UNLIMITED PRODUCTION

eXpress

Communication System

Administrator’s Guide

Volume 2. Operation of the CTS Server

Build 3.36
03/17/2025

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 a corporate 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 applications and server applications
JSON	JavaScript-based text-based data interchange format
KeyCloak	User directory service. An open source identity and access management solution for use in information systems
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
SmartApp	SmartApp is a web application, which is implemented as an add-on, executed inside Express, and designed for accessing corporate services and systems
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.
VoEx	Voice Over Express — part of Express CS, which includes call management, call recording, SIP telephony, and integration with other types of telephony
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.

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

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 registration of users;
- 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 (internal company contour) is used for:

- registration of 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:

- registration of 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. The CTS server users, which are connected to the ETS server, receive SMS messages and push notifications from this ETS server (for more details, see the document "Administrator's Guide. Volume 3. Operation of the ETS Server").

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.

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.

For integration of the ATE system, the SIP-telephony module is used, which allows making and receiving voice calls, maintaining the phone book and matching users with ATE numbers ("Caller ID").

Voice Over Express (VoEx) — part of Express CS, which includes call management, call recording, SIP telephony, and integration with other types of telephony.

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 of Express CS, the following roles are identified during installation (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
Security Manager	• viewing messages in the DLPS web interface; • viewing logs in the DLPS web interface;	Internal User

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.

Within the framework of the role model for individual user groups, the administrator can set restrictions for users with regard to operations with attachments and the use of the PIN code:

- prohibition of sending/forwarding attachments to chats;
- prohibition of downloading/viewing attachments in chats;
- prohibition of downloading attachments from CTS users;
- prohibition of the ability to forward/share/save attachments to the device's memory;
- mandatory use of the PIN code when the user enters the application.

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.

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.

REGISTRATION SYSTEMS

The following methods are available to the administrator to configure user registration/authorization in the system:

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

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 a registration/authorization method, Express CS uses the integration of the CTS server 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

CORPORATE SERVER OPERATION

This chapter describes the main sections and procedures for working in the CTS server 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://cts_host/admin).

   An authorization window will open (see Figure 1):

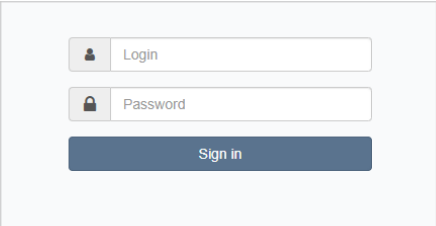
   

   Figure 1

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

   The main window of the administrator web interface will open — “Chats” (see Figure 2).

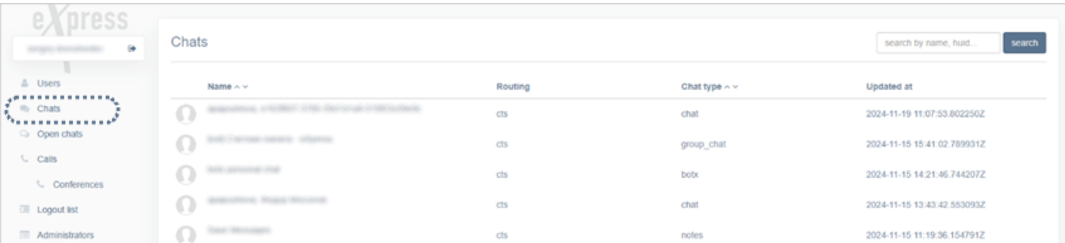
   

   Figure 2

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).

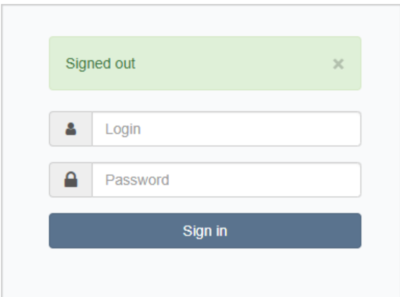


Figure 3

DESCRIPTION OF ADMINISTRATOR WEB INTERFACE

This subsection describes the appearance of the administrator web interface using the example of the appearance of the "Users" section (see Figure 4).

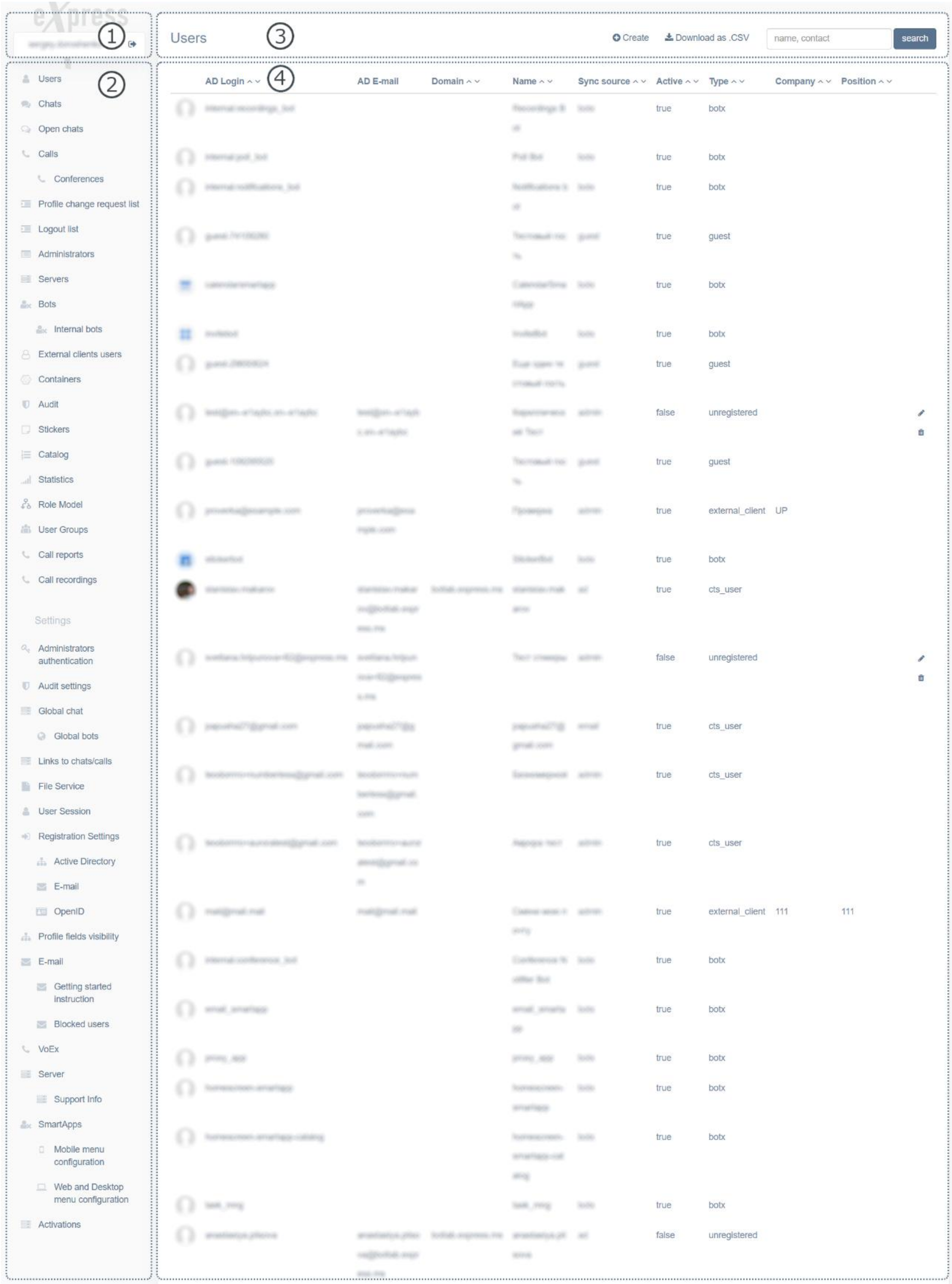


Figure 4

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 web interface, 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 ⌄ 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 below in Table 2.

Table 2

Document section	Menu item	Purpose	Description in the document
Server Management	Servers	Viewing and setting up connections to other servers	page 17
	Server	Setting up the appearance of the application. Setting up the TLS and Botx SSL certificates. Viewing the identifiers of the current CTS server and the RTS server it is connected to. Viewing versions of installed services	page 25
	VoEX	Setting up Media server. Setting up IP telephony	page 31
	E-mail	Setting up the SMTP server and e-mail from which e-mails are sent from the server to recipients	page 35
Contacts Management	Setting Up Registration	Setting up user account connections	These sections are described in the document "Administrator's Guide. Installation”.
	Active Directory	Setting up account registration via Active Directory	
	E-mail	Setting up an e-mail mask for account registration	
	OpenID	Setting up account registration via OpenID	
	Users	Viewing account information; Exporting data to a file	page 37
		Creating an account	page 38
		Setting up an Account	page 41
	Visibility of Profile Fields	Setting up data access levels in a corporate server user profile	page 46
	Activations	Setting up user session activity time	page 48
	Instructions to Get Started	Setting up sending and text of the instruction to start working with the application	page 48
	Locked Out Users	Setting up sending options and text of account lockout e-mail notifications	page 50
	Logout Requests	Viewing the list of requests to log out from the corporate server. Accepting and rejecting requests	page 51
	List of Change Requests	Viewing the list of requests to change user profile data. Accepting and rejecting requests	page 53
	Support Contacts	Setting up support contacts	page 54
	Users of external clients	Section under development	

Document section	Menu item	Purpose	Description in the document
Role Model and User Groups	Role Model	Creating restrictions for users on operations with attachments and using a PIN code when entering the application	page 54
	User Groups	Creating user groups for use in the role model	page 54
Managing Administrator Accounts	Administrators	Viewing information about administrators and administrator groups	page 54
		Setting up administrator accounts	page 65
		Creating, deleting, setting Up administrator groups	page 66
	Authentication of Administrators	Setting up administrator connections from Active Directory	page 64
Calls and Conferences	Calls	Viewing information about group calls. Terminating unfinished group calls	page 72
	Conferences	Viewing information about the conferences. Terminating unfinished group calls and conferences	page 72
	Call Quality Ratings	Viewing user ratings of call or conference quality	page 77
	Call Recording	Viewing the processing queue of call and conference records	page 80
	Links to Chats and Calls	Setting up personalized links to join a closed chat, channel, video conference, or call	page 83
Managing Chats	Catalog	Managing the display of the chat directory "showcase": sorting the list of open corporate chats, channels and chatbots	page 86
	Chats	Viewing information about chats and chat events:	page 86
	Open Chats	• viewing information about the chats; • creating and deleting open chats; • changing chats from open to closed	page 92
	Global Chat	• enabling and disabling global chat; • setting up global chat settings	page 94
Chatbots and SmartApp	Bots	Chatbot management: viewing information, setting up, deleting, establishing connections:	page 95
	Internal Bots	• changing and setting up internal bots; • adding administrator for bots	page 99
	Global Bots	• adding global bots to the global chat; • removing global bots from global chat	page 99
	SmartApps	• management of the display of the SmartApp item in the main menu of eXpress CS; • setting up display parameters in the main menu of the SmartApp items "Home" and "Services"	page 102
	Mobile Clients Menu	Setting up the SmartApp menu configuration for mobile clients	page 105
	Setting up Web and Desktop clients menus	Setting up the SmartApp menu configuration for web and desktop apps	page 107
Managing File Service	File Service	Setting up access paths to files transmitted in chats	page 108
		Setting up storage and deletion periods for files	page 109
Logs	Containers	View Docker containers list and logs	page 111
	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 112
	Audit	Audit of administrator and user actions	page 114

Document section	Menu item	Purpose	Description in the document
Application Performance Statistics	Statistics	Viewing application performance statistics	page 118
Managing Stickers	Stickers	Viewing sticker packs and their elements. Adding and removing sticker packs and their elements. Customizing sticker packs	page 121

SERVER MANAGEMENT

This section describes the following administrator web interface menu items:

- Servers;
- Server;
- VoEx.

The "Servers" section contains information about connecting the CTS server to other servers. The administrator can view the interactive graphical connection routing diagram, as well as configure connection to the CTS:

- to transport servers (TTS);
- to other corporate servers using trusts;
- to RTS/ETS servers.

The "Server" section contains information about the CTS server and its operation settings.

In the VoEx section, the administrator can configure the operating parameters of Media server, SIP telephony and user rating of call or conference quality.

SERVERS

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

Figure 5

Connection between servers is achieved using trusts. A trust is a service for data transmission between the CTS, ETS and RTS and other services in their contour.

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.

The administrator can configure and establish trusts with other corporate servers, including those linked to different RTS/ETS servers. When trusts are established, information exchange between the CTS servers takes place directly, not through the ETS/RTS servers.

CONNECTING TO OTHER CORPORATE SERVERS

The following functionality is available to the administrator:

- Viewing information about a configured trust with another CTS server;
- creating a trust with another CTS server;
- editing a trust with another CTS server;
- deleting a trust with another CTS server.

To view information about a configured trust with another CTS server:

1. In the “Servers” section, go to the “Trusts” tab.

   A window will open (see Figure 6):

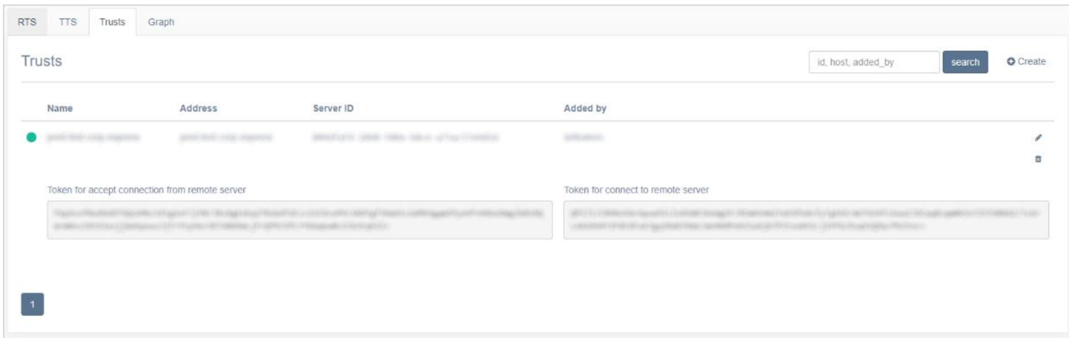


Figure 6

2. Click on the name of the CTS server with which the trust has been established.

   A window will open (see Figure 7):

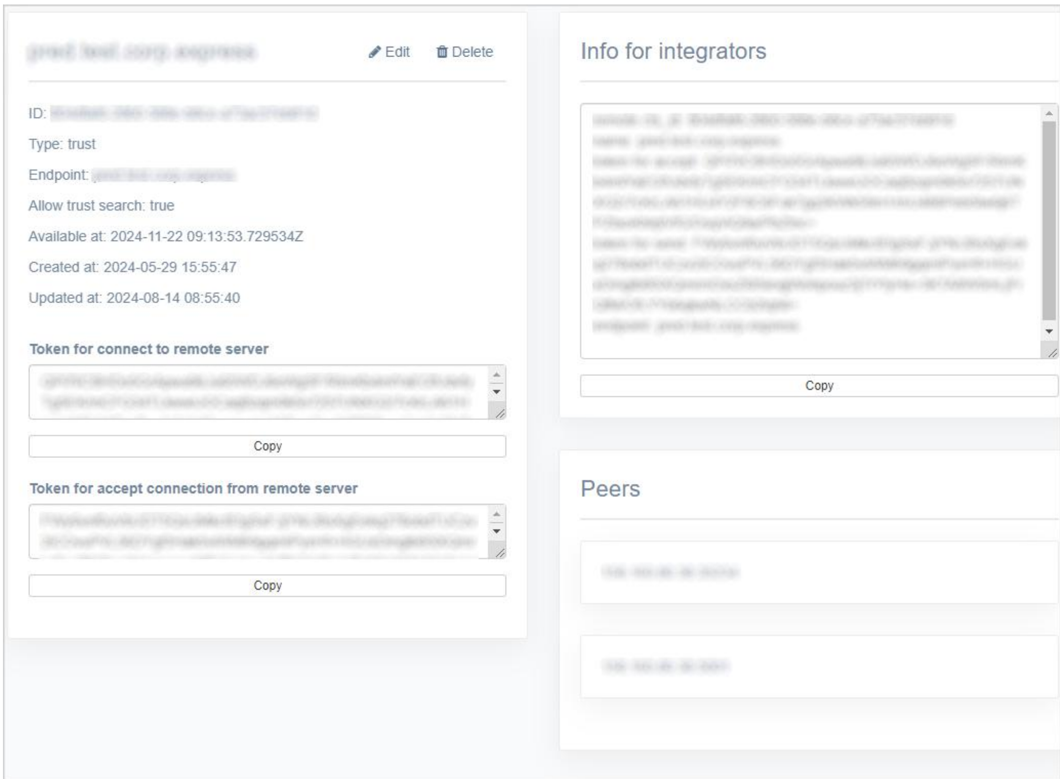


Figure 7

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

Table 3

Parameter	Description
ID	ID of the CTS server with which the connection has been established
View	Connection type
Endpoint	CTS server connection address
Allow trust search	Allows another server to access the corporate contact book of the server on which the trust is created. Possible values: • true — access granted; • false — access denied
Availability	Date and time of last connection
Creation date	Trust creation date
Update date	Date on which the trust was last modified
Token for connection to a remote server	Connection token
Token for connection from a remote server	Token for accepting connection
Information for integrators	Data for setting up trusts between servers

Trust creation date:

1. Click "Create" in the upper right corner.

   A window for creating a trust and setting its parameters will open (see Figure 8).

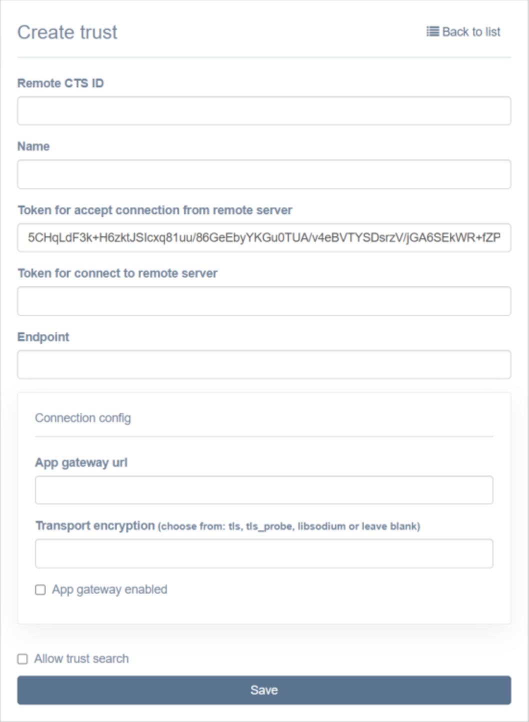


Figure 8

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

Table 4

Field	Description
CTS ID	ID of the CTS server with which the connection will be established. The CTS server ID is stored in the "Server" menu item in the administrator web interface of this server
Name	Short designation for the trust to be created
Token for accepting connection	Token name. **Example:** You need to create a trust between two servers: CTS1 and CTS2. To solve this issue, the administrator creates a trust on each of the servers, while specifying tokens in the settings in such a way that the token for conneciton on the CTS1 server matches the token for accepting connection on the CTS2 server, and vice versa
Connection token	Token name
Endpoint	Server connection address. In the table with the list of tokens, the data from this field is displayed in the "Address" column
Allow trust search	Allows another server to access the corporate contact book of the server on which the trust is created. Trust search is available if Corporate Search is enabled in the server settings

3. Click "Save".
4. Go to the administrator web interface of the corporate server (in the example given in the description "Token to accept the connection" — CTS2) with which the connection is established, and create a trust with the current server (CTS1).

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

To delete a trust, click .

CONNECTING TO TRANSPORT SERVERS

Transport servers (TTS — Transport Transfer Server) are 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). The system determines the optimal route for transmitting messages: via RTS or TTS. If RTS is not available, traffic is sent via TTS.

The following functionality is available to the administrator:

- Viewing information about connected transport servers;
- establishing connections to transport servers;
- editing connections to transport servers;
- deleting connections to transport servers.

To view information about connected transport servers:

1. In the "Servers" section, open the "TTS" tab

   Information about connections to transport servers will be displayed on the screen (see Figure 9).

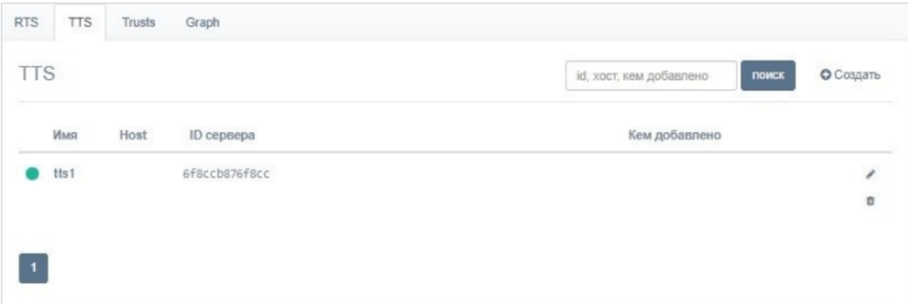


Figure 9

2. Click on the name of the transport server.

   A window will open (see Figure 10):

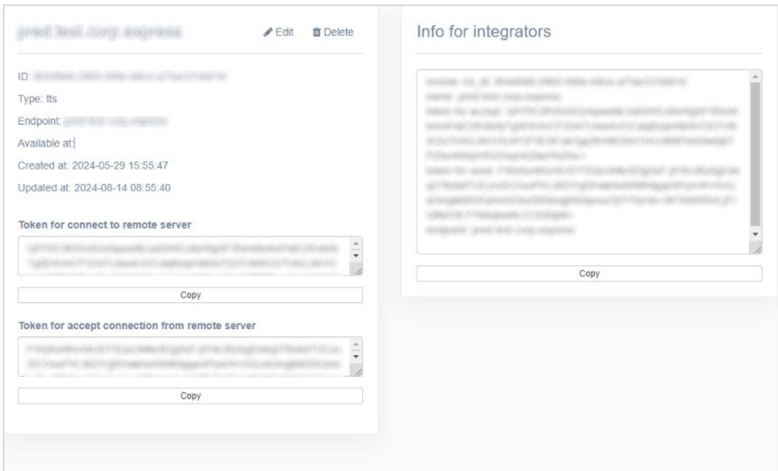


Figure 10

The window that opens contains the following information (see Table 5):

Table 5

Parameter	Description
ID	ID of the TTS server with which the connection has been established

Parameter	Description
View	Connection type
Endpoint	TTS server connection address
Availability	Date and time of last connection
Creation date	Connection creation date
Update date	Date on which the connection was last modified
Token for connection to a remote server	Connection token
Token for accepting a connection from a remote server	Token for accepting connection
Information for integrators	Data for setting up trusts between servers

To establish a connection to the transport server, click "Create" and fill in the form fields (see Figure 11, Table 6).

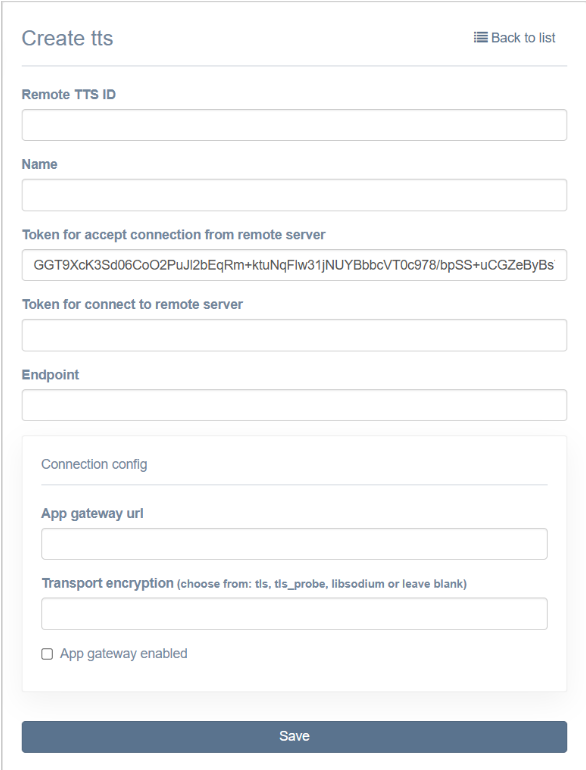


Figure 11

Table 6

Field	Description
TTS ID of the server to which the connection is established	ID of the TTS server with which the connection will be established
Name	Short designation for the transport server being created
Token for accepting a connection from a remote server	Token name. Generated automatically
Token for connection to a remote server	Token name
Endpoint	Server connection address

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

To delete a connection to the transport server, click .

CONNECTING TO REGIONAL AND ENTERPRISE SERVERS

The following functionality is available to the administrator:

- viewing information about connected RTS/ETS servers;
- reconnecting to RTS/ETS servers;
- editing connection to RTS/ETS servers;
- removing connection to RTS/ETS servers.

To view information about connection to RTS/ETS servers:

1. In the "Servers" section, open the "RTS"/"ETS" tab.

   The screen will display information about the RTS server (if this CTS server is connected to the RTS server — see Figure 5) or about the ETS server (if this CTS server is connected to the ETS server — see Figure 12).

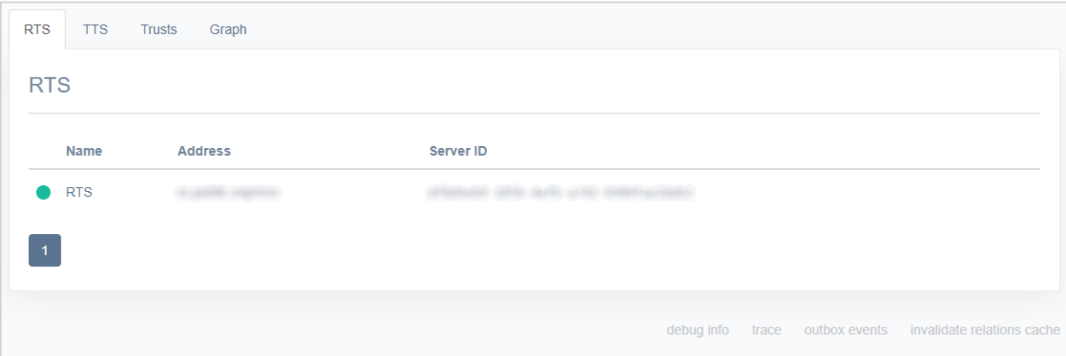


Figure 12

2. Click on the RTS/TTS server name.

   A window (Figure 13) will open with information about the server and a menu of available operations:

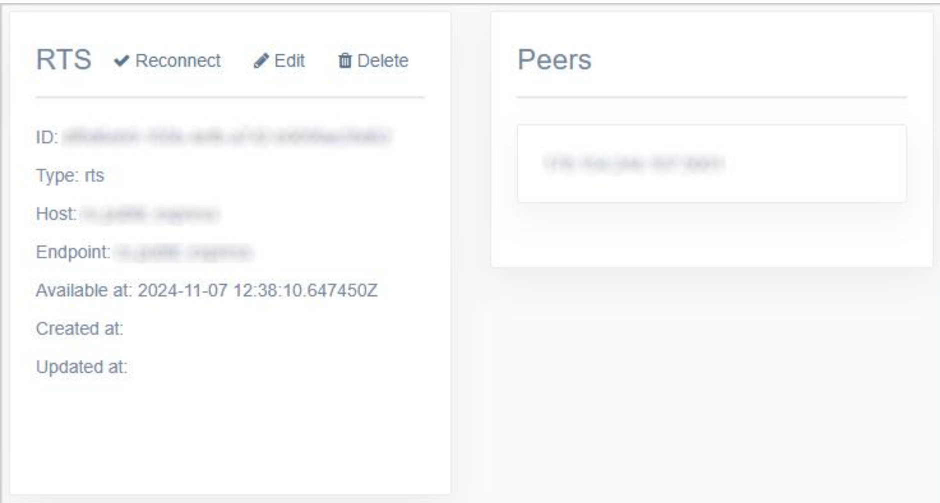


Figure 13

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

To reconnect to the RTS/ETS server, click on the "Reconnect" link and confirm the action by clicking "OK" in the modal box that opens.

To edit a connection to the RTS/ETS server, click and make changes in the window that opens.

To delete a connection to the RTS/ETS server, click 🗑 and confirm the action by clicking the "OK" button in the modal box that opens.

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 14):

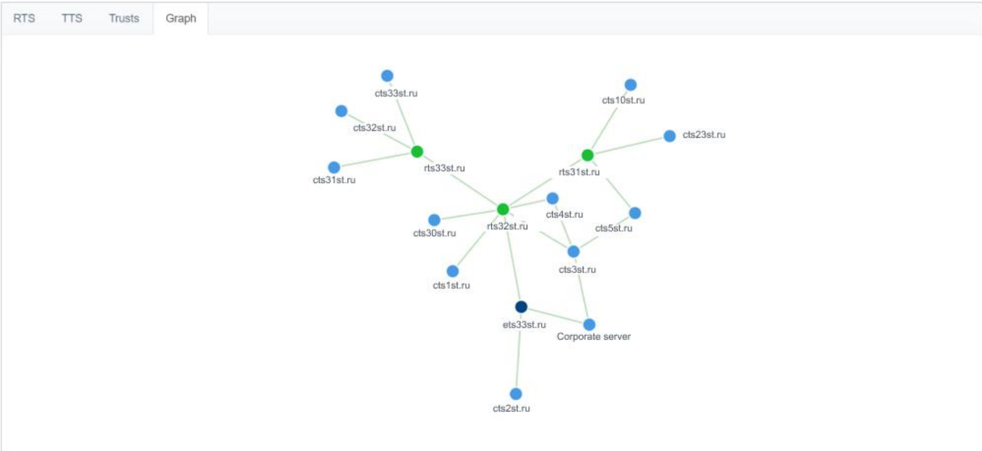


Figure 14

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 15).

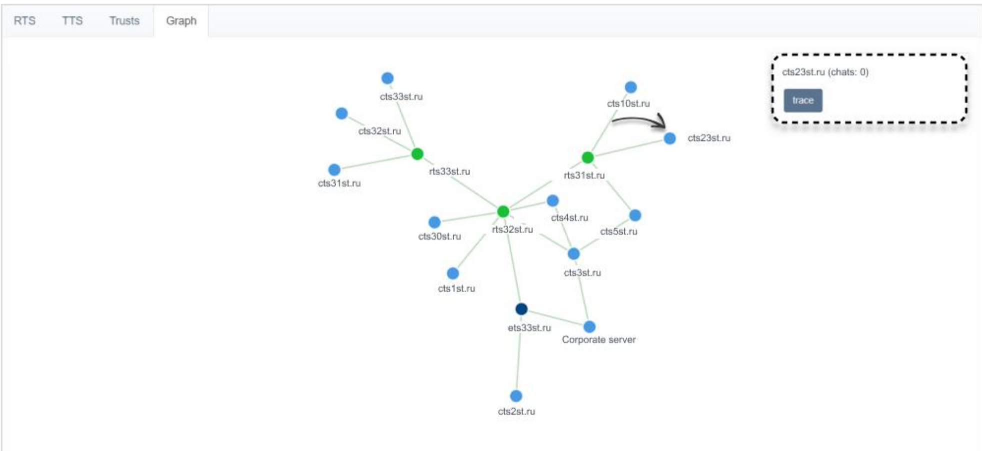


Figure 15

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

   A window will open with information about the RTS/ETS/TTS server through which data is exchanged with the current server (see Figure 16 and Figure 17).

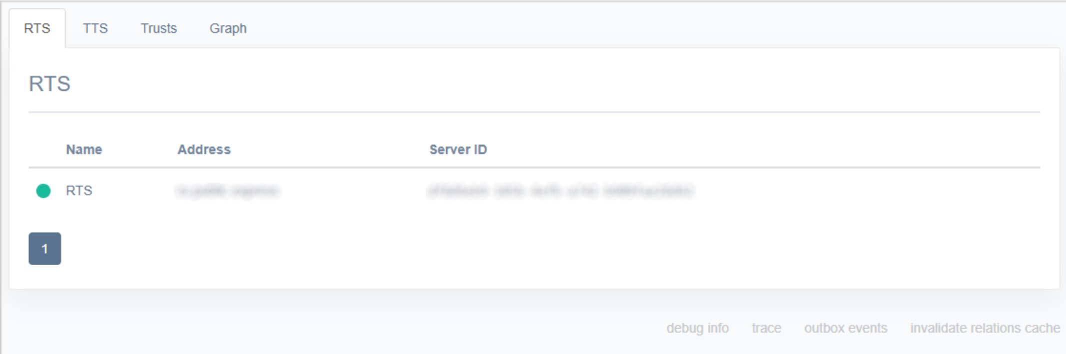


Figure 16

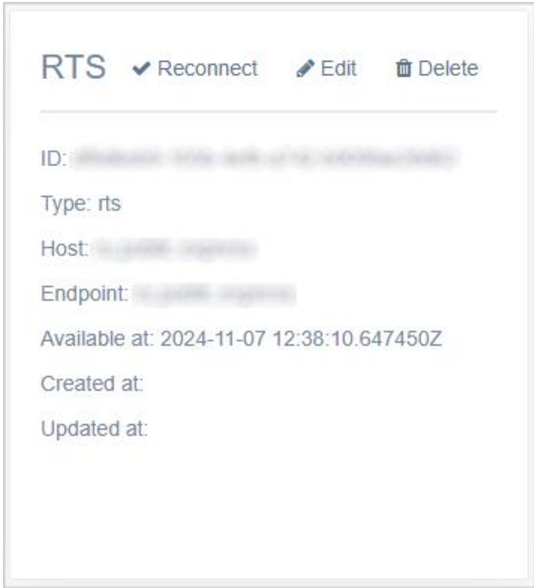


Figure 17

SERVER

The “Server” section consists of several sections that provide information about this CTS server (see

Figure 18), as well as the parameters for setting up its operation.

The following functionality is available to the administrator:

- setting up display of server information and loading of application backgrounds on user devices;
- setting up the display of the contact list and searching for contacts in the application;
- setting up end-to-end encryption in group chats and channels;
- setting up the user consent screen with the rules of information exchange;
- setting up user notification parameters about server maintenance;
- setting up user notification settings for application version updates;
- viewing information about CTS server identifiers;

- setting up parameters for using the TLS protocol in trust connections;
- setting up chatbot certificate application parameters;
- entering administrator contact information;
- setting up customer support contact settings;
- viewing the list of services installed on the CTS server and their versions.

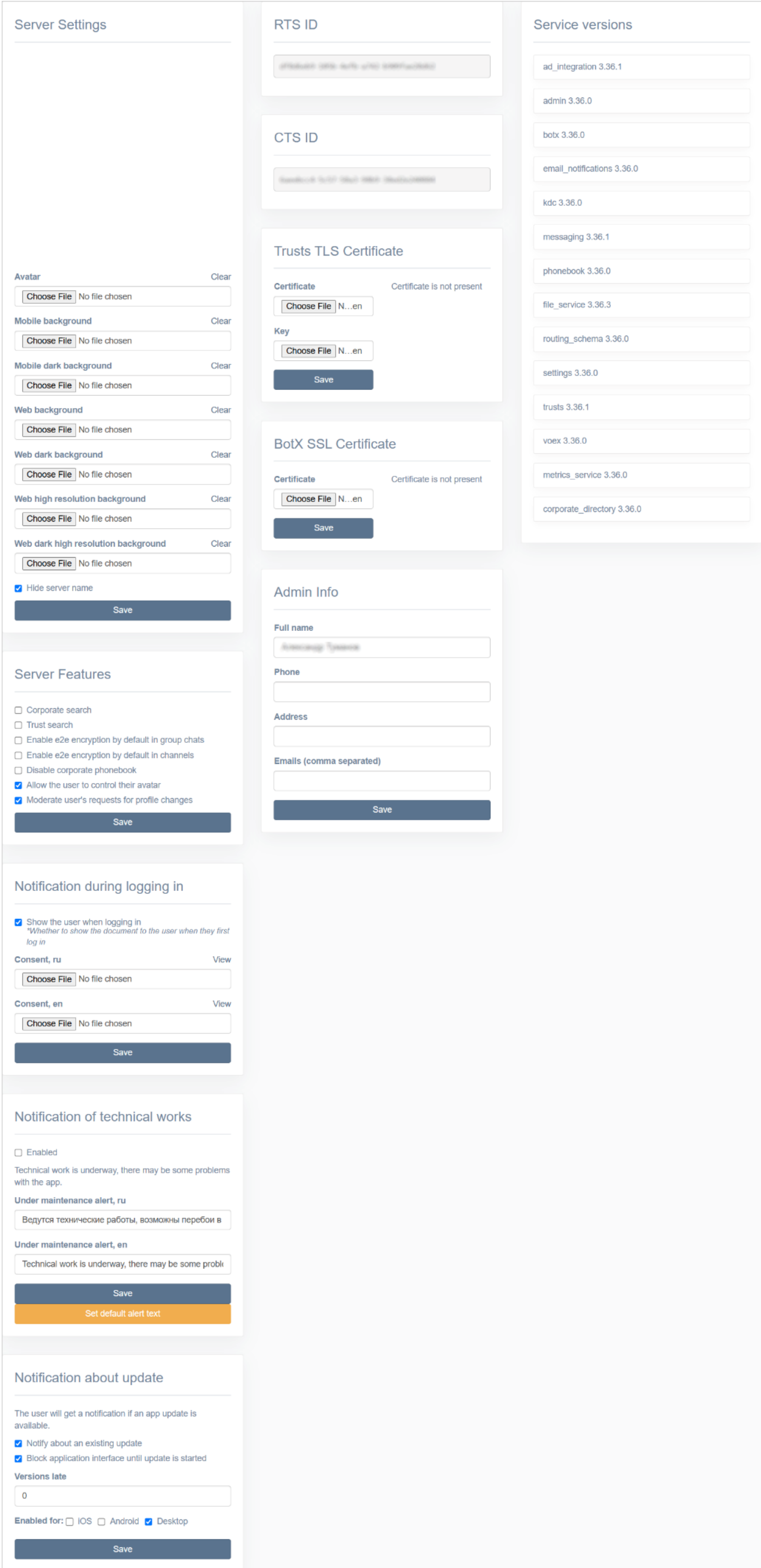

Server Settings
Avatar
Clear
Choose File No file chosen
Mobile background
Clear
Choose File No file chosen
Mobile dark background
Clear
Choose File No file chosen
Web background
Clear
Choose File No file chosen
Web dark background
Clear
Choose File No file chosen
Web high resolution background
Clear
Choose File No file chosen
Web dark high resolution background
Clear
Choose File No file chosen
Hide server name
Save
Server Features
Corporate search
Trust search
Enable e2e encryption by default in group chats
Enable e2e encryption by default in channels
Disable corporate phonebook
Allow the user to control their avatar
Moderate user's requests for profile changes
Save
Notification during logging in
Show the user when logging in
*Whether to show the document to the user when they first log in
Consent, ru
View
Choose File No file chosen
Consent, en
View
Choose File No file chosen
Save
Notification of technical works
Enabled
Technical work is underway, there may be some problems with the app.
Under maintenance alert, ru
Ведутся технические работы, возможны перебои в
Under maintenance alert, en
Technical work is underway, there may be some probl
Save
Set default alert text
Notification about update
The user will get a notification if an app update is available.
Notify about an existing update
Block application interface until update is started
Versions late
0
Enabled for: IOS Android Desktop
Save
RTS ID
CTS ID
Trusts TLS Certificate
Certificate
Certificate is not present
Choose File N...en
Key
Choose File N...en
Save
BotX SSL Certificate
Certificate
Certificate is not present
Choose File N...en
Save
Admin Info
Full name
Phone
Address
Emails (comma separated)
Save
Service versions
ad_integration 3.36.1
admin 3.36.0
botx 3.36.0
email_notifications 3.36.0
kdc 3.36.0
messaging 3.36.1
phonebook 3.36.0
file_service 3.36.3
routing_schema 3.36.0
settings 3.36.0
trusts 3.36.1
voex 3.36.0
metrics_service 3.36.0
corporate_directory 3.36.0

Figure 18

SERVER SETTINGS

In the "Server Settings" section, the administrator sets the corporate style and wallpaper in chats by uploading files with the following images:

- CTS avatar;
- mobile application background;
- web application background;
- dark web application background;
- high resolution web application background;
- dark high resolution web application background,

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

Note. A 1000x1000 px raster square seamless image or a 1000x1000 px vector image should be used for the background.

These settings are recommended for use in cases where the number of connected users is less than 500. When the number of connected users is more than 500, the active setting will overload mobile devices.

To save your settings, click "Save".

SERVER FEATURES

The "Server Features" section allows to customize:

- display of contact list and search for contacts in the application;
- end-to-end encryption in group chats and channels;
- settings for changing user profile data.

To customize the display of the contact list and contact search, check the corresponding fields. The available customization options are described below in Table 7.

Note. To perform a Trust search, be sure to enable "Corporate search" and ensure that "Trust Search" is enabled for the trust connection (see page 18).

Table 7

Corporate search	Trust search	Disable corporate phonebook	Result
✓	✓	✗	The app's contact list only displays contacts from the user's phone and corporate contacts. Starting from the 3rd character entered in the search line, the search for contacts on the corporate and trust servers is enabled, as well as the search for contacts with whom the user has common chats.
✓	✗	✗	The app's contact list only displays contacts from the user's phone and corporate contacts. Starting from the 3rd character entered in the search line, the search for contacts on the corporate server is enabled, as well as the search for contacts with whom the user has common chats. Trust server search is not performed.
✗	✗	✓	The app's contact list only displays contacts from the user's phone. When performing a search, contacts from the user's phone

Corporate search	Trust search	Disable corporate phonebook	Result
			are available, as well as contacts with whom the user has shared chats.
✕	✕	✕	The app's contact list displays contacts from the corporate server and from the user's phone. When performing a search, contacts from the corporate server are available, and starting from the 3rd character entered in the search line, the search for contacts with whom the user has common chats is enabled.

To enable/disable end-to-end encryption in new group chats, set/unset the "End-to-end encryption enabled by default in group chats" flag. If the checkbox is checked, end-to-end encryption will be enabled immediately in group chats after creation by default. This setting does not affect end-to-end encryption in existing group chats.

To enable/disable end-to-end encryption in new channels, set/unset the "End-to-end encryption enabled by default in channels" flag. If the checkbox is checked, end-to-end encryption will be enabled immediately in channels after creation by default. This setting does not affect end-to-end encryption in existing channels.

To enable/disable the ability for users to change their avatar, check/uncheck the "Allow user to change avatar" box. If the box is checked, changing the avatar becomes available in the user profile.

To enable/disable moderation of data change requests in the user profile, set/unset the "Moderation of profile change requests" flag. If the box is checked, all changes to data in user profiles will be sent for moderation and will be displayed in the section "List of Change Requests".

AUTHORIZATION NOTIFICATION

In the "Authorization Notification" section, the user consent screen with the rules of information exchange is configured.

To enable/disable user notification upon authorization, check/uncheck "Display to user upon authorization" in the "Authorization Notification" block.

To upload a file with instructions, click "Choose file", select a file in .html format from the file system in Russian or English and click "Save".

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

MAINTENANCE NOTIFICATION

In the "Maintenance Notification" section, notifications to the user about maintenance work being carried out on the server (disabled by default) can be configured.

To enable/disable maintenance notification:

1. In the "Maintenance Notification" block, check/uncheck the "Enabled" box.
2. Enter the notification text in Russian and/or English or click "Set default notification text" (see Figure 19).

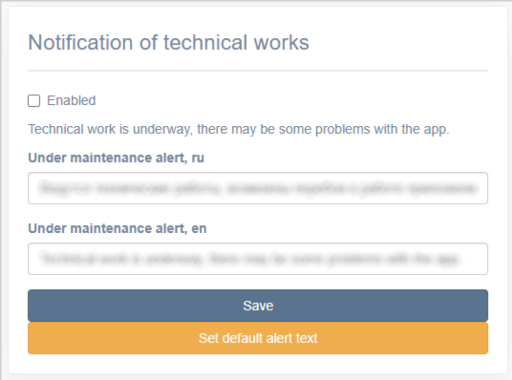


Figure 19

3. Click “Save”.

   After enabling the setting in the application, a notification will be displayed in the settings section stating that maintenance work is being carried out on the server.

   If the setting is enabled, an icon will be displayed next to the “Server” section in the administrator panel.

UPDATE NOTIFICATION

In the "Update Notification" section you can configure the following:

- user notification about the availability of an updated version of the application for installation;
- the ability to block the application interface until the update.

To disable application /server update notifications, in the “Update Notification” block, uncheck the “Notify about available update” option and click “Save”.

To enable interface blocking until application update, set the “Block application interface until update is started” flag in the “Update notification” block.

To disable interface blocking until application update, unset the “Block application interface until update is started” flag in the “Update notification” block.

To set up app/server update notifications:

1. In the “Update Notification” block, set the “Notify about available update” checkbox.
2. In the “Versions Backlog” field, specify the number of updates after which the notification will start to be displayed.
3. Check the box next to the name of the operating system on which the notification will be displayed.
4. Click “Save”.

Note. The indicator indicates the lag in the numbering of intermediate versions, for example 3.1; 3.2. That is, if the current version of the application is 3.3, then the notification will be displayed on client apps with version 3.0 and below. When the next version of the product is released, for example , 4, a notification about the update will be displayed in the user’s application settings automatically.

RTS ID AND CTS ID

The “RTS ID” and “CTS ID” sections show the identifiers of the CTS server on which the administrator web interface is opened and the RTS server to which the CTS server is connected. Identifiers are used when setting up trusts.

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 CTS server installation stage.

BOTX SSL CERTIFICATE

To connect the BotX SSL chatbot certificate, upload the certificate file and click “Save”.

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 CTS server and their versions.

VOEX

Voice Over Express (VoEx) — section of Express CS, which includes call management, call recording, SIP telephony, and integration with other types of telephony.

The following functionality is available to the administrator in the “VoEx” section:

- setting up the work of Janus instances;
- setting up the operation of TURN Server and STUN Server call servers and the VoEx local network;
- setting up the work of user rating of call quality;
- setting up SIP calls.

SETTING UP JANUS INSTANCES

The administrator can manage the operation of Janus servers in the web interface.

The following functionality is available to the administrator:

- adding Janus server;
- enable/disable Janus server;
- viewing information about the operation of Janus server;
- removing Janus server.

To set up a Janus instance (see Figure 20), in the "Janus Instances" section, enter the address of the Janus server and click . The server be displayed in the list on the screen, and the message "Janus URL added" will be displayed in the window header.

The server is disabled by default. To turn off the server manually, slide the switch to the left.

The server operating parameters are shown in Table 8:

Table 8

Parameter	Description
Disabled by whom	Shows who disabled the server. The server can be disabled automatically by the system or manually by the administrator.
Load	Total server load
Janus WS URL	Janus server address
Janus external host	Public IP of the Media server
publishers_n	Number of server users
audio_n	Number of users using a microphone
video_n	Number of users using a camera
screen_n	Number of users using the screen sharing function
recording_n	Number of users recording the call
rooms_n	Number of users using group call

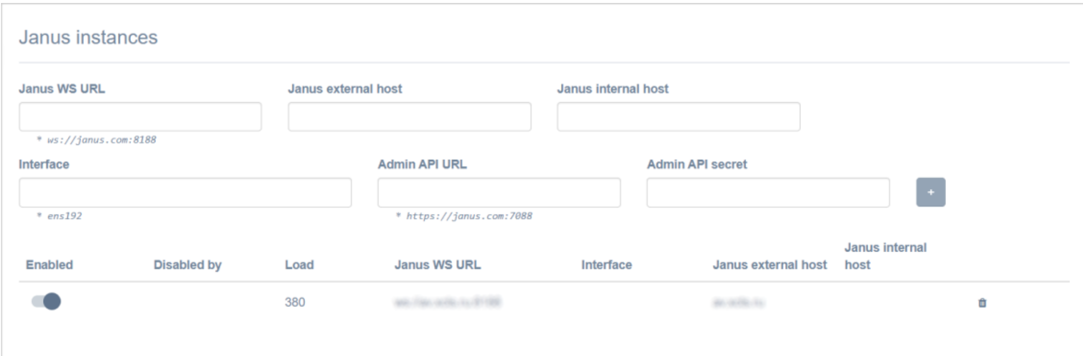


Figure 20

Note. The load on the Janus server is calculated as follows: number of publishers + number of audio * n + number of video * m + number of screen * k + number of recording * l + number of rooms * i (the variables n, m, k, l, i are static and can be changed by the developer).

To remove a Janus server, select it from the list and click . The server will be removed from the list and the message "Janus URL removed" will be displayed in the window header.

To set up TURN SERVER and STUN SERVER and the VoEx Local Network:

1. Go to the "VoEx" section (see
2. Figure 21).

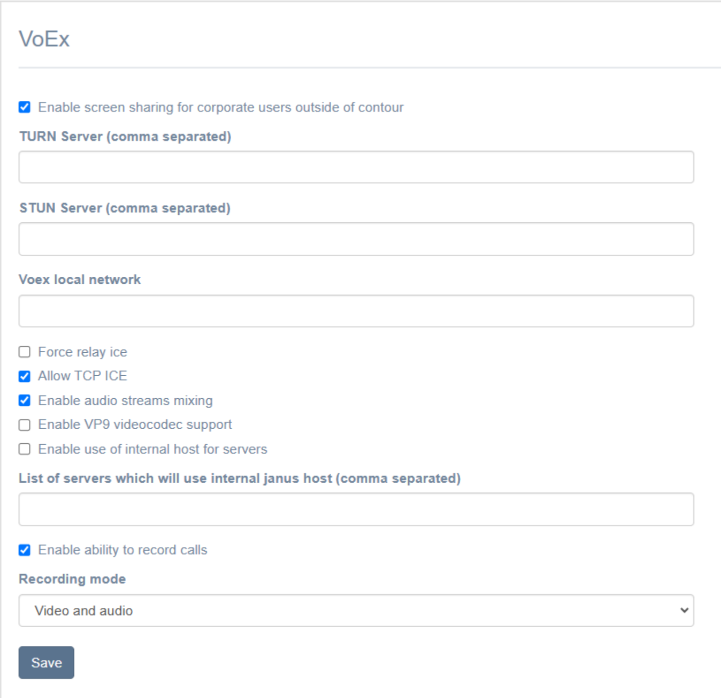


Figure 21

3. in the "TURN Server (comma separated)" field, enter the external FQDN of your Server and the port number separated by a colon, for example: ,,"express.firma.ru:3478".
4. in the "STUN Server (comma separated)" field, enter the external FQDN of your Server and the port number separated by a colon, for example: ,"express.firma.ru:3478".
5. In the "Local VoEX network" field, specify the local network mask.
6. Check the following boxes if necessary (see Table 9):

Table 9

Setting up	Description
Allow screen sharing outside of the closed contour	Allows the users to share their device screens with other users outside the CTN (RTS server users, trust server users, users who have left the CTN zone)
Use only Relay Ice candidates	Forced use of TURN server
Allow TCP ICE	The mark is set — TCP connection in TURN server is allowed. The mark is not set — TCP connection in TURN server is not allowed.
Enable audio stream mixing	Combines audio streams of calls directed from users to the server into one stream
Enable VP9 video codec	Item under development
Enable use of internal janus host for servers	Use the internal Janus host for the servers specified in the field below (see item 6)
Enable the ability to record calls	Allows users to record individual and group calls

Note. It is recommended to check "Allow screen sharing outside of the closed contour" and "Enable mixing of audio streams".

7. In the "List of servers that will use the internal Janus host (comma separated)" field, enter a list of the CTS IDs of the servers with which communication will be conducted via the internal host.
8. Select the recording mode from the drop-down list.
9. Click "Save".

SETTING UP USER RATING OF CALL OR CONFERENCE QUALITY

To set up the user rating of call or conference quality feature:

1. Go to the "User Rating" section (see Figure 22).
2. Check the box "Enable call logging".
3. Enter the data in the "User log storage" field from 0 to 36 (the default value is 12).
4. Enter the data in the "Call Quality Rating Frequency" field from 0 to 256 (the default value is 50).

Note. The "Always ask if there is an error in a call" checkbox is enabled by default. It is recommended to check the box Enable call logging".

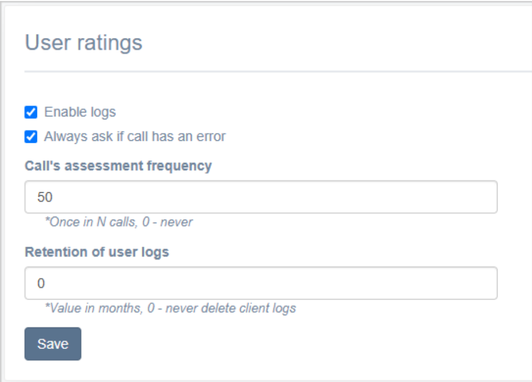


Figure 22

5. Click "Save".

SETTING UP SIP TELEPHONY

To set up SIP telephony:

1. Go to the "SIP" section.
2. Check the "SIP enabled" box (see
3. Figure 23).

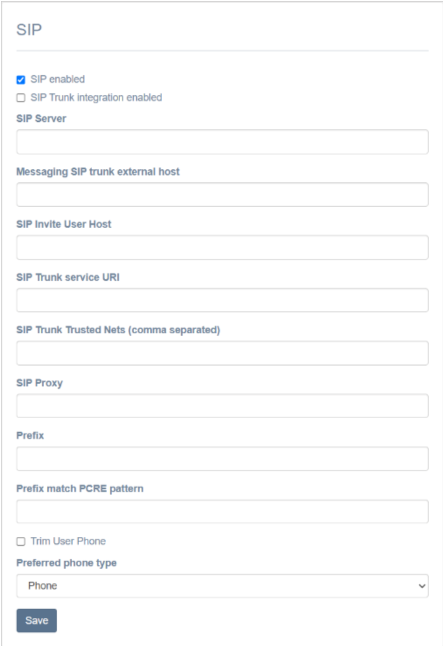


Figure 23

4. Fill in the fields as follows (see Table 10):

Table 10

Column name	Information
SIP server	SIP server address
External address for Messaging SIP trunk	The field that adds the specified CTS server IP address to SIP INVITE messages. If the field is not filled, the default value of 127.0.0.1 is used. Example of filling in the field: 10.129.0.9
Host, which is added to username when registering the SIP terminal	A field that is transmitted in the invite message towards the ATE. By default, the ccs_host value is added. If necessary, specify the host address from the configuration file
URI to connect to SIP Trunk	IP Trunk address
SIP Proxy	Proxy server address
List of allowed addresses for SIP Trunk	Allowed IP addresses for SIP calls
Prefix	Prefix value
PCRE template for prefix substitution	Substitution template
Preferred phone type	Phone type for SIP calls: IP phone or other

5. Click “Save”.

CONNECTING THE SMTP SERVER

This operation is mandatory when using automatic account creation via e-mail and when creating accounts manually.

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.

To connect the SMTP Server:

1. Select “E-mail” from the menu.

   The "E-mail Settings" window will open for entering parameters (see Figure 24).

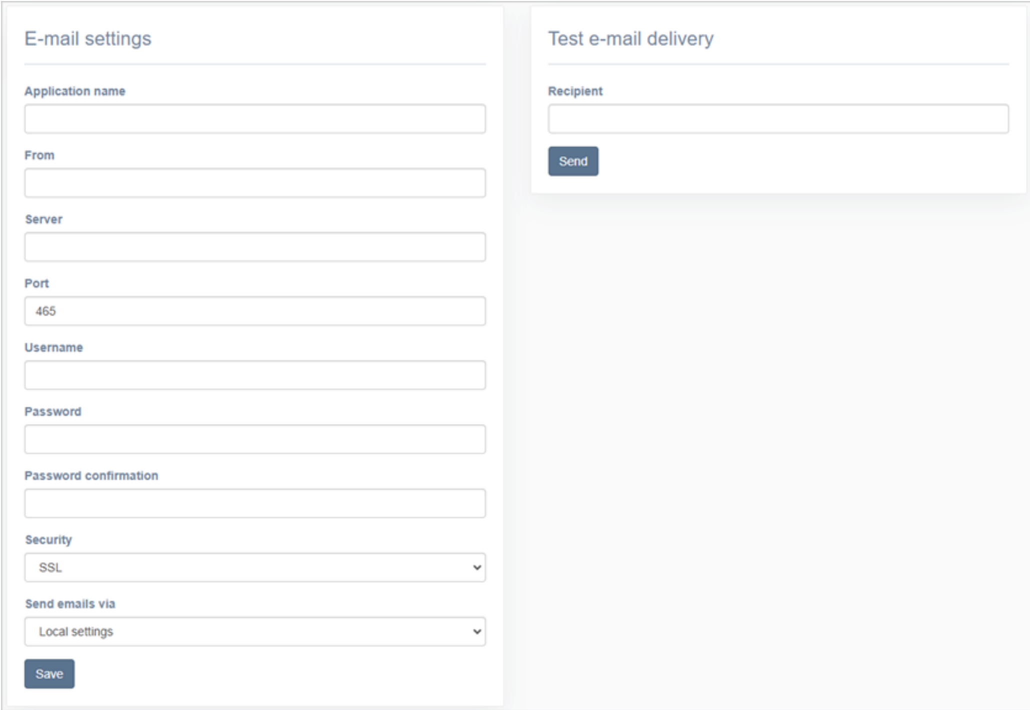


Figure 24

2. In the "E-mail Settings" window, fill in the fields as follows (see Table 11):

Table 11

Field	Description
Application name	The name of the application from which e-mails will be sent
From	Return address
Server	FQDN or IP address of the mail server
Port	Port number for retransmission of outgoing mail: 25, 587 or 465. The port number depends on the type of connection
User name	E-mail address
Password	Data for authorization on the SMTP server. If authentication on the mail server is not used, then leave these fields blank
Password confirmation	Data for authorization on the SMTP server. If authentication on the mail server is not used, then leave these fields blank
Connection protection	Type of secure connection (drop-down list: SSL, Start/TLS or empty value)
Send e-mail via	Drop-down list for selecting a server from which e-mails will be sent (if you select "Local settings" in the drop-down list, e-mails will be sent via the server configured in this window; if you select "RTS", e-mails will be sent via RTS).

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:

- Setting Up Registration;
- Users;
- Visibility of Profile Fields;
- Activations;

- Instructions to Get Started;
- Locked Out Users;
- Logout Requests.

SETTING UP REGISTRATION

The procedure for setting up user registration is described in the document "Administrator's Guide. Installation".

USERS

The section is a table that lists the user accounts registered in the application (see Figure 25).

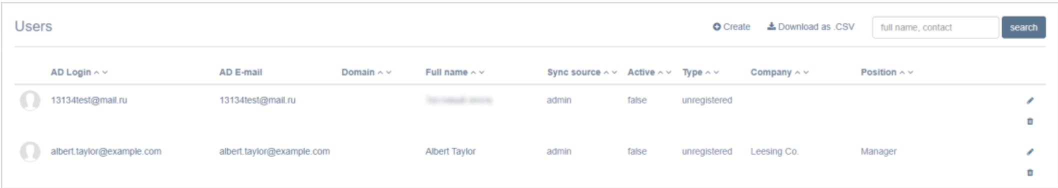


Figure 25

The table consists of the following columns (see Table 12):

Table 12

Column name	Information
AD login	The identification name of the account in Active Directory. Used when authorizing a user
AD e-mail	Active Directory/OpenID account e-mail
Domain	The domain, on which the account is registered
Name	User name
Source	Information about the method by which the account was added to the server. The parameter takes the following values: • ad (account loaded from Active Directory); • admin (an account created by the administrator); • botx (chatbot); • openid (account loaded via OpenID)
Active	Account status: activated (true) and not activated (false)
Type	Account type: • cts_user (created and authorized); • unregistered (created but not authorized); • botx (chatbot)
Company name	The company, with which the user is registered
Position	User position

To download the user table to a file, click

in the upper right corner of the window.

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

The following user authorization methods are available (see Table 13):

Table 13

Authorization method	Account type	Setup Method
Via AD login and password	AD	Specify the NTLM method in registration settings (see page 37)
Via e-mail	AD; Admin	Connect the SMTP server to the CTS server in the "E-mail" section (see "Connecting the SMTP server", page 35), indicate E-mail method in the registration settings (see page 37)
Via OpenID login and password	cts_user	Specify the OpenID method in registration settings (see page 37)

Authorization by AD login and password is available only for accounts added from AD, if the NTLM method is specified in the registration settings.

Authorization by OpenID login and password is available only for accounts added from OpenID, if the OpenID method is specified in the registration settings.

When creating accounts using the administrator web interface, only user authorization via e-mail is supported.

For authorization by e-mail address, connect SMTP server to the CTS server.

OPERATIONS WITH USER ACCOUNTS

The following operations are available to the administrator:

- creating an account;
- editing the created account. The operation is available if the account is not confirmed and activated by the user;
- viewing account information;
- account deletion from the table using the button. The operation is available if the account is not confirmed and activated by the user;
- personalized operations with a specific account.

CREATING AN ACCOUNT

User accounts are displayed in the "Users" section in the form of a table. Accounts are created manually, by creating users in the administrator's web interface in the "Users" section (see the operation below) or automatically in the following ways:

- from Active Directory;
- from OpenID;
- at the stage of registering a new user using e-mail. Using this method will require a preliminary connection to the SMTP server (see section "Connecting the SMTP Server").

To add an account from Active Directory, select the appropriate registration method and configure the settings.

To add an account from OpenID, select the appropriate registration method and configure the settings.

Attention! Integration with Active Directory directory service or directory service with KeyCloak (for OpenID) must be pre-configured. The integration procedure is described in the document "Administrator's Guide. Installation".

Changes made to user accounts in the directory service are automatically synchronized and reflected in the corresponding accounts in Express.

To create an account when registering a user using an e-mail address select the "E-mail" registration method in the "Registration Settings" section and specify the e-mail mask in the "Registration Settings" section and select "E-mail".

To create an account in the administrator web interface:

1. In the upper right corner of the "Users" section, click "Create". The "New User" window will open (see Figure 26).

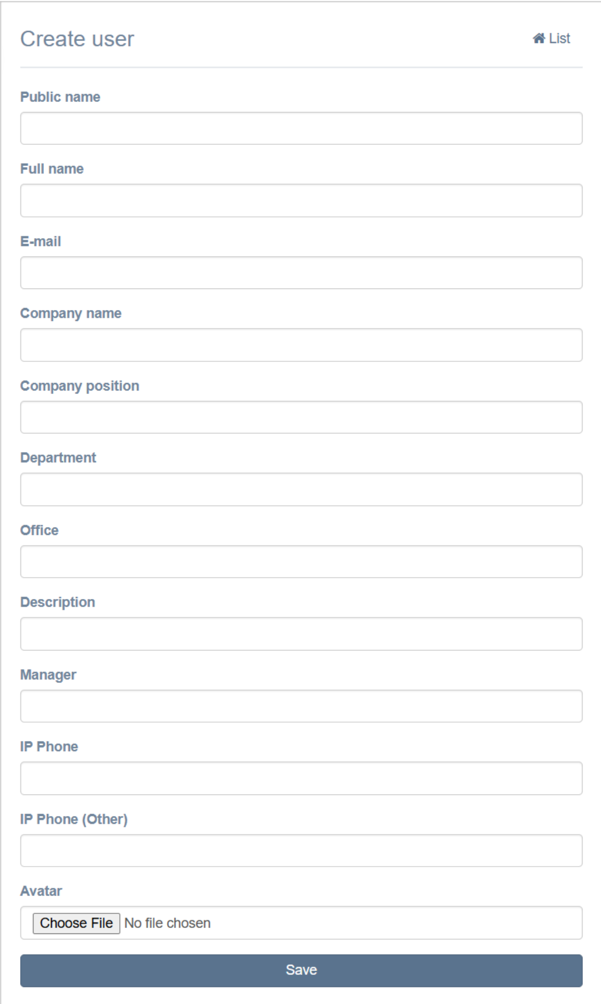


Figure 26

2. Fill in the fields of the form.

   An example of filling out the form is shown in Figure 27.

Note. The file to be uploaded in the "Avatar" field shall meet the following requirements:

- JPG format;
- file size not more than 100 kb;
- the image shall fit into a 500x500 pixel square.

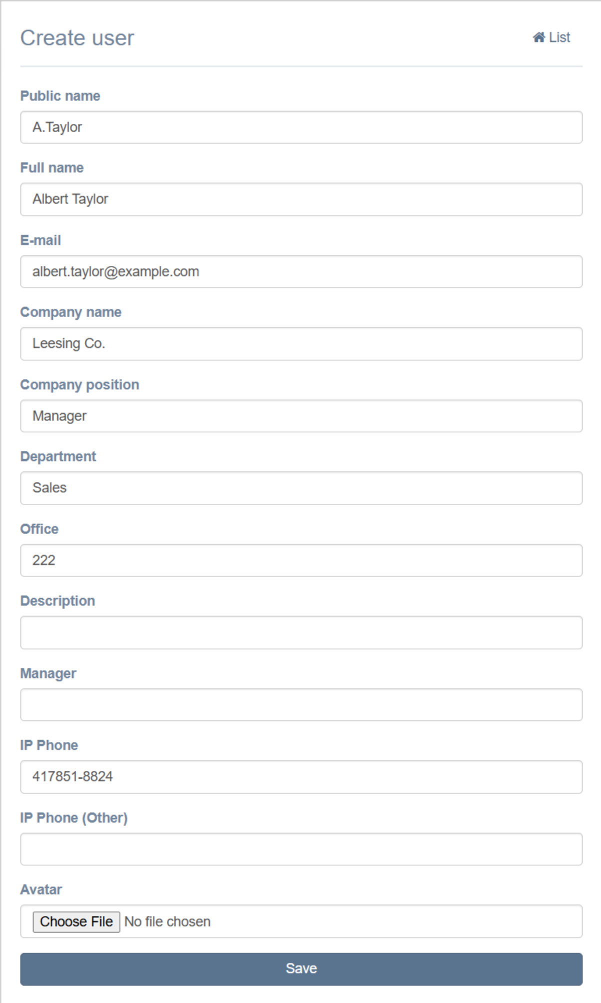


Figure 27

3. Click “Save”.

   An example of created account display is shown in Figure 28.

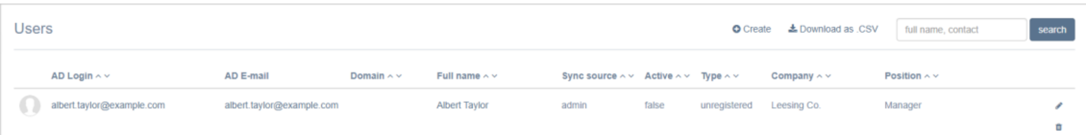


Figure 28

For more details on account settings, see the relevant section (“Viewing Account Information”).

VIEWING ACCOUNT INFORMATION

Each account has a card containing full information about the account (see Figure 29):

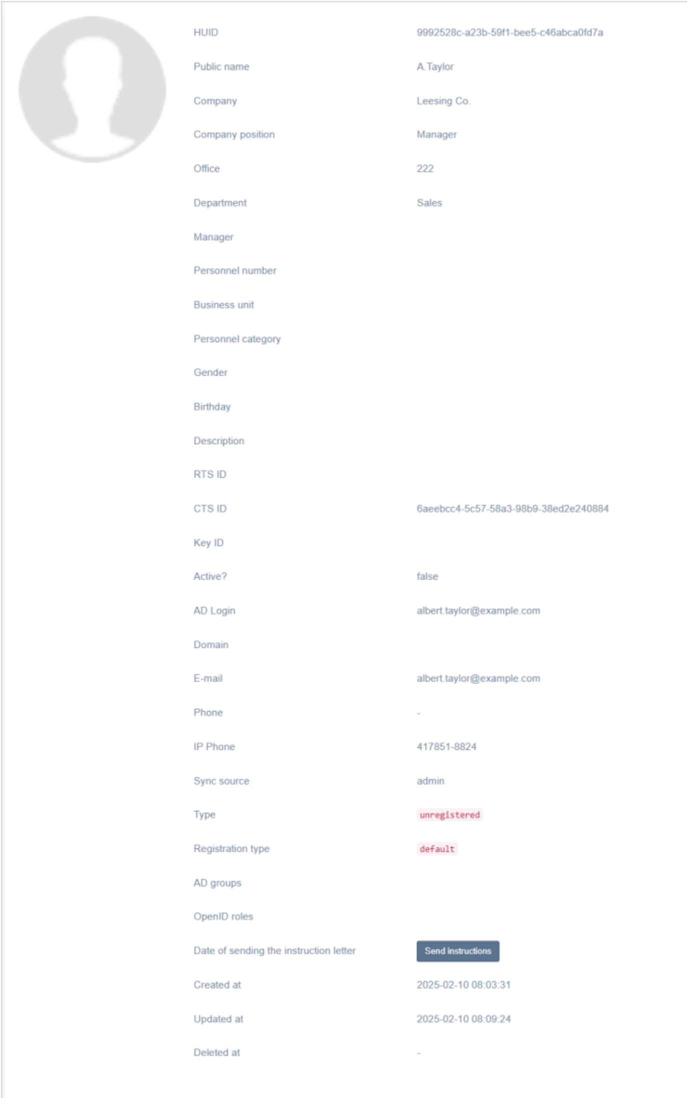


Figure 29

The information in the user card, which was added via AD or OpenID, is for reference only and cannot be edited.

The information in the user card, which was created through the administrator web interface, can be changed. For such a user, buttons for editing data and deleting an account are available (see Figure 30).

Note. The update date of the user's profile changes when the user enters the corporate server or when users are synchronized with the corporate directory.

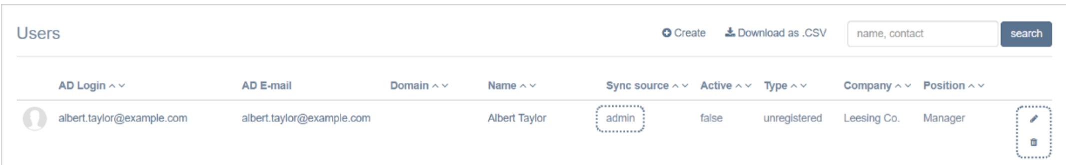


Figure 30

EDITING AN ACCOUNT

Accounts added from Active Directory or OpenID cannot be modified in the administrator web interface. Changes to such accounts are made by synchronizing data with these systems.

If the server allows user avatar changes, the user can change their avatar. Information about this change will be displayed in the list of change requests.

To edit the account:

1. Go to the "Users" section (see Figure 30).
2. Click .

   The profile editing window will open (see Figure 31).

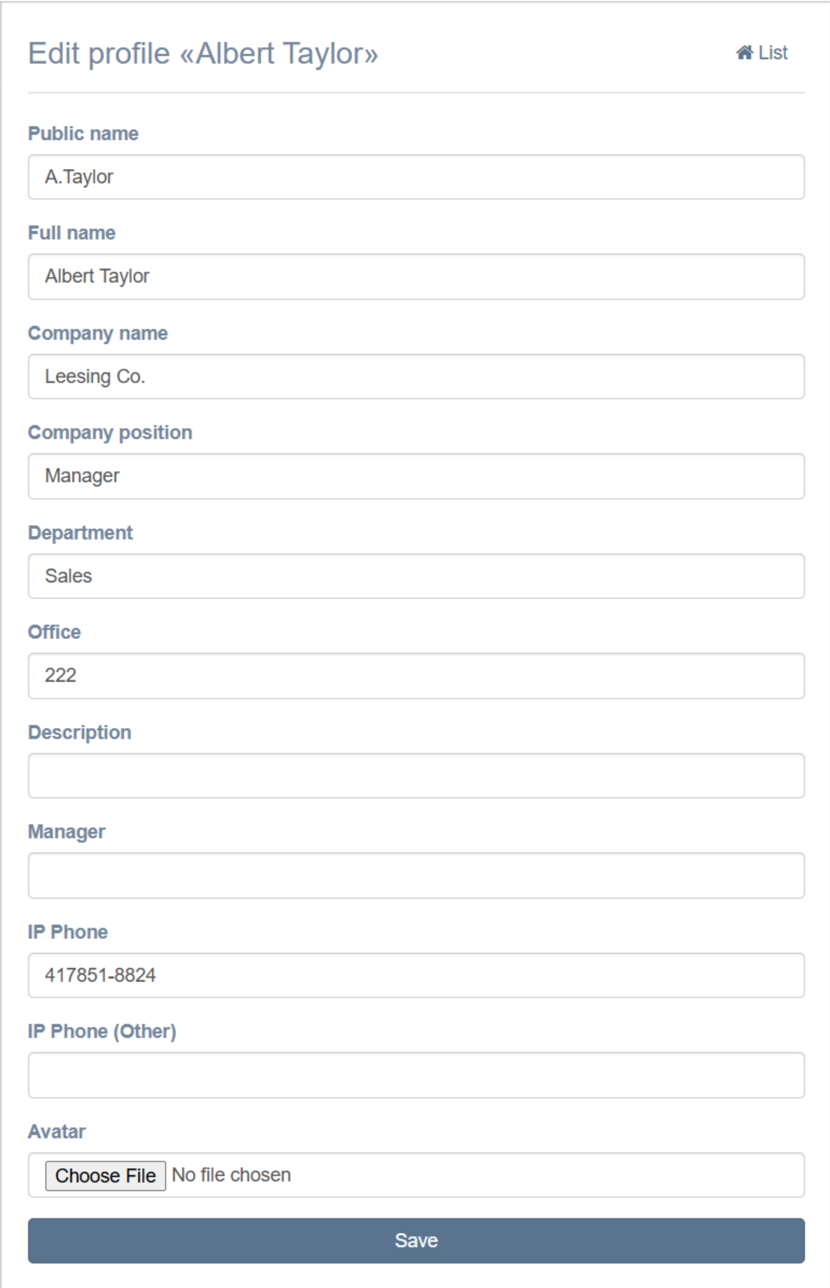


Figure 31

3. Make changes and click "Save".

> **Note.** Changing the external user name in an account created in the administrator web interface is available after activating the user account.

OPERATIONS WITH A SPECIFIC USER ACCOUNT

To perform operations with a specific user account, use the buttons on the toolbar (see Figure 32).

Figure 32

The list of available operations:

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

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

To view information about lockouts, click "Lockouts".

A window will open with a list of lockouts for the user added from AD (see Figure 33.).

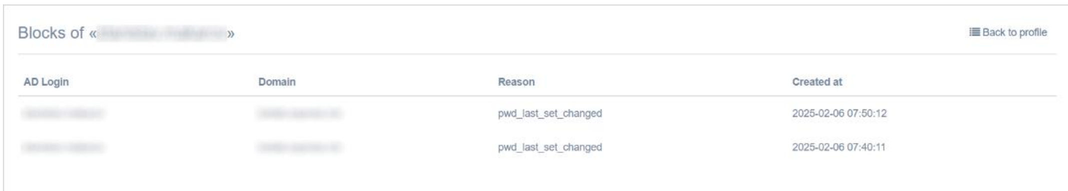


Figure 33.

The table contains the following information (Table 14):

Table 14

Column name	Information
AD login	The identification name of the account in AD. Used when authorizing a user
Domain	The domain, on which the account is registered
Reason	Reason for user lockout in AD. The field takes the following values: • pwd_last_set_changed (password change); • account_disabled (account disabled); • lockout (account lock); • password_expired (password expired); • account_expired (account expired)
Creation date	Lockout creation date. It is entered in the format "year-month-day hour:minutes:seconds"

To view information about open sessions of the registered corporate user, click "Activation".

Each session is represented by an information card (see Figure 34). To view all information cards, scroll down the page.

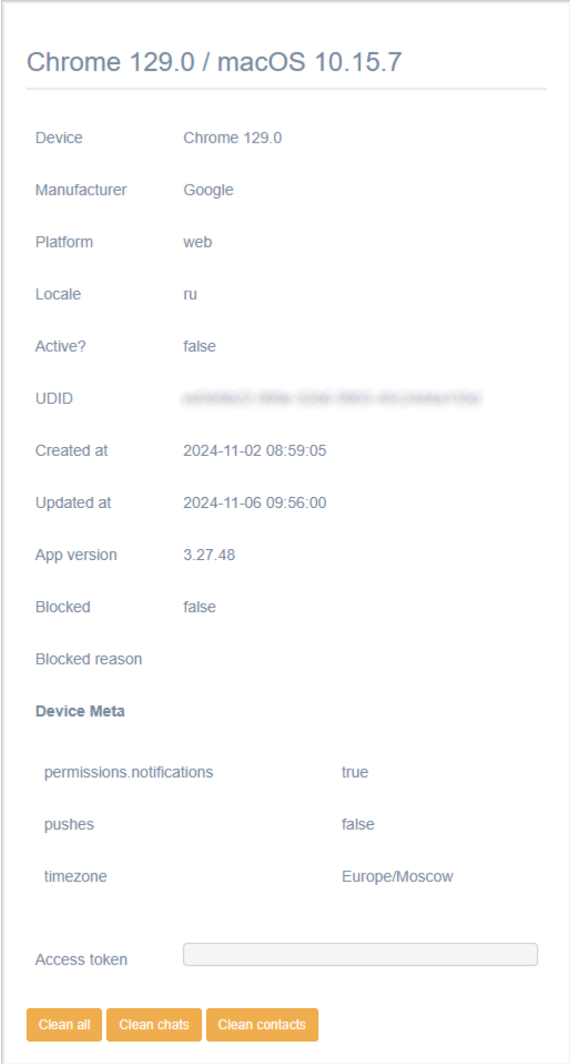


Figure 34

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 application (web application notifications are managed by the browser) or in the mobile application (iOS application notifications are managed by the operating system);
- Permissions.contacts — is access to contacts allowed;
- Permissions.storage — is access to device storage allowed.

At the bottom of the card, there are session management buttons:

- "Clear all" — clears the chat and contact cache, terminates the session;
- "Clear chats" — forcibly clears the chat cache;
- "Clear contacts" — forcibly clears the contacts cache.

Note. After clearing the cache, chats/contacts are downloaded again from the server.

To view reference information about the keys assigned to the user, click "Keys". Opens a window with help information (see Figure 35.).

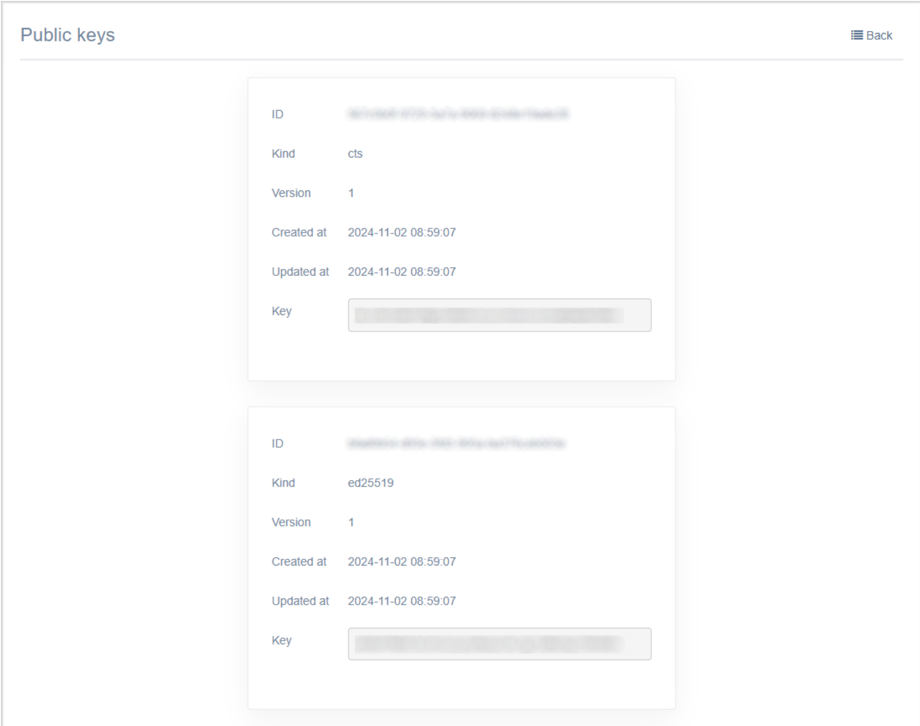


Figure 35.

To view the list of chats the user is connected to, click "Chats" (see Figure 36):

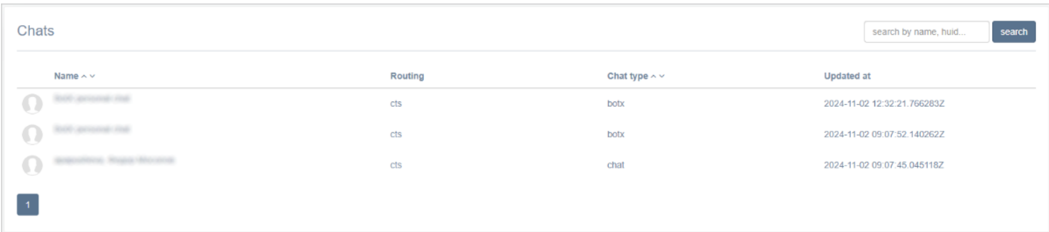


Figure 36

The table contains the following information (see Table 15):

Table 15

Column name	Information
Name	Chat name
Routing	Information about the server on which the chat was created: • cts (chat data is stored on the CTS server); • rts (chat data is stored on the RTS server); • hybrid (chat data is stored on the CTS RTS server)
Chat type	Chat type: • chat (chat); • group_chat (group chat);

Column name	Information
	• channel (channel); • botx (chatbot)
Update date	Time of the last event in the chat (message, adding a user, etc.)

Chat names are hyperlinks to the personal chat card.

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.

To forcibly disconnect a user from the corporate server, click "Logout". This button is available only in the cards of registered corporate users added via AD and openID. Clicking this button logs the user out of the corporate server. The user can log back in until their account is deleted.

DELETING AN ACCOUNT

Only unregistered accounts created manually and accounts with a confirmed exit request from the CTS server can be deleted in the administrator web interface.

Accounts added from Active Directory or OpenID cannot be deleted in the administrator web interface. Removing accounts from AD is performed by synchronizing data with AD, however accounts are not removed from OpenID.

To delete an account from the table, click and confirm the action in the modal window that opens by clicking "OK". The account will be deleted.

Note. Deleting a user is only possible after he/she logs out of the corporate server.

SETTING UP VISIBILITY OF USER PROFILE FIELDS

The "Visibility of Profile Fields" section (Figure 37) is designed to configure access levels to data in the profile of a registered user of a corporate server.

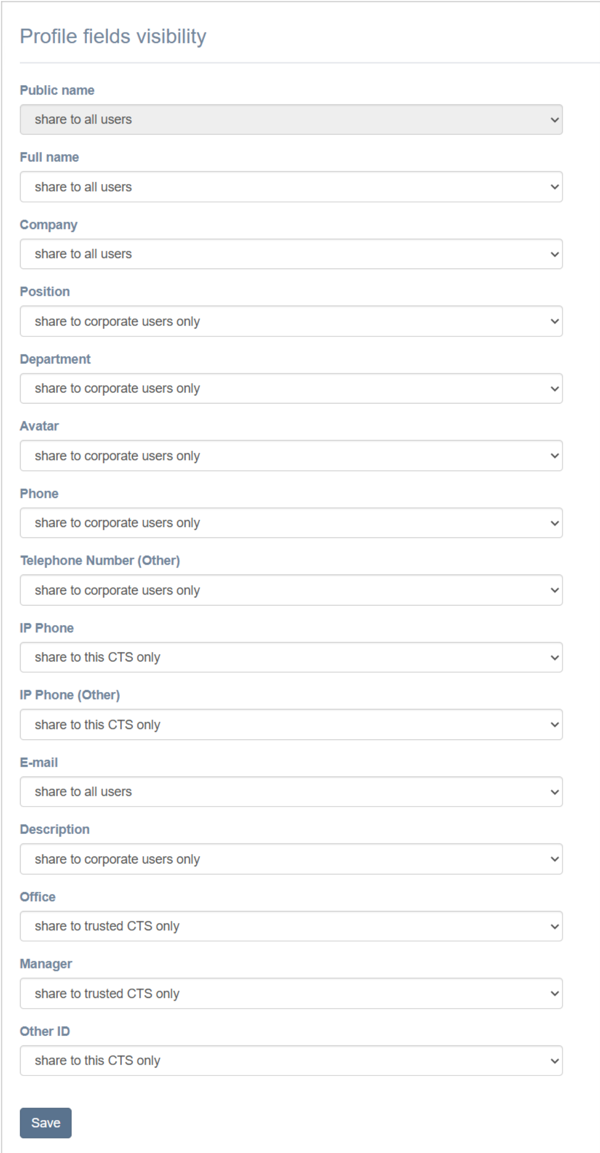


Figure 37

To set up the visibility of profile fields:

1. Go to the "Visibility of Profile Fields" section (see Figure 37).
2. Click on the field below the name of the attribute whose data access you want to configure.
3. Select one of the access levels from the drop-down list:
   - no one;
   - for users from the same CTS server only;
   - for users from trust CTS servers only;
   - for corporate users only;
   - for all.
4. Click "Save".

   The configured fields will become available to the specified users. The system message "Profile fields visibility settings saved" will be displayed at the top of the screen.

SETTING UP USER SESSION ACTIVITY TIME

In the "Activations" section, you can set the time in seconds after which the user session on iOS, Android, web, and desktop devices 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 38.).

2. Specify the session duration in seconds.

   To disable automatic closing of user session, leave the field blank.

3. Click "Save".

Figure 38.

SENDING INSTRUCTIONS FOR GETTING STARTED WITH THE APPLICATION

There are two options for sending instructions to the user:

- personally by using a contact card;
- via centralized mailing.

To send the user instructions on how to get started with the application

1. Go to the "Users" section and open the account information card.
2. Click "Send instructions" (see Figure 39).

   The date and time the instruction was sent will be displayed in the line "Date of sending the letter with the instruction".

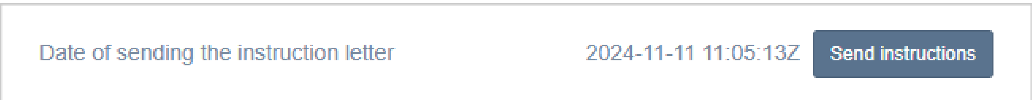


Figure 39

To set up centralized mailing, go to the "E-mail" → "Instructions to Get Started" section (see Figure 40).

This section allows you to create/edit instructions to get started with the application, configure its sending to new users, and also send instructions to all unregistered users.

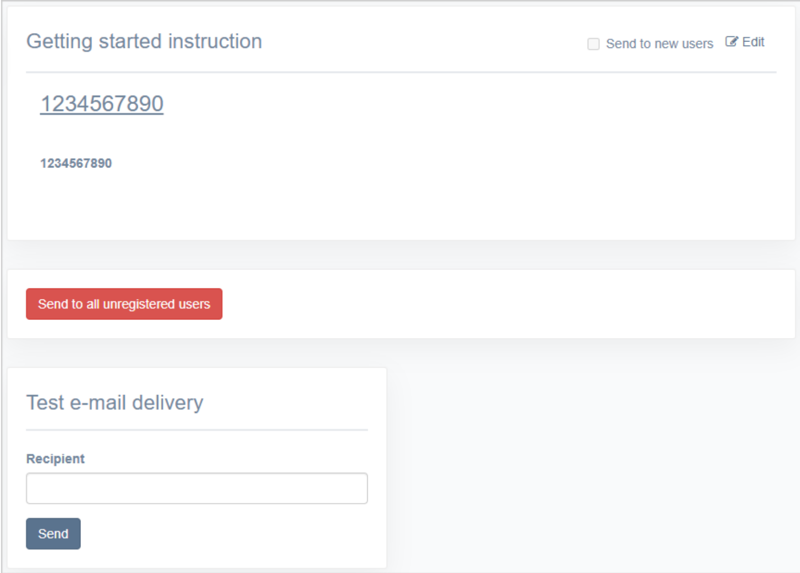


Figure 40

The main part of the window displays the text of the instructions.

To create or change the text of a letter click "Edit" and make changes to the body of the e-mail.

Attention! The body of the e-mail is a mandatory field. If you attempt to send an empty e-mail, a prompt will be displayed in the body of the e-mail saying "Fill in the body of the e-mail (mandatory field)".

To send instructions to all users not registered on the server, click "Send to all unregistered users" .

To set up automatic sending of instructions to new users, go to the editing mode and check the box "Send to new users" in the upper right corner of the window.

Note. New users are those that appear in the Users section with the unregistered entry type (for more information on the account type, see Table 12).

The instruction will be sent to the user immediately after they authorize on the corporate server. This option is disabled by default.

To switch to the instruction editing mode, click "Edit" in the upper right part of the window (see Figure 40). A window will open for editing the text of the instructions to get started (see Figure 41).

The tags below the e-mail editing field are used to substitute recipient data and are replaced during mailing with real user names, their corporate e-mail addresses, and corporate server names.

To save your changes, click "Save".

To test the instructions sending feature, enter the recipient's e-mail address in the "Testing e-mail sending" field and click "Send". If the operation is completed successfully, an e-mail with instructions will be sent to the specified address.

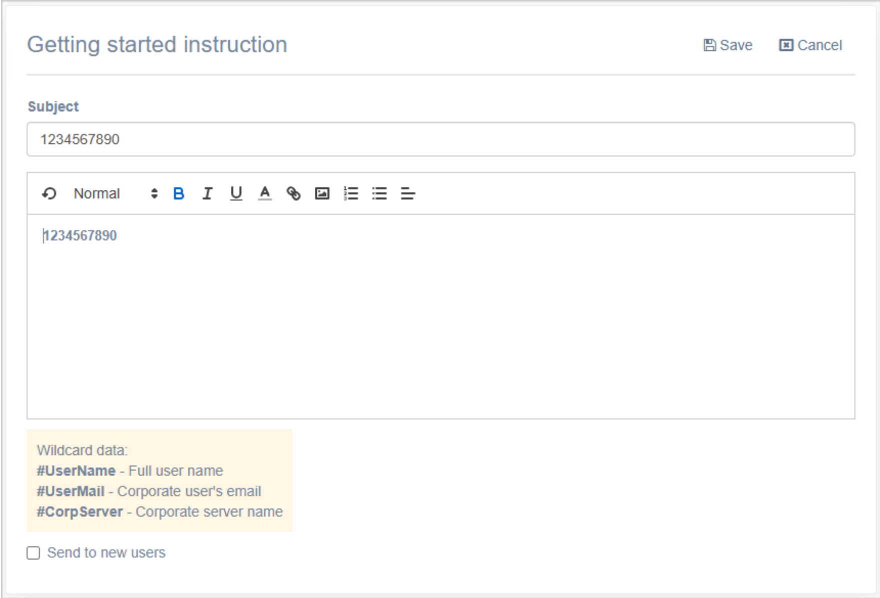


Figure 41

SENDING NOTIFICATIONS ABOUT USER LOCKOUTS

The "E-mail" section → "Locked Out Users" (Figure 42) allows you to configure e-mail notifications about account lockouts.

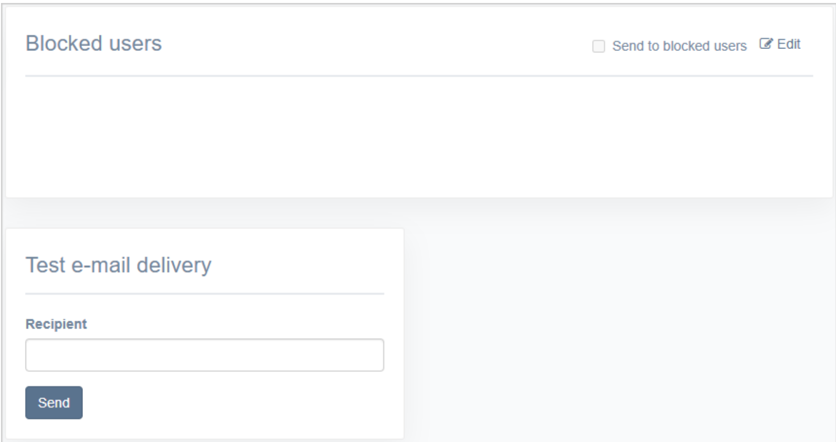


Figure 42

The main part of the window displays the text of the notification.

To create or change the text of a letter click "Edit" and make changes to the body of the e-mail.

Attention! The e-mail must contain some text. If you attempt to send an empty e-mail, the administrator will receive the message "Error sending e-mail: you must fill in the body of the e-mail."

To set up automatic sending of notification to new users, go to the editing mode and check the box "Send to new users" in the upper right corner of the window. The notification will be sent to the user immediately after they authorize on the corporate server. This option is disabled by default.

To go to the editing mode, click "Edit" in the top right corner. A window will open for editing the text of the user lockout notification (see Figure 43).

To save your changes, click "Save".

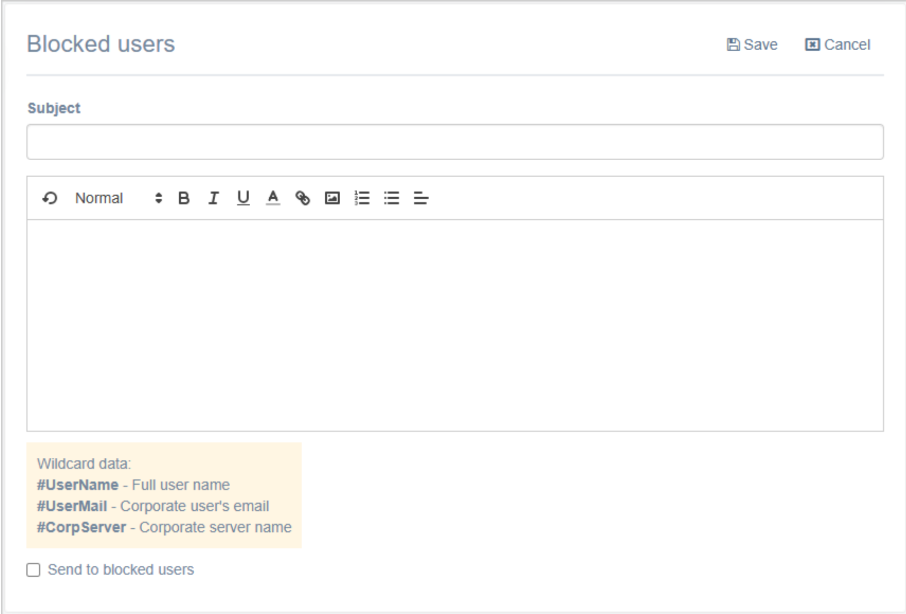


Figure 43

To test the user lockout notification sending feature, enter the recipient's e-mail address in the "Testing e-mail sending" field and click "Send". Once the operation is completed successfully, an e-mail with notification will be sent to the specified address.

REQUESTS TO EXIT FROM THE CORPORATE SERVER

Logging out users from a corporate server can be carried out as follows:

- a logout request made by the user in the client application and confirmed by the administrator;
- by clicking the "Logout" button on the toolbar in the user card in the administrator web interface (see "Operations with a Specific User Account").

Once the user logs out of the corporate server, the button to delete the user from the corporate server becomes available (see "Deleting an Account").

When the user clicks the "Logout" button in the "Profile" section of application settings, the application sends a logout request to the CTS server.

Requests are displayed Table in the "Logout Requests" menu item (see Figure 44.).

Figure 44.

The parameters of registered displayed requests are shown in the following table (Table 16):

Table 16

Column name	Information
Name	User name
AD login	The identification name of the account in Active Directory. Used when authorizing a user
Domain	The domain, on which the account is registered

Column name	Information
AD e-mail	Active Directory/OpenID account e-mail
Company name	The company, with which the user is registered
Position	User position
Reason	Reason for logout
Creation date	Date of creation of the logout request

The reasons for the logout request are shown in the following table (Table 17):

Table 17

Event	Description
user_request	The logout request was sent by the user
pwd_last_set_changed	Logout due to password change in AD
account_disabled	The user's account has been disabled in AD
account_deleted	The user's account has been deleted
lockout	The user has been locked out in AD
password_expired	The user’s AD password has expired
account_expired	The user’s account in AD has expired
admin_request	Logout request was sent by the administrator
excluded_from_search_filter	The autologout option was enabled and the user was not included in the sample (removed from the AD group)

To search for requests in the table, use fields at the top of the window (see Figure 45.).

Figure 45.

Search types:

- search by user name — search is performed by user’s name in the system;
- search by login — search is performed by user’s login in the system;
- Search by reason — the reason for the logout request is selected in the drop-down list.

Note. The button to mark all users to the left of the “Name” column is only active if the search is activated due to a logout request. If no filter is selected, you can only mark users one by one.

To confirm the user's request, click “Accept” and confirm the action by clicking “OK” in the modal box that opens.

To confirm several requests at the same time, check the names of the required users and click “Accept all” and confirm the action by pressing “OK” in the modal window that opens. If necessary, use the search function.

To reject the user's request, click “Reject” and confirm the action by clicking “OK” in the modal box that opens.

To reject several requests at the same time, check the names of the required users and click “Reject all” and confirm the action by pressing “OK” in the modal window that opens. If necessary, use the search function.

To remove a user whose logout request has been confirmed from the CTS server, go to the “Users” section, click on the right in the user's entry line, and confirm the action by clicking the “OK” button in the modal window that opens.

To forcefully remove a user from the CTS server:

1. Select the "Users" menu item.
2. In the table, select a contact and open the contact card.
3. On the toolbar, click "Logout".

   A request will be displayed in the "Logout Requests" menu item.
4. Open the "Logout Requests" menu item and click "Accept" next to the username.

LIST OF CHANGE REQUESTS

Changing user data on the corporate server can be performed by a change request made by the user himself in the client application and confirmed by the administrator.

When a user changes data in the application settings in the Profile section, the application sends a request to CTS.

Requests are displayed Table in the "List of Change Requests" menu item (see Figure 46.).

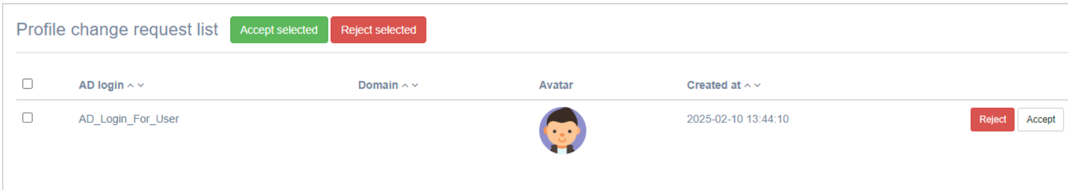


Figure 46.

The parameters of registered displayed requests are shown in the following table (Table 18):

Table 18

Column name	Information
AD login	The identification name of the account in Active Directory. Used when authorizing a user
Domain	The domain, on which the account is registered
Avatar	User avatar
Creation date	Date of creation of the change request

To search for requests in the table, use fields at the top of the window (see Figure 46.). User search is performed by the user's login in the system.

To confirm the user's request, click "Accept" and confirm the action by clicking "OK" in the modal box that opens.

To confirm several requests at the same time, check the names of the required users and click "Accept all" and confirm the action by pressing "OK" in the modal window that opens. If necessary, use the search function.

To reject the user's request, click "Reject" and confirm the action by clicking "OK" in the modal box that opens.

To reject several requests at the same time, check the names of the required users and click "Reject all" and confirm the action by pressing "OK" in the modal window that opens. If necessary, use the search function.

SUPPORT CONTACTS

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 47).

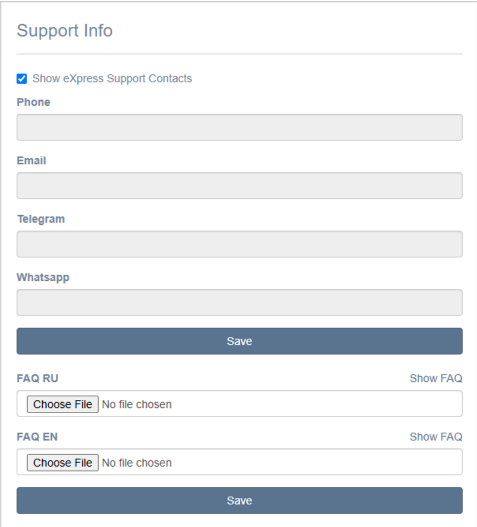


Figure 47

3. Click "Save".

To upload a file with instructions, in the "Support Settings" section of the client's administrator panel, click "Select File" (in Russian or English), select a file in .html format from the file system and click "Save".

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

ROLE MODEL AND USER GROUPS

This section describes the following administrator web interface menu items:

- Role Model;
- User Groups.

Within the framework of the role model for individual user groups, the administrator can set restrictions for Express ("In messenger") and its SmartApps ("In SmartApps"):

Table 19

Rule	**Scope**	
	In messenger	**In SmartApps**
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	✓	✓
Prohibition of downloading attachments from CTS users;	✓	✗

Rule	Scope	
	In messenger	In SmartApps
Mandatory use of the PIN code when the user enters the application.	✓	✗

Restrictions may apply to:

- attachment type (image, video, document);
- document format (e.g. PDF, DOCX, TXT, etc.);
- attachment size (for example, 300 MB);
- specific chats/channels;
- discussions and chats of calls/conferences;
- users.

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.

OPERATIONS WITH USER GROUPS

In the “User Groups” section (Figure 48), the following functionality is available to the administrator:

- creating a group;
- editing parameters of the group;
- deleting a group.

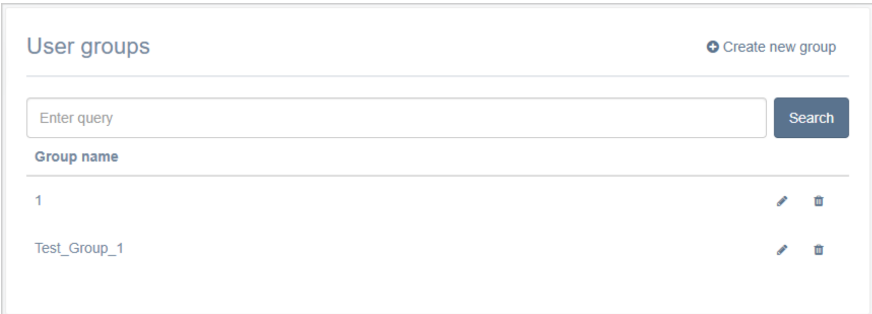


Figure 48

To create a new group:

1. Go to the “User Groups” section and click “Create New Group”.

   The group settings form will open (see Figure 49).

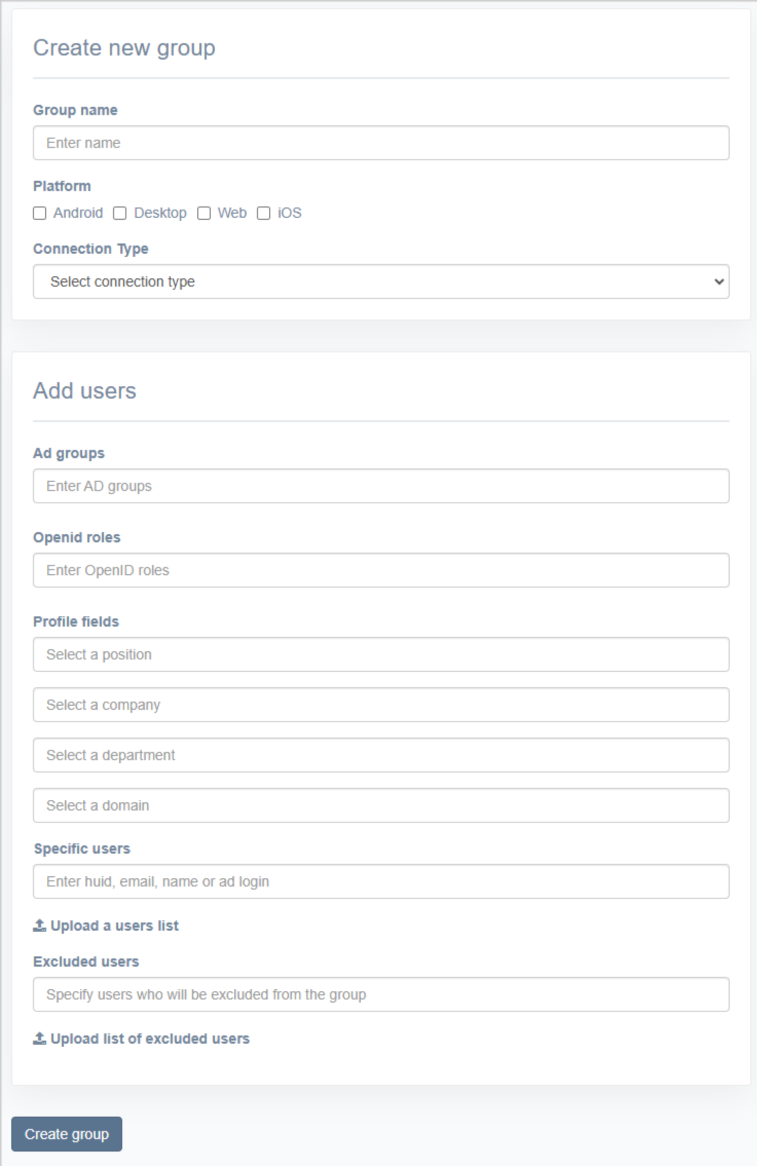


Figure 49

2. Fill in the fields of the form. Field values are shown in Table 20.

Table 20

Column name	Information
Group name	Group name (mandatory field)
Platform	Platforms for which the restriction will apply (the field is mandatory)
Connection type	Select the connection type from the drop-down list (mandatory field). The division into "External contour" and "Internal contour" works on the basis of contour settings in the "File Service" section. In order the CTN settings to not interfere with the operation of the role model, turn on the contour (check "Enabled"), in all the settings fields of the contour rules, specify "any" and specify the IP masks of your corporate network
AD group	Specify AD user groups
OpenID roles	Specify OpenID user roles
Profile field	Enter user's profile data
Specific users	Specify user's HUID, e-mail, name or AD login. Download the user list if necessary
Exception users	Specify the users that will not be subject to the rule. Download the user list if necessary

3. Click “Create Group”.

To edit a user group:

1. Select a group from the list (Figure 50) and click “Edit” .

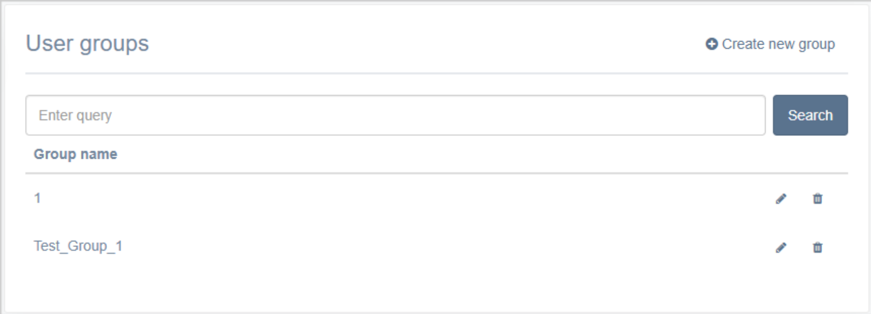


Figure 50

The “Edit Group” window will open (Figure 51):

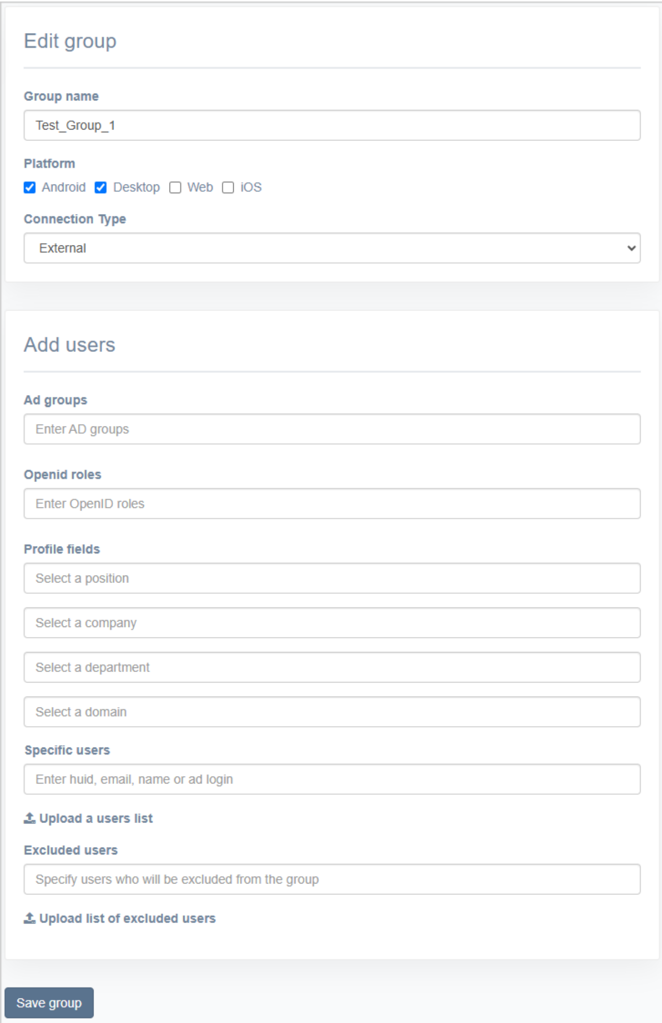


Figure 51

2. Make changes and click “Save Group”.

To delete a group, select it from the list click and confirm the action in the modal window that opens by clicking “OK”.

ROLE MODEL

In this section, the administrator can activate the role-based access restrictions model. Restrictions on user actions with attachments and the use of a PIN code are regulated by the created rules. By default, the section is not activated. The page contains a list of rules (see Figure 52.).

To view the list of rules, open the corresponding section by clicking . Active rules have the status of "Activated". The rules that have not been applied have the "Paused" status. After creation, all rules have the "Paused" status.

Attention! To start applying the rule, select the "Activated" status from the rule status drop-down list.

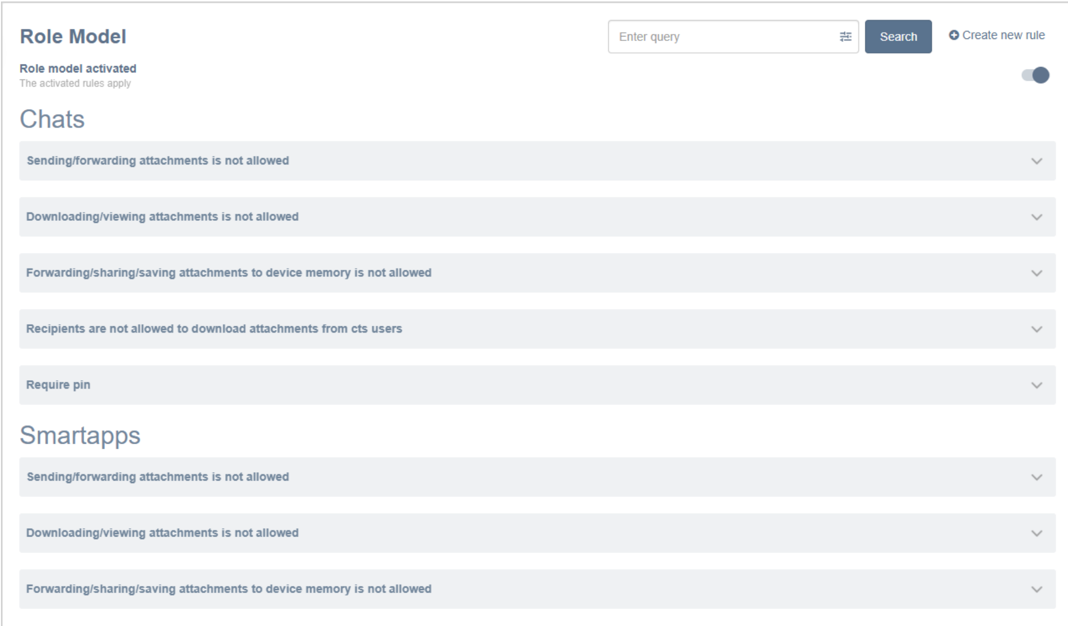


Figure 52.

OPERATIONS WITH RULES

The administrator can create, copy, edit and delete rules.

CREATING GENERAL RULES

This section describes the rules that apply both in the "In Messenger" and the "In SmartApp" scopes.

Attention! The drop-down list of restrictions changes depending on the selected scope. When you select the "In messenger" scope, additional rules will appear in the list.

Creating rules:

- 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.

To create a rule:

1. Click "Create New Rule".

   The rule creation form will open (see Figure 53).

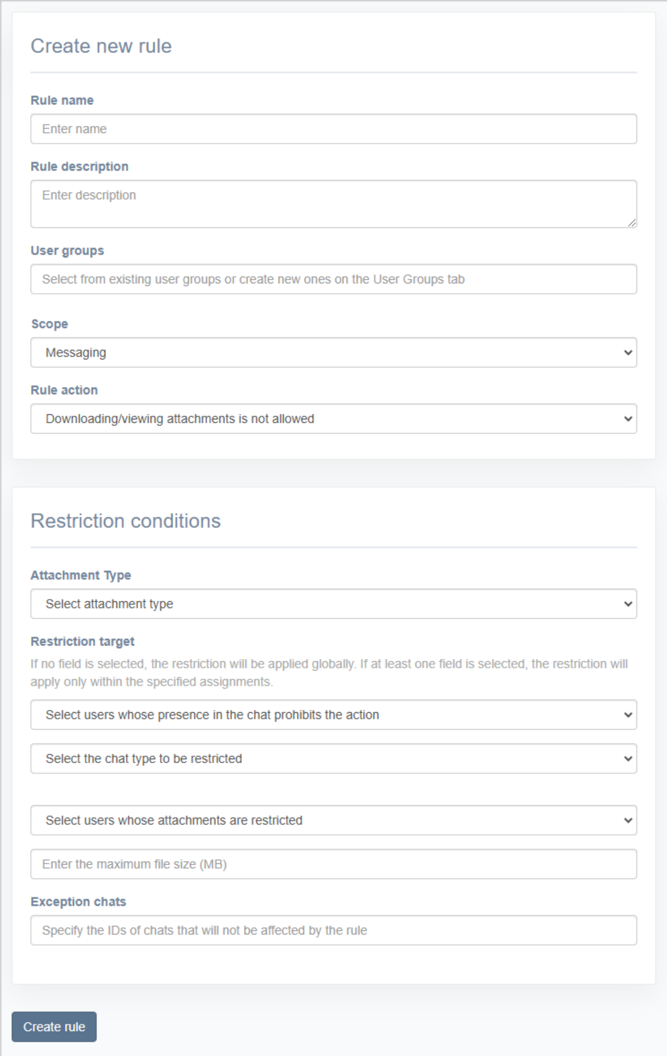


Figure 53

The presence of form fields depends on the attachment type.

2. Fill in the fields of the form. Field values are shown in Table 21.

Table 21

Column name	Information
Rule name	Rule name (mandatory field)
Rule description	Description of the restriction action (maximum 1,000 characters)
User group	Select the user groups from the drop-down list
Scope	Select the scope "In Messenger" or "In SmartApps" from the drop-down list
Rule type	Select the rule type from the drop-down list (mandatory field)
Attachment type	Select the attachment type from the drop-down list (mandatory field)
Prohibition function	Select the following from the drop-down list: • users whose presence in the chat disallows an action; • type of chat that falls under a prohibition; • enter the maximum allowable file size (MB); • specify the list of prohibited file extensions (for documents)
Exception chats	Specify the IDs of chats that will not be subject to the rule

Attention! If no fields are filled in the prohibition function, the prohibition will apply to all chats. If at least one field is filled in, prohibition will be applied only the specified assignments.

3. Click "Create Rule".

The rule will be displayed in the list in the corresponding restrictions section (see Figure 52.).

CREATING AN "IN MESSENGER" RULE

This section describes the rules that apply only in the "In messenger" scope.

PROHIBITION OF DOWNLOADING ATTACHMENTS FROM CTS USERS;

To create a rule:

1. Click "Create New Rule".

   The rule creation form will open (see Figure 54).

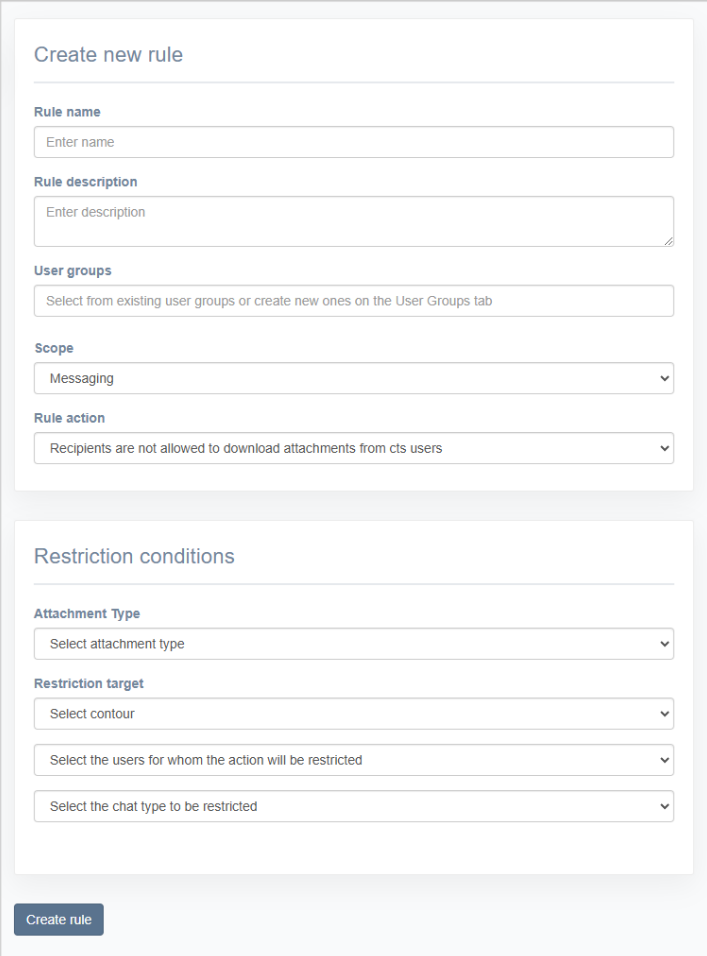


Figure 54

2. Fill in the fields of the form. Field values are shown in Table 22.

Table 22

Column name	Information
Rule name	Rule name (mandatory field)
Rule description	Description of the restriction action (maximum 1,000 characters)
User group	Select the user groups from the drop-down list
Scope	Select the scope "In Messenger" from the drop-down list
Rule type	Select the rule type "Prohibition for recipients to download attachments from CTS users" from the drop-down list
Attachment type	Select the attachment type from the drop-down list (mandatory field): • video files; • documents; • images

Column name	Information
Prohibition function	Choose a contour delineation from the drop-down list: • "Everyone, except for users from the internal contour" (prohibition for all CTN users, except users from the same server); • "Everyone, except for users from the trusted contour" (prohibition for all CTN users, except for users from the same server and trust servers). **Attention!** For more information about setting up contour access, see page 108. Choose from the drop-down list of users for whom the action will be prohibited: • "Everyone, except for users from the trusted servers" (prohibition for everyone, except users from the same server and trust servers). • "Everyone, except for users from the same server" (prohibition for everyone, except users from the same server); • "Public users and guests" (prohibition for "green" users and guests). **Attention!** At least one of the specified purposes must be filled. If both purposes are filled, the most stringent one — the contour restriction — will apply. Select the type of chat for which the prohibition is configured from the drop-down list: • "Only group chats and channels without end-to-end encryption"; • "Only group chats and channels with end-to-end encryption"; • "Only personal chats". If necessary, specify the chat ID
Exception chats	Specify the IDs of chats that will not be subject to the rule

3. Click "Create Rule".

   The rule will be displayed in the list in the corresponding restrictions section (see Figure 52.).

MANDATORY PIN CODE SETTING

The rule obliges the user to set a PIN code to enter the app. After setting a PIN code, the user will not be able to turn it off.

To create a rule:

1. Click "Create New Rule".

   The rule creation form will open (see Figure 55).

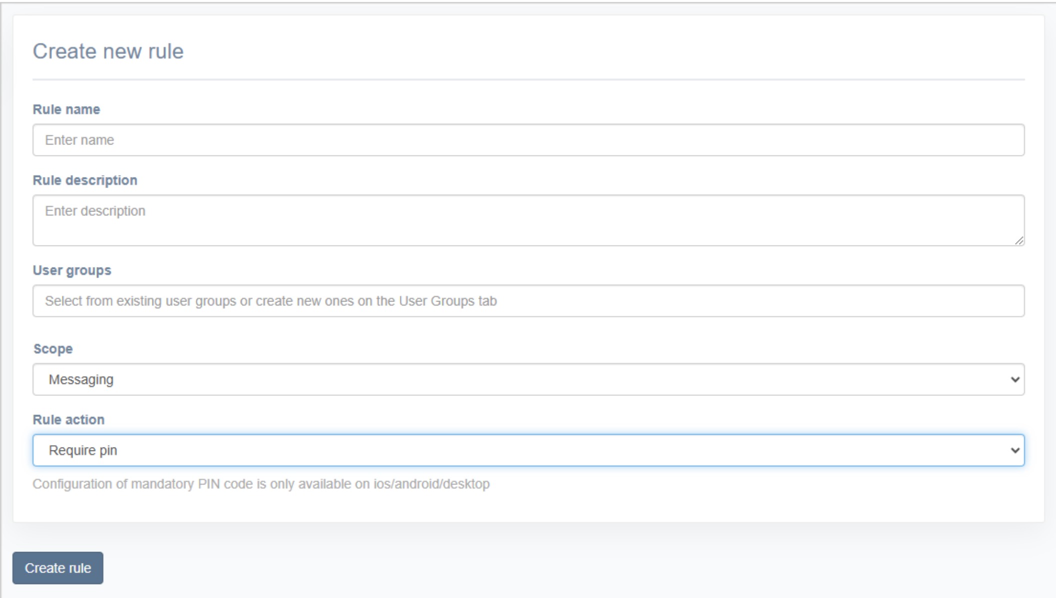


Figure 55

2. Fill in the fields of the form. Field values are shown in Table 23.

Table 23

Column name	Information
Rule name	Rule name (mandatory field)
Rule description	Description of the restriction action (maximum 1,000 characters)
User group	Select the user groups from the drop-down list (mandatory field)
Scope	Select the scope "In Messenger" from the drop-down list
Rule type	Select the rule type "Mandatory PIN code" from the drop-down list

Note. The rule for setting a mandatory PIN code applies only to iOS/Android/Desktop.

3. Click "Create Rule".

   The rule will be displayed in the list in the corresponding restrictions section (see Figure 52.).

COPYING RULES

To copy a rule:

1. Select a rule from the list and click .

   A window for creating a copy of the selected rule will open. The word "Copy" will be added to the beginning of the rule name (see Figure 56).

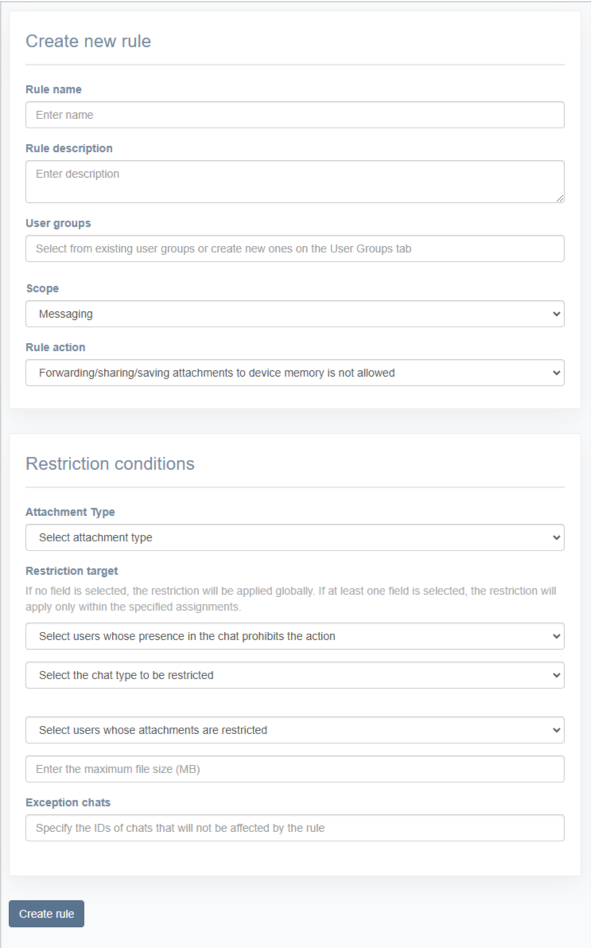


Figure 56

2. Make the necessary changes to the fields of the form.
3. Click "Save Rule" at the bottom of the form.

EDITING RULES

To edit a rule:

1. Select a rule from the list and click .

   The form for editing a previously created rule will open (see Figure 57).

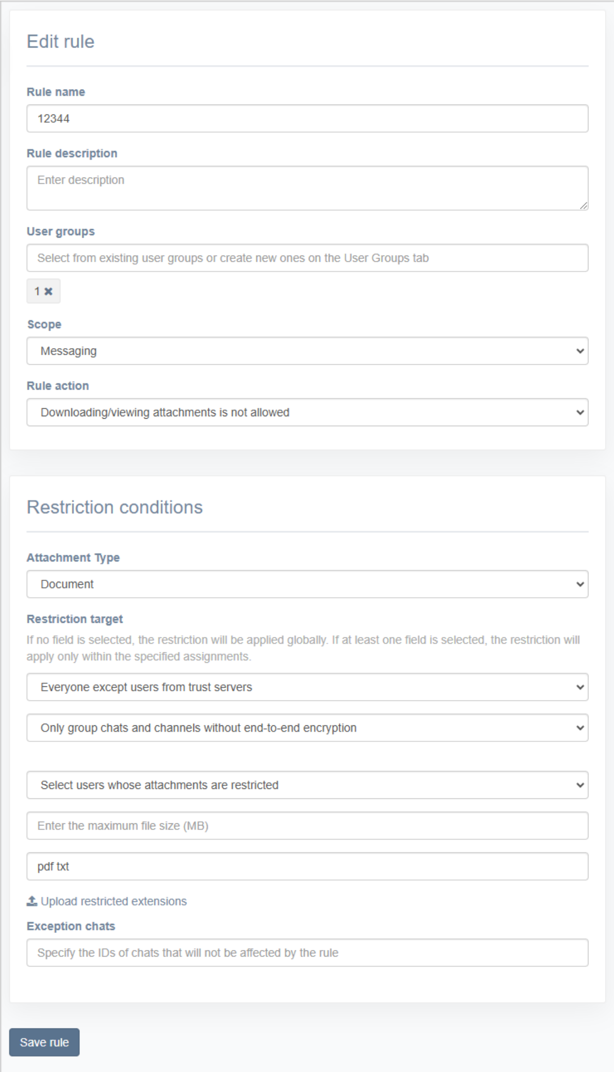


Figure 57

2. Make the necessary changes to the fields of the form.
3. Click “Save Rule” at the bottom of the form.

DELETING RULES

To delete a rule, select it from the list, click and confirm the action in the modal window that opens by clicking “OK”.

MANAGING ADMINISTRATOR ACCOUNTS

This section describes the following administrator web interface menu items:

- Administrators;
- Authentication of Administrators.

Administrator accounts are managed in the "Administrators" section. This section allows you to perform the following operations:

- create administrator accounts;
- edit administrator account details;
- lock out administrator accounts;
- delete administrator accounts;
- create, edit and delete administrator groups;
- configure administrator group rights.

A complete list of administrators is provided in the "Administrators" menu item (see Figure 58).

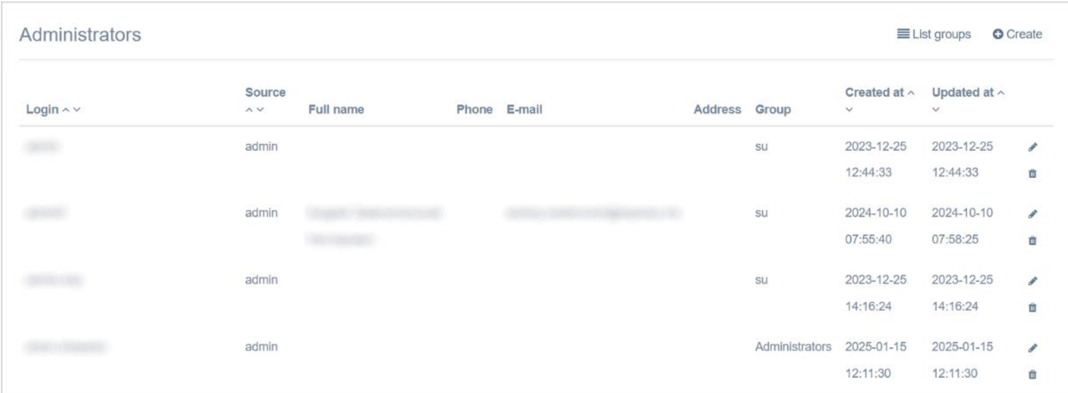


Figure 58

The table with the list of administrators contains the following information (see Table 24):

Table 24

Column name	Information
Login	The identification name of the account in Active Directory. Used when authorizing a user
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
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 web interface 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 manually:

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

   The "Add Administrator" window will open (Figure 59):

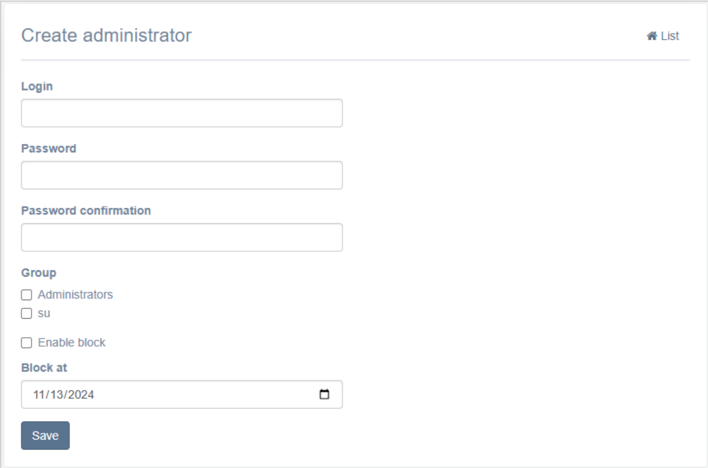


Figure 59

3. Fill in the fields of the form.

   In the "Group" block, select the groups that the created administrator account will belong to.
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 60).

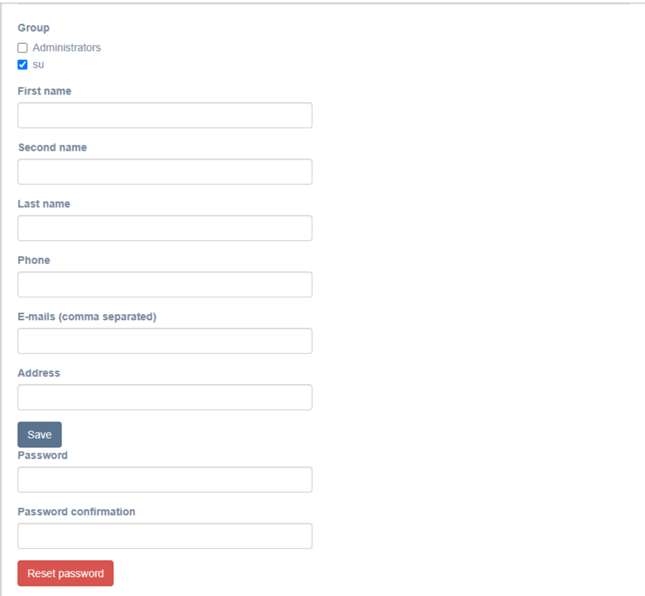


Figure 60

To set up loading of administrator accounts from AD:

1. Go to the "Administrator Authentication" section (see Figure 61).

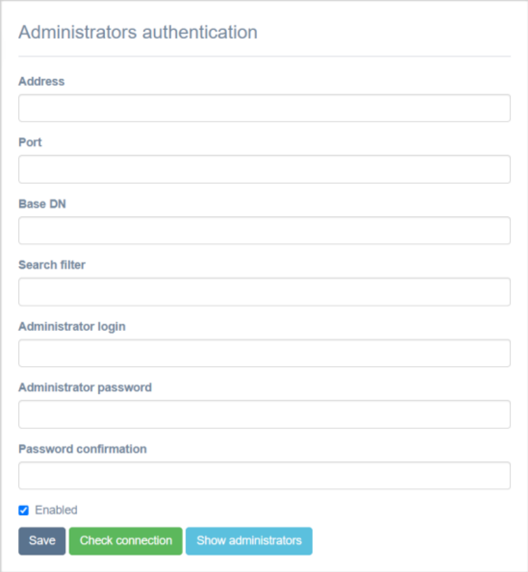


Figure 61

2. Configure the settings as shown in Table 25.

   The parameter values are provided by the Active Directory administrator.

Table 25

Parameter	Description
Address	Active Directory address
Port	AD connection port
Base DN	Directory object from which the search is performed
Search filter	Filter for searching in Active Directory
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 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 all groups and their rights – "Groups" (Figure 62):

Figure 62

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

A window for creating a group and setting its rights will open (Figure 63):

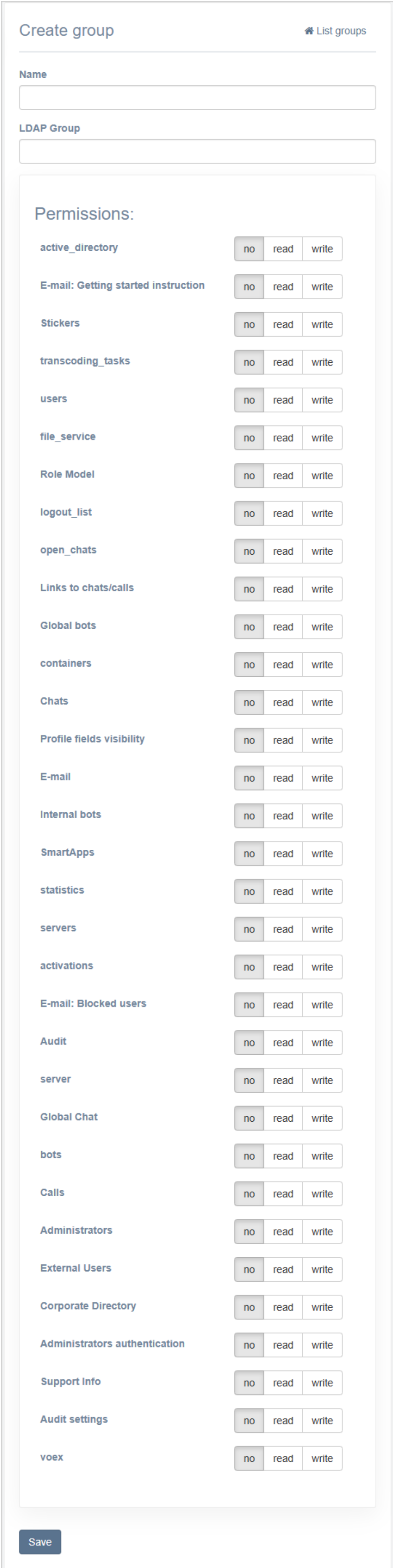


Figure 63

The rights buttons have the following meanings:

- 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.

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

The list of administrator rights is presented in Table 26.

Table 26

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
Audit	No access to the section	Viewing audit events	Viewing audit events
E-mail: Instructions to Get Started	No access to the section	Viewing the instructions to get started with the application. Testing e-mail sending	Changing the instruction to start working with the application. Enable/disable the e-mail sending function. Testing e-mail sending
Links to chats/calls	No access to the section	Viewing settings: • links host; • access type	Changing settings: • links host; • access type. Enabling/disabling the ability to generate links for guest users.
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
Call Recording	No access to the section	Enabling a filter by record type: • "All records"; • "Records with error"; • "Completed recordings" • "Recordings in process". Call search by name or ID	Enabling a filter by record type: • "All records"; • "Records with error"; • "Completed recordings" • "Recordings in process". Call search by name or ID
Stickers	No access to the section	View information about sticker packs	Creating, deleting sticker packs Managing sticker packs settings

Menu item name	Rights		
	NO	READ	WRITE
Internal Bots	No access to the section	Viewing the list of internal bots	Changing and setting up internal bot Adding a bot administrator
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 bot 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
Calls	No access to the section	Viewing: • viewing the list of calls and conferences; • viewing information about the chat in which the call was made; • viewing information about the call; • downloading a call, conference log	Terminating a call, conference Deleting all call logs
SmartApps	No access to the section	Viewing SmartApp settings	Changing SmartApp display settings in the main menu
Chats	No access to the section	Viewing: • the list of chats; • chat users	Converting a closed chat to an open chat. Adding users to chat
Support Contacts	No access to the section	Viewing attached files	Viewing and editing attached files
Global Chat	No access to the section	Viewing global chat settings	Enabling and disabling global chat. Setting Up Global Chat Settings
Authentication of Administrators	No access to the section	Viewing administrator authentication settings	Changing administrator authentication settings
Setting up Web and Desktop clients menus	No access to the section	Viewing menu configuration settings for web and desktop applications	Changing menu configuration settings for web and desktop applications
Logout Requests	No access to the section	Viewing the list of user logout requests	Accepting and rejecting user logout requests
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
Role Model	No access to the section	Viewing the list of rules	Creating, editing, copying, and deleting a rule. Changing the status of a rule. Enabling/disabling the role model

Menu item name	Rights		
	NO	**READ**	**WRITE**
Open Chats	No access to the section	Viewing information about open chats and channels	Creating an open chat. Deleting an open chat. Adding contacts to chat. Conversion: • open chat to closed chat; • closed chat to open chat Granting/removing administrator rights from a user
Users of external systems	Item under development		
Statistics	No access to the section	Viewing application performance statistics	Viewing application performance statistics
Active Directory	No access to the section	Viewing AD connection settings	Changing AD settings: • Connections to AD; • user registration – via SMS/e-mail
Servers	No access to the section	Viewing configured trusts	Connecting and changing trust settings
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
Mobile client menu configuration	No access to the section	View of mobile application menu configuration settings	Change of mobile application menu configuration settings
Containers	No access to the section	Viewing Docker containers lists and logs	Viewing Docker containers lists and logs
Corporate directory	No access to the section	View a list of open corporate chats, channels and chatbots	Managing the display of the chat directory "showcase": sorting the list of open corporate chats, channels and chatbots
VoEx	No access to the section	Viewing TURN server settings	Changing TURN server settings
Bots	No access to the section	Viewing the list of bots	Creating, editing and deleting chatbots
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	Create an account. Changing an account created in the administrator web interface. Deleting an account created in the administrator web interface, or if a logout request has been accepted
Administrators	No access to the section	Viewing: • list of administrators; • administrator groups	Creating, editing and deleting administrators. Setting Up Administrator Rights
Visibility of Profile Fields	No access to the section	Viewing data access settings in a corporate server user profile	Setting up data access levels in a corporate server user profile
E-mail: Locked Out Users	No access to the section	Viewing user lockout notification Testing e-mail sending	Changing user lockout notification. Enable/disable the notification sending function. Testing e-mail sending

Menu item name	Rights		
	NO	**READ**	**WRITE**
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
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

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

EDITING ADMINISTRATORS

There are two ways to edit the administrator account.

FIRST METHOD

To edit the administrator account:

1. Select the “Administrators” menu item.
2. Click opposite the account name.

   A window with administrator profile settings will open (Figure 64):

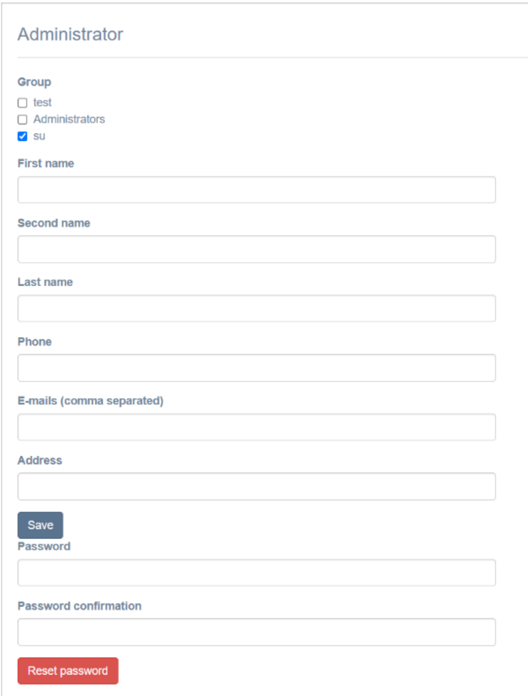


Figure 64

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 65).

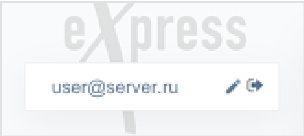


Figure 65

If "write" is set in the "Administrators" item of the administrator rights settings, the window with the administrator profile settings (Figure 64) 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 66.).

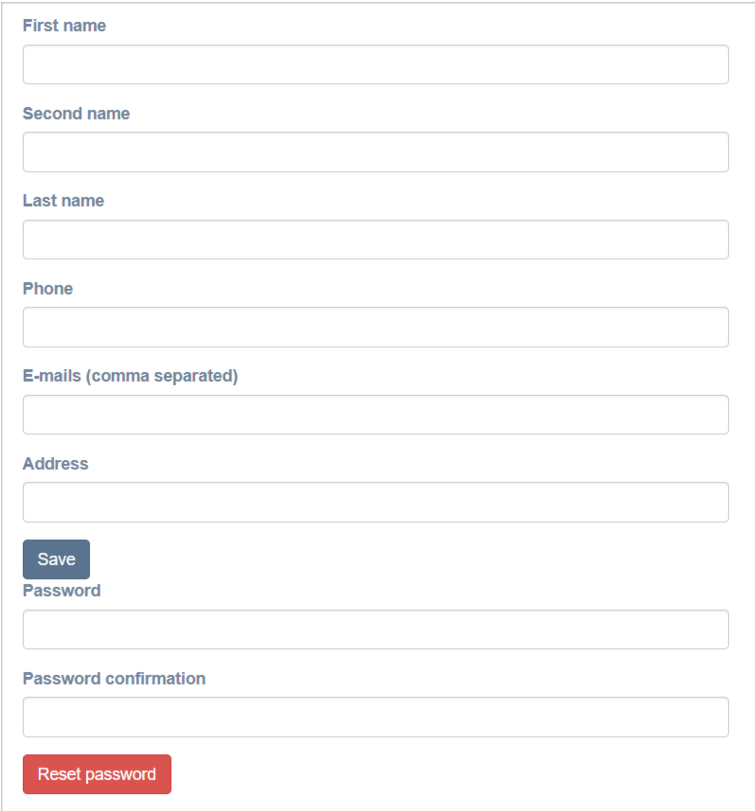


Figure 66.

2. Make the necessary changes to the fields.
3. Click "Save".

LOCKING OUT ADMINISTRATOR ACCOUNTS

To lock out an administrator account:

1. Select the "Administrators" menu item.
2. Click opposite the account name.
   A window with administrator profile settings will open.
3. Click on the "Lockout on" field.
4. Select the lockout date from the calendar (Figure 67):

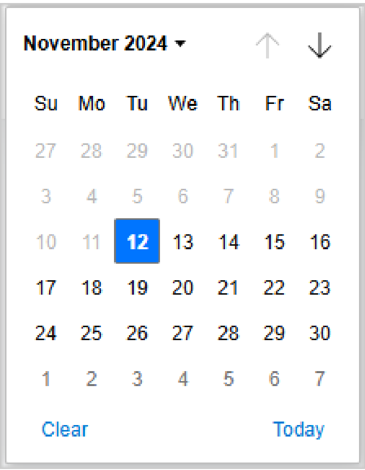


Figure 67

5. Click "Lockout".

   The operation confirmation modal window will open.

6. Confirm the action by clicking the "Yes" button.

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

To change the administrator account lockout settings:

1. Select the "Administrators" menu item.
2. Click opposite the account name.

   A window with administrator profile settings will open.

3. Select a date in the "Lockout on" field and click "Lockout".

   The operation confirmation modal window will open.

4. Confirm the action by clicking the "Yes" button.
5. Click "Save".

   The created account will be displayed in the table.

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

To unlock a locked out administrator account, click "Unlock" (Figure 68) and confirm the action in the modal window that opens by clicking "Yes".

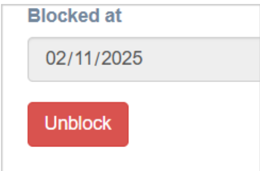


Figure 68

REMOVING ADMINISTRATORS

To remove the administrator account:

1. Go to the list of administrators.
2. Click to the right of the corresponding account.
3. Confirm the action in the model window that opens by clicking "OK".

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

CALL AND CONFERENCE MANAGEMENT

This section describes the following administrator web interface menu items:

- Calls;
- Conferences;
- Call Quality Ratings;
- Call Recordings;
- Links to Chats and Calls.

The “Calls” and “Conferences” sections contain lists of calls and conferences (see Figure 69 and Figure 70). Calls and conferences are displayed in reverse chronological order.

The following actions are available in the administrator web interface of the corporate server:

- managing conferences and calls (searching, terminating, downloading logs and member lists, clearing logs, etc.);
- setting up call and conference recording;
- setting up links to Chats and Calls;
- setting up call quality ratings.

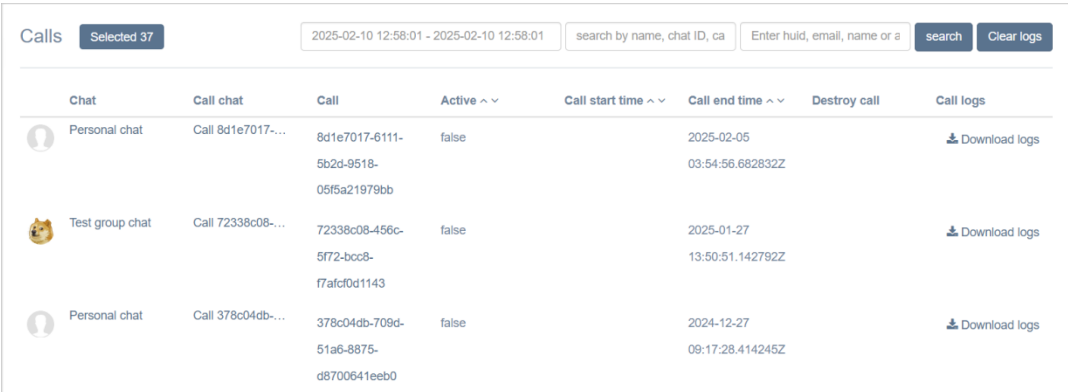


Figure 69

The “Calls” table contains the following information (Table 27):

Table 27

Column name	Information
Chat	The name of the chat in which the call is made
Call chat	Call chat ID
Call	Call ID
Active	Call status
Call start	Date and time of call start
Call termination	Date and time of call termination
Terminate call	The call termination option is available, if the call has not been terminated yet
Call logs	Downloading call logs is available

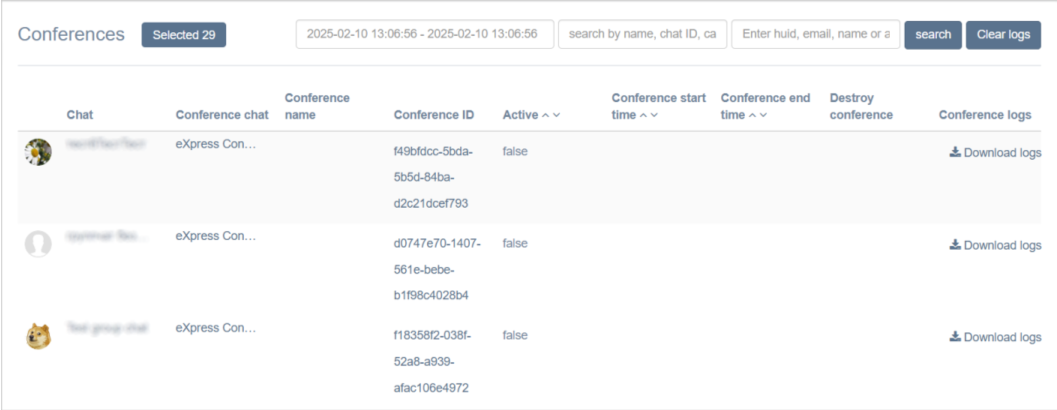


Figure 70

The "Conferences" table contains the following information (Table 28):

Table 28

Column name	Information
Chat	The name of the chat in which the user started the conference
Conference chat	The conference chat name that is displayed in the application
Conference title	The conference name that is displayed in the application
Conference ID	Conference identification number
Active	Conference status
Conference start	Date and time of conference start
Conference end	Date and time of conference termination
Terminate conference	The conference termination option is available, if the conference has not been terminated yet
Conference logs	Downloading call logs is available

CALL AND CONFERENCE MANAGEMENT

Available operations:

- terminating current call/conference;
- setting up the rating filter;;
- searching for a call/conference;
- downloading the log;
- deleting the log;
- exporting the list of participants.

To terminate the current call/conference

1. Click ×.

   A modal window will open.

2. Click "OK" in the modal window that opens.

The name of the chat or conference is a hyperlink to a window with detailed information about the conference or chat in which the call is made (see Figure 71.).

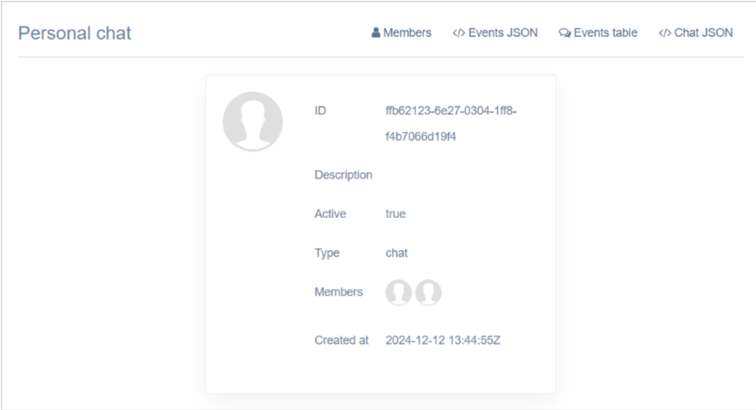


Figure 71.

The call ID is a hyperlink to a window with information about the call (see Figure 72.).

Figure 72.

Information about call events and call participants is viewed in the same way as in the "Chats" section — see page 88.

The user can rate the quality of the call or conference by receiving a corresponding request at the end of the conversation. The administrator can configure user rating filter (for more information on setting up call/conference rating feature, see page 34).

To search for a call, enter its name or ID, e-mail or HUID (in full or in part) in the corresponding search bar and click "Search" (see Figure 69).

To search for a conference, enter its name, ID, e-mail or HUID (in whole or in part) in the appropriate search box and click "Search" (Figure 70).

To download the call or conference log, click "Download Logs" in the call/conference line (see Figure 69 and Figure 70). The log will be exported to a TXT format (see Figure 73).

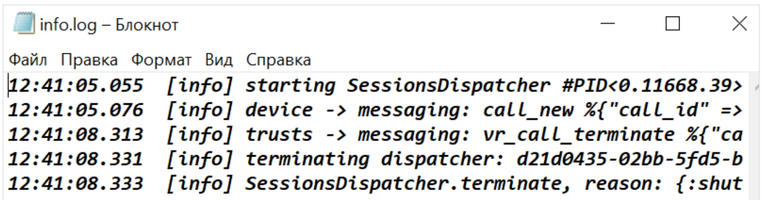


Figure 73

To delete all call and conference logs, click "Clear Logs" in the upper right corner (see Figure 69 and Figure 70).

The message "Logs cleared" will be displayed in the window header (see Figure 74).

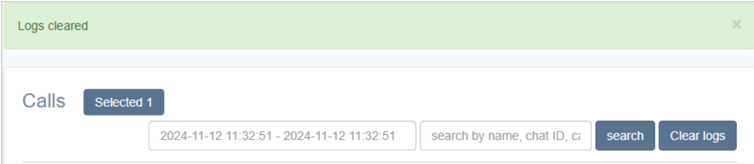


Figure 74

If all logs are deleted, when you click "Download Logs", a notification will be displayed saying "No logs for call <call ID> are available" (see Figure 75).

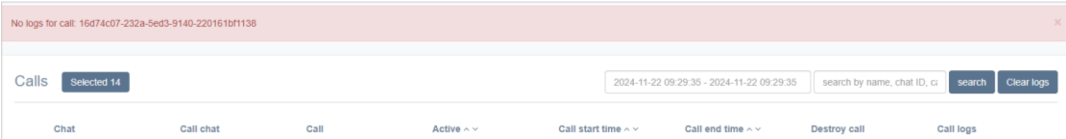


Figure 75

To export the list of chat participants in the CSV format, click "Users" in the chat window. In the window that opens, click

.

SETTING UP CALL AND CONFERENCE RECORDING

To set up videoconferencing recording, you need to:

- Install recording components (see the document "Administrator's Guide. Installation", section "Installing call and conference recording components");
- enable and configure Recordings Bot;
- configure the recording mode;
- configure the records retention period.

SETTING UP RECORDINGS BOT

To set up Recordings Bot:

1. In the main menu of the CTS server administrator web interface, click on the "Internal Bots" item.

   The "Internal Bots" window will open (see Figure 76):

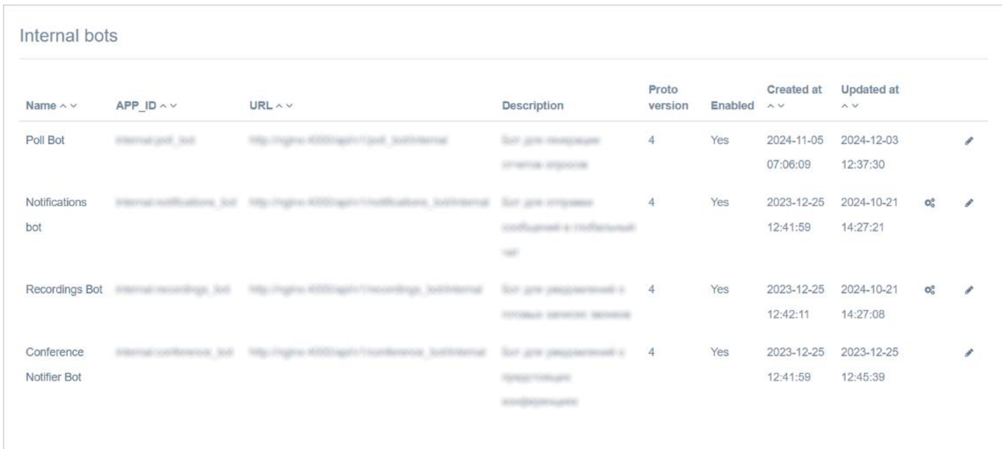


Figure 76

2. In the “Recordings Bot” line, click .

   The “Edit Bot” window will open (see Figure 77):

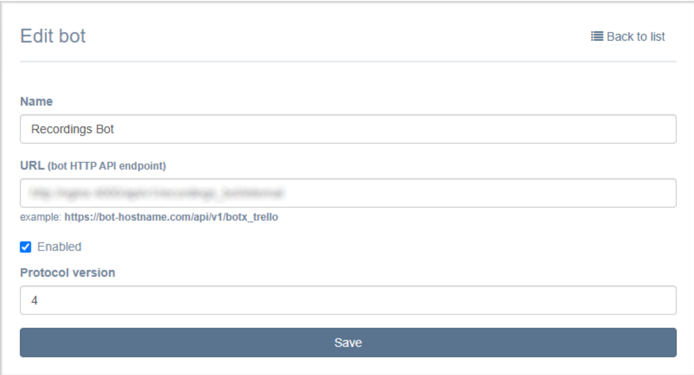


Figure 77

3. Check the “Enabled” box and click “Save”.
4. In the “Recordings Bot” line, click .
5. The “Configure Recordings Bot” window will open (see Figure 78):

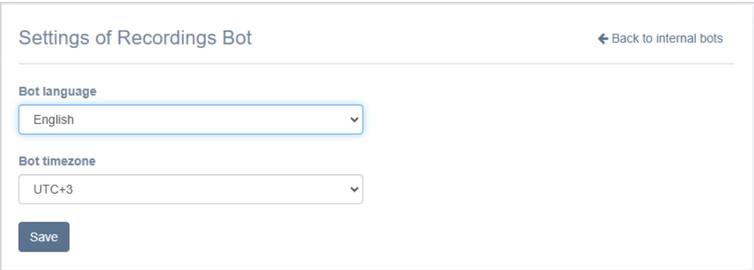


Figure 78

6. In the “Bot Language” list, select the language for the bot's messages.
7. In the “Bot time zone” list, select the time zone that will be indicated in the bot's messages.
8. Click “Save”.

SETTING UP RECORDING MODE

To set up the recording mode:

1. In the main menu of the CTS server administrator web interface, click on the “VoEx” item.
2. In the “VoEx” block, check the box “Enable the ability to record calls” (see Figure 79).

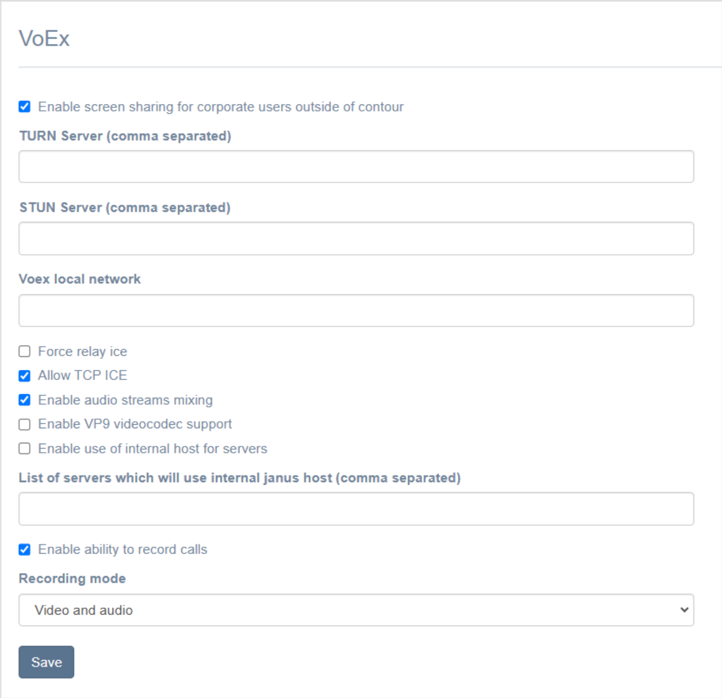


Figure 79

3. Click on the "Recording mode" drop-down list and select the required recording mode (see Table 29):

Table 29

Recording mode	Result
Video and audio	Two files are created: • an MP4 file — recording of video broadcast, screen sharing and sound from participants' microphones. If the screen is not displayed and/or no participant has turned on the camera, the video recording will show a black background with the names of the participants; • an MP3 file — a recording sound from participants' microphones
Screen sharing and audio	Two files are created: • an MP4 file — a recording of screen sharing and sound from participants' microphones. If the screen is not shared, the video recording will show a black background with the names of the participants; • an MP3 file — a recording sound from participants' microphones
Audio	Only an MP3 file is created — a recording of sound from participants' microphones

4. Click "Save".

CALL RECORDING

The section is a table in which the administrator can (see Figure 80):

- view the status of call and conference recording processing;
- configure the search filter;
- view the call recording page.

The list shows information about the processing status of terminated calls and conferences. Recordings of calls and conferences in progress are not displayed.

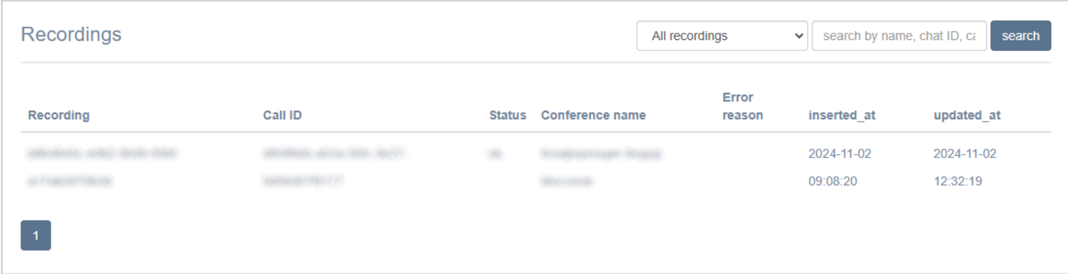


Figure 80

The table consists of the following columns (see Table 30):

Table 30

Column name	Information
Recording	Recording ID
Call ID	Call or conference ID (call_id)
Status	Recording status: • new. Recording is in the queue for processing; • in_progress. Recording is in the process of processing; • ok. Recording is ready; • error. An error occurred while processing the recording
Conference title	The name of the conference or the name of the group chat in which the call was made, or of the personal chat if it was a one-to-one call or a group call that was started as a one-to-one call
Error reason	Indicates the reason for the error of the transcoding service
inserted_at	Date and time of recording start
updated_at	Date and time of any change to the recording (ready or ready with an error)

To set the call/conference recording status filter

1. Select the desired recording parameters from the drop-down list.
   - "All records";
   - "Recordings with error";
   - "Completed recordings"
   - "Recordings in process".
2. Click "Search".

   A list of selected recordings will be displayed on the screen.

You can search for calls and conferences in the table using the search bar at the top of the window.

To search for a recording, enter its name or ID (in full or in part) in the search bar and click "Search".

To view information about a specific recording, select it from the list. A window with recording data will open (see Figure 81).

Figure 81

SETTING UP RECORDS RETENTION PERIOD

To set up the records retention period:

1. In the main menu of the CTS server administrator web interface, go to the "File Service" item.
2. In the "File Service Retention" block, in the "Call Recordings" field, specify the number of days during which files will be stored on the server (see Figure 82):

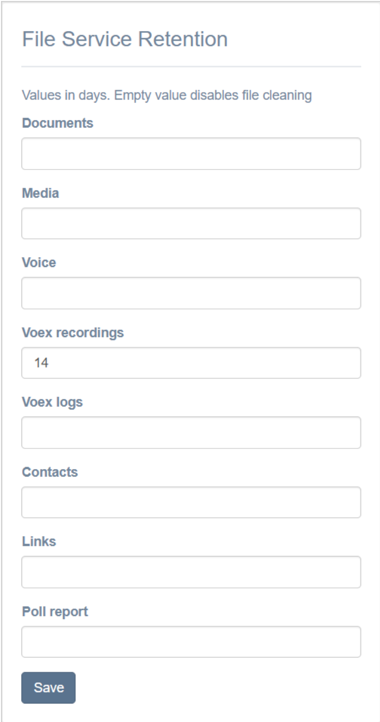


Figure 82

Note. If you leave this field blank, files will not be deleted from the server.

3. Click "Save".

CALL QUALITY RATINGS

The section is a table in which the administrator can:

- view call and conference ratings;
- configure the search filter;
- download call and conference logs.

Calls and conferences are displayed in reverse chronological order (see Figure 83.).

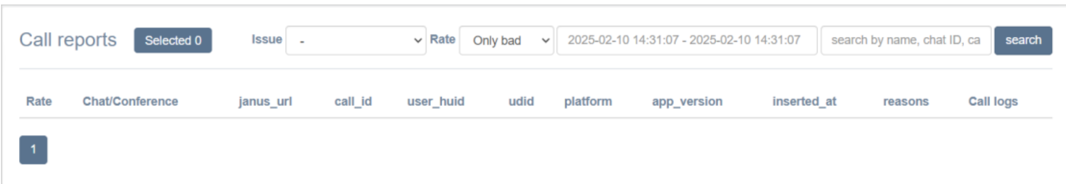


Figure 83.

The table contains the following information (see Table 31):

Table 31

Column name	Information
Rating	Rating types: • good — positive rating; • Bad — negative rating
Chat/Conference	Name of the chat/conference in which the call is made
Janus_url	Madia server address
Call_id	Call ID
User_huid	User ID
Udid	Device ID
Platform	The platform on which the call was made

Column name	Information
App_version	Application version
Inserted_at	Call time
Reasons	Reason for the poor grade. Some reasons are set automatically by the system. Types of reasons: • input_issue (issue with incoming audio); • output_issue (issue with outgoing audio); • poor_sound (poor audio quality); • poor_connection (issues with connection); • poor_video (issues with video); • poor_sharing (issues with screen sharing); • toggler_disabled (microphone/camera will not turn on (only web)); • user_disconnected (call disconnection); • other (other — enter a description of your problem in the call or conference); • webrtc (reason is submitted by the system without user participation. Reports network issues when establishing connections); • session (reason is submitted by the system without user participation. Reports issues with the session microservice); • domain (reason is sent by the system without user participation. Reports issues in the application server part that caused the call to close, or errors in sending call_offer, call_answer, vr_publish, vr_publish_audio, vr_unpublish, room_leave, call_terminate, room_join, call_new events)
Call logs	Downloading call logs

At the top of the window are buttons that can be used to set up the filter to display the necessary calls and conferences (Figure 83.).

To set up the user call/conference quality rating filter by Reason:

1. Select the desired rating parameter from the "Reason" drop-down list.
2. Click "Search".

   A list of calls and conferences in which the specified problem occurred will be displayed on the screen.

To set up the user call/conference quality rating filter by Rating:

1. Select the desired rating type from the "Rating" drop-down list.
2. Click "Search".

   A list of calls and conferences with the specified rating will be displayed on the screen.

To set the call/conference rating filter for a specific time interval:

1. Specify the time interval by clicking on the date filter box. In the window that opens, select the required values and click "Done".
2. Click "Search".

   A list of calls and conferences for a specific time interval will be displayed on the screen.

You can search for calls and conferences in the table using the search bar at the top of the window (see Figure 69 and Figure 70).

For details on setting the call quality rating, see section "Setting Up User Rating of Call or Conference Quality".

LINKS TO CHATS/CALLS

The "Chat/Call Links" section allows you to set up personalized links to join a closed chat, channel, video conference, or call (see Figure 84). Links of this type are shorter than standard links.

A standard link is a link, which has been generated based on a host (for example: https://xlink.ms).

A personalized link is a link generated based on the host specified by the administrator (for example: https://link.companyname.ru).

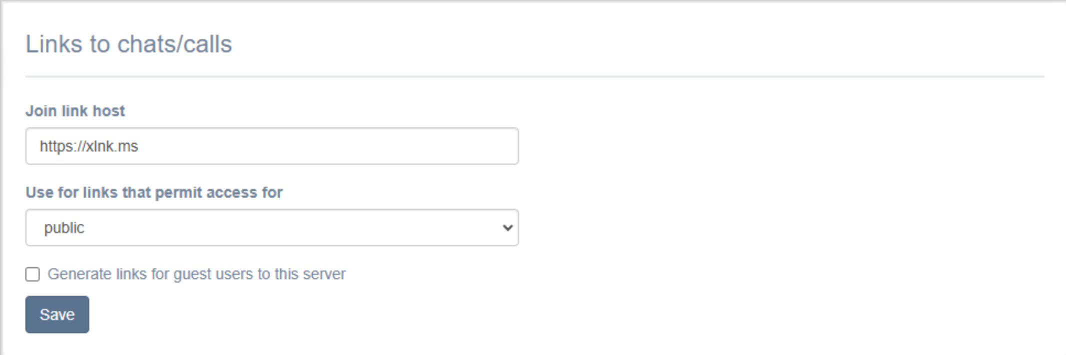


Figure 84

In the "Link Host" field, the administrator enters the address of the company's local link server. The default value of this field is https://xlink.ms.

In the "Use for links that allow access at least" drop-down list, the administrator selects one of the access levels for joining by link. The following values exist (see Table 32):

Table 32

Value	Access level
public (by default)	Unlimited access level. The link is available to everyone, including unregistered users.
corporate	Medium access level. The link is available to users from corporate servers
trusts	Limited access level. The link is available to users from the same server and trust servers

When clicking on a personalized link, the user is redirected to the link server. Users who do not have the application installed will first be redirected to the store to download and install the customer's corporate application.

Standard and personalized links are generated depending on the ratio of access levels set in the administrator web interface and in the application (see Table 33):

Table 33

<table>
<tr><th>Setting up access in the administrator web interface</th><th>Setting up access in the client application</th><th>Which link is generated</th></tr>
<tr><td rowspan="3">public</td><td>All users (including guests)</td><td rowspan="3">Personalized link</td></tr>
<tr><td>Any corporate server</td></tr>
<tr><td>Trusted corporate servers</td></tr>
<tr><td rowspan="3">corporate</td><td>All users (including guests)</td><td>Standard link</td></tr>
<tr><td>Any corporate server</td><td rowspan="2">Personalized link</td></tr>
<tr><td>Trusted corporate servers</td></tr>
<tr><td rowspan="3">trusts</td><td>Trusted corporate servers</td><td rowspan="2">Standard link</td></tr>
<tr><td>All users (including guests)</td></tr>
<tr><td>Any corporate server</td><td>Personalized link</td></tr>
</table>

Note. To generate a link for guests, check the box "Generate links for guest users to this server".

To set up the link:

1. Go to the "Chat/Call Links" section (see Figure 84).
2. In the "Link Host" field, enter the link service address.
3. In the "Use for links that allow access at least" drop-down list, select the desired link access level.
4. Click "Save".

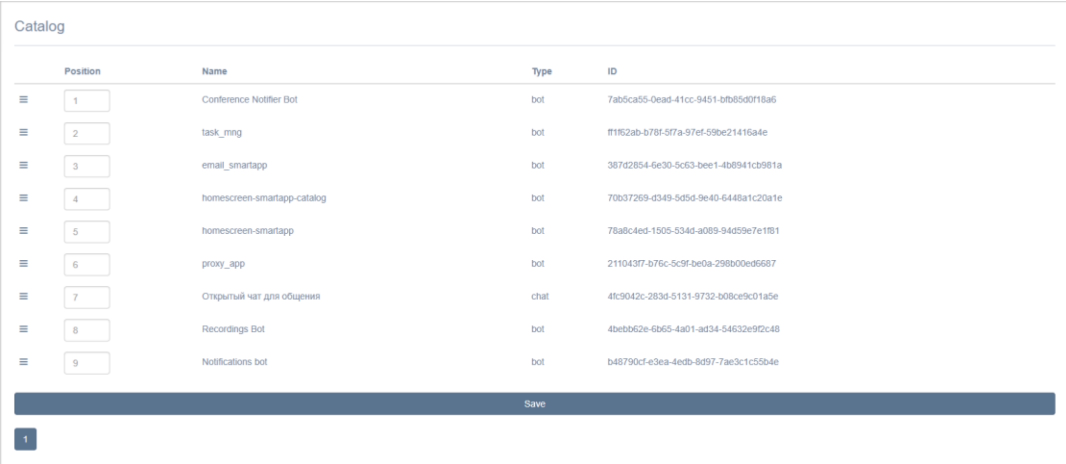
MANAGING CHATS

This section describes the following administrator web interface menu items:

- Catalog;
- Chats;
- Open Chats;
- Global Chat;
- Links to Chats and Calls.

CATALOG

Open corporate chats, channels and bots are displayed in the "Catalog" filter on the "Chats" page in Express CS. The list of chats, channels and bots is provided in the "Catalog" section of the administrator web interface (see Figure 85).


Catalog

Position	Name	Type	ID
1	Conference Notifier Bot	bot	7ab5ca55-0ead-41cc-9451-bfb85d0f18a6
2	task_mng	bot	ff1f62ab-b78f-5f7a-97ef-59be21416a4e
3	email_smartapp	bot	387d2854-6e30-5c63-bee1-4b8941cb981a
4	homescreen-smartapp-catalog	bot	70b37269-d349-5d5d-9e40-6448a1c20a1e
5	homescreen-smartapp	bot	78a8c4ed-1505-534d-a089-94d59e7e1f81
6	proxy_app	bot	211043f7-b76c-5c9f-be0a-298b00ed6687
7	Открытый чат для общения	chat	4fc9042c-283d-5131-9732-b08ce9c01a5e
8	Recordings Bot	bot	4bebb62e-6b65-4a01-ad34-54632e9f2c48
9	Notifications bot	bot	b48790cf-e3ea-4edb-8d97-7ae3c1c55b4e

Save

1

Figure 85

The table contains the following information (see Table 34):

Table 34

Column name	**Information**
Position	Position of the chat in the list on the "Catalog" tab
Name	Chat name
View	Chat type: • chat (chat); • group_chat (group chat); • channel (channel); • bot (chatbot)
ID	Chat ID

To change the position of a chat in the list:

- Click ≡ in the chat data line and drag it to a new position;
- enter the desired value in the "Position" field in the chat data line.

  The order in which chats are displayed on the user's device will change.

CHATS

Information about the app's chats is presented in the "Chats" section in the form of a table (see Figure 86).

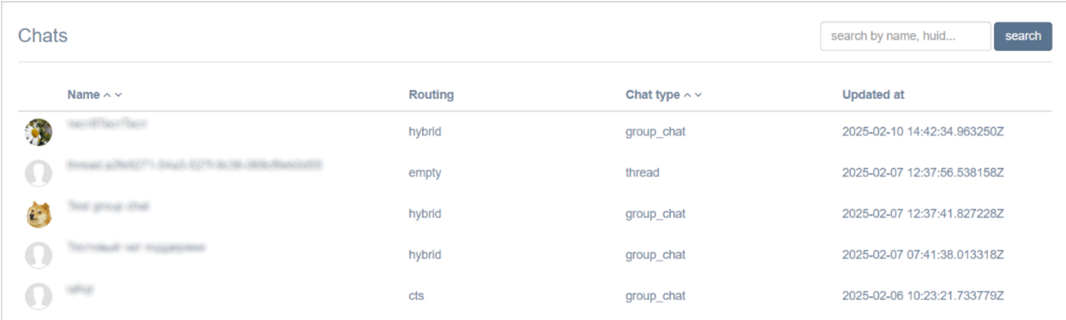


Figure 86

The table contains the following information (see Table 35):

Table 35

Column name	Information
Name	Chat name
Routing	Information about the server on which the chat was created: • cts (chat data is stored on the CTS server); • rts (chat data is stored on the RTS server); • hybrid (chat data is stored on the CTS RTS server)
Type	Chat type: • chat (chat); • group_chat (group chat); • channel (channel); • botx (chatbot)
Update date	Time of the last event in the chat (message, adding a user, etc.)

The chat name is a hyperlink to the chat window with detailed information about the chat (see Figure 87).

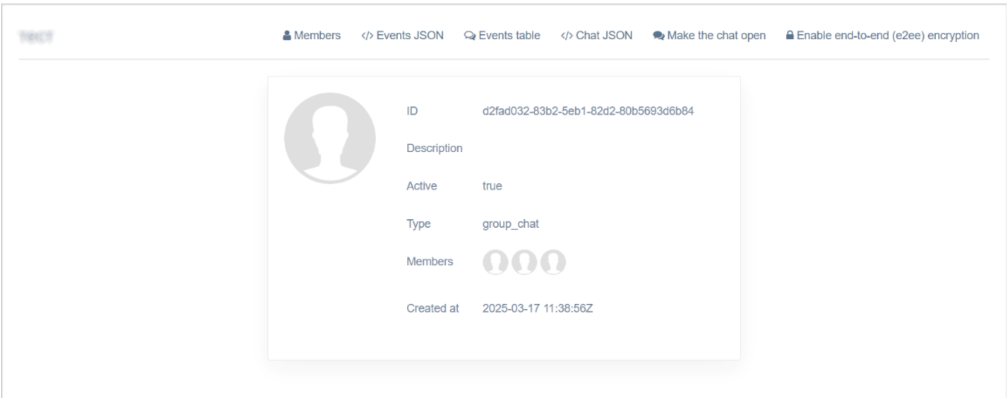


Figure 87

The information card contains: the chat avatar, its ID, description, status, type, chat participants and creation date.

The top part of the window contains the following buttons (see Table 36):

Table 36

Button	Purpose
Users	Transition to the chat participants list
JSON events	Displaying chat events in JSON format
Events table	Displaying chat events in the form of a table
JSON chat	Displaying chat in JSON format
Convert to open chat/Convert to closed chat	Convert group chat to closed/open

CHAT OPERATIONS

The following functionality is available to the administrator:

- viewing of chat events;
- viewing information about an event;
- viewing detailed information about chat participants;
- changing the user's status in chat;
- downloading chat participants list in the CSV format;
- adding a contact to the chat;
- adding a contact list from a file;
- deleting a contact from the chat.

To view chat events, click “Events Table”. A table will open containing information about chat events: message transmission, calls, adding/removing users (see Figure 88):

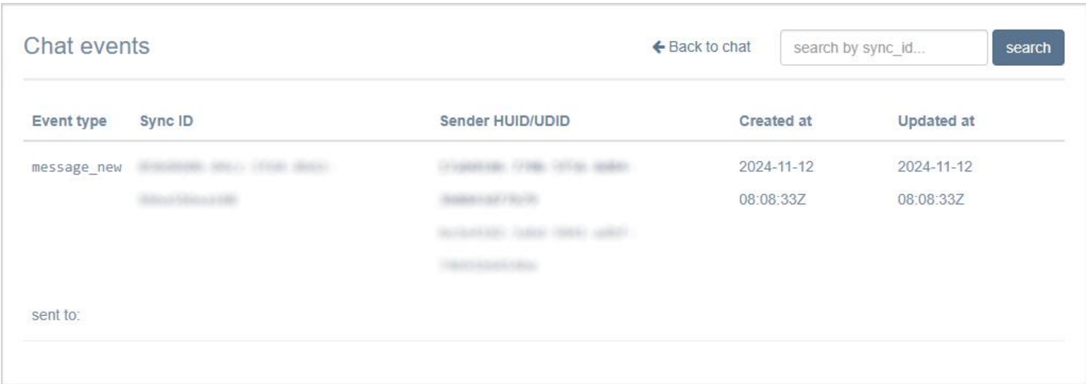


Figure 88

Note. Sender HUID/UDID are a hyperlink to the user profile.

The events table contains the following fields (see Table 37):

Table 37

Column	Purpose
Event type	Event types are shown in the table below
Sync ID	Event ID
Sender HUID/UDID	Sender ID

Column	Purpose
Creation date	Date and time of event
Update date	Date and time of event update

The list of chat event types is shown in Table 38.

Table 38

Event type	Value
chat_name_changed	Chat name has been changed
chat_description_changed	Chat description has been changed
chat_settings_changed	Chat settings have been changed
message_new	New message was sent in the chat
message_pinned	A message was pinned in the chat
message_unpinned	A message was unpinned in the chat
call_start	Call start
call_end	Call termination
routing_changed	The connection routing diagram has been changed
user_joined_to_chat	A user has joined the chat
left_from_chat	A user has left the chat
admin_added_to_chat	A user was assigned a chat administrator
added_to_chat	A user was added to the chat by the administrator
deleted_from_chat	A user was deleted from the chat by the administrator

To view information about the event, click on its Sync ID. A window will open (see Figure 89):

Figure 89

To view detailed information about chat participants, click "Users" on the toolbar.

A window will open with a list of chat participants in the form of a table (see Figure 90).

Figure 90

The table contains the following information (see Table 39):

Table 39

Column name	Information
Name	Contact name and avatar. A hyperlink that opens the user details window
Company name	The company the contact belongs to

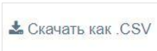
Column name	Information
HUID	Contact ID
Conn type	The server through which the message traffic goes
CTS endpoint	Server URL
Admin	Chat participant status: • true — the contact is the chat administrator; • false — the contact is not the chat administrator
Routing diagram	Hyperlink to the chat participants routing diagram

Important! Chat management has certain limitations. If there are users from different servers in the chat, the chat can be managed in the administrator web interface of only the server where the chat administrators are located. In the web interface of the administrator of other servers, the chat is only displayed in the general list of chats. If users of such a server are removed from the chat, it will no longer be displayed in the general list of chats.

To assign a chat administrator:

1. Open the "Chat Users" window.
2. Select the user with the value "false" in the "Admin" column.
3. Left click on the "false" value. In the modal window that appears, confirm the operation.
4. The "false" value will change to "true" and the user will be assigned as an administrator.

Note. To make a chat administrator a regular user, repeat the previous operation by changing the above value from "true" to "false".

To export the list of chat participants in the CSV format, click "Users" in the chat window. In the window that opens, click 

.

To add a contact to a chat, click "Add Users" in the upper right corner. In the window that opens, select a contact.

You can also import a list of users from a .CSV file.

To add a contact list from a file:

1. Click "Import Users" (see Figure 90).
2. In the window that opens, click "Select file" (see Figure 91).

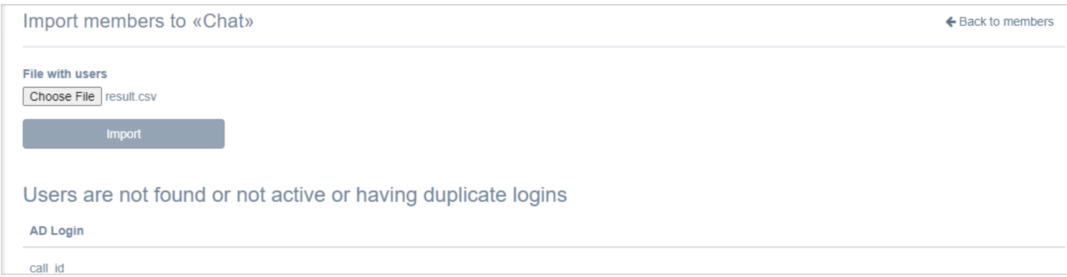


Figure 91

3. Select the file containing the user list from the file system.

   The system will search the server for users specified in the file by login and e-mail address. Login and e-mail must be unique. The user will not be added if:

   - the user was not found on the server;
   - multiple users were found with the specified login/e-mail.

To delete a contact from the chat, click 🗑.

OPEN CHATS

Information about open chats and channels is presented in the "Open Chats" section (see Figure 92). Only corporate chats can be open chats.

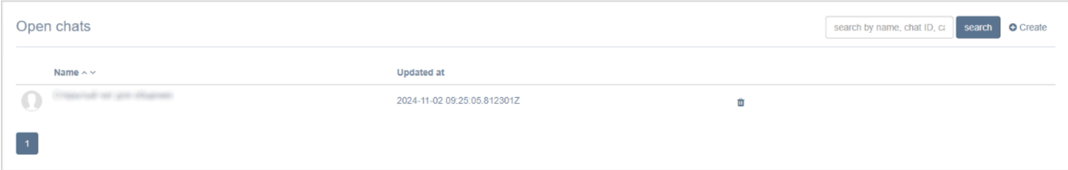


Figure 92

The chat name is a hyperlink that opens a chat window with detailed information. The "Update Date" column shows the time of the last event in the chat.

Information about chat events and chat participants is viewed in the same way as in the "Chats" section — see page 88.

Operations with open chat:

- creating a chat;
- changing the chat status;
- adding a contact;
- exporting the list of participants;
- assigning administrator;
- deleting a chat.

To create an open chat:

1. In the upper right corner of the "Open chats" section, click "Create".

   A window will open (see Figure 93):

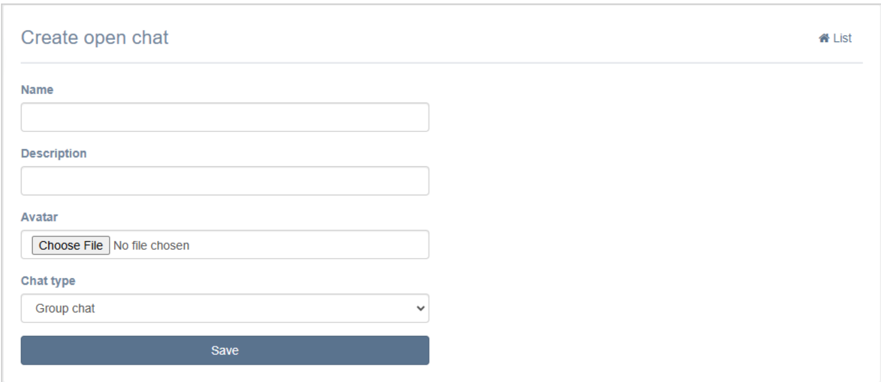


Figure 93

2. Fill in the fields of the form (see Table 40):

Table 40

Field	Description
Name	Chat name
Description	A brief description of the chat, its purpose
Avatar	An image that will be used as the chat avatar
Chat type	Drop-down menu for choosing the type of chat: group chat or channel

3. Click “Save”.

   The chat will be displayed in the list of open chats and any user assigned to this server will be able to join it.

To change chat status to closed chat, open the chat window and click “Convert to closed chat” in the upper right corner.

To change the status of a closed chat to open chat, open the chat window and click “Convert to open chat”.

To add a contact to a chat:

1. In the chat window, click “Users”.
2. Click “Add Users” in the upper right corner.

   The “Users” window will open.
3. Click “+” to add a contact.

Note. The “Add Users” button will be displayed after at least one user has been added to the chat.

By default, every newly created chat is set to public.

To export the list of chat participants in the CSV format, click “Users” in the chat window. In the window that opens, click Download as .CSV.

To assign a chat administrator:

1. Click “Chat Users”.
2. Select the user with the value “false” in the “Admin” column.
3. Left click on the “false” value. In the modal window that appears, confirm the operation.

   The “false” value will change to “true” and the user will be assigned as an administrator.

To make a chat administrator a regular user, repeat the previous operation by changing the above value from “true” to “false”.

If the number of users joining the chat exceeds 256, the open chat goes into optimization mode.

In the optimization mode, the appearance of the window with detailed information about the chat changes (Figure 94.):

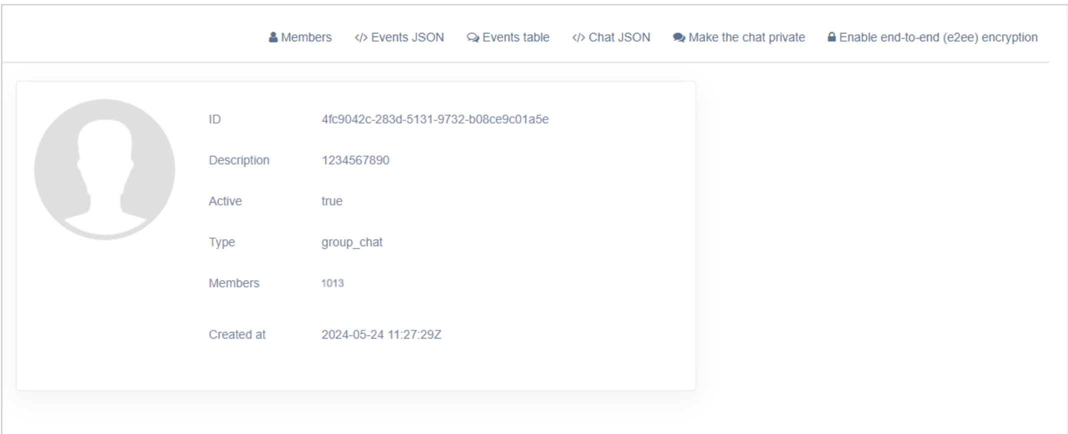


Figure 94.

Instead of avatars of specific users, the total number of users who joined the chat is indicated.

Pagination is added to the chat participant list window: the previously single list of users is divided into pages.

The appearance of the routing diagram is changing: instead of avatars attached to servers, the total number of users on each involved server is shown.

To delete an open chat, click . The message "Open chat was deleted" will be displayed at the top of the window.

GLOBAL CHAT

Global chat (see Figure 95) is a system chat that allows you to send messages that are relevant to all users, for example:

- information about application 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 101).

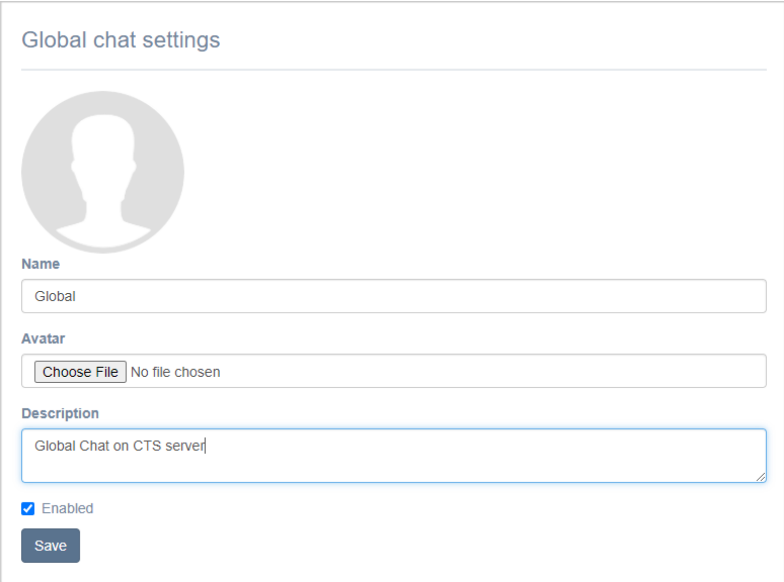


Figure 95

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".

LINKS TO CHATS/CALLS

The procedure for creating personalized links for joining a closed chat and channel is described above in the section "Links to Chats/Calls".

CHATBOTS AND SMARTAPP

This section describes the following administrator web interface menu items:

- Bots;
- Global Bots;
- Internal Bots;
- SmartApp.

CHATBOTS

All data about chatbots is presented in the "Bots" menu item in the form of a table (see Figure 96).

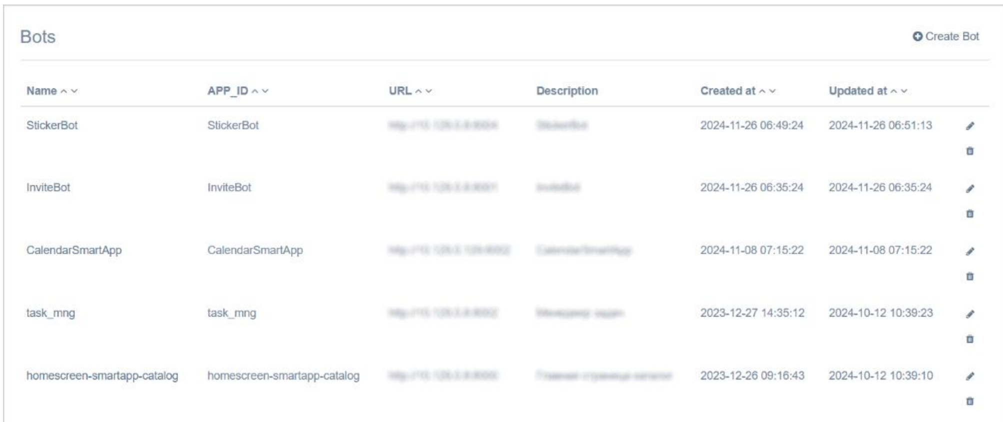


Figure 96

The table contains the following information (see Table 41):

Table 41

Column name	Information
Name	Chatbot name
APP_ID	Unique text identifier of the chatbot
URL	Link to the bot API
Description	Information that gives an idea of the purpose of the chatbot
Creation date	The date when the chatbot was connected
Update date	Date of last access to the chatbot

To edit chatbot information, click .

To delete a chatbot from the server, click .

CONNECTING A CHATBOT

To connect a chatbot:

1. To go the "Bots" menu item.
2. In the upper right corner, click "Create Bot".

   A window for entering parameters for a new bot will open (see Figure 97).

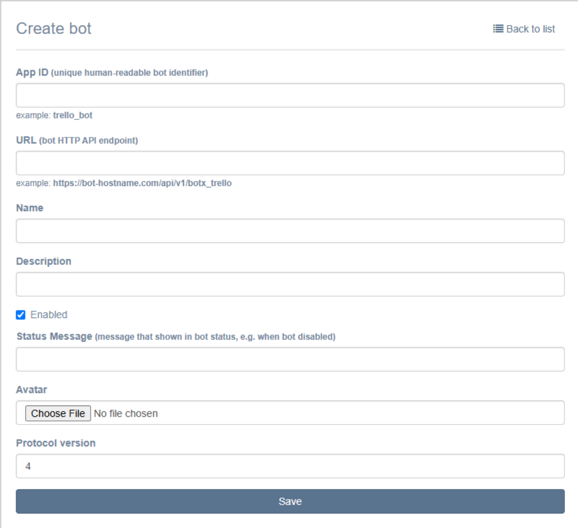


Figure 97

3. Fill in the fields of the settings (see Table 42).

Table 42

Field name	Information
Name	Chatbot name
APP_ID	Unique text identifier of the chatbot APP_ID must not contain spaces. Instead of spaces, it is permissible to use the underscore character "_".
URL	Link to the chatbot API
Description	Information that gives an idea of the purpose of the chatbot
Message`s status	The message that will be displayed on behalf of the administrator when a user accesses the chatbot. The chatbot must be disabled
Protocol version	The version of the BotX platform code used to send commands to the chatbot
Enabled	Enables/disables the chatbot

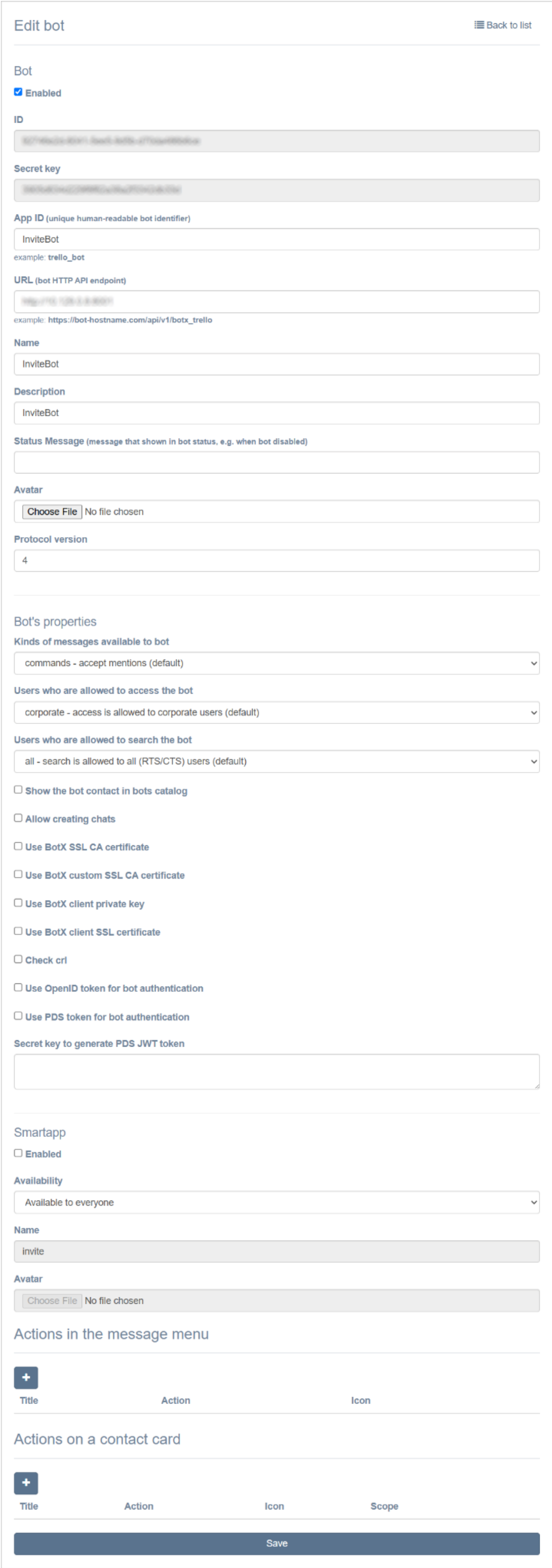
4. Click "Save".

CHANGING CHATBOT PARAMETERS

To change chatbot parameters:

1. Click on ✎ in the line of the chatbot that needs to be configured.

   A window will open (see Figure 98):



Edit bot
Back to list
Bot
Enabled
ID
Secret key
App ID (unique human-readable bot identifier)
InviteBot
example: trello_bot
URL (bot HTTP API endpoint)
example: https://bot-hostname.com/api/v1/botx_trello
Name
InviteBot
Description
InviteBot
Status Message (message that shown in bot status, e.g. when bot disabled)
Avatar
Choose File No file chosen
Protocol version
4
Bot's properties
Kinds of messages available to bot
commands - accept mentions (default)
Users who are allowed to access the bot
corporate - access is allowed to corporate users (default)
Users who are allowed to search the bot
all - search is allowed to all (RTS/CTS) users (default)
Show the bot contact in bots catalog
Allow creating chats
Use BotX SSL CA certificate
Use BotX custom SSL CA certificate
Use BotX client private key
Use BotX client SSL certificate
Check crl
Use OpenID token for bot authentication
Use PDS token for bot authentication
Secret key to generate PDS JWT token
Smartapp
Enabled
Availability
Available to everyone
Name
invite
Avatar
Choose File No file chosen
Actions in the message menu
Title
Action
Icon
Actions on a contact card
Title
Action
Icon
Scope
Save

Figure 98

Each chatbot has customizable settings (Table 43):

Table 43

Function name	Description
Message types available to the bot	Responsible for the types of messages that the chatbot accepts. Possible values: • all — the chatbot accepts all messages sent to the chat; • commands — the chatbot accepts a message if it is mentioned in the message; • none — chatbot does not accept any messages
Who is allowed to access the bot	Determines the types of users that are allowed to access the chatbot. Possible values: • all – access is granted to all (RTS/CTS) users; • corporate – access is granted to corporate users (default value); • trust – access is granted to corporate users from trusted servers; • local – access is granted to users from a local CTS server
Who is allowed to search for the bot	Determines the types of users who are allowed to access the chatbot search feature in the app. Possible values: • all – access is granted to all (RTS/CTS) users; • corporate – access is granted to corporate users (default value); • trust – access is granted to corporate users from trusted servers; • local – access is granted to users from a local CTS server
Show bot contact in bot channel	Display in the list of chatbots
Allow creating chats	Creation of chats by the chatbot
Use BotX SSL CA certificate	The chatbot uses a chain of SSL certificates from certification authorities that issued the bot's certificate. The SSL certificate data for the chatbot is entered in the "Server Settings" section (see page 25)
Use personal SSL CA BotX certificate	Using a separate SSL certificate from the CA that issued the bot's certificate
Use BotX client SSL private key	Uploading a file containing the private key of the client certificate, in order to ensure mTLS, when BotX accesses the bot
Use client SSL BotX certificate	Uploading a file containing the client certificate for mTLS purposes, when BotX accesses the bot
Check CRL	Checking the bot's certificate for its presence in the list of revoked certificates
Use OpenID token for bot authentication	Using OpenID token for bot authentication
Use PDS token for bot authentication	Electronic signing of documents using the PDS service
Secret key for generating JWT PDS token	PDS key

To activate the functions "Allow creating chats", "Show bot contact in bot channel", "Use BotX SSL CA certificate", "Use OpenID token for bot authentication"» and "Use PDS token for bot authentication", check the corresponding boxes.

To add a secret key for generating a JWT PDS token, enter it in the appropriate field.

To connect SmartApp, check the appropriate box, enter the chatbot name and select an avatar from the file system.

2. Click "Save".

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 99).

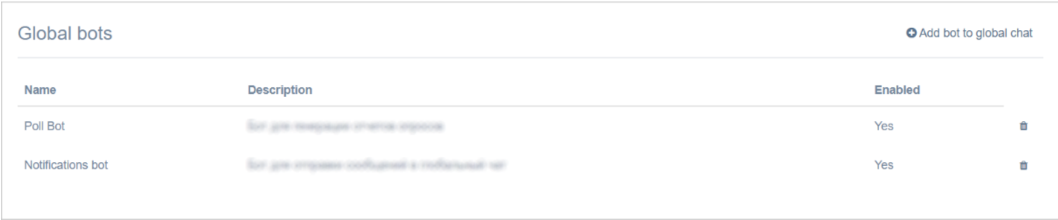


Figure 99

The table contains the following information (see Table 44):

Table 44

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.

   The list of global bots will open and the message "Bot added to global chat" will appear 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.

INTERNAL BOTS

Information about internal bots is provided in the "Internal Bots" subsection (Figure 100) of the administrator web interface.

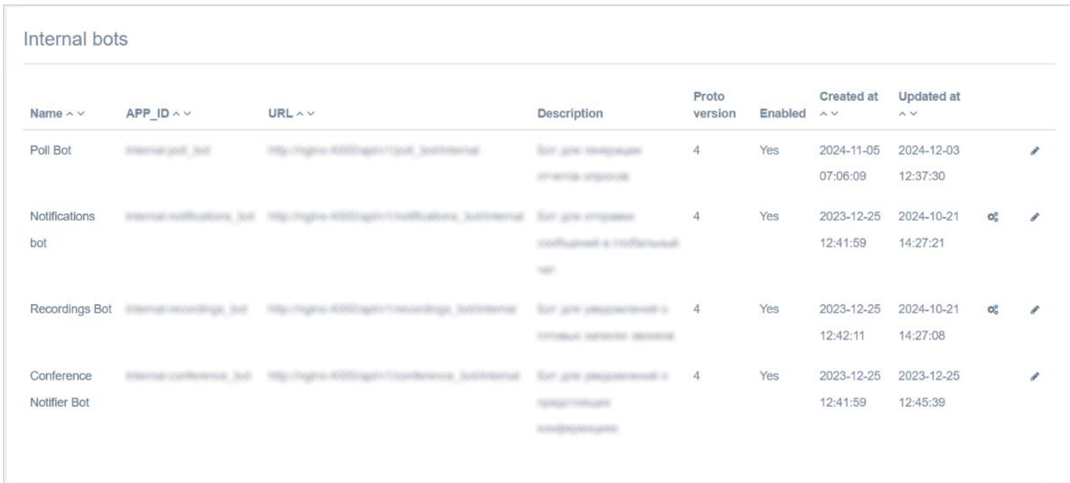


Figure 100

Internal bots are created automatically after the system is deployed.

The table contains the following information (see Table 45):

Table 45

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 101).

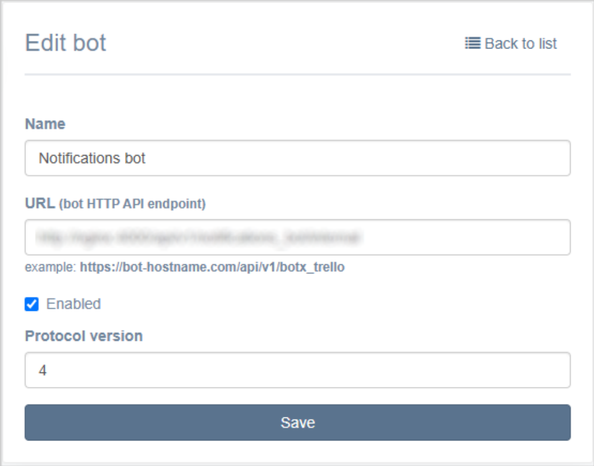


Figure 101

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 edit 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;
- 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.

To reset the time zone in Conference Bot for a particular user, go to the "Users" table of the conference_bot_prod database and indicate the value "null" for the required HUID in the "timezone" field.

To set the default timezone in Conference Bot, use the "DEFAULT_TIMEZONE" variable in the settings.yaml file on the server.

For example, to set the time zone to "Europe/Samara" add the value:

```
conference_bot_env_override:
  ...
  DEFAULT_TIMEZONE: Europe/Samara
  ...
```

Then run the command:

```
sudo dpl -d conference_bot
```

Note. Users who have already configured the time zone value in their application will not have their data changed. The configuration will only work for new users.

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 102) and click .

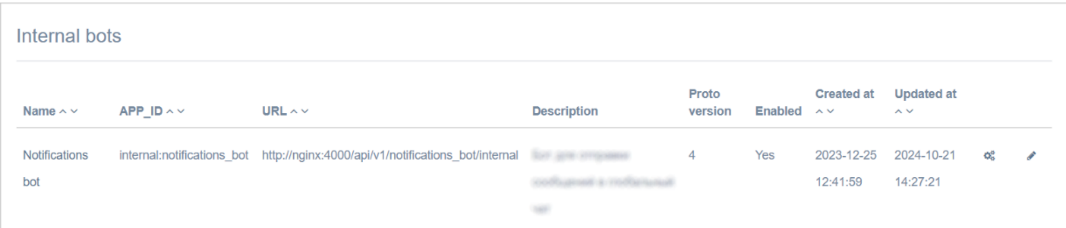


Figure 102

   The list of administrators will be displayed in the window that opens.
2. Click "Add Bot Administrator".

   In the list that opens, select the user who should receive administrator rights and click +.
3. The message "Administrator added" will be displayed at the top of the screen.

DESCRIPTION OF RECORDINGS BOT

Recordings Bot is designed to notify the user when a call or conference is ready to be recorded. Configuring Recordings Bot is described in the section "Configuring Call and Conference Recording".

DESCRIPTION OF POLL BOT

Poll Bot is designed to generate poll reports.

In order for the users to be able to create polls, Poll Bot must be enabled (see Figure 103).

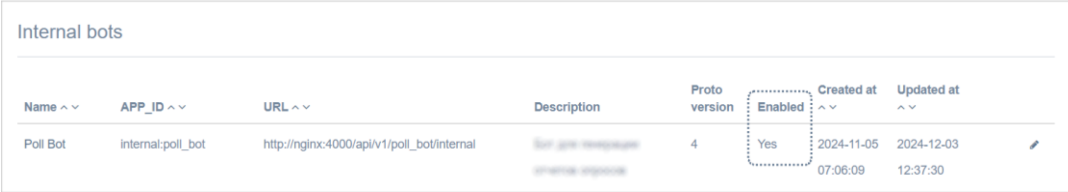


Figure 103

SMARTAPP

SmartApp is a web application, which is implemented as an add-on, executed inside Express, and designed for accessing corporate services and systems.

The "SmartApp" section consists of the following blocks:

- general settings in the "SmartApp" section;
- settings of SmartAppProxy hosts;
- mobile client menu configuration;
- setting up menu configuration for web and desktop apps.

SETTING UP THE DISPLAY IN THE MAIN MENU

The "SmartApp" block contains the following settings:

- enable/disable displaying the SmartApp item in the main menu of Express CS, which allows you to open a section with built-in web applications;
- options for the display of the "Main" (home page) and "Services" SmartApp items in the main menu (Figure 104);
- choosing SmartApp as the e-mail client.

> **Note.** Home page is the section that opens by default. The home page displays basic corporate information.

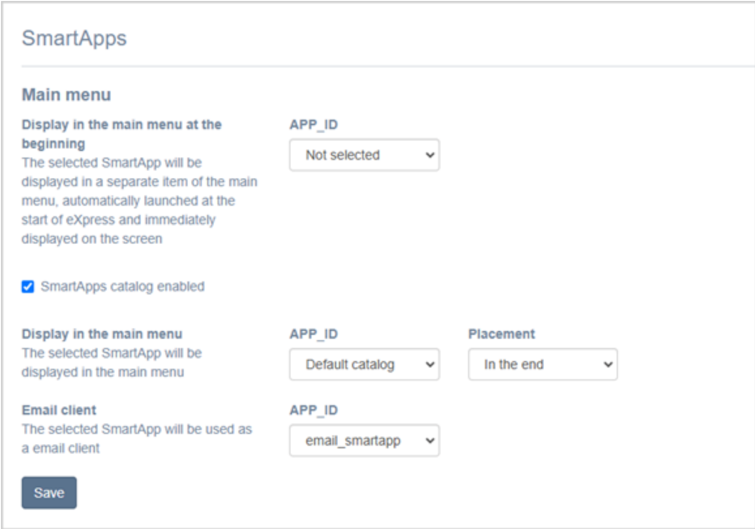


Figure 104

Clicking on the "APP_ID" field in the "Main Menu" section opens a list of all APP_ID bots (Figure 105). At the end of the APP_ID of bots that do not have SmartApp enabled in their settings, the suffix "Off" is displayed.

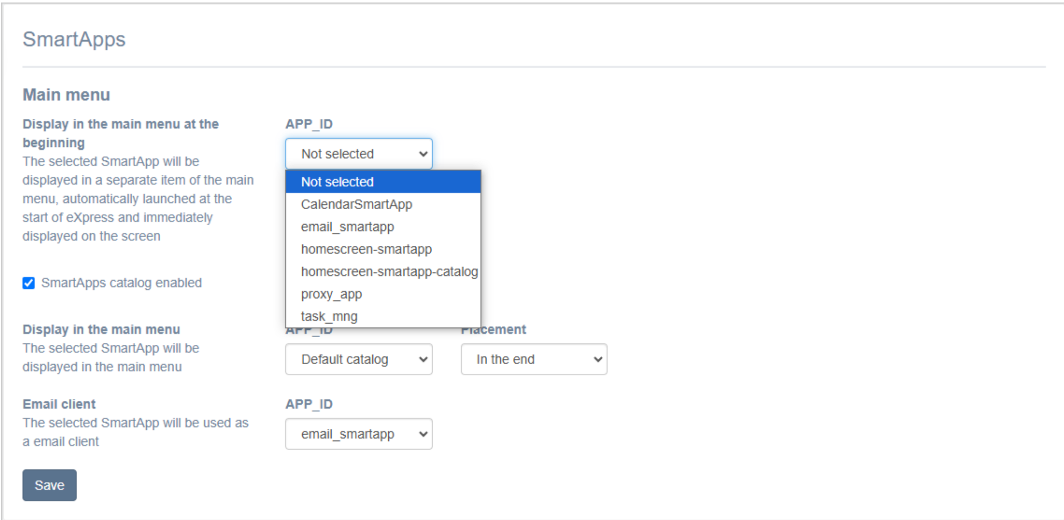


Figure 105

To set up the display of the SmartApp menu on user devices:

1. Check/uncheck the "SmartApp Catalog Enabled" checkbox to display the menu.

   On user devices, all enabled SmartApp are displayed in the menu by default.
2. To selectively display SmartApp, go to the "Bots" section.
3. Select the desired bot from the list and click ✎ in the line of the chatbot that needs to be configured (for more information on configuration, see "Changing Chatbot Parameters").
4. In the form that opens, go to the "SmartApp" block (see Figure 106).

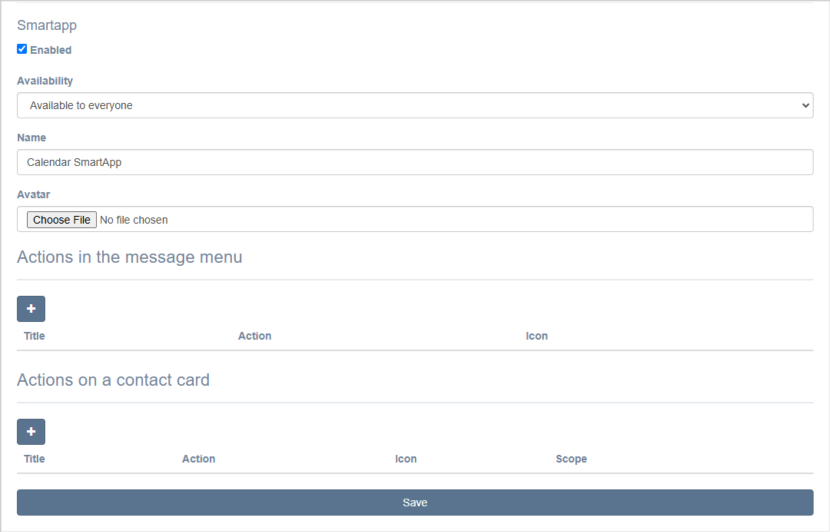


Figure 106

5. In the “Accessibility” field, select an access mode from the list.

Note. In the “Available to groups” mode, an additional field for specifying a user group will be displayed in the form. For more information about user groups, see “Operations with User Groups”.

In the “Available to all” mode, the enabled SmartApp will be displayed on all user devices. In the “Available to groups” mode, the enabled SmartApp will be displayed only for the specified user groups.

6. If necessary, enter the name of the group or leave the field blank.
7. Click “Save”.

To select a SmartApp that will be displayed in the first position in the main menu and on the Express CS start screen as the home page:

1. Click on the “APP_ID” field (see Figure 105).
2. Select the desired application from the drop-down list.
3. Click “Save”.

To set up the parameters of the SmartApp that will be displayed in the main menu:

1. Click on the “APP_ID” field (see Figure 105).
2. Select the desired application from the drop-down list.
3. Click on the “Location” field.
4. Select one of the following options (Table 46):

Table 46

Parameter	Value
In the end	The SmartApp icon is displayed last, after all the main menu items.
After the previous SmartApp	The SmartApp icon is displayed after the SmartApp item, which is displayed in the first position in the main menu.

5. Click “Save”.

A description of configuration of SmartApp parameters in the main menu of Express CS is shown below (Table 47 and Table 48):

Table 47

Display in the beginning of the main menu	**Result**
APP_ID: "Not selected"	No icon is displayed in the main menu; home page is opened as start page when Express CS is loaded
APP_ID: "APP_ID value"	The icon is displayed as the first item in the main menu; home page is opened as start page when Express CS is loaded

Table 48

Display in the main menu	**Location: "In the end"**	**Location: "After the previous SmartApp"**
APP_ID: "Not selected"	The icon is displayed as the last item in the main menu; clicking on the icon opens a list of enabled SmartApps	The icon is displayed as the second item in the main menu; clicking on the icon opens a list of enabled SmartApps
APP_ID: "APP_ID value"	The icon is displayed as the last item in the main menu; clicking on the icon opens a list of enabled SmartApps	The icon is displayed as the second item in the main menu; clicking on the icon opens the selected SmartApp

SETTING UP SMARTAPPPROXY HOSTS

If a file from the KSPD should become part of a SmartApp Frontend web page (for example, a video in the player), transmission of files through the File Service does not work. For this task, there is an option to transmit files via smartapp_proxy (see Figure 107).

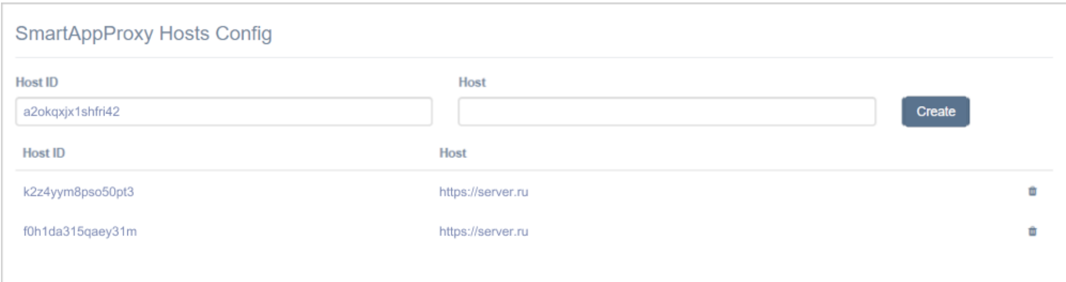


Figure 107

The configuration of SmartAppProxy hosts is described in Appendix 7 of the document "Volume 1. "Administrator's Guide. Installation".

MOBILE APPLICATION MENU CONFIGURATION

The "Mobile Client Menu" (Figure 108) section contains the following settings:

- "Mobile clients menu" (enable/disable the possibility to customize the menu of mobile apps via the administrator web interface);
- "Menu configuration" (configuring the parameters of displaying menu items in mobile apps).

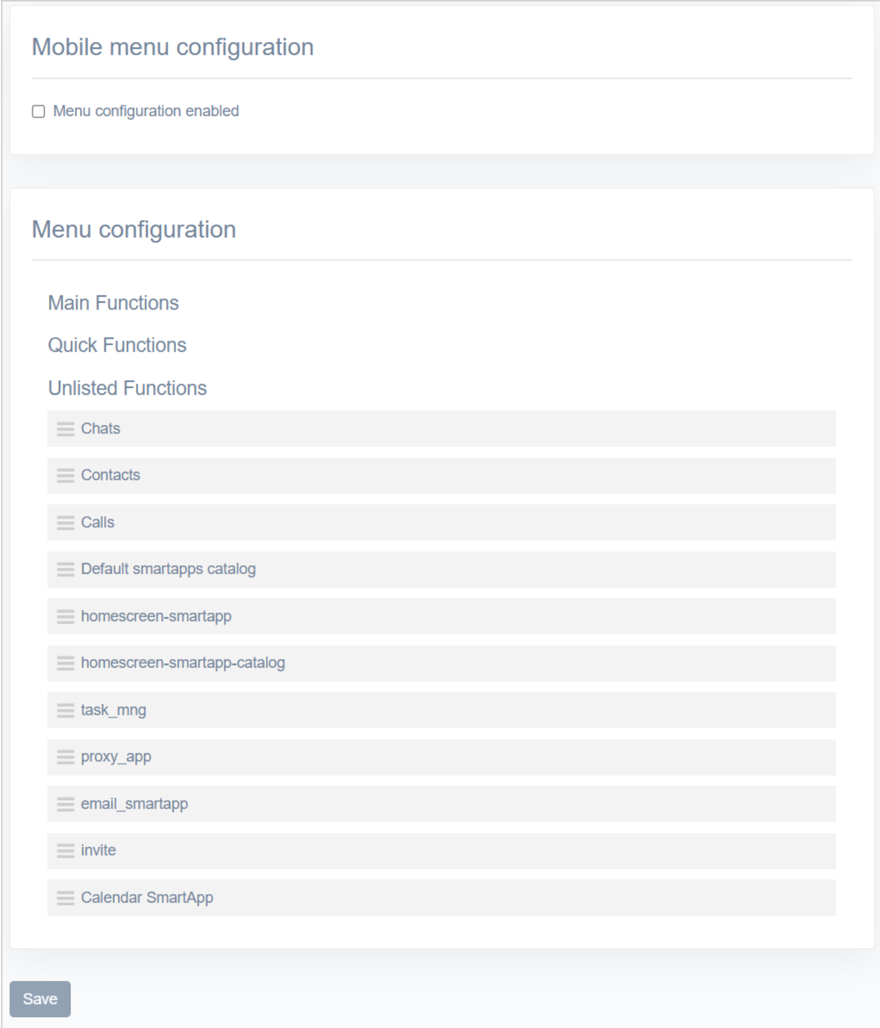


Figure 108

The SmartApp display settings in the eXpress mobile application are described below (Table 49):

Table 49

Block name	Value
Bottom navigation	SmartApp are displayed in the bottom menu of the eXpress mobile app. There must be at least two and no more than four items in a block
Quick Features	SmartApp are displayed in the "Quick Features" window of the mobile application
Unused functions	SmartApp are not displayed in the mobile app

To move a SmartApp , left-click the SmartApp name bar, hold, and drag it.

To pin SmartApp, check the "Pinned" box (Figure 108). Pinning an item imposes the following restrictions on mobile application users:

- they are always at the beginning of the SmartApp list;
- they can only be shifted among themselves.

If SmartApp is selected in the APP ID field, "Home" (Figure 108) appears next to its name in the "Menu configuration" block. The selected SmartApp will be displayed in the main menu and automatically started when the application is launched.

SETTING UP MENU CONFIGURATION FOR WEB AND DESKTOP APPS

The "Web and desktop client menu configuration" section (Figure 109) contains the following settings:

- "Web and Desktop client menu configuration" (enable/disable the possibility to customize the menu of web and desktop applications via the administrator web interface);
- "Menu configuration" (configuring the parameters of displaying menu items in web- and desktop applications).

The configuration of the menu of web and desktop applications is set up in the same way as mobile application menu configuration.

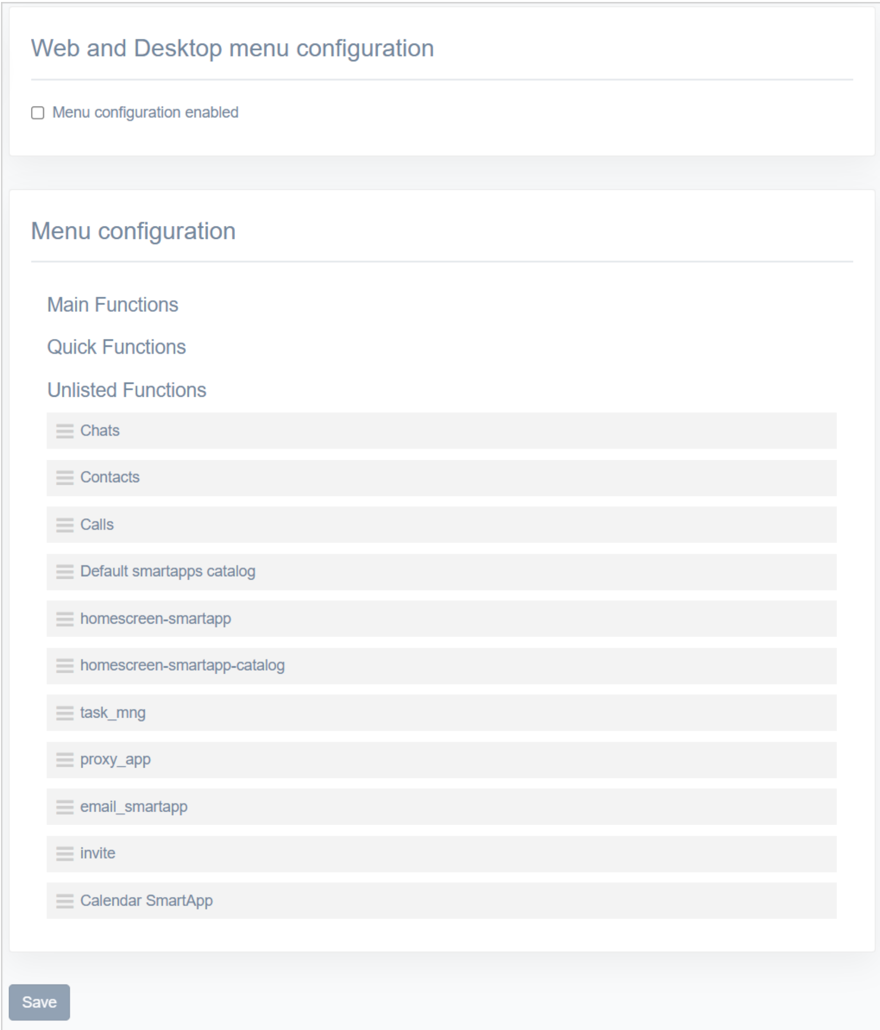


Figure 109

MANAGING FILE SERVICE

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

- access contour to files transmitted in chats;
- file storage periods;
- proxying when delivering static content.

SETTING UP DATA ACCESS CONTOUR

A user's access to sending or reading a file depends on their affiliation with the server, the CTN, and the contour (network IP address).

To set up access contour:

1. Go to the "File Service" section.
2. Check "Enabled" to enable access according to access contour.
3. Fill in the following fields (Figure 110, Table 50):

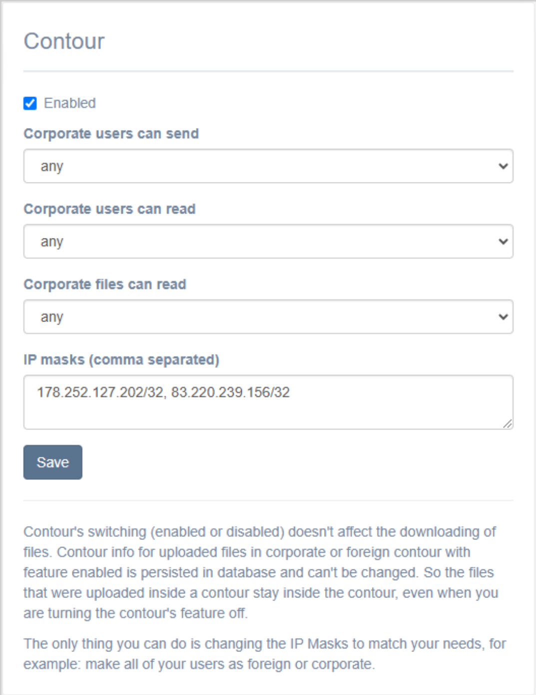


Figure 110

Table 50

Parameter	Value
mask IP (separated by commas)	IP address of the CTS server contour and subnet mask (separated by slash)
CTN users can send	Setting up file sending options. Possible values: • **any** — a CTN user can send files to a user from any server, but only the CTN user can open this file; • **corporate** — a CTN user can send files to a user from the CTS server of his organization, but only the CTN user can open this file; • **trust** — a CTN user can send files to a user with whose server the sender has established a trusted connection, but only the CTN user can open this file. Files cannot be sent to open chats/channels and to chats with disabled end-to-end encryption; • **local** — a CTN user can send files to a user from the same server as the sender, but only the CTN user can open this file. Files cannot be sent to open chats/channels and to chats with disabled end-to-end encryption.
CTN users can read	Setting up receipt and viewing of files by CTN users. Possible values: • **any** — a CTN user can receive and open files from a sender from any server. • The sender's and recipient's contour does not affect access to files; • **corporate** — a CTN user can receive and open files from a sender from his organization's CTS server. The sender's and recipient's contour does not affect access to files; • **trust** — a CTN user can receive and open files, provided that a

Parameter	Value
	trusted connection is established between the sender's and recipient's servers. The sender's and recipient's contour does not affect access to files; • **local** — CTN user can receive and open files from a sender from the same server as the sender. The sender's and recipient's contour does not affect access to files; • **contour** — a CTN user can receive and open files from a sender from the same contour as the sender
Who can read CTN files	Setting up receipt and viewing of files sent from CTN. Possible values: • **any** — a user from any server can receive and open files sent from the CTN. The sender's and recipient's contour does not affect access to files; • **corporate** — a user from the CTS server of the sender's organization can receive and open files sent from the CTN. The sender's and recipient's contour does not affect access to files; • **trust** — a user with whose server the sender has established a trusted connection can receive and open files sent from the CTN. The sender's and recipient's contour does not affect access to files; • **local** — a user from the same server as the sender can receive and open files sent from the CTN. The sender's and recipient's contour does not affect access to files; • **contour** — a user from the same contour as the sender can receive and open files sent from the CTN.

4. Click "Save".

SETTING UP FILE STORAGE PERIODS

To set up file storage periods:

1. Go to the "File Service" section.

   The "File Service Retention" window will open (see Figure 111).
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".

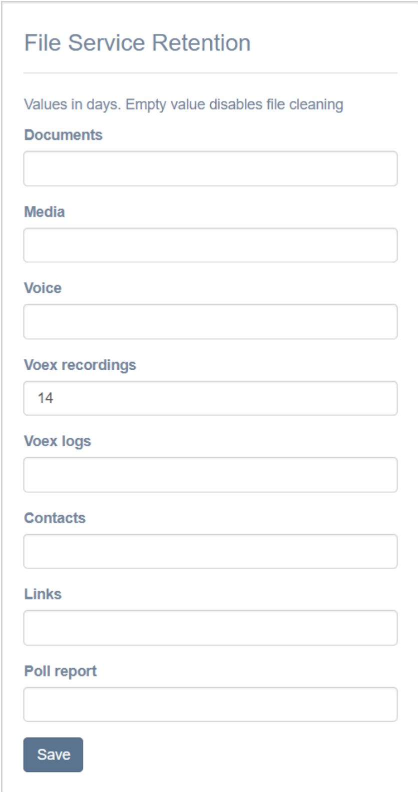


Figure 111

Proxying when Delivering Static Content

To enable/disable proxy settings:

1. Go to the "File Service" section.

   The "Proxying" window will open (see Figure 112).
2. Check/uncheck the "Enabled" field.
3. Click "Save".

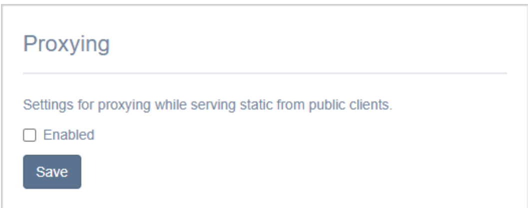


Figure 112

LOGS

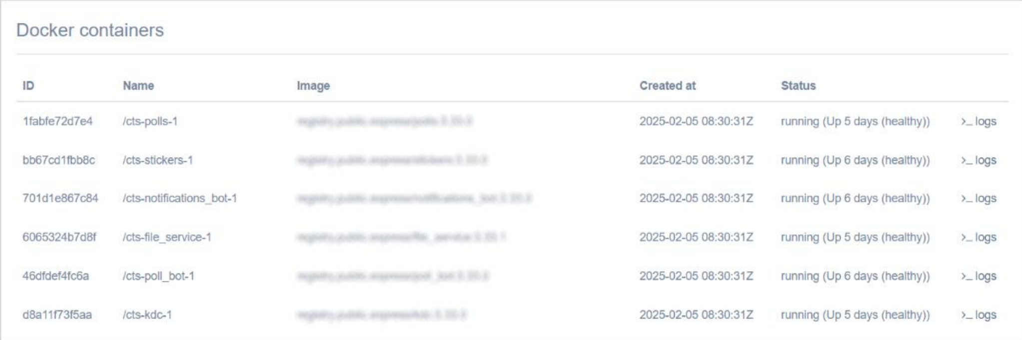
This section describes the following administrator web interface menu items:

- 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” item. A page will open with a list of installed containers in a table format (see Figure 113).


Docker containers

ID	Name	Image	Created at	Status	
1fabfe72d7e4	/cts-polls-1	[illegible]	2025-02-05 08:30:31Z	running (Up 5 days (healthy))	>_ logs
bb67cd1fbb8c	/cts-stickers-1	[illegible]	2025-02-05 08:30:31Z	running (Up 6 days (healthy))	>_ logs
701d1e867c84	/cts-notifications_bot-1	[illegible]	2025-02-05 08:30:31Z	running (Up 6 days (healthy))	>_ logs
6065324b7d8f	/cts-file_service-1	[illegible]	2025-02-05 08:30:31Z	running (Up 5 days (healthy))	>_ logs
46dfdef4fc6a	/cts-poll_bot-1	[illegible]	2025-02-05 08:30:31Z	running (Up 6 days (healthy))	>_ logs
d8a11f73f5aa	/cts-kdc-1	[illegible]	2025-02-05 08:30:31Z	running (Up 5 days (healthy))	>_ logs

Figure 113

The table with the list of installed Docker containers consists of the following columns (Table 51):

Table 51

Column name	Information
ID	Container ID
Name	Container name in the “server_container” format
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.

   The "Docker Container Logs" window will open (see Figure 114).

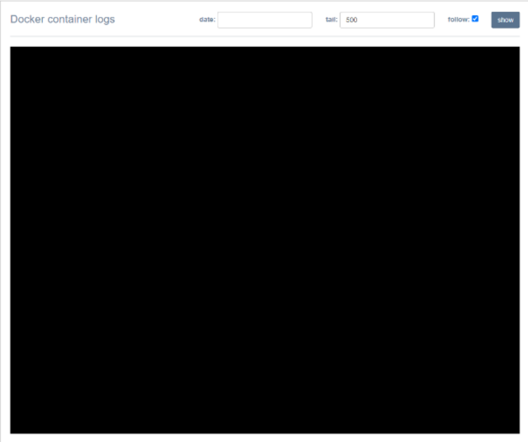


Figure 114

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 checkbox is set, 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 115).

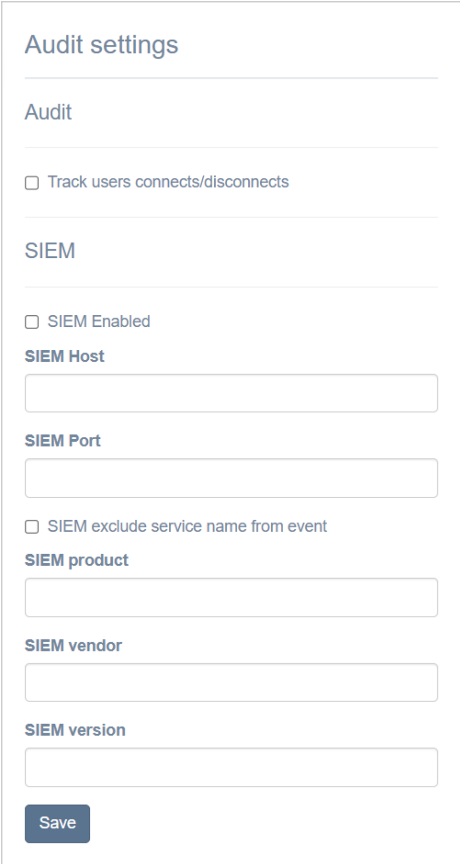


Figure 115

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 116).

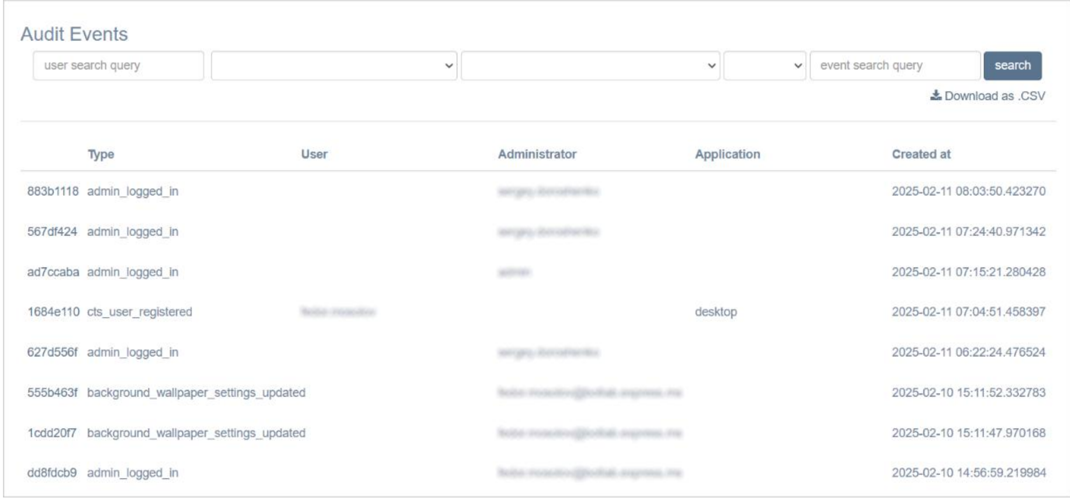


Figure 116

The parameters of the events recorded in the audit log are shown in the following table (Table 52):

Table 52

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 53):

Table 53

Event	Description
account_deleted	Deleting an account
activations_platform_lifetimes_settings_updated	Activation lifetime settings for platforms have been updated
ad_integration_settings_changed	AD integration settings have been changed
ad_settings_have_been_set	AD settings have been set using the CLI method
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

Event	Description
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
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 login 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
blocked_user_instruction_updated	Instructions for sending e-mails to blocked users have been updated
bot_added	Chatbot has been added
bot_deleted	Chatbot has been deleted
bot_properties_updated	Chatbot settings have been updated
bot_smartapp_properties_updated	SmartApp settings have been updated
bot_updated	Chatbot has been updated (for the RTS and ETS servers only applies to internal bots)
botx_certificate_deleted	BotX certificate has been deleted
botx_certificate_updated	BotX certificate has been updated
call_logs_cleaned	Calll logs have been cleaned
chat_converted_to_open	Chat converted to open
chat_created (chat_type=channel)	Open channel has been created
chat_created (corporate=true)	Open chat has been created
chat_deleted	Chat has been deleted
chat_deleted (chat_type=channel)	Channel has been deleted from open chats
chat_deleted (corporate=true)	Open chat has been deleted
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 lost chat administrator rights
chat_member_deleted	Chat member has been deleted from chat
clean	Chat history has been cleared
consent_notification_settings_updated	Consent notification settings have been updated
cts_user_registered	CTS user has been registered
cts_user_registration_failed	Unsuccessful attempt of user self-registration on the CTS server
custom_profile_updated	Avatar in the user profile has been updated
devops_token_created	DevOps token has been created
e2e_encryption_disabled	End-to-end encryption has been disabled in ordinary chat
e2e_encryption_disabled_in_open_chat	End-to-end encryption has been disabled in open chat
e2e_encryption_enabled	End-to-end encryption has been enabled in ordinary chat
e2e_encryption_enabled_in_open_chat	End-to-end encryption has been enabled in open chat
email_registration_settings_changed	Settings of registration by e-mail have been

Event	Description
	changed
email_settinds_changed	Mail server settings changed
email_settings_changed	SMTP server settings have been set using the CLI method
external_client_user_created	External client user has been created
external_client_user_deleted	External client user has been deleted
external_client_user_updated	External client user has been updated
faq_updated	FAQ have been updated
field_permissions_changed	Profile field visibility settings changed
file_contour_settings_updated	Settings of contour file access 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
local_user_created	Local user has been created
local_user_deleted	Local user has been deleted
local_user_updated	Local user has been updated
max_failed_login_attempts_reached	Maximum number of attempts for a corporate user to log in to the application (with an indication of the platform) has been reached
messaging_links_to_chats_changed	Settings for generating links to chats/calls have been changed
new_user_instruction_updated	New user instructions have been updated
open_chat_created	Open chat has been created
open_chat_deleted	Open chat has been deleted
openid_settings_changed	OpenID settings have been changed
profiles_download	The list of users has been downloaded to a file
registration_by_email_mask_settings_changed	E-mail mask setting have been changed
registration_settings_changed	Registration settings have been changed
roles_group_created	User group in the role model has been created
roles_group_deleted	User group in the role model has been deleted
roles_group_updated	User group in the role model has been updated
roles_rule_created	Rule in the role model has been created
roles_rule_deleted	Rule in the role model has been deleted
roles_rule_toggled	Status of a rule in the role model has been changed
roles_rule_updated	Rule in the role model has been updated
server_avatar_updated	Server avatar has been updated
server_features_changed	Feature settings on the corporate server have been changed
server_under_maintenance_changed	Notification of maintenance work has been changed
server_update_alert_changed	Update alert changed
sip_settings_updated	SIP settings have been updated
smartapp_proxy_host_created	SmartAppProxy host has been created
Smartapp_proxy_host_deleted	SmartAppProxy host has been deleted
smartapp_updated	Settings of a specific SmartApp have been updated
smartapps_settings_changed	SmartApp settings have been updated
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
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

Event	Description
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 have been changed
user_added	User has been added using the CLI method
user_added_to_logout_list	User has been added to the corporate server logout request list
user_connected	User has logged in to the application (with an indication of the platform)
user_custom_profile_confirmed	Request to change the user profile has been confirmed
user_custom_profile_rejected	Request to change the user profile has been rejected
user_deleted_from_logout_list	User has been deleted from the list of requests to logout from the corporate server
user_disconnected	User has logged out of the application (with an indication of the platform)
user_logout_confirmed	User system logout has been confirmed
user_logout_rejected	User logout has been rejected
user_logout_requested	User system logout has been requested
user_requested_logout	User corporate server logout has been requested
user_unblocked	User has been unblocked (by IP or phone after exceeding the number of login attempts)
vinteo_settings_updated	Vinteo settings have been updated
voex_etcd_settings_have_been_set	Setting Media Server Settings in ETCD using CLI method
voex_etcd_settings_updated	Call settings have been updated
voex_logs_settings_updated	Media call server log settings have been updated
voex_settings_have_been_set	Media server settings have been configured using the CLI method
voex_settings_updated	Media call server settings have been updated

To search for events in the table, fields at the top of the window are used (Figure 117.).

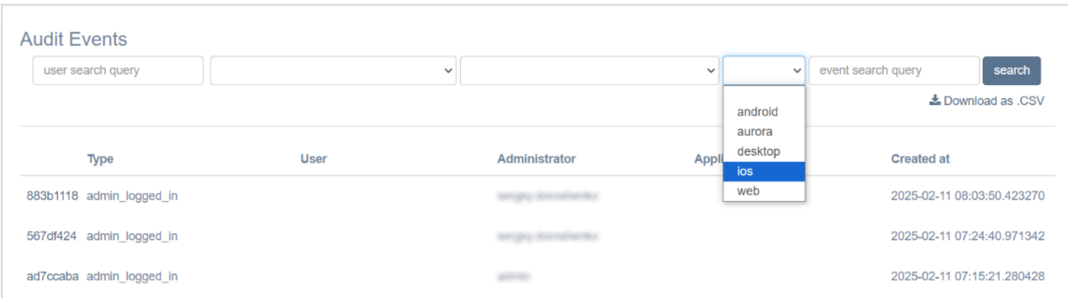


Figure 117.

- 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.

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

.

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 118).

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

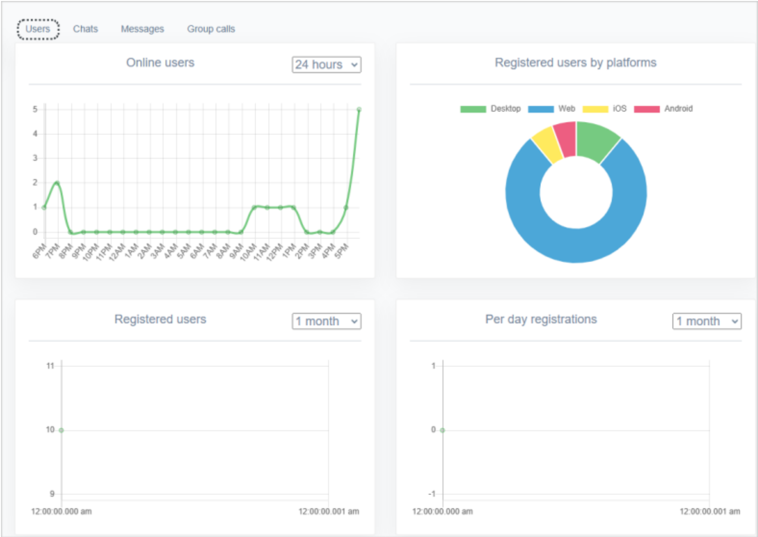


Figure 118

The following functionality is available to the administrator:

- selecting the information viewing interval ;
- viewing information about the users;
- 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 118).

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 119.).

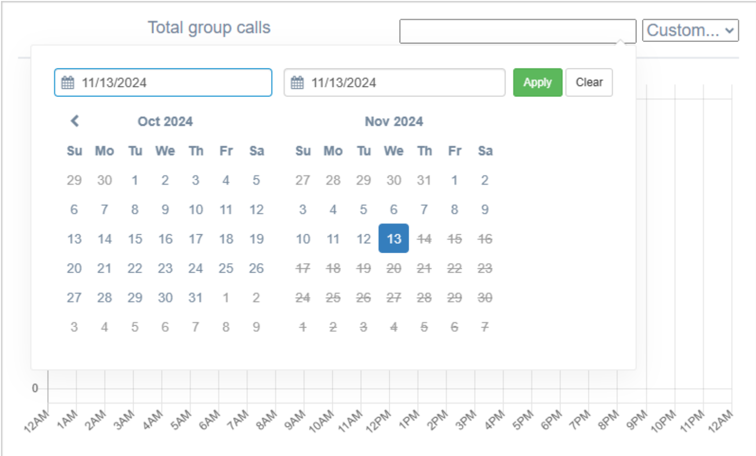


Figure 119.

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 view statistical information about newly created chats, open the "Chats" tab (see Figure 120).

Figure 120

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 121).

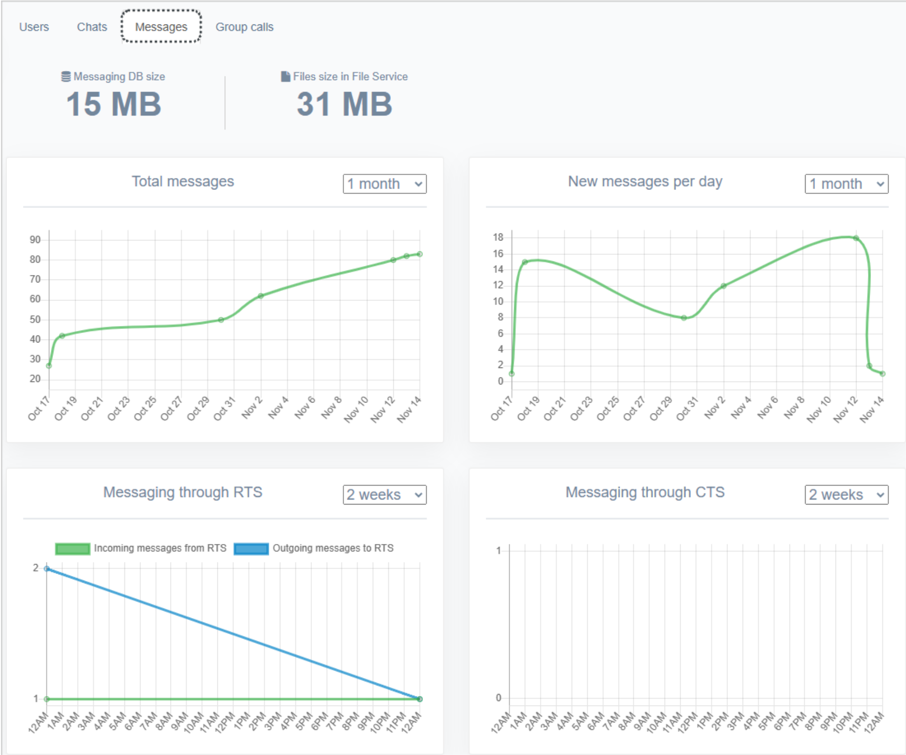


Figure 121

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 122).

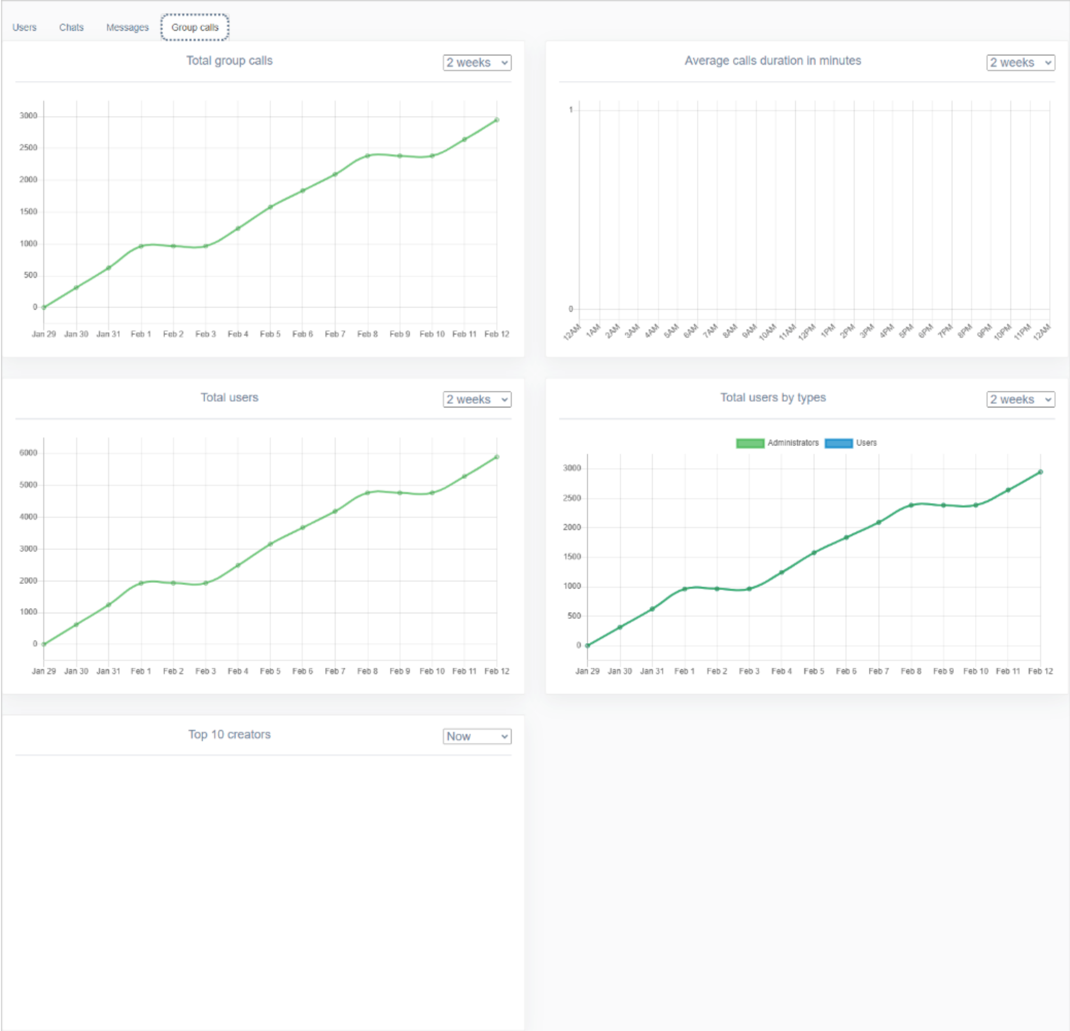


Figure 122

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 123).

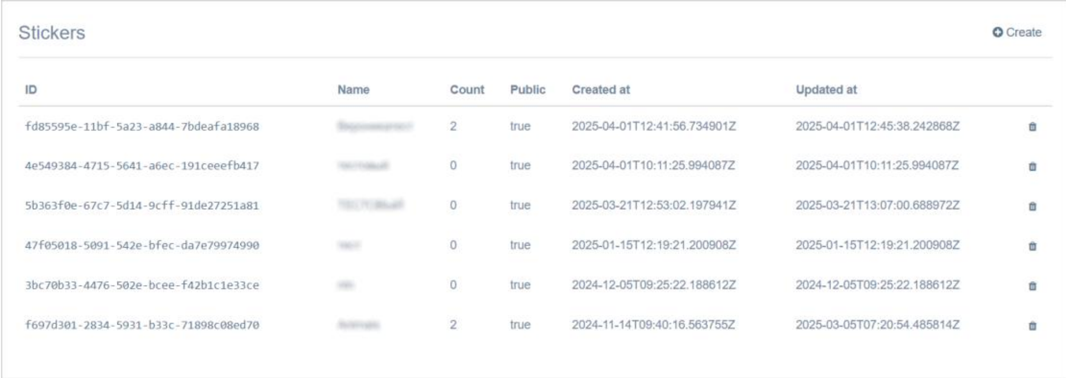


Figure 123

The sticker catalog table contains the following data (see Table 54):

Table 54

Column name	Information
ID	Sticker catalog identifier. Assigned automatically
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 124).
2. In the "Name" field, enter the name of the catalog.
3. Click "Create".

Figure 124

A window for uploading stickers will open (Figure 125):

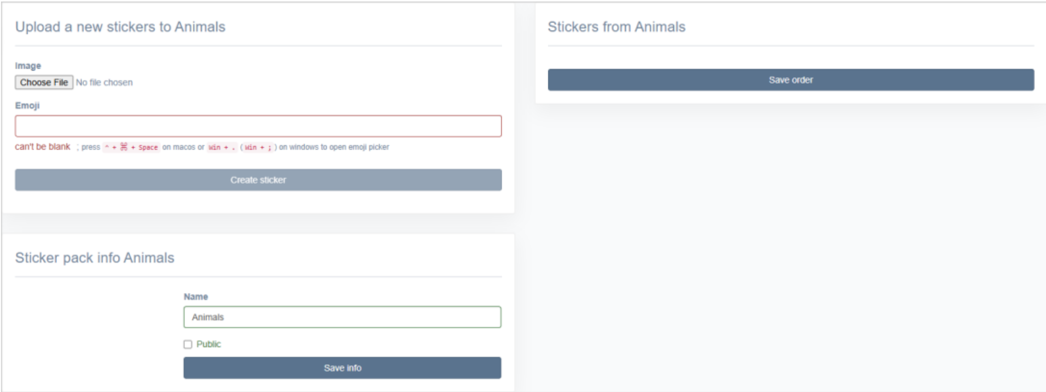


Figure 125

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:

- PNG format;
- 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 (Figure 126):

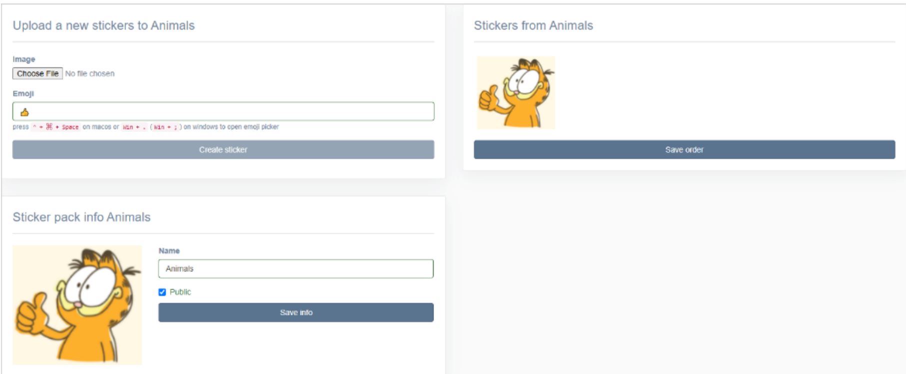


Figure 126

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 sticker catalog preview:

1. Hover the cursor over the uploaded sticker and click (see Figure 127).

Figure 127

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 128).

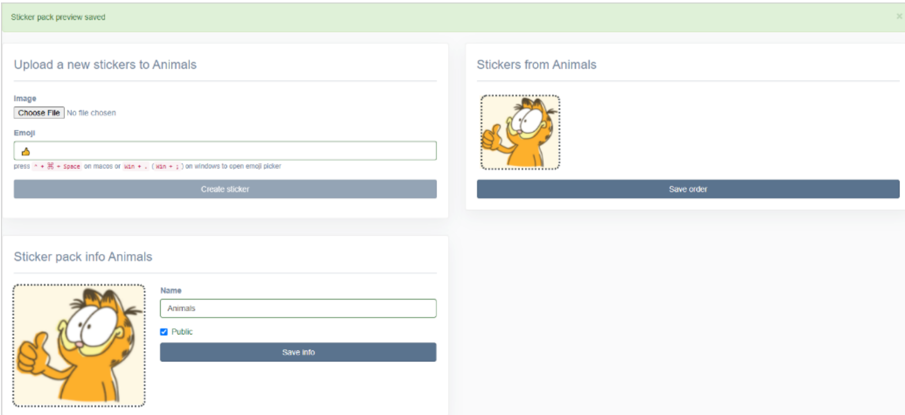


Figure 128

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 129.):

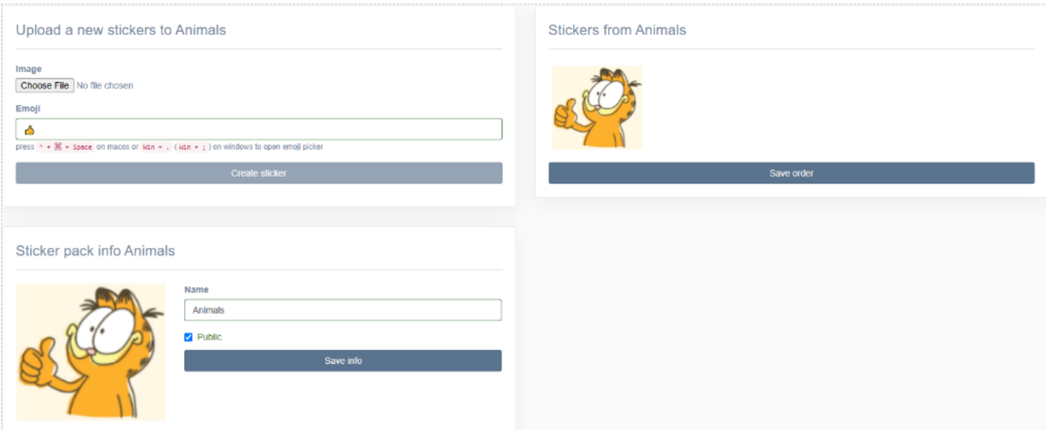


Figure 129.

To sort stickers:

1. Open the required catalog by selecting it from the list.
2. In the window that opens , move the desired stickers using the mouse (see Figure 129.).
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 , select a sticker to be deleted (see Figure 129.).
3. Hover the cursor over the sticker and click (see Figure 127).
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 123).
2. Confirm the action.

ADDITIONAL SETTINGS

Additional settings are divided into two groups:

- requiring container re-creation;
- requiring generation of a new configuration and container restart.

REQUIRING CONTAINER RE-CREATION

All parameters shall be specified in the settings.yaml file:

- global logging level:

```
logger_level: warning
```

- Disabling the docker_socket container (will disable the ability to view logs from the administrator panel):

```
docker_socket_proxy_enabled: false
```

- changing S3 and NFS data storage driver (file_service):
  - Example of configuration of connection to S3 storage:

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

  - Example of configuration of connection to NFS storage:

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

After changing the configuration to recreate the container, while in the /opt/express directory, run:

```
dpl -d
```

REQUIRING GENERATION OF A NEW CONFIGURATION AND CONTAINER RESTART

All parameters shall be specified in the settings.yaml file:

- restricting access to the administrator interface:

```
admin_allow:
   - 10.0.0.0/8
```

- restricting access to the Prometheus interface:

```
prometheus_allow:
   - 10.0.0.0/8
```

- changing the path to the administrator interface:

```
admin_url: /express-admin-ui
```

- changing the path to the DLPS administrator interface:

```
dlps_url: /dlps-admin-ui
```

After changing the configuration, in order to apply it, while in the /opt/express directory, run the following command:

```
dpl -p && dpl -dc restart nginx
```

Chapter 3

DLPS SERVICE

This chapter describes how to configure the DLPS service and use the DLPS administrator web interface.

AUTHORIZATION IN THE DLPS WEB INTERFACE

To log into the DLPS administrator web interface:

1. Enter the following in the address bar of your browser: https://ccs_host/dlps.
2. In the window that opens, enter your login and password and click “Login” (see Figure 130).

Note. By default, login is “admin”, and password is “admin”.

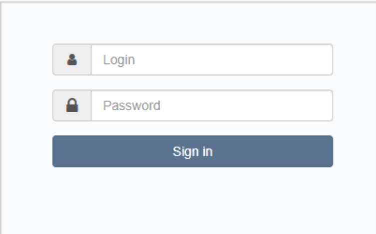


Figure 130

After the user has authorized, the main window of the DLPS web interface opens — “Chats” (see Figure 131).

CHATS

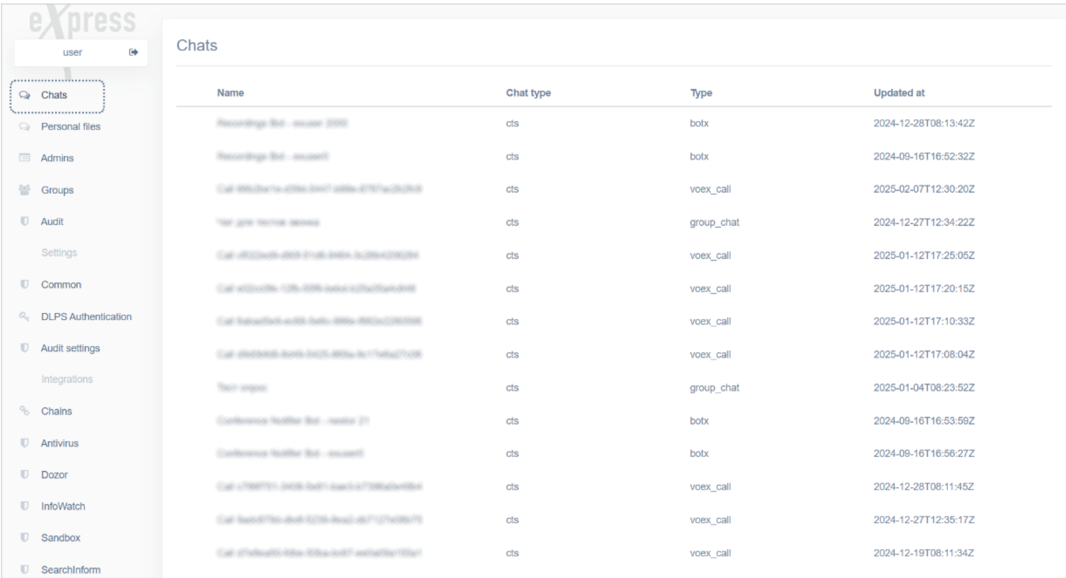


Figure 131

The “Chats” section contains a list of all created chats and calls made. The table below contains a description of the data in the “Chats” section (see Table 55).

Table 55

Column	Information
Name	Chat name or call ID
Chat type	Chat type: • cts — corporate; • rts — regional; • hybrid — hybrid
Type	User interaction type: • chat — personal chat; • group_chat — group chat; • notes — the “Favorites” chat; • botx — chat with bot; • channel — channel; • voex_call — call
Updated	Date and time of the last event

Clicking on the chat name opens a window containing the information sent in the chat (see Figure 132).

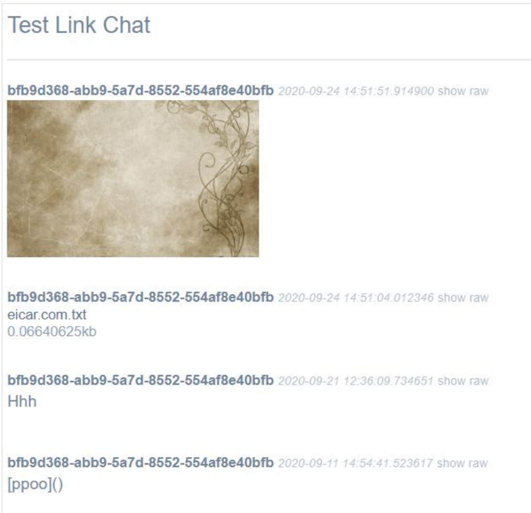


Figure 132

The DLPS web interface stores the following information sent in chat:

- messages;
- media files;
- documents.

PERSONAL FILES

This section allows you to export the entire history of user activity in the form of a personal file — an archive in 7Z format.

The DLPS web interface administrator can create, download or delete a personal file.

The section displays data on personal files, which were generated at the request of the administrator, in tabular form (see Figure 133).

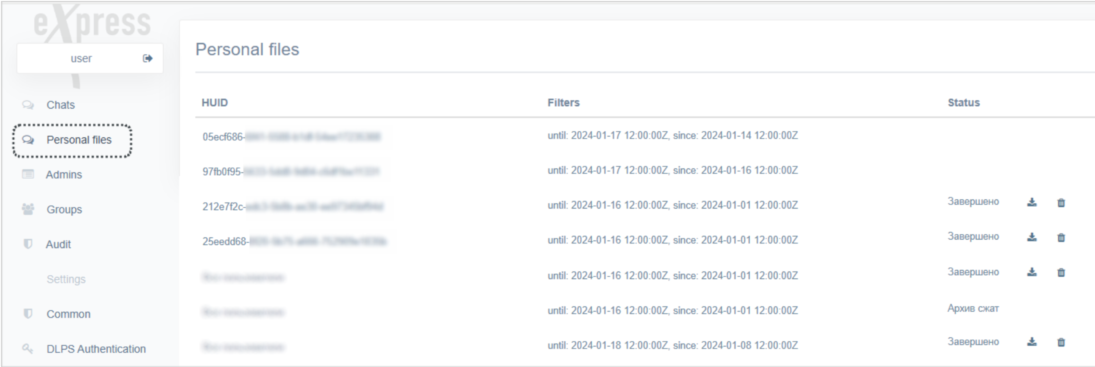


Figure 133

The table below contains a description of the data in the "Personal Files" section (Table 56):

Table 56

Column	Information
HUID	Contact ID
Filters	The period for which data is requested
Status	Status of the generated file: • completed; • started; • archive compressed; • HTML generated

To create a personal file:

1. Click "Generate Archive" in the upper right corner.
2. In the window that appears (Figure 134), enter HUID to export a specific contact's history or leave the field blank to create an archive for all contacts.
3. Specify a password that will be requested when opening the generated archive.

   Note. The minimum password length is 8 characters. The password must contain at least one special character #!?&@$%^&*(), one number, one lowercase and one uppercase letter.

4. Configure a date filter by entering data in the "From" and "To" fields.
5. Click "Generate".

   An archive with a personal file will be generated. The system message "Personal file created" will be displayed.

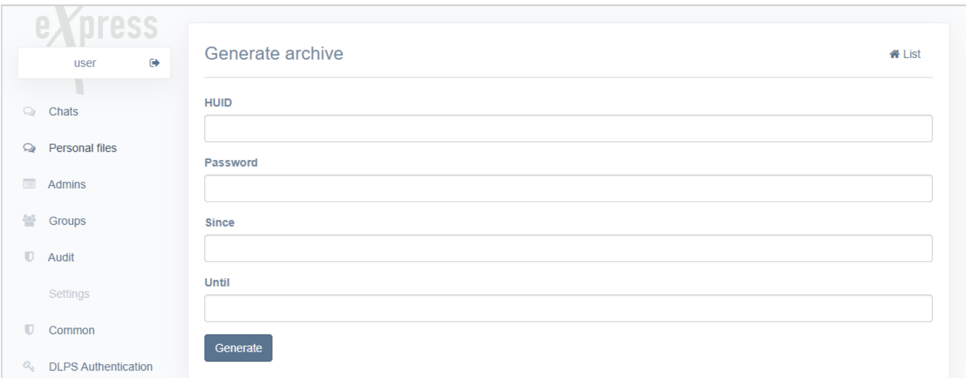


Figure 134

To download a personal file, click (see Figure 133). The archive will be exported in 7Z format. Example of archive contents (Figure 135):

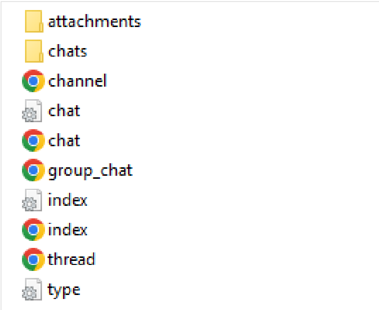


Figure 135

To download a personal file, click (see Figure 133). The generated archive and information about it will be deleted from the section. The system message "Personal file deleted" will be displayed.

AUDIT OF DLPS WEB INTERFACE

To audit events, a special interface has been implemented in DLPS.

To view the events table, select the "Audit" item (see Figure 136).

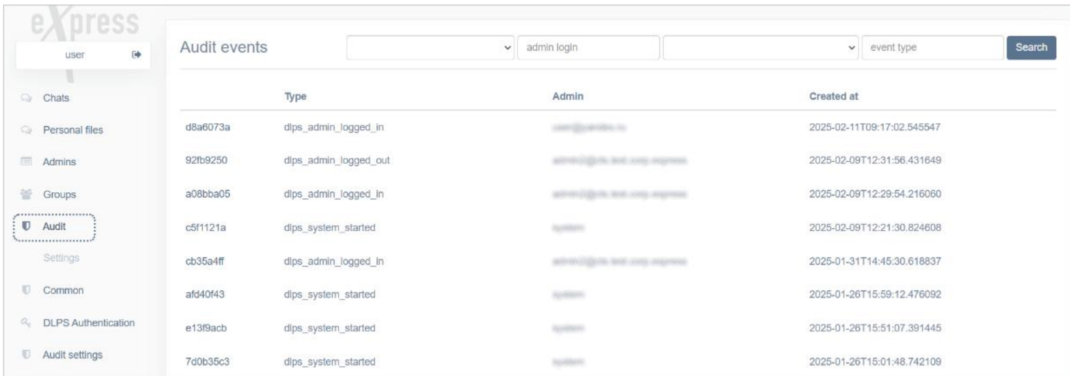


Figure 136

The parameters of the events recorded in the audit log are shown in Table 57:

Table 57

Column name	Information
Type	Event ID as a hyperlink and its type. Clicking the hyperlink opens the event's program code
Administrator	Name of the administrator
Created	Event registration date

The following events are logged in the audit log (see Table 58):

Table 58

Event	Description
dlps_admin_added_to_group	Administrator account has been added to the group
dlps_admin_blocked	Administrator account has been locked out
dlps_admin_changed_antivirus_configuration	Antivirus configuration has been changed
dlps_admin_changed_audit_log_cleaning_schedule	Settings for clearing the audit event log have

Event	Description
	been changed
dlps_admin_changed_audit_settings	Audit settings have been changed by the administrator
dlps_admin_changed_authentication_settings	DLPS authentication settings have been changed
dlps_admin_changed_chains_configuration	Configuration of the validation chains has been changed
dlps_admin_changed_confidential_mode_settings	Sending of confidential mode events has been enabled/disabled
dlps_admin_changed_dozor_configuration	Dozor configuration has been changed
dlps_admin_changed_infowatch_configuration	Infowatch configuration has been changed
dlps_admin_changed_sandbox_configuration	Sandbox configuration has been changed
dlps_admin_changed_searchinform_configuration	Searchinform configuration has been changed
dlps_admin_changed_session_ttl	TTL settings have been changed
dlps_admin_changed_stakhanovets_configuration	Stakhanovets settings have been changed
dlps_admin_created	An administrator account has been created
dlps_admin_deleted	An administrator account has been deleted
dlps_admin_group_created	An administrator group has been created
dlps_admin_group_deleted	An administrator group has been deleted
dlps_admin_group_updated	The name of the administrator group has been updated
dlps_admin_logged_in	Administrator has logged in
dlps_admin_logged_out	Administrator has logged out
dlps_admin_login_backoff_timeout	Failed to authorize administrator in the system during locking out
dlps_admin_login_op_disabled	Locking out of administrator account after the maximum number of authorization attempts
dlps_admin_login_op_failed	Failed to authorize administrator in the system
dlps_admin_removed_from_group	Deleting the administrator account from the administration group
dlps_admin_unblocked	Administrator account lockout has been canceled
dlps_admin_updated_password	Administrator account password has been updated
dlps_system_started	DLPS service has been started

To search for events in the table, fields at the top of the window are used (see Figure 137.):

- admin login — field for entering the administrator login manually;
- event type — field for entering the event type manually;
- in the drop-down lists, you can select the administrator name and event type.

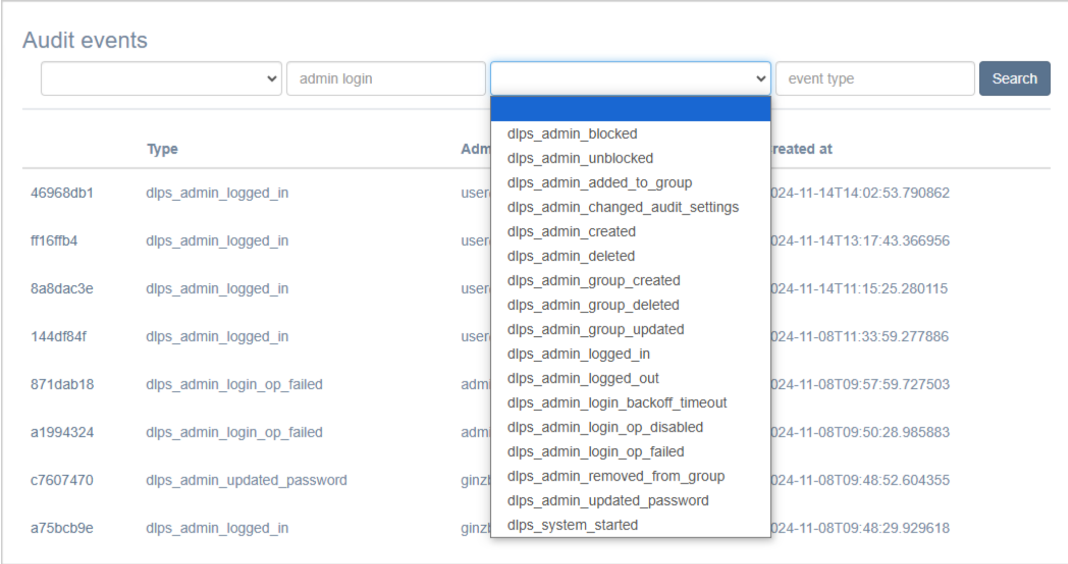


Figure 137.

MANAGING DLPS WEB INTERFACE ADMINISTRATORS

Managing DLPS web interface administrators includes the following actions:

- creating and deleting accounts;
- setting up accounts (changing login/password, setting up lockouts and access);
- setting up DLPS authentication;
- management of administrator access rights.

Information about all administrators of the DLPS web interface is available in the "Administrators" section in the form of a table (see Figure 138).

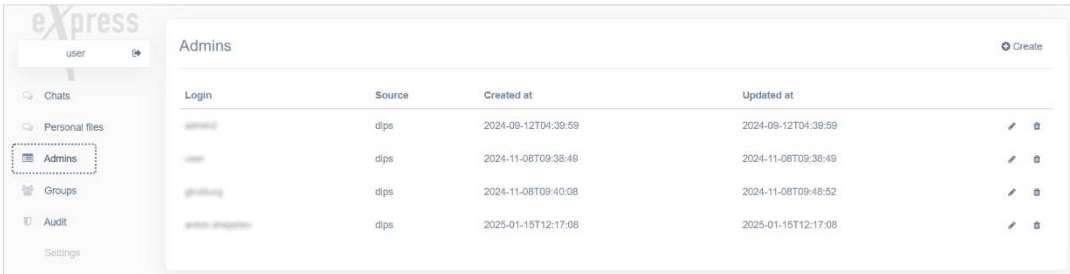


Figure 138

The table below contains a description of the data in the "Administrators" section (see Table 59).

Table 59

Column	Information
Login	Name of the administrator
Source	Where the account is created: • ad — loaded from Active Directory; • dlps — created in this section of the DLPS web interface
Created	Date and time when the administrator account was created
Updated	Date and time of the last update

AN ADMINISTRATOR ACCOUNT HAS BEEN CREATED

To create an administrator account, click “Create” in the upper right corner. In the window that opens, enter your login and password, confirm the password and click “Save” (see Figure 139).

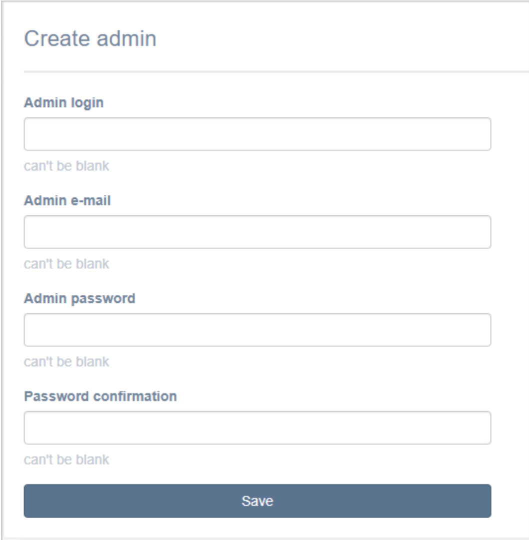


Figure 139

SETTING UP ADMINISTRATOR ACCOUNT

Setting up administrator account involves the following steps:

- changing password;
- changing access rights;
- lockout/unlocking.

These actions are performed in the account settings window.

To go to the account settings window, click ✎ in the entry information line (see Figure 138). The settings window for the selected administrator account will open (see Figure 140).

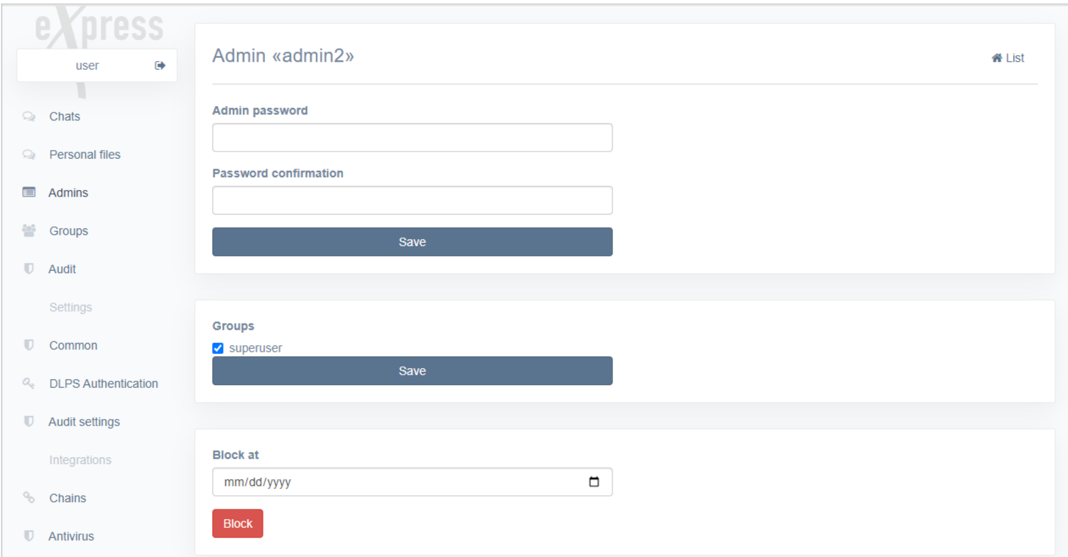


Figure 140

To change the administrator login/password, enter new data and click “Save”.

To change administrator access rights, select one or more groups and click “Save”.

For more information on managing access rights, see the “Setting Up Administrator Access Rights” section.

To set up the administrator account lockout settings:

1. Click on the “Lock out by” field.
2. Select the date of locking from the calendar.
3. Click “Lockout”.
4. In the modal window that appears, confirm the action by clicking “Yes”.

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

To cancel administrator account lockout, click “Unlock” and then click “Yes” in the modal window to confirm the operation.

SETTING UP ADMINISTRATOR ACCESS RIGHTS

Access rights of DLPS web interface administrators are distributed using roles. Role-based division of rights is implemented by combining administrators into different groups. Each group has its own set of rights.

In the DLPS web interface, the “Groups” section is intended for working with administrator groups. The section displays a list of all groups and the rights assigned to them (see Figure 141).

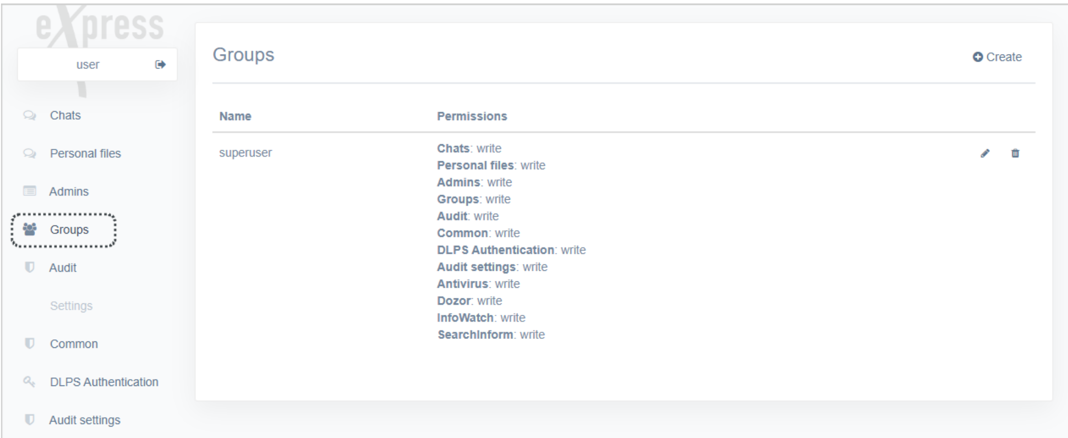


Figure 141

To create a group:

1. Go to the “Groups” section.
2. In the upper right corner, click “Create”.

A window for creating a group and setting its rights will open (Figure 142):

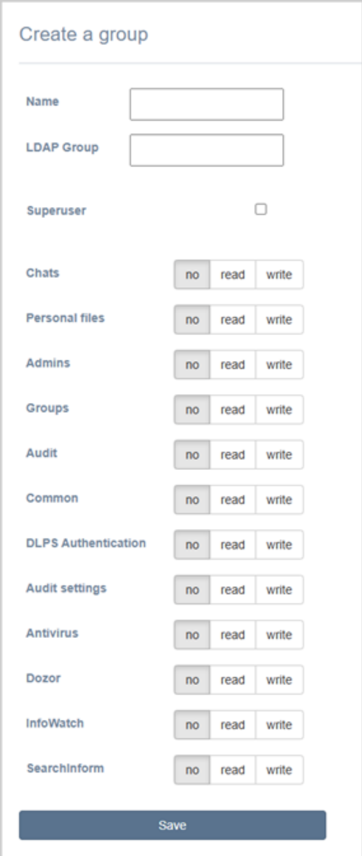


Figure 142

The buttons have the following meanings:

- no — the administrator does not have access rights to the DLPS web interface;
- read — the administrator can only view the information in the section.
- write — the administrator can view the information in the section and make changes to it.

3. In the "Name" field, enter the name of the group.
4. In the "LDAP Group" field, the name of the administrator group in Active Directory can be specified.

   If the administrators of the group being created or edited are members of the specified group in AD, they will receive the rights of this group.
5. Set up access rights for the group.

To grant full rights to view and make changes:

1. Check the "Superuser" field.
2. Click "Save".

   The created group will be displayed in the "Groups" window.

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.

To set up loading administrator accounts from AD:

1. Go to the "Settings" → "DLPS Authentication" section.
2. Fill in the fields of the form (see Figure 143):

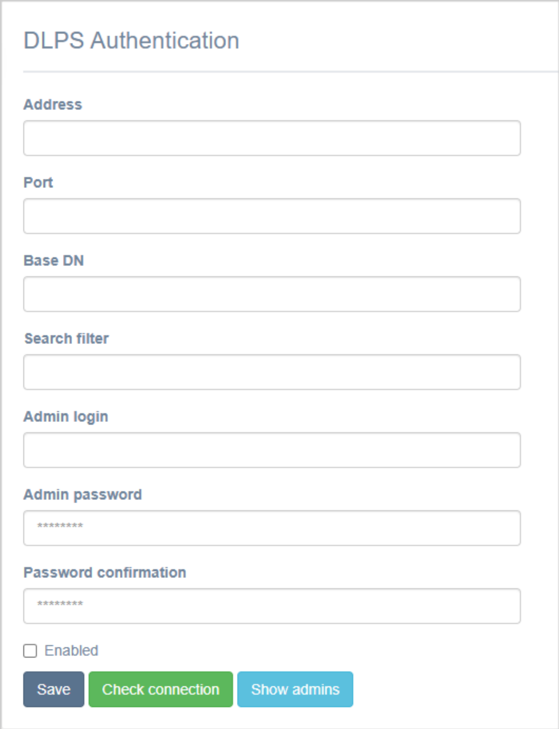


Figure 143

The parameter values are provided by the Active Directory administrator (see Table 60).

Table 60

Parameter	Description
Address	Active Directory address
Port	AD connection port
Base DN	Directory object from which the search is performed
Search filter	Filter for searching in Active Directory
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".

To view the list of Active Directory administrators, click "Show Administrators".

AN ADMINISTRATOR ACCOUNT HAS BEEN DELETED

To delete an account, click 🗑 in the entry information line (Figure 138), and then click "OK" in the modal window that opens.

MANAGING DLPS WEB INTERFACE SETTINGS

GENERAL SETTINGS

The "Settings" → "General" (Figure 144) section allows you to enable and disable:

- DLPS;
- sending confidential data exchange mode audit events.

You can also set:

- audit log clearing schedule;
- the number of days after which the events in the log will be cleared;
- the time of inactivity of the administrator until the session is terminated.

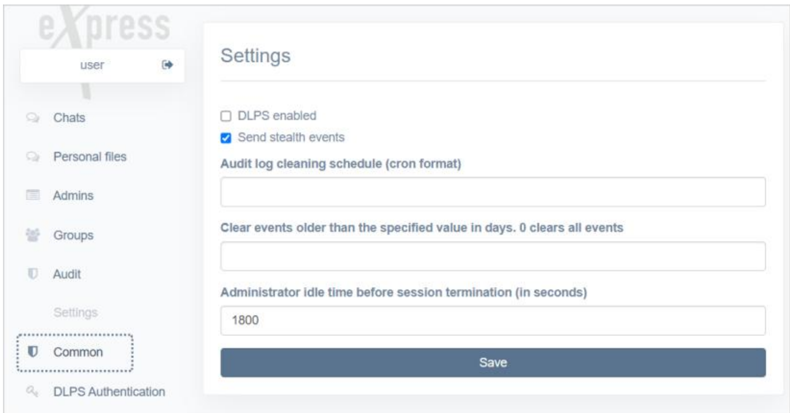


Figure 144

AUDIT SETTINGS

In this section, the administrator can configure which administrator action audit events will be displayed in the "Audit" section.

To set up audit settings:

1. Go to the "Settings" → "Audit settings" section (see Figure 145).
2. Check/uncheck the boxes next to the events you want to enable/disable.
3. Click "Save".

   The settings will be saved. For a description of event types, see the "Audit of DLPS Web Interface " section.

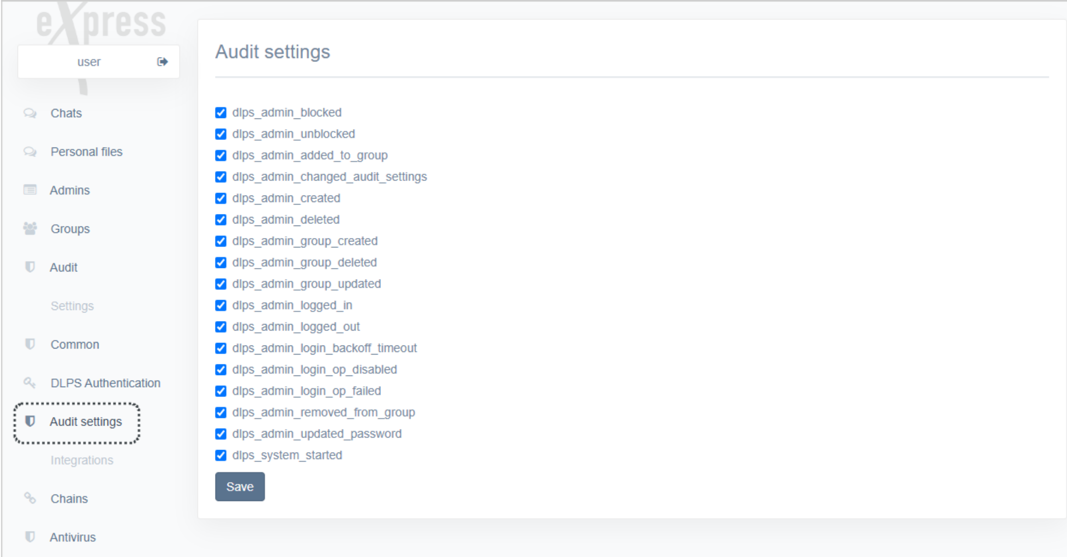


Figure 145

SETTING UP SEQUENCE OF CHECKS AND INTEGRATIONS

The administrator can configure the verification sequence in the "Chains" section, as well as directly configure the following integrations:

- integration with antivirus;
- integration with Sandbox;
- integration with DLP Solar Dozor;
- integration with DLP InfoWatch;
- integration with DLP Searchinform.

CHAINS

In this section, the administrator can configure the sequence of sending data transmitted in the system by users for verification. There are two sections available:

- Configuration of verification chains;
- Configuration of verification chains for files and messages sent within the contour.

Configuration of verification chains is responsible for the transmission of user-submitted data:

- connected from the Internet;
- connected both from the Internet and from CTN without a configured access contour (for more information about the access contour, see the section "Setting Up Data Access contour").

Configuration of verification chains for files and messages sent within the contour is responsible for the sequence of verification of files sent from the CTN by users connected from the list of networks configured in accordance with the "Setting Up Data Access contour" section. User messages sent from the CTN are managed in the "Verification Chain Configuration" section.

Each section has three states available:

- "Parallel";

- "Sequential";
- "Disabled".

When the integration is set to the "Parallel" state, the data transmitted in the system is received by each integration simultaneously.

When the integration is set to the "Sequential" state, the data transmitted in the system is received by each integration sequentially from the upstream to the downstream integration. If the upstream integration returns a deny response code, further transmission to downstream integrations is stopped.

The "Disabled" state allows you to prohibit transmission of data to the integration with this state.

When data is received by the DLPS service, it is simultaneously sent to the integrations with the "Parallel" and "Sequential" states; further, the process of data transmission in the integration is carried out according to the logic for each of the two states.

It is possible to enable the "In series" mode for messages and files transferred to the DLP system. The "In series" mode allows the DLP system to affect the ability of users to receive messages and files depending on their content (support for this function from the DLP system is required) (see Figure 146).

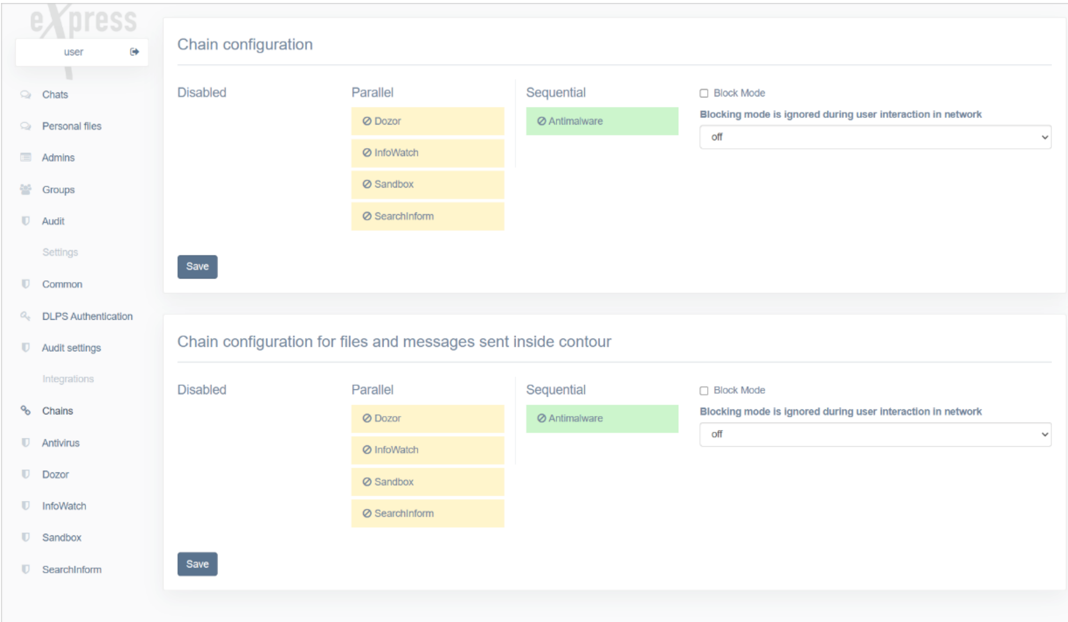


Figure 146

In case of a positive result of checking the message or file by the DLP system, the user is given the opportunity to receive the transmitted message or file. In case of a negative result of checking the message or file by the DLP system, the user is prohibited from receiving the transmitted message or file.

The "In series" mode is enabled separately for each of the chain sections. In the drop-down list "The "In series" setting is ignored for user interactions", the administrator can select one of the levels of exception for the application of this mode. The following values are available (see Table 61):

Table 61

Value	Exception level
disabled	All messages and files transmitted in this chain are awaiting the result of the DLP system check
own server	Messages and files transmitted in chats that include only users of the CTS

Value	Exception level
	server to which the custom DLPS is connected are transmitted without DLP system check. Messages and files transmitted in chats that include any other users are awaiting the result of DLP system check
own and trust servers	Messages and files transmitted in chats that include only users of the CTS server to which the configured DLPS is connected, or that contain users from other CTS servers with whom direct trust connections are configured, are transmitted without DLP system check. Messages and files transmitted in chats that include any other users are awaiting the result of DLP system check
any corporate server	Messages and files transmitted in chats in which users of any CTS server are members are transmitted without DLP system check. Messages and files transmitted in chats that include public users are awaiting the result of DLP system check

ANTIVIRUS

To set up connection to the antivirus via the ICAP protocol:

1. Go to the “Antivirus” section (see Figure 147).
2. Check the box “Antivirus enabled”.
3. Set the following parameters (Table 62):

Table 62

Parameter	Description
ICAP host	IP address or FQDN of the antivirus
ICAP port	Port used by the ICAP antivirus service
ICAP service	Request modification service path. Specify the Request Modification (REQMOD) service path
Connection timeout (ms)	Timeout in milliseconds after which a connection attempt will be made again
Response wait timeout (ms)	Timeout in milliseconds to wait for a response with a verification code for the transmitted file
Request send timeout (ms)	Timeout in milliseconds during which a response is expected about successful receipt of a request to verify the transmitted file
Number of threads	The value is set depending on the available CPU resources

Note. The following antivirus response codes are used during setup: "204" -> no_virus_found; "200" -> virus_found.

4. Click “Save”.

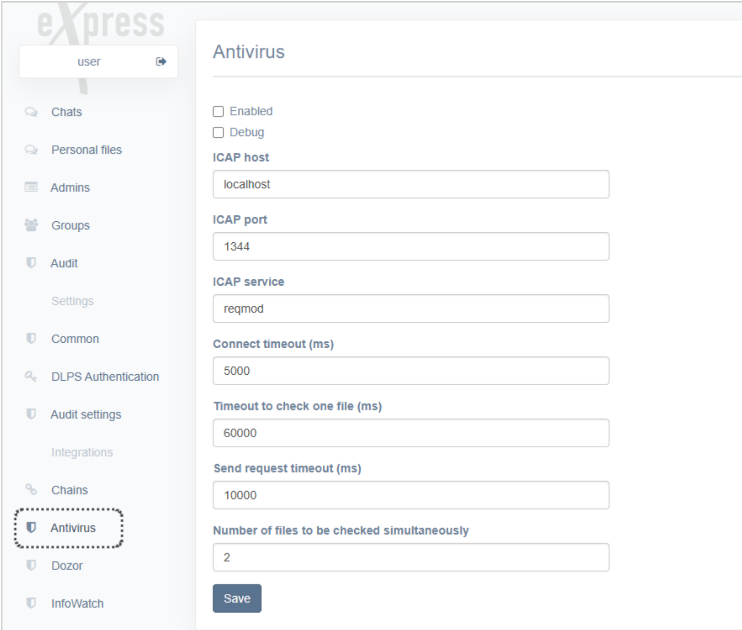


Figure 147

SANDBOX

To set up connection to Sandbox via the ICAP protocol:

1. Go to the “Sandbox” section (see Figure 148).

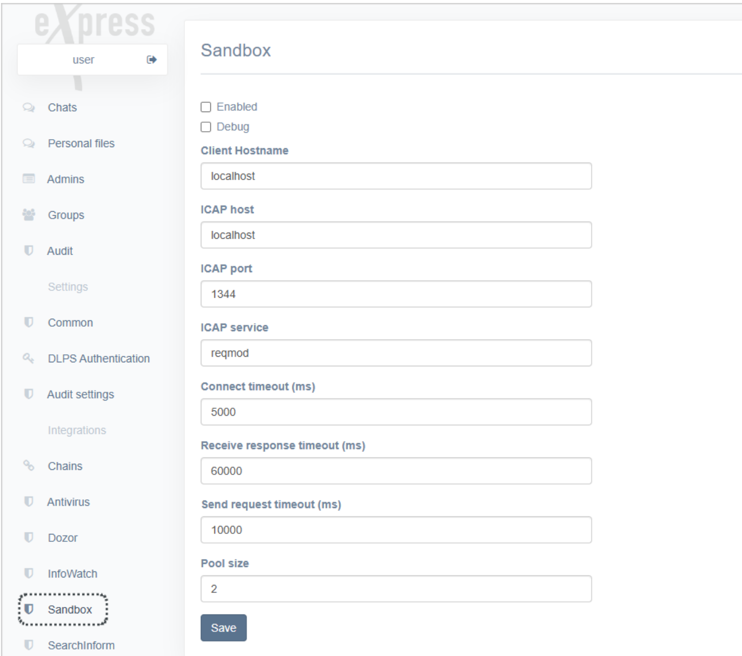


Figure 148

2. Check the “Enabled” box.
3. Set the following parameters (Table 63):

Table 63

Parameter	Description
ICAP host	IP address or FQDN of Sandbox
ICAP port	Port used by the ICAP Sandbox service
ICAP service	Request modification service path. Specify the Request Modification

	(REQMOD) service path
Connection timeout (ms)	Timeout in milliseconds after which a connection attempt will be made again
Response wait timeout (ms)	Timeout in milliseconds to wait for a response with a verification code for the transmitted file
Request send timeout (ms)	Timeout in milliseconds during which a response is expected about successful receipt of a request to verify the transmitted file
Number of threads	The value is set depending on the available CPU resources

Note. The following antivirus response codes are used during setup: "204" -> no_virus_found; "200" -> virus_found.

4. Click "Save".

SOLAR DOZOR

To set up integration with the Solar Dozor system:

1. Add the following parameters to the /opt/express/settings.yaml settings file located on the Back CTS server:

```
dlps_icap_client_host: 10.128.0.63
dlps_icap_client_port: 2344
dlps_icap_additional_headers:
 client_ip: 10.128.0.61
 server_ip: 10.128.0.63
 network_segment: CTS
 application: PROD
```

A description of the parameters is provided in Table 64:

Table 64

Parameter	Description
dlps_icap_client_host	IP of the Dozor server
dlps_icap_client_port	The port number on which the mailfilter component of Dozor software is running
server_ip	CTS or DLPS server address
client_ip	IP of the Dozor server

2. Run the following command:

```
dpl -d dpls
```

3. In the DLPS web interface, go to the "Integrations" → "Dozor" section (see Figure 149.).
4. Check the "Integration with Solar Dozor Enabled" box and click "Save" (see Figure 149.).

Attention! Do not .change other settings and data in the fields.

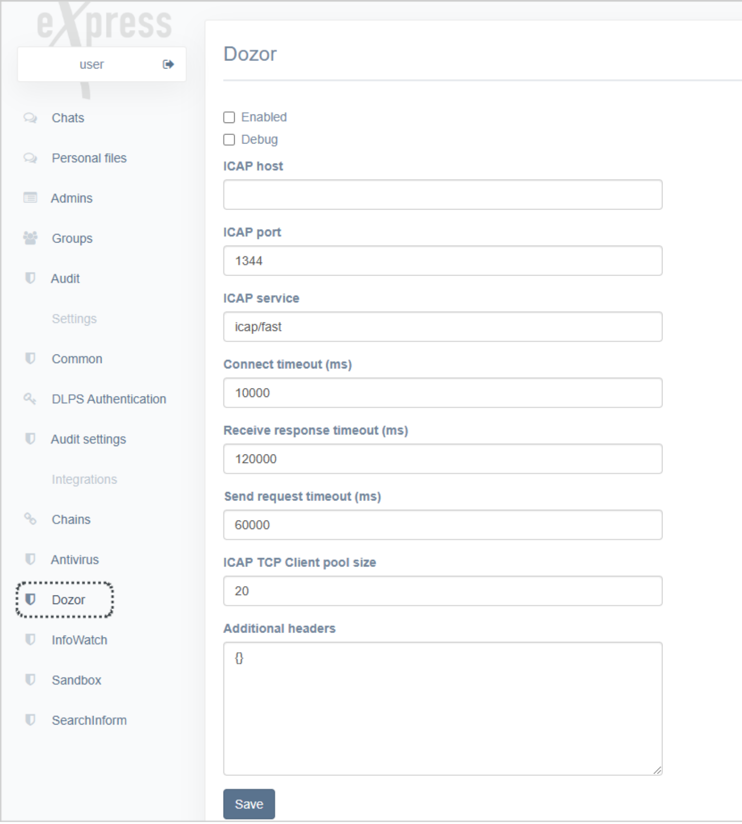


Figure 149.

INFOWATCH

Attention! Before proceeding to configuration, it is necessary to acquire the DLPS plugin for integration with InfoWatch Traffic Monitor and the license file to this plugin from the developer.

To set up integration with InfoWatch:

1. Go to the "Integrations" → "Infowatch" section (see Figure 150).
2. Check the "Integration with Infowatch enabled" box.
3. Set the following parameters (Table 65):

Table 65

Parameter	Description
Traffic Monitor host	IP address of the InfoWatch Traffic Monitor server
Traffic Monitor port	InfoWatch Traffic Monitor port number (by default — 9101)
Traffic Monitor company name from the license file	The name of the company that has been licensed to use the Express integration plugin. See the data in the Infowatch Traffic Monitor interface (the value from the "Manufacturer" field in the "Plugins" section or the VENDOR parameter from the manifest.json file)
Traffic Monitor token from the license file	Token from plugin settings, see data in Infowatch Traffic Monitor interface
Traffic Monitor service name from the license file	Service name (SERVICE_MNEMO parameter from manifest.json file)

4. Click "Save".

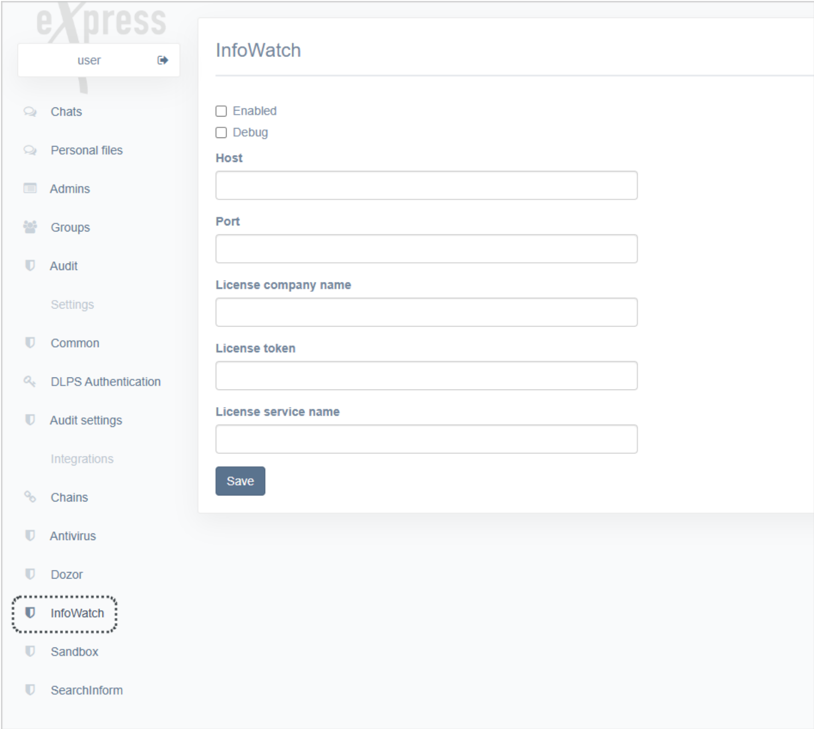


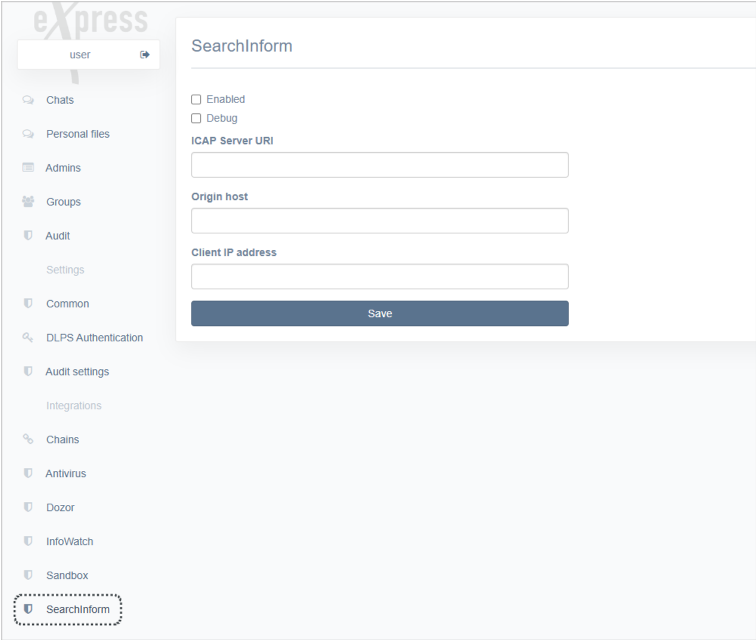
Figure 150

SEARCHINFORM

To set up integration with Searchinform:

1. Go to the "Integrations" → "Searchinform" section (see Figure 151).
2. Check the "Integration with Searchinform enabled" box.
3. In the "ICAP server URI" field, specify the value "icap://1.2.3.4:1344/icap/fast" (for an example, see Figure 151), where "1.2.3.4" is the IP address of SearchInform.

   The remaining fields are optional.
4. Click "Save".



eXpress
user
Chats
Personal files
Admins
Groups
Audit
Settings
Common
DLPS Authentication
Audit settings
Integrations
Chains
Antivirus
Dozor
InfoWatch
Sandbox
SearchInform
SearchInform
Enabled
Debug
ICAP Server URI
Origin host
Client IP address
Save

Figure 151

Chapter 4

TROUBLESHOOTING TYPICAL ERRORS

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

eXpress CS supports the following message types (see Table 66):

Table 66

Error message	Value
403 Forbidden — You don't have access to view this page	The administrator does not have access rights
404 Page Not Found	The page is missing
413 Request is too large	Occurs if the administrator attempts to upload a file that is too large, for example, an avatar
500 Internal Server Error	Exceptional error

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
```

Table 67 shows possible errors that may occur in the event of an incorrect combination of user registration settings:

Table 67

No.	Description of the combination of settings	Description of consequences
1.	The "Phone and Credentials" button is disabled in the build, and the "Registration without Telephone Number is Allowed" option is disabled in the administrator web interface.	Thus, both registration methods are prohibited. Only those users who have previously added their telephone number to their profile via a redirect to SMS input will be able to access the app
2.	All buttons except for "Phone and Credentials" button are disabled in the build, and adding the telephone number is disabled in the administrator web interface	The users who have not added their telephone number to their profile will not be able to log into the app.
3.	In the administrator web interface, registration without the telephone number has been disabled without prior notification to users about the need to add their telephone number	The users who have not added their telephone number to their profile will not be able to log into the app
4.	Users were initially registered on a public server, after which they were asked to log in using their credentials via "Corporate E-Mail" or "Corporate Server Address"	In this case, the users have two accounts: a public one with the telephone number and a corporate one without the telephone number. It is technically impossible to combine the two into one. The only way out of this situation is to add the same telephone number to the corporate account and delete the public account, losing all correspondence.
5.	In the branded build, all buttons are disabled except for "Phone and Credentials", and in the administrator web interface, the users are allowed to delete their telephone number	A user who has deleted their telephone number will not be able to log into the app
6.	In the administrator web interface, registration without the telephone number is prohibited, but the users are allowed to delete their telephone number	A user who has deleted their telephone number will not be able to log into the app

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 66
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 66
3.	Calls	Call logging has been added	page 75
4.	Servers	TTS description has been added	page 21
5.	Servers	Description of the graphical connection routing diagram has been added	page 24
6.	Server	The setting for administrator name visibility has been added	page 25
7.	Server	Administrator data setup capability has been added	page 25

Build 2.0.0

No.	Section	Change	Reference
1.	Chats	Viewing of chat events has been added	page 87

Build 2.1.0

No.	Section	Change	Reference
1.	Setting up Calls VoEX Server	The fields in SIP integration settings have been changed	page 34

Build 2.5

No.	Section	Change	Reference
1.	Contacts Management	Information about authorization using Open ID has been added	page 12
2.	Description of administrator web interface	Description of menu items and operations available in the administrator web interface have been supplemented	page 14
3.	Users	Information about authorization using Open ID has been added	page 37
4.	Creating an account	Information about authorization using Open ID has been added	page 38
5.	Setting Up Registration	The section and subsections have been added	page 37
6.	Setting Up Visibility of User Profile Fields	Added	page 46
7.	Setting Up Administrator Rights	Illustrations have been updated, description of administrator rights has been supplemented	page 66
8.	Server Management	Illustrations have been updated, and a description of the data for integrators has been added	page 17
9.	Managing Stickers	Illustrations have been updated, description of operations has been supplemented	page 121
10.	Managing SmartApps	Added	page 102
11.	Setting Up Event	Illustrations have been updated, information on	page 112

No.	Section	Change	Reference
	Information Transmission	working with SIEM has been added	
12.	Audit of administrator and user actions	Graphics have been updated, the list of audit events has been supplemented	page 114
13.	Catalog	Added	page 86
14.	Index retention period in Elasticsearch	Deleted	

Build 2.5.7

No.	Section	Change	Reference
1.	Creating an account	Requirements for user avatars were added	page 38
2.	Server Settings	Information has been updated	page 25
3.	Connecting the SMTP Server	Added information in the "E-mail Settings" list	page 35
4.	Sending instructions for getting started with the application	The figure has been updated	
5.	Chatbots	SmartApp description has been moved to the "Managing SmartApps" section	
6.	Setting Up Administrator Authentication	The figure has been updated, a menu item was renamed in the text	
7.	Server Settings	The figure has been updated. Information about Trust search has been added	
8.	Setting up Calls VoEX Server	The figure has been updated	
9.	Managing SmartApps	Updated	
10.	Chats	Updated	

Build 2.6.0

No.	Section	Change	Reference
1.	Open Chats	Optimization description has been added	page 92
2.	Managing Additional Support Settings	Added	

Build 2.7.0

No.	Section	Change	Reference
1.	Chats	The note regarding hyperlinks has been added	page 87
2.	Open Chats		page 92
3.	Calls		page 75
4.	Setting Up Administrator Rights	Updated	page 66
5.	Managing Additional Support Settings	Moved to the "Server Management" section	

Build 2.9.0

No.	Section	Change	Reference
1.	Description of CONFERENCE BOT	Updated	page 100
2.	Setting Up E-mail	The regular expression example has been added	
3.	Calls	Updated	page 75

Build 2.10.0

No.	Section	Change	Reference
1.	Managing SmartApps	Updated. The note about home page has been added	page 102

Build 2.11.0

No.	Section	Change	Reference
1.	Chats	The note concerning the limitation in chat management has been added	page 91

Build 2.12.0

No.	Section	Change	Reference
1.	Audit of administrator and user actions	Events have been added to the table	page 114
2.	Requests to Exit from The Corporate Server	The note has been added	page 51

Build 2.13.0

No.	Section	Change	Reference
1.	Creating an account	Graphics have been updated	page 38
2.	Setting up an Account	Graphics have been updated	page 41
3.	Calls and Conferences	Updated	page 75

Build 3.1.0

No.	Section	Change	Reference
1.	Server Settings	Updated	page 25
2.	Links to chats/calls	Subsection added	page 84

Build 3.2.0

No.	Section	Change	Reference
1.	Links to chats/calls	Updated	page 84

Build 3.3.0

No.	Section	Change	Reference
1.	Chats	Information about exporting the list of users in CSV format has been added	page 87
2.	Open Chats		page 92
3.	Calls and Conferences		page 75
4.	Chatbots	Information about setting up a chatbot search has been added	page 95
5.	Server Settings	Information on setting up end-to-end encryption in group chats and channels has been added	page 25

Build 3.4

No.	Section	Change	Reference
1.	File Service	Information about enabling proxy settings when distributing statics has been added	page 110

Build 3.6

No.	Section	Change	Reference
1.	Setting Up the Server	Information about the "Update Notification" and "Maintenance Notification" blocks has been added	page 25
2.	Creating an account	Information about the possibility of editing the public name has been added	page 38
3.	Managing SmartApps	The "Proxy Smartapp_proxy" subsection has been added	page 105
4.	Setting Up Data Access contour	The description of "trust" and "local" settings has been added: files cannot be sent to open chats/channels and to chats with disabled end-to-end encryption	page 108
5.	Additional Capabilities	The dlps_allow parameter has been removed	

Build 3.7

No.	Section	Change	Reference
1.	Setting Up the Server	Information about the settings of the "Update Notification" and "Maintenance Notification" blocks has been added	page 25
2.	Global Chat	The Global Chat section has been added	page 94
3.	Internal Bots	The description of Notifications bot has been added	page 101

Build 3.8

No.	Section	Change	Reference
1.	Setting Up Data Access contour	Updated	page 108
2.	Setting Up OpenID	Updated	
3.	Setting up "Send To" menu	Updated	
4.	Setting up Calls VoEx Server	Updated	

Build 3.9

No.	Section	Change	Reference
1.	Links to chats/calls	Description has been supplemented, Table 33 has been updated	page 84
2.	Setting Up Data Access contour	The "Who can read CTN files" parameter has been edited	page 108
3.	Chatbots	Moved to the "Chat and Bot Management" section	page 95
4.	Connecting a Chatbot	APP_ID field description, Table 42 have been supplemented, illustrations have been updated	page 95
5.	DLPS Service	Illustrations have been updated The "Managing DLPS Web Interface Settings" section has been updated, the "Setting Up Integrations with DLPS" section has been added	page 126

Build 3.10

No.	Section	Change	Reference
1.	Users	Table 12 has been updated, the description of the "Source" field has been supplemented	page 37
2.	DLP Service	The structure has been updated. The following subsections have been added/supplemented: • Personal Files; • Audit of DLP Web Interface Events; • Managing Administrator Accounts; • Managing DLPS Web Interface Settings	page 126

Build 3.11

No.	Section	Change	Reference
1.	Chatbots	The description of the Icon field in the Send to menu setting has been added	
2.	Chatbots	"Setting Up Action on the Contact Card" subsection has been added	
3.	Setting Up Integrations with DLPS	The note containing antivirus response codes has been added	page 141

Build 3.12

No.	Section	Change	Reference
1.	Server Settings	The notification setting for maintenance work has been updated	page 29

Build 3.13

No.	Section	Change	Reference
1.	Server Settings	The notification setting for maintenance work has been updated	page 29

Build 3.14

No.	Section	Change	Reference
1.	Calls and Conferences	The "Conferences" section has been updated: descriptions of the "Conference Name" and "Conference ID" columns have been added	page 75
2.	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 6
2.	Main Components	Links to volumes devoted to ETS and RTS operation have been added	page 8
3.	Setting Up Active Directory	Step 3 of the procedure for setting up registration with Active Directory has been updated	
4.	Setting Up Calls VoEx Server	This section has been updated. Descriptions of Janus instances and user settings have been added. Description of VoEx server settings has been updated	
5.	Calls and Conferences	The section interface figure has been updated	

No.	Section	Change	Reference
6.	Call and Conference Management	A description of settings for call quality rating filter has been added	page 76
7.	Support Contacts Management	User support contact management section has been updated	
8.	Role Model and User Groups	A section describing the application of the role model has been added	page 54
9.	Registration Systems	The section has been added	page 12
10.	File Service	The figure has been updated	page 110
11.	Internal Bots	Description of Recordings bot has been added	page 102

Build 3.17

No.	Section	Change	Reference
1.	Audit of administrator and user actions	System event "deleted_by_admin" => true, which registers the deletion of user messages by the chat administrator, has been added	page 114

Build 3.18

No.	Section	Change	Reference
1.	Setting Up Janus Instances	A note about overall Janus server load has been added	page 31
2.	Throughout the document	Module name has been corrected from DLP to DLPS	

Build 3.19

No.	Section	Change	Reference
1.	Operations with a Specific User Account	The description of the “Activations” operation has been updated	page 43
2.	Setting Up Event Information Transmission	Configuration description has been updated	page 112
3.	Links to chats/calls	A note about creating a link for guest access has been added	page 84
4.	Role Model and User Groups	A section describing the application of the role model has been added	page 54
5.	Operations with User Groups	A note about required fields when creating a user group has been added	page 57
6.	Setting Up Antivirus, DLP and Sandbox Integration	The section has been updated and supplemented with descriptions of the “Chains” subsection and integration with Sandbox	page 139
7.	Internal Bots	Description of Recordings bot has been added	page 102

Build 3.20

No.	Section	Change	Reference
1.	Setting Up Registration	The “Registration without Telephone Number” subsection has been added.	
2.	Setting Up Registration	The “Setting Up E-mail” subsection has been added	

Build 3.21

No.	Section	Change	Reference
1.	Operations with User Groups	A description of restrictions for user groups when working with SmartApp has been added	page 55
2.	Setting Up the Display in the Main Menu	The section has been updated. A description of SmartApp display for user groups has been added, images have been updated	page 102

Build 3.22

No.	Section	Change	Reference
1.	Throughout the document	VoEx server changed to Media server	
2.	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 8
3.	Operations with User Groups	A note about the specifics of setting up the connection type has been added	page 55

Build 3.24

No.	Section	Change	Reference
1.	Sending instructions for getting started with the application	The subsection has been updated, a note has been added about the need to fill in the body of the letter	page 48
2.	Sending Notifications about User Lockouts	The subsection has been updated, a note has been added about the need to fill in the body of the letter	page 50

Build 3.25

No.	Section	Change	Reference
1.	Description of Administrator Web Interface	The subsection has been updated, the figure has been replaced, a description of the "Call Ratings" and "Call Recordings" sections has been added to the table	page 14
2.	Call Recording	Subsection added	page 80

Build 3.26

No.	Section	Change	Reference
1.	Setting Up Registration	The section has been completely transferred to the document “Volume 1. “Administrator's Guide. Installation”.	
2.	Description of Administrator Web Interface	Table 2 has been changed.	page 14
3.	Throughout the document	A definition of VoEx (Voice Over Express) — part of Express CS, which includes call management, call recording, SIP telephony, and integration with other types of telephony — has been added	
4.	Throughout the document	The document structure has been optimized	
5.	Additional Capabilities	The section has been removed. Information contained therein has been transferred to the document “Volume 1. “Administrator's Guide. Installation”.	
6.	Eliminating Vulnerabilities	The section has been completely transferred to the document “Volume 1. “Administrator's Guide. Installation”.	
7.	Call Quality Ratings	Subsection added	
8.	Throughout the document	The figure have been updated	
9.	Viewing Account Information	A note about updating the user profile has been added	page 37
10.	Operations with User Groups	A table with a description of the fields of the group creation form has been added	page 55
11.	Setting Up Administrator Rights	Table 26 has been updated	page 66

Build 3.27

No.	Section	Change	Reference
1.	Main Components	The description of the Transcoding server has been added	page 8
2.	Available Roles	A description of the new restrictions has been added	page 11
3.	Requests to Exit from The Corporate Server	The section has been updated	page 51
4.	Role Model and User Groups	The section has been updated. A description of the process for creating new rule types has been added	page 54
5.	Global Chat	The section has been updated	page 94
6.	Global Bots	A description of global bots has been added	

Build 3.28

No.	Section	Change	Reference
1.	Deleting an Account	The section has been updated	page 46
2.	Sending instructions	Note about new users has been added	page 48

No.	Section	Change	Reference
	for getting started with the application		
3.	Role Model and User Groups	The section has been updated. A description of the process for creating new rule types has been added	page 54
4.	Setting Up Administrator Rights	Table 26 has been updated	

Build 3.29

No.	Section	Change	Reference
1.	Setting Up Records Retention Period	The figure has been updated	page 82
2.	Setting Up File Storage Periods	The figure has been updated	page 109

Build 3.30

No.	Section	Change	Reference
1.	Setting up “Send To” menu	The section has been removed	
2.	Setting Up Action on the Contact Card	The section has been removed	
3.	Requests to Exit from The Corporate Server	Information about user marking has been updated	page 51

Build 3.31

No.	Section	Change	Reference
1.	Deleting an Account	Information has been updated	page 46
2.	Call and Conference Management	The figures have been updated, and information about searching for calls and conferences has been updated	page 75
3.	Changing Chatbot Parameters	The figure and information in the table have been updated	page 96
4.	Chains	The section has been completely updated	page 139
5.	Internal Bots	The figure has been updated	page 99
6.	Description of Poll Bot	The section has been added	page 102

Build 3.32

No.	Section	Change	Reference
1.	Server	The figure has been updated	page 25
2.	Update Notification	New information has been added	page 30

Build 3.33

No.	Section	Change	Reference
1.	Authorization in the ADMINISTRATOR WEB INTERFACE	The figure has been updated	page 13
2.	Description of Administrator Web Interface	The figure has been updated, the table has been updated and supplemented	page 14
3.	Setting Up Janus Instances	The figure has been updated	page 31

No.	Section	Change	Reference
4.	List of Change Requests	The section has been added	page 53
5.	Support Contacts	Moved from the section "Support Contacts Management"	page 54
6.	Additional settings	The section has been added	page 126
7.	Server	The figure has been updated	page 25
8.	Server Features	Information about new settings has been supplemented	page 28

Build 3.34

No.	Section	Change	Reference
1.	Description of Administrator Web Interface	Table updated	page 14
2.	Setting up TURN Server and STUN Server and the VoEx Local Network	Figure updated, information on settings added	page 33
3.	Setting Up Administrator Rights	Figure and table updated	page 66
4.	Call Quality Ratings	Table updated	page 83
5.	Description of Conference Bot	Information has been updated	page 100
6.	Mobile application menu configuration	The section has been added	page 105
7.	Setting up menu configuration for web and desktop apps	The section has been added	page 107
8.	DLPS web interface event audit (Audit)	Figure and table updated	page 131
9.	Managing DLPS web interface settings	Figure and information updated	page 133
10.	Audit Settings	The figure has been updated	page 138

Build 3.35

No.	Section	Change	Reference
1.	Setting up SIP telephony	Table and figure updated	page 34
2.	Operations with Rules	The figure have been updated	page 58
3.	Audit of administrator and user actions	Audit log event table updated	page 114
4.	DLPS web interface event audit (Audit)	Audit log event table updated	page 131
5.	Audit Settings	The figure has been updated	page 138

Build 3.36

No.	Section	Change	Reference
1.	Description of Administrator Web Interface	Information about profile edit button added	page 14
2.	Setting up TURN Server and STUN Server and the VoEx Local Network	Information about the "List of servers that will use the internal janus host (comma separated)" field updated	page 33

No.	Section	Change	Reference
3.	Editing an Account	Information about the possibility of changing the avatar by the user added	page 42
4.	Operations with a Specific User Account	Figure updated, information about the “Device hostname” field added	page 43
5.	Setting Up Visibility of User Profile Fields	Information on access levels updated	page 46
6.	Prohibition of downloading attachments from CTS users;	Figure updated, information about the “Exception chats” field added	page 60
7.	Editing Administrators	2 editing method added	page 72
8.	Mobile application menu configuration	Figure updated, description expanded	page 105
9.	Audit of administrator and user actions	Audit log event table updated	page 114