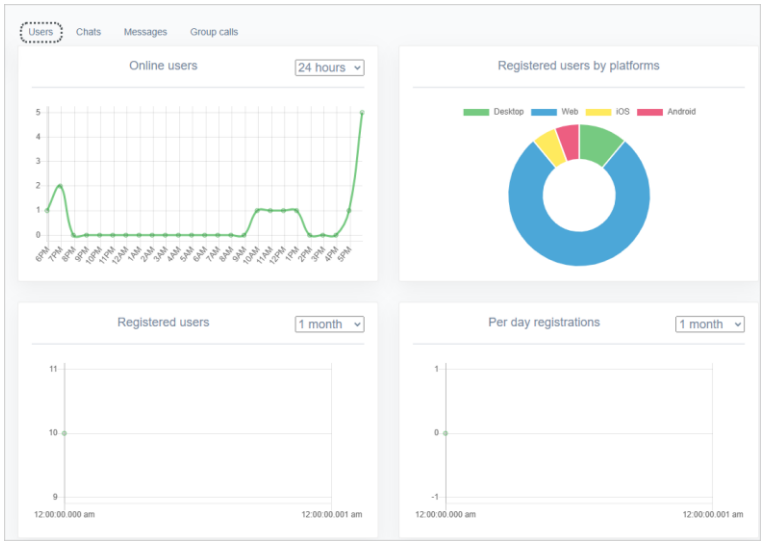

Figure 61.

The following functionality is available to the administrator:

- selecting the information viewing interval ;
- viewing information about the users;
- export of data on the number of users registered on the CTS server;;
- viewing information about the chats;
- viewing information about the messages;
- viewing information about group calls.

To set the interval for which you want to display statistical information, select a value from the drop-down list in the upper right corner of the widget (see Figure 61.).

To set an interval different from the predefined values, select "Other", click in the field to the left of the drop-down list and set the start and end of the period using the calendar that opens (see Figure 62.).

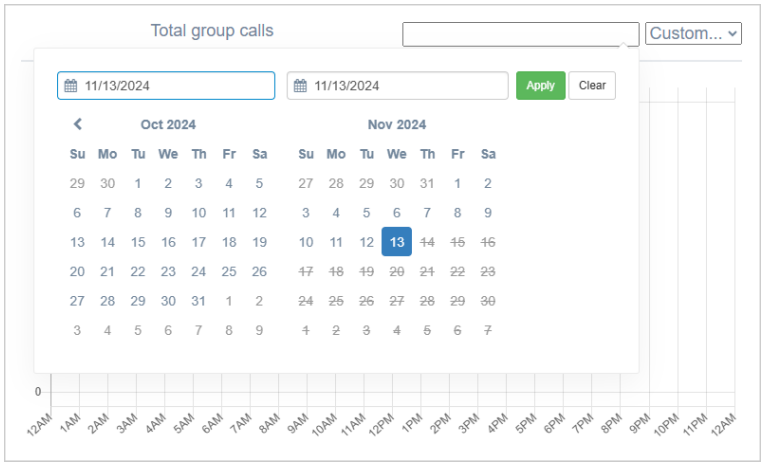

Figure 62.

Hovering over a point on the graph will display statistics for a specific day.

To view statistical information about users, open the "Users" tab.

The following widgets will be available in the window that opens:

- number of online users;
- number of registered users;
- registrations by platforms;
- number of registrations per day.

To download data on the number of users registered on the CTS server, in the "Number of users on CTS" block, select the required time interval and click

.

To view statistical information about newly created chats, open the "Chats" tab (see Figure 63.).

Figure 63.

The window that opens will display statistics on chat creation for the selected period:

- total number of created chats;
- number of chats created per day.

To view statistical information about sent messages, open the “Messages” tab (see Figure 64.).

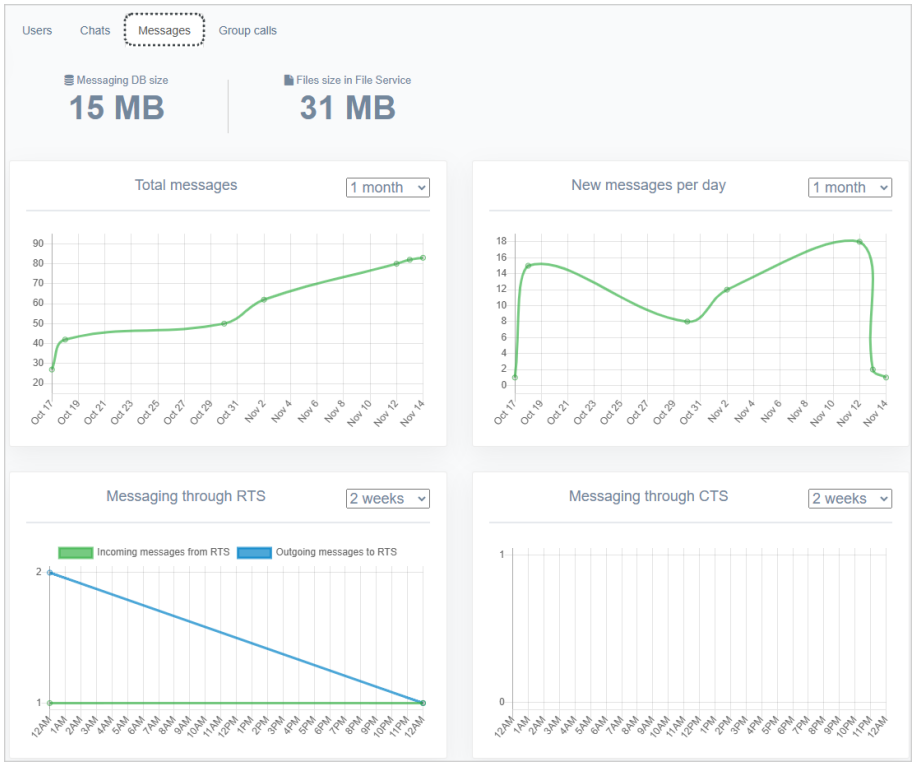

Figure 64.

The following widgets will be available in the window that opens:

- total volume of messages stored in the database;
- total volume of files stored in the database;
- total number of messages for a given period;
- total number of new messages for a given period;
- number of messages sent from the corporate server (CTS);
- number of messages sent from the regional server (RTS).

To view statistical information about group calls, open the “Group Calls” tab (see Figure 65.).

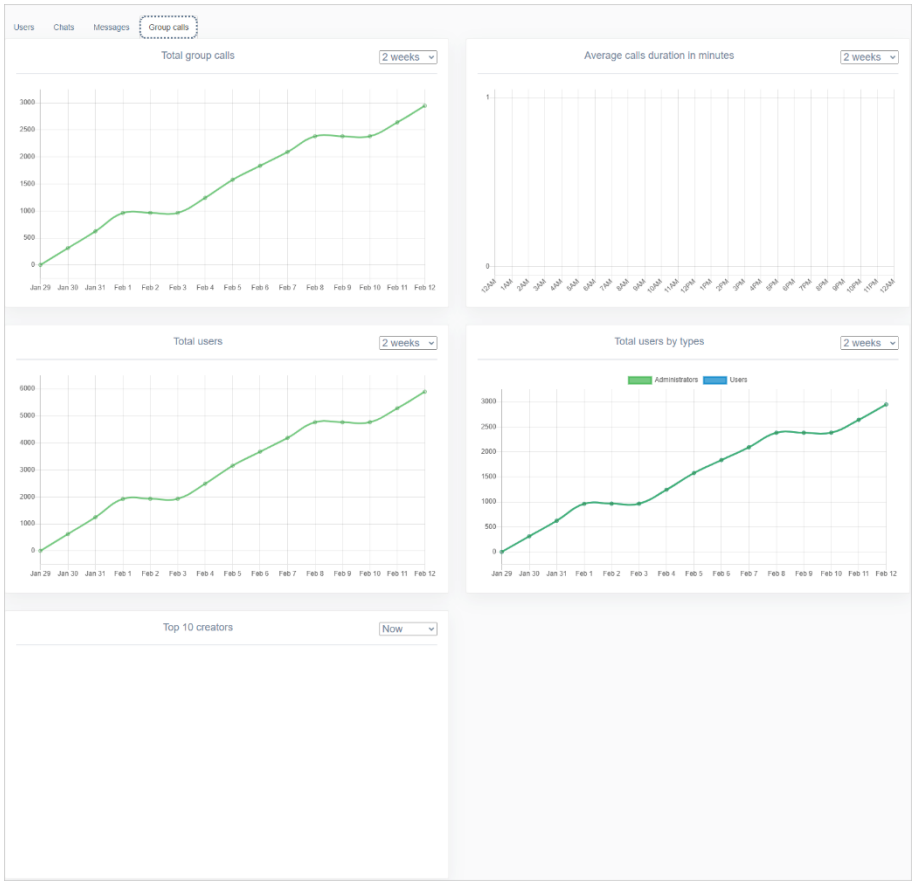

Figure 65.

The following widgets will be available in the window that opens:

- number of group calls for a given period;
- average duration of group calls in minutes;
- number of participants in group calls by type;
- top 10 users who created group calls.

MANAGING STICKERS

The "Stickers" section is a table with information about sticker catalogs (see Figure 66.).

Figure 66.

The sticker catalog table contains the following data (see Table 23):

Table 23

Column name	Information
ID	Sticker catalog identifier. Assigned automatically

Column name	Information
Name	Sticker catalog name
Q-ty	Number of stickers contained in the catalog
Public	Possible values: • false — the catalog is available only to users of the current server; • true — the catalog is available to all users
Creation date	Sticker catalog creation date
Update date	Date of last change in the sticker catalog

The following functionality is available to the administrator:

- creating a sticker catalog;
- creating a sticker catalog preview;
- viewing a sticker catalog;
- sorting stickers;
- deleting stickers;
- deleting a sticker catalog.

To create a sticker catalog:

1. Click “Create ” in the upper right corner.

   The “Create Sticker Pack” window will open (see Figure 67.).
2. In the “Name” field, enter the name of the catalog.

Figure 67.

3. Click “Create”.

   A window for uploading stickers will open (see Figure 68.).

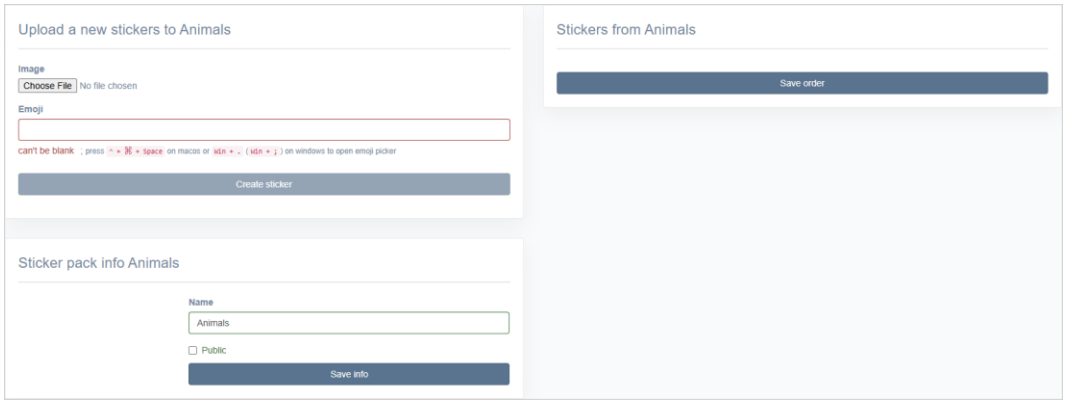

Figure 68.

4. In the “Upload New Sticker” area, click “Select File” and select an image from your file system.

Note. The image file must meet the following requirements:

- format: PNG;

- file size not more than 512 Kb;
- the image shall fit into a 512x512 pixel square.

5. In the “Emoji” field, insert an emoji using one of the following methods:
   - follow the instructions below the “Emoji” field;
   - copy the corresponding image on the website https://emojipedia.org/.
6. Click “Create Sticker”.

   The sticker will be displayed on the right side of the window (see Figure 69.).

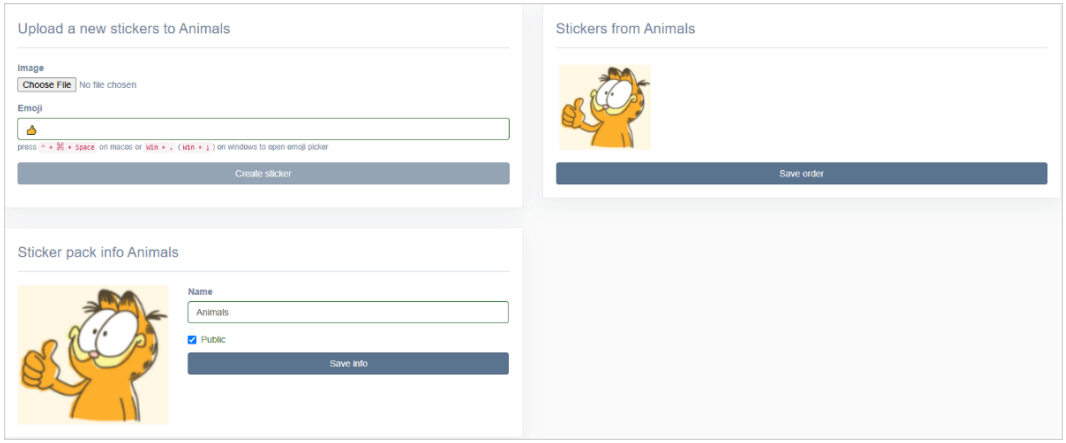

Figure 69.

7. Repeat steps 4-6 to upload all stickers in the catalog.
8. Check the “Public” field if the catalog you are creating should be accessible to all users.
9. Click “Save information”.

To create a catalog preview:

1. Hover the cursor over the uploaded sticker and click  (see Figure 70.).

Figure 70.

2. Confirm the action in the modal window that opens.

   The selected sticker will be displayed in the lower left part of the window. The message “Sticker pack preview has been set” will be displayed at the top of the window (see Figure 71.).

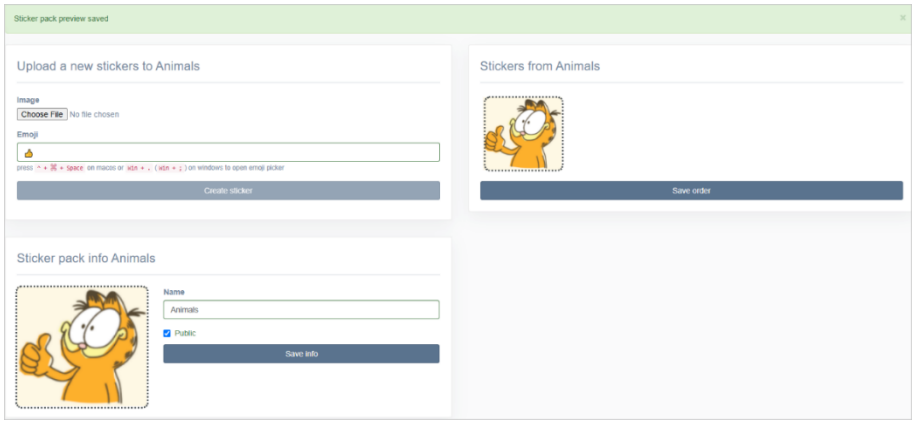

Figure 71.

3. Click “Save information”.

   The message “Sticker pack has been set” will be displayed at the top of the window.

To view the sticker catalog, click on its name. A window will open (see Figure 72.):

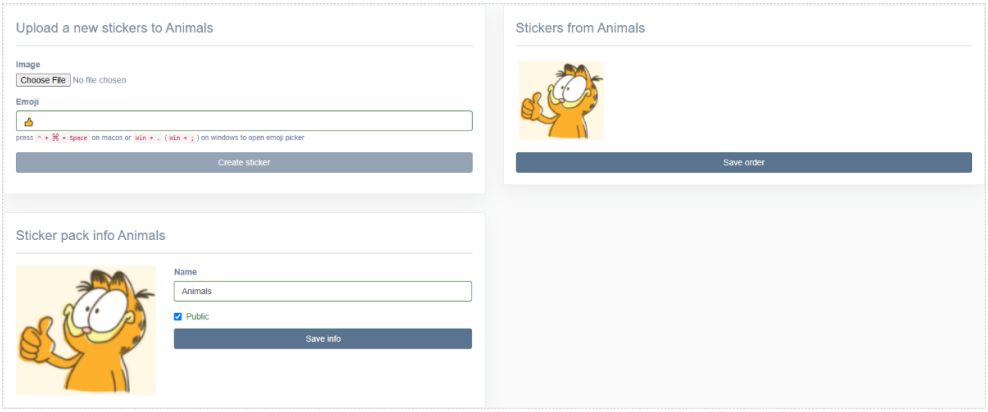

Figure 72.

To sort stickers:

1. Open the required catalog by selecting it from the list.
2. In the window that opens (see Figure 72.), move the desired stickers using the mouse.
3. Click “Save Sorting”.

To delete a sticker from the catalog:

1. Open the required catalog by selecting it from the list.
2. In the window that opens (see Figure 72.), select a sticker to be deleted.
3. Hover the cursor over the sticker and click (see Figure 70.).
4. Confirm the action.

To delete a sticker catalog:

1. Select the desired catalog from the list and click to the right of the catalog (see Figure 66.).
2. Confirm the action.

Chapter 3

TROUBLESHOOTING TYPICAL ERRORS

Note. All operations on the servers shall be carried out on behalf of the superuser.

To obtain superuser rights, run the following commands:

```
sudo -s
```

eXpress CS is built on a microserver architecture using containerization based on Docker software. In eXpress CS, all maintenance operations and troubleshooting operations are performed with Docker containers.

In case of problems in the operation of eXpress CS, first of all it is necessary to check the operation status of the containers.

To check the status of containers ("Up" or "Exited"), run the following command:

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

The normal status of containers is "UP".

If a container has the "Exited" status, start it with the following command:

```
docker start <container name, for example "cts_containername_1">
```

If the problem has not been resolved, collect system logs.

To collect logs, run the following command:

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

Send the collected logs to the administrators responsible for eXpress CS.

If the user cannot log into the server, collect logs with the following command:

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

To restart all containers, run the following command:

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

If users have a problem with the order in which messages are displayed in conversations, check the time on the server with the following command:

```
date
```

If the time is incorrect, check the status of the chronyd time service. **To check the status of the time service**, run the following command:

```
systemctl status chronyd
```

If the status "active" has the value of "inactive", start the service with the following command:

```
systemctl start chronyd
```

Chapter 4

ELIMINATING VULNERABILITIES

To eliminate the log4j (CVE-2021-44228), CVE-2021-45046 vulnerability:

Note. If the version is less than 2.16, but not 1.x, then an update to the latest version is required. In versions 1.x, this vulnerability is not present.

1. Check the Log4j version using the following command:

   ```
   find / -name 'log4j*.jar'
   ```

   or find it via the CLASSPATH output of your java installation:

   ```
   echo $CLASSPATH
   ```

2. In the Java Virtual Machine (JVM) settings for Log4j packages version 2.0 to 2.15, add the following flag for the application:

   - Dlog4j2.formatMsgNoLookups=true;

   Attention! Install the latest Log4j 2.16.0 service pack, which fixes the service pack that was made for CVE-2021-45046 Log4j 2.15.0. Installing the latest package is no different from the previous installation and is not required unless you are using the additional APM program with logging set to "tracing" mode.

   Otherwise, it is highly recommended to upgrade your current Elasticsearch version to 7.16.1 (or 6.8.21) and perform a sequential restart of your nodes.

   - for elasticsearch — /etc/elasticsearch/jvm.options;
   - for logstash — /etc/logstash/jvm.options.

   Note. The path may differ and depends on the installation method.

3. Restart the app using the following command:

   ```
   systemctl restart elasticsearch
   ```

4. Check that the jvm setting is active:

   ```
   ps axw | grep formatMsgNoLookups
   ```

   The flag should be visible in the app launcher.

Example of Log4j update for Elasticsearch:

```
wget https://dlcdn.apache.org/logging/log4j/2.16.0/apache-
log4j2.16.0-bin.tar.gz
tar zxvf apache-log4j-2.16.0-bin.tar.gz
cd apache-log4j-2.16.0-bin/
ls /usr/share/elasticsearch/lib/log4*
cp log4j-api-2.16.0.jar /usr/share/elasticsearch/lib/
cp log4j-core-2.16.0.jar /usr/share/elasticsearch/lib/
rm -f /usr/share/elasticsearch/lib/log4j-api-2.11.1.jar
rm -f /usr/share/elasticsearch/lib/log4j-core-2.11.1.jar
```

For Logstash versions earlier than 6.8.21 and 7.16.0 run the following commands:

```
zip -q -d <LOGSTASH_HOME>/logstash-core/**/*/log4j-core-2.*
org/apache/logging/log4j/core/lookup/JndiLookup.class
```

or

```
wget https://dlcdn.apache.org/logging/log4j/2.16.0/apache-log4j-
2.16.0-bin.tar.gz
tar zxvf apache-log4j-2.16.0-bin.tar.gz
cd apache-log4j-2.16.0-bin/
ls /usr/share/logstash/lib/log4*
cp log4j-api-2.16.0.jar /usr/share/logstash/lib/
cp log4j-core-2.16.0.jar /usr/share/logstash/lib/
rm -f /usr/share/logstash/lib/log4j-api-2.11.1.jar
rm -f /usr/share/logstash/lib/log4j-core-2.11.1.jar
```

CHANGE HISTORY

The "Change History" section contains a list of changes in the document related to changes/modifications of eXpress CS.

Build 1.47

No.	Section	Change	Reference
1.	Administrators	The ability for an administrator to be a member of multiple groups has been added	page 15
2.	Administrators	Granting administrator rights based on group membership in AD. If the administrators of the group being created or edited are members of the specified group in Active Directory, they will receive the rights of the corresponding AD group.	page 15
3.	Server	The setting for administrator name visibility has been added	page 22
4.	Server	Administrator data setup capability has been added	page 22
5.	SMS	Added settings for integration with SMS service providers	page 30

Build 2.5

No.	Section	Change	Reference
1.	Description of the Administrator Console Interface	Description of menu items and operations available in the administrator console have been supplemented	page 13
2.	Setting Up Administrator Rights	Illustrations have been updated, description of administrator rights has been supplemented	page 52
3.	Server Management	Illustrations have been updated, and a description of the data for integrators has been added	page 15
4.	Managing Stickers	Illustrations have been updated, description of operations has been supplemented	page 66
5.	Setting Up Event Information Transmission	Illustrations have been updated, information on working with SIEM has been added	page 58
6.	Setting Up SMS Service	Updated illustrations, added description of security settings	page 30
7.	Setting Up Push Notifications	Added mechanism for connecting notifications depending on the platform and creating a connection on HMS Android	page 36

Build 2.5.7

No.	Section	Change	Reference
1.	Creating an account	Requirements for user avatars were added	page 24
2.	Server Settings	Information has been updated	

Build 2.6.0

No.	Section	Change	Reference
1.	Audit of administrator and user actions	New audit events have been added	page 60
2.	Setting Up SMS Service	Information has been updated	page 30

Build 2.7.0

No.	Section	Change	Reference
1.	Setting Up Administrator Rights	Updated	page 52

Build 2.9.0

No.	Section	Change	Reference
1.	Setting Up Connections to the Enterprise Server	Updated	page 16

Build 2.10.0

No.	Section	Change	Reference
1.	SMS captcha	The section has been added	page 34

Build 2.12.0

No.	Section	Change	Reference
1.	Audit of administrator and user actions	Events have been added to the table	page 60
2.	Unblocking a User Account	Added	page 35

Build 3.1.0

No.	Section	Change	Reference
1.	Setting Up Integration with Provider	Updated	page 31

Build 3.7

No.	Section	Change	Reference
1.	Global Chat	The Global Chat section has been added	page 42
2.	Internal Bots	Description of Notifications Bot, Recordings bot has been added	page 53

No.	Section	Change	Reference
3.	Setting Up Push Notifications	A description of connection to Android RuStore has been added	page 36

Build 3.9

No.	Section	Change	Reference
1.	UI Alerts	Added description of parameters when creating UI Alert	page 36

Build 3.14

No.	Section	Change	Reference
1.	Throughout the document	The description of integration with Vinteo and Mind has been removed	

Build 3.16

No.	Section	Change	Reference
1.	Introduction	Updated due to the separation of the Administrator's Guide into volumes	page 5
2.	Main Components	Added links to volumes on operating the ETS and RTS servers	page 7
3.	Main Functions	Added a note about the need to match the versions of the server and client parts of the application for the correct operation of the system	page 7
4.	File Service	The section has been updated, a description of proxying when delivering statics has been added	page 55
5.	Managing User Accounts	A section has been created that combines information about user accounts and operations with them	page 15
6.	Authentication and Authorization	A section has been created that brings together information about user authentication and authorization methods.	page 28
7.	Managing administrator user accounts	This section has been updated	page 15
8.	Setting Up the SMS Provider Mask	Subsection added	page 31

Build 3.19

No.	Section	Change	Reference
1.	Operations with a Specific User Account	The description of the “Activations” operation has been updated	page 26
2.	Setting Up Event Information Transmission	Configuration description has been updated	page 58
3.	Setting Up Push Notifications	Google FCM address has been added to the note about the necessity of access to APN Push services	page 36

Build 3.21

No.	Section	Change	Reference
1.	Throughout the document	The section describing VoEx has been removed, all information related to it has been removed	
2.	Setting Up Push Notifications	The figure and Table 10 have been updated in the procedure for setting up push notifications for Android	page 36
3.	SETTING UP SIMPLIFIED AUTHORIZATION	Matching type and Table 7 have been updated	page 29

Build 3.22

No.	Section	Change	Reference
1.	Main Components	Due to changes in the system architecture, the Media server is used instead of the VoEx server to provide video and voice communications	page 7

Build 3.23

No.	Section	Change	Reference
1.	SETTING UP SIMPLIFIED AUTHORIZATION	Added a note about the specifics of user login to the application	page 29

Build 3.26

No.	Section	Change	Reference
1.	Throughout the document	The document structure has been optimized	Throughout the document

Build 3.27

No.	Section	Change	Reference
1.	Throughout the document	The document structure has been optimized	Throughout the document
2.	Throughout the document	The figure have been updated	Throughout the document
3.	Description of the Administrator Console Interface	The section has been updated	page 13
4.	Support Contacts Management	The section has been added	page 23
5.	Registration Instructions	The section has been added	page 28
6.	Connecting SMTP Server	The note has been added	page 24
7.	Unblocking a User Account	The note has been added	page 35
8.	Setting Up Push Notifications	The section has been updated	page 36
9.	Setting Up Administrator Access Rights	The section has been updated	page 46
10.	Managing Bots	The section has been added	page 53
11.	Global Bots	Subsection added	page 55

Build 3.28

No.	Section	Change	Reference
1.	Main Components	The section has been updated	page 7
2.	Server Management	Added description of the section "Connecting SMTP Server"	page 15
3.	Setting Up Push Notifications	The images illustrating third-party software have been removed	page 36

Build 3.34

No.	Section	Change	Reference
1.	Setting Up Administrator Access Rights	Figure and table updated	page 46

Build 3.35

No.	Section	Change	Reference
1.	Audit of administrator and user actions	Table of events updated	page 60

Build 3.36

No.	Section	Change	Reference
1.	Description of Administrator Web Interface	Information about profile edit button added	page 13
2.	Operations with a Specific User Account	Figure updated, information about the "Device hostname" field added	page 26
3.	EDITING ADMINISTRATOR ACCOUNTS;	2 editing method added	page 49
4.	Audit of administrator and user actions	Table of events updated	page 60