



TrueConf Server

Administrator guide



Version 5.5

Table of Contents

1. Description	10
1.1. Why do you need a video conferencing server	10
1.2. Capabilities	11
1.2.1. Supported Protocols and Codecs	11
1.2.2. Modules of the video conferencing server and their functionality	12
1.3. Selecting the Server Version	14
1.4. Advantages	15
1.5. Useful Resources	15
2. User Types	16
2.1. User roles	16
2.2. User ID	16
2.3. Participant roles in a conference	17
2.3.1. Moderator	17
2.3.2. Owner	17
2.3.3. Operator	18
2.3.4. Speaker	18
2.3.5. Translator	18
2.4. Administrative roles	18
2.4.1. Administrator with full access	19
2.4.2. Security Administrator	19
3. Types of Conferences	20
3.1. What is a video call	20
3.2. What is a video conference? Types of video conferences	20
3.3. Video Conference Modes	22
3.4. Conference ID	22
3.5. What is a waiting room	23
4. Enhancements	24
4.1. SIP / H.323 / RTSP gateway	24
4.2. Integration with LDAP and Active Directory	24
4.3. Public Web Conferences	24
4.4. Live Streaming	25
4.5. Simultaneous Interpretation	25
4.6. Federation	25
4.7. Integration with DLP	26
4.8. Support for SDK applications	26
4.9. Integration with AI server	26
4.10. Integration with a corporate calendar	27
4.11. Using UDP Multicast	27
4.12. TrueConf Directory	28
4.13. TrueConf License Manager	28
4.14. TrueConf Border Controller	28
4.15. TrueConf Enterprise	29

4.16. Advanced monitoring of video conferencing servers	29
5. Licensing	30
5.1. Online users	32
5.2. PRO Users and Conference Participation	32
5.2.1. Features of using PRO connections	33
5.2.2. Using PRO connections in federation	34
5.2.3. Examples of PRO connections	34
5.3. SIP/H.323/RTSP connections	35
5.4. Guest connections	36
6. Preparing for Installation and System Requirements	37
6.1. Helpful explanations	37
6.2. Requirements for Administrators	39
6.3. Detailed system requirements	39
6.4. Optimizing swap file usage	41
7. Installation and Update	43
7.1. Checking the registration key	43
7.2. Server Installation	43
7.2.1. Which services will be added to the OS after installation	44
7.2.2. Installation on Windows OS	44
7.2.3. Installation on Linux OS	46
7.2.4. How to change the port to access the control panel without reinstalling server	49
7.3. Updating the video conferencing server	51
7.4. How to solve typical installation issues	51
7.4.1. gnupg error when installing from the repository on Debian	51
7.4.2. Administrator login input error during installation	51
7.4.3. Unable to access the control panel	52
7.4.4. What is the default administrator login and password?	52
8. Registration	53
8.1. What are a registration key and server ID?	53
8.2. Server Name (Имя сервера)	54
8.3. Server registration process online	55
8.4. Offline Registration	56
8.4.1. Registering a new server or after a clean reinstallation	56
8.4.2. Re-registering the server in a closed network	57
8.5. How to re-register the server	59
8.6. Re-registering with a previously used server name	59
8.7. Frequently Asked Questions about Registration	60
8.7.1. Is it possible to register the free version of the server without an Internet connection?	60
8.7.2. What should I do if I get the message "Computer change is not available for this server code"?	60
8.7.3. How to reset the binding?	60
8.7.4. What should I do if I get the message "The registered server doesn't have valid licenses"?	
8.7.5. What should I do if I get the message "Server name is already registered"?	6060

8.7.6. Why is it necessary to maintain connection with the registration server and what kind of data will be sent there?	60
9. Accessing the control panel and configuring preferences	61
9.1. How to access the control panel (admin area)	61
9.2. Adding Administrators	64
9.2.1. For Windows	64
9.2.2. On Linux OS	66
9.3. Server Status	66
9.4. Server log	67
9.5. Configuring Preferences	67
10. Server Information and General Settings	69
10.1. Server Information	69
10.2. PRO licenses	71
10.3. Basic settings	73
10.3.1. Server settings	73
10.3.2. How quickly will stdout.log fill up if detailed logging is activated?	74
10.3.3. Application Settings	74
10.3.4. Transferring server settings	76
10.3.5. Configuring client application connections	76
10.3.6. Updating applications for Windows without reinstalling the server	77
10.4. How to use other folders on Linux with symlink	78
10.5. Mounting a network storage on Linux	80
10.6. Configuring access to network storage in Windows	82
10.7. File storage	82
10.8. Call and Conference Recordings	84
10.8.1. Frequently asked questions about recordings	86
10.9. Connecting Users	86
10.9.1. Where can I find client applications	87
10.9.2. Configuring automatic server discovery	87
10.9.3. Configuring automatic server connection using corporate email	89
11. Network and federation settings, STUN/TURN servers	91
11.1. Network Settings	91
11.2. Federation	93
11.2.1. Examples of federation in operation	94
11.3. TURN/STUN servers settings	95
12. Configuring email notifications (SMTP)	96
12.1. Integration with a mail server via the SMTP protocol	96
12.2. Configuring email templates	97
12.2.1. Missed Call Notifications	97
12.2.2. Conference invitations	97
12.2.3. Registration confirmations for a public conference	97
12.2.4. Reminders for upcoming conference	97
12.2.5. Conference Rescheduling Notifications	98

12.2.6. Conference cancellation notifications	98
12.2.7. Notifications about removal from a conference	98
12.3. List of parameters used in email templates	98
13. SIP/H.323/RTSP gateway and transcoding	101
13.1. SIP Gateway	101
13.1.1. Block "Network Settings"	102
13.1.2. Section "Rules for SIP Connections"	102
13.1.3. Form for creating a new rule	102
13.1.4. Setting up integration with Skype for Business	105
13.1.5. Global SIP settings	106
13.1.6. Invitation of the SIP endpoint to the conference on your server	106
13.1.7. How to join a conference with its CID (conference ID) from an SIP endpoint	107
13.2. H.323 Gateway	107
13.2.1. Block "Network Settings"	108
13.2.2. Section "Rules for H.323 Connections"	108
13.2.3. Form for creating a new rule	108
13.2.4. Global H.323 Settings	110
13.2.5. Methods for calling subscribers and conferences on your server using H.323 devices	111
13.2.6. Registering H.323 devices on the video conferencing server	111
13.2.7. Sending DTMF Commands	111
13.3. Chat during calls on MCU	112
13.4. RTP	112
13.5. WebRTC	112
13.6. Transcoding	113
13.6.1. Adjusting Quality	113
13.6.2. Adding Background and Watermark	115
14. Web and HTTPS Settings	117
14.1. HTTPS	117
14.1.1. Block "HTTPS Configuration"	117
14.1.2. Self-signed and complete certificates	118
14.1.3. Block "Self-signed Certificate"	119
14.1.4. Block "Uploaded Certificate"	119
14.2. Web Settings	120
14.2.1. Guest Page Settings	120
14.2.2. Additional documents	121
14.3. Security	123
15. Users and groups. Integration with LDAP/Active Directory	126
15.1. Accounts	126
15.2. Endpoint authentication under the user's account	128
15.3. User Profile	128
15.3.1. User Deactivation	129
15.3.2. User device history	130
15.3.3. Calls and Conferences	130

15.3.4. Application Settings	131
15.3.5. User's Address Book	132
15.4. Groups	133
15.4.1. List of rights for the user group	134
15.4.2. How permissions restrictions work	135
15.4.3. Configuring Groups in Registry Mode	135
15.4.4. Configuring Groups in LDAP Mode	136
15.4.5. Editing a group	138
15.5. Alias	142
15.5.1. Description of operation	142
15.5.2. Using in Federation	144
15.6. Authentication	144
15.6.1. Access Zone Settings	146
15.6.2. SSO Settings	147
15.6.3. How to add two-factor (2FA) authentication providers	148
15.7. LDAP / Active Directory	150
15.8. Registry Mode	150
15.9. LDAP Mode	151
15.9.1. Authorization as an NT user on Windows	154
15.9.2. Generation of a keytab file for Kerberos server authentication	156
15.9.3. Additional LDAP Parameters	157
15.9.4. How to upload user accounts from different domains	160
15.9.5. Certificate installation for LDAPS connection	160
15.10. How to address typical issues when using LDAP	161
15.11. Password and Lock Settings	162
15.11.1. Password Requirements	162
15.11.2. Automatic Lock	163
15.11.3. Display of fields from a user card	164
16. Group conferences and broadcasts	166
16.1. List of group conferences	166
16.1.1. Conference Sources	168
16.2. Conference Page	168
16.3. Saving guest connection data	169
16.4. Managing an ongoing conference	170
16.4.1. The "Information" tab	170
16.4.2. The "Participants" Tab	171
16.5. Editing a conference	172
16.6. Creating a New Conference	173
16.6.1. The "General" tab	173
16.6.2. The "Participants" Tab	177
16.6.3. "Interpretation" Tab	179
16.6.4. The "Video Layout" Tab	180
16.6.5. "Media" Tab	184

16.6.6. The "Advanced" Tab	184
16.6.7. Webinar Limitations	189
16.6.8. Registration Tab	189
16.7. Automatic conference termination	192
16.8. Templates	193
16.9. Streaming	194
16.9.1. Streaming on YouTube, Wowza, Rutube, VK, OK	195
16.9.2. Manual configuration	197
16.10. Conference Settings	200
16.10.1. Automatic conference deletion	200
16.10.2. Limiting the quality of outgoing video from participants	201
16.10.3. Methods to connect to conferences	201
16.10.4. Conference ID and participant call rules	202
17. Chat Settings	203
17.1. Timeout settings for editing messages	203
17.2. Automatic deletion of empty conference chats	203
18. Surveys	205
18.1. Types of questions and limits	205
18.2. Creating and editing a survey	206
18.2.1. Creating a Survey	206
18.2.2. Settings	208
18.2.3. Polling campaigns	208
18.3. Results of survey campaigns	210
19. Working with the server API	212
19.1. How API and OAuth 2.0 work	212
19.2. Permissions description	213
19.3. Form for creating a new OAuth 2.0 application	213
19.4. Application Editing Page	214
19.5. Built-in API Documentation	214
20. Conference recordings and logs (reports)	216
20.1. Differences between a session and a conference	216
20.2. Event Log	216
20.2.1. Decoding event types	218
20.3. Call History	219
20.3.1. Call History List	219
20.3.2. Connection session information	220
20.3.3. Connection properties	222
20.4. Settings changes	222
20.5. Conference recordings	223
20.6. Connections	224
20.6.1. Events that update device information	226
21. Configuring Extensions	227
21.1. TrueConf Directory	227

21.2. Integration with DLP	227
21.2.1. Configuring Connection with the DLP System	228
21.2.2. Configuring Message Verification	228
21.2.3. File transfer verification in chats	229
21.2.4. Trusted servers and advanced configuration for sending the list of chat participants	230
21.2.5. Variables in ICAP request templates	231
21.3. Email Plugins	232
22. Integration with Calendars and Email	233
22.1. Integration with a corporate calendar	233
22.2. Email Plugins	234
22.2.1. Configuring an invitation template	236
22.2.2. Plugin configuration when using a self-signed certificate	236
23. Integration with AI server	237
23.1. General data transmission and storage scheme for integration with an AI server	238
23.2. Access levels for conference protocols	238
23.3. AI server connection settings	238
23.4. Viewing the list of completed and pending transcripts	239
23.5. Conference transcription settings	240
24. Security Admin Role Capabilities	243
24.1. How to add a Windows account to the Security Admin group	243
24.2. How to add an account to a group with the Security Admin role on Linux OS	244
24.3. How to configure rights for an existing user	245
24.4. How to access the control panel (admin panel)	246
24.5. Server Status	246
24.6. Configuring Preferences	246
24.7. Server Log	246
24.8. Access Parameters	246
24.9. Transcripts	247
24.10. Reports	248
24.10.1. Event Log	249
24.10.2. Call History	250
24.10.3. Connection session information	250
24.10.4. Chat messages	251
24.10.5. Changes to settings	251
24.10.6. Conference recordings	252
24.10.7. Connections	252
25. Security in TrueConf Server: How we protect user data	254
25.1. Level 1. Administrative settings	254
25.2. Level 2. Unique chats for different sessions	255
25.3. Level 3. Proprietary video codec	255
25.4. Level 4. Single port operation	255
25.5. Level 5. Administration access control in the video conferencing server	255
25.6. Level 6. Control data encryption	256

25.7. Level 7. Media data encryption	256
25.8. Level 8. End-to-end encryption using VPN gateways	256
25.9. Level 9. Offline operation in your corporate network	256
25.10. Level 10. Flexible settings of file storage period	257
25.11. Level 11. Access to API via OAuth 2.0 protocol	257
25.12. Level 12. Regular security updates	257
25.13. Level 13. Encryption support for all stored data	258
25.14. Level 14. Integration with DLP	258
25.15. Level 15. Connection of external users via a separate server	258
25.16. Level 16. Traffic protection with the border controller	258
25.17. Level 17. Custom push notification service	258

1. Description

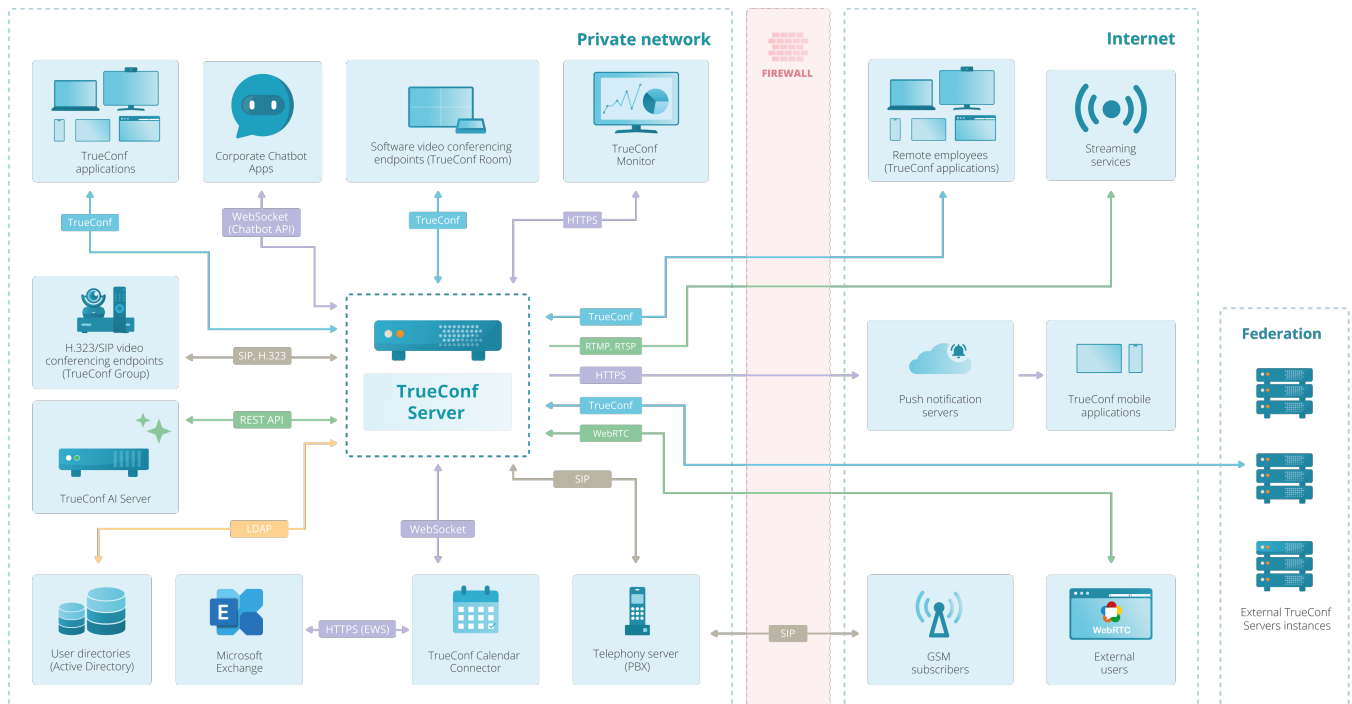
1.1. Why do you need a video conferencing server

TrueConf Server is a software-based video conferencing and team messaging platform. With our solution, your employees can communicate and collaborate remotely, organize webinars and remote training.



This guide is intended for TrueConf Server administrators. For information on the personal area, call strings, and other useful features for subscribers and guests of your video conferencing server, refer to the [user manual TrueConf Server](#).

TrueConf Server operates in LAN/VPN and can be used as a unified communication system that connects users of your local network, remote employees, and SIP.H.323/RTSP devices:



1.2. Capabilities

TrueConf Server core features can be extended by the following solutions:

- TrueConf for Windows, Linux, macOS
- TrueConf for Android;
- TrueConf for Android TV;
- TrueConf for iOS/iPadOS;
- TrueConf Room;
- TrueConf Kiosk;
- TrueConf Videobar.

1.2.1. Supported Protocols and Codecs

1.2.1.1. Protocols

- Proprietary SVC-based TrueConf protocol used by all client applications.
- H.323 protocol set: H.239 for content sharing; H.281, H.224, Q.922 for camera control; H.235 for media stream encryption; H.225, H.241, H.245 signaling protocols.
- SIP protocol suite: BFCP for content sharing; FECC for camera control; SRTP for media stream encryption; TLS for the secure signaling protocol (SIPS).
- WebRTC: SRTP and DTLS for media stream encryption.
- Connection of IP cameras and external streams (e.g., conferences) via the RTSP protocol.
- Stream your conferences to third-party services via RTSP and RTMP protocols.
- Integration with mail servers via the SMTP protocol.
- QoS support: DSCP, DiffServ.
- Integration with directory services using LDAP and LDAPS protocols. There are ready-made templates available for **Active Directory**, **OpenLDAP**, **389 Directory Server**, **FreeIPA**.
- Working with TrueConf API via the OAuth 2.0 protocol.

1.2.1.2. Supported Video Compression Standards

- VP8 SVC, VP8, AV1, VP9, H.264, H.264 AVC, H.264 SVC, X-H264UC, H.263, H.263+, H.263++, H.261

1.2.1.3. Supported audio compression standards

- Opus, G.711, G.722, G.722.1, G.722.1C, G.723, G.728, G.729A, Speex, MP3, AAC, PCM

1.2.2. Modules of the video conferencing server and their functionality

TrueConf Server is a software-based solution with several components that can be deployed on Windows and Linux.

You can also expand your video conferencing capabilities with the help of TrueConf [software development kit \(SDK\)](#).

You can find the main features of each component below.

1.2.2.1. System Services

This component is a software video conferencing server which is installed as [multiple services](#) of the operating system. This component ensures:

- user authentication and authorization: multilogin is also supported which means that it is possible to work in several client applications under the same account
- hosting [multi-user video conferences](#) and [one-on-one video calls](#);
- server events logging (calls, user authentications, chat messages, etc.)
- NAT traversal and proxy servers to connect users
- processing media streams using [SVC \(Scalable Video Coding\)](#) technology;
- compatibility of video conferences with third-party protocols and systems ([SIP/H.323](#), [RTSP](#), [WebRTC](#), [LDAP](#), DLP systems);
- synchronization with auxiliary solutions TrueConf: [TrueConf Monitor](#), [TrueConf Calendar Connector](#), [TrueConf AI Server](#);
- the ability to combine multiple servers into a [federation](#) to maintain communication between them;
- the ability to deploy the system based on multiple VCS servers using the [TrueConf Enterprise](#) solution.

1.2.2.2. Administrator Control Panel

This component is used to [control and modify server configuration](#) during its operation. The control panel provides the following capabilities:

- Manage user accounts and personal settings.
- Create, edit and delete groups, change group rights.
- Store TrueConf Server user account data either locally or using a third-party service via LDAP protocol.
- Configure authentication in the video conferencing system (via login/password; through SSO; using two-factor authentication providers, such as AD FS, Keycloak);
- Add aliases for SIP/H.323/RTSP devices or for users from another TrueConf Server instance to make it easier to call them.
- Create webinars for guest connections.

- Schedule conferences with weekly recurrence on specific days.
- PIN-protected conferences to prevent unauthorized access.
- Customize registration settings for public conferences (webinars)
- Create conferences supporting simultaneous interpretation for international online events
- Create a general layout for all participants, for SIP/H.323/WebRTC participants or individual layout for each user.
- Manage cameras and microphones of active conference participants, change their devices remotely.
- Add and remove participants from ongoing conferences.
- conference streaming configuration: Wowza Streaming Engine, Wowza Streaming Cloud, YouTube, etc. (extension required **Streaming**);
- Send email invitations and newsletters to users via external SMTP server.
- configure the media traffic transmission directly between conference participants bypassing the server (extension **UDP Multicast Conferences** required);
- Store and access conference recordings in the TrueConf Server control panel, view records with video and chat synchronized, download and delete them.
- Store the files shared in conferences on the server side.
- Create and start surveys, both internal and public (for external participants)
- Create backups and restore server settings.
- Customize your guest page and indicate administrator's contact info.
- Limit access to the TrueConf Server control panel for certain admin roles or using IP filters.
- Monitor server performance both in real time and for a certain time range.
- View server reports (log files) and all user actions (call history, message history, connection history, etc.).
- Check information about the mail plugins that can be used to create conferences when adding new events to the calendar (MS Outlook and Thunderbird are supported)
- Configure access to the TrueConf Server API.

1.2.2.3. Administrator control panel with the Security Admin role

Individual administrators can be added to the [TrueConf Server Security Admin](#) group. They will be able to view the server's operational details in its control panel without the configuration capabilities available to the TrueConf Server administrator.

The rights of TrueConf Server Security Admin provide access to:

- information about the current server state
- the list of addresses for administrative access
- history of settings changes
- server operation logs
- call and conference history
- current connections to the server
- chat history.

1.2.2.4. Personal area

Personal Area is a dedicated web page available to every user registered in TrueConf Server. The Personal Area allows you to:

- view features available to them
- access their address book
- use different conferencing modes to create meetings, launch and end conferences
- invite new users to ongoing conferences
- set different layouts when creating or holding meetings
- manage users' devices
- view detailed analytics about ongoing and past conferences
- download conference recordings saved on the video conferencing server
- save conference templates for further use
- edit their profiles (if LDAP/AD extension is enabled, users can only change their avatars).

1.2.2.5. Guest Page

The guest page TrueConf Server is a webpage where you can download client applications for [connecting to this server](#). The link can be shared with all employees and [guests](#) who will participate in conferences.

On the guest page, users can:

- log in to their personal area
- download client applications for various operating systems
- schedule a meeting (authorization required)
- connect to the conference with conference ID
- refer to the [user guide](#);
- view administrator contacts for TrueConf Server.

1.3. Selecting the Server Version

We provide a free TrueConf Server Free, a fully functional trial version for 3 weeks, and a paid version. A comparison of all three versions is available [here](#). You can calculate the cost of the right license with our [pricing calculator](#).

To obtain a fully functional version of TrueConf Server for 3 weeks of testing, [contact us](#) using any method convenient for you.

Thus, you can obtain a solution with all the necessary features by using the free version of [TrueConf Server Free](#), although with some minor limitations. This will be sufficient to deploy a video conferencing system for small and medium-sized businesses and to experience all its benefits.

1.4. Advantages

The video conferencing system TrueConf Server offers several advantages and unique technologies:

- Relatively low [system requirements](#). More examples of typical configurations are provided in [the following article](#).
- Work in a corporate (private) network without connecting to the Internet and sending data to third-party servers.
- Additional [data protection levels](#).
- Convenient administration.
- Advanced [technologies to enhance the quality and reliability of video communication](#).
- Video conferencing in [in 4K resolution](#). The total video resolution in a group conference may reach 7680×4320 (Ultra HD 8K).
- Collaboration tools.
- Streaming conferences to popular services.
- Managing video layouts and participants' devices.

1.5. Useful Resources

We offer administrators and TrueConf users plenty of helpful links to our resources and communities:

- [Knowledge base with helpful articles](#)
- [Training portal](#)
- [Getting started with the TrueConf](#) client application – a brief guide for beginners who find it challenging to understand our video conferencing system from scratch.
- [Official Telegram channel with news about the company's products](#)
- [Telegram community of administrators and TrueConf users](#) – here you can find answers to many frequently asked questions and get a better understanding of video communication. You can talk to other channel participants, including our employees.
- [YouTube channel with video reviews and webinars](#)
-
-
- [Community on Facebook](#)

2. User Types

TrueConf Server It supports flexible role separation for users and administrators working with our video conferencing system. Below, we will outline the features available for each role.

2.1. User roles

All users connected to TrueConf Server are divided into the following categories:

- **User** – a user account registered on TrueConf Server. Each user can sign in with their account in one of the following ways:
 - in the client application ([for Windows/macOS/Linux](#), [for Android](#), [for iOS/iPadOS](#), and even [for Android TV](#));
 - in the [personal area](#);
 - on terminals [TrueConf Group](#) or [TrueConf Videobar](#);
 - in the software terminal [TrueConf Room](#);
 - using SIP/H.323 devices that support registration on a Gatekeeper or PBX, for example, a [Phoenix Spider](#) speakerphone or a [Polycom HDX](#) terminal.

If a user is registered on the server, but is not currently authenticated, he/she will not be counted as one of **online users** whose number is limited by the license.

Please note that a conference can be created only by users authorized in the client application or in the personal area.

- **Guest** – an unauthorized user who joins a TrueConf meeting. Guest access is only supported in public web conferences (webinars) only. Guests can join the meeting via a link or after preliminary registration. Guest can be assigned with a moderator or speaker role. These roles are described below.

When creating a public conference, you can restrict guest permissions, prohibiting them from sending messages, audio, and video.

Unlike authenticated users, guests can only see TrueConf ID (login) and the display name in the cards of other conference participants. This restriction is set due to security reasons and cannot be removed by the server administrator.

- **SIP, H.323 and RTSP devices** – SIP/H.323 endpoints that participate in a meeting (but are not registered on the VCS), and [RTSP streams](#) (for instance, for IP camera broadcasting).

For more information on how connection to TrueConf Server for each type of user is licensed, refer to the "Licensing TrueConf Server" section.

2.2. User ID

Each user of the TrueConf Server video conferencing server (as well as the TrueConf Online online service) must have TrueConf ID.

TrueConf ID is a unique TrueConf user identifier designed for authorization in client applications and participation in video calls and conferences.

TrueConf IDIt typically takes the form `<user_id>@<server>`, where `<user_id>` represents the username provided during registration, and `<server>` is the server name TrueConf.

Examples:

User with the name `maria` on the corporate TrueConf Server named `server.example.com` :
`maria@server.example.com`

Despite the use of the `@` symbol, TrueConf ID is not an email address. If you send an email to the user's TrueConf ID, it will not be delivered.

2.3. Participant roles in a conference

All registered users and guests (in public events) attending a TrueConf conference are referred to as **participants**. In addition to video conferencing, they can interact with each other through chat, reactions, and audio remarks (in a moderated role-based conference). Each participant is visible to everyone else in the conference participant list and cannot be hidden. They also have additional rights depending on their role.

2.3.1. Moderator

A **moderator** is a conference participant who manages the event. This user is allowed to:

- Invite users to the video conference
- Remove participants from the event
- Invite attendees to the podium during a moderated role-based conference
- "Pin" speakers on the podium during a smart meeting
- Control the devices of any other conference participant
- Change the video layout
- Select an audio track for participants in a conference with simultaneous interpretation
- Change the PIN code and ID for an ongoing conference
- Lock an ongoing conference for new participants
- Manage the waiting room and send participants to this room
- End the conference.

Unlike the **owner**, there can be multiple moderators in a TrueConf conference. Moderators can be appointed by the conference owner or any other moderator.

A [guest](#) or a participant from another TrueConf Server, with whom your [federation](#) is set up, can also be appointed as the moderator.

2.3.2. Owner

The **owner** is either the user who created the conference or was given the owner role by the administrator when the [event was scheduled or edited](#). When this user joins the conference, he/she receives:

- All [moderator rights](#) listed above
- Access to event analytics
- The right to manage video recording on the server side
- Ability to download video recordings of this conference stored on the server.

A moderator cannot remove the owner from the conference.

2.3.3. Operator

An **operator** is a user who is automatically given the **moderator** rights in all video conferences that this person joins on his/her server. This role can be helpful if it is necessary to appoint an experienced person who can assist in conference management.

In addition to moderator rights, an operator can:

- Join any conferences protected by a PIN code without having to enter it
- Join locked conferences.

Operator rights, unlike moderator rights, are not transferred via [federation](#). This means that if you are an operator on your TrueConf Server, you will not be an operator when joining a conference hosted on a different server (with a different address).

2.3.4. Speaker

A **speaker** is a conference participant who is allowed to make a presentation to other participants.

Depending on the selected conference mode, the role of a speaker can be given to:

- in an ["everyone on screen"](#) mode conference – each participant;
- In [video lecture](#) mode – only one participant (teacher), who can be heard and seen by other participants (students). However, it is possible to add another speaker by giving the selected participant the moderator role. This person will also be displayed in the layout.
- In a [moderated role-based conference](#), any participant can become a speaker after sending a special request for the podium. Additionally, a moderator can invite a participant to the podium. The number of spots on the podium has to be specified when creating the conference.
- In a [smart meeting](#) – any user who starts speaking or sharing content. This person will be displayed in the layout instead of the participant who keeps silence longer than others or who started content sharing earlier than others (if his/her microphone is muted). The number of spots on the podium is limited and can be specified when the conference is created. A moderator can “pin” any participant on the podium so this person is displayed in the layout even if he/she is silent.

2.3.5. Translator

An **interpreter** is a conference participant who is allowed to translate the presentations of other participants simultaneously in [conferences with corresponding settings](#). The interpreter selects the language from the language pair assigned to him/her (e.g., English-Spanish). All attendees, who select the translated language, can hear the interpreter, although they do not see the interpreter in the video layout (in the participant list, the interpreter is displayed in the separate **Interpreters** section).

2.4. Administrative roles

In TrueConf Server, there are two types of administrators based on user groups that are automatically added to the OS during the server [installation](#).

2.4.1. Administrator with full access

An administrator with full access is a role that offers complete control over TrueConf Server settings via the control panel. This role is given to a user of the OS where the video conferencing server is installed. The user has to be added to the special OS group:

- **TrueConf Server Admin** on Windows
- **tcadmins** on Linux.

To manage server settings, you need to log in to the control panel with this user's credentials (username/password).

2.4.2. Security Administrator

A security administrator is a role that provides limited read-only access (without modification) to certain data in the TrueConf Server control panel: event reports, connection data, conference and call recordings (if available), and chats. This role is given to a user of the OS where the server is installed. The user has to be added to the special OS group:

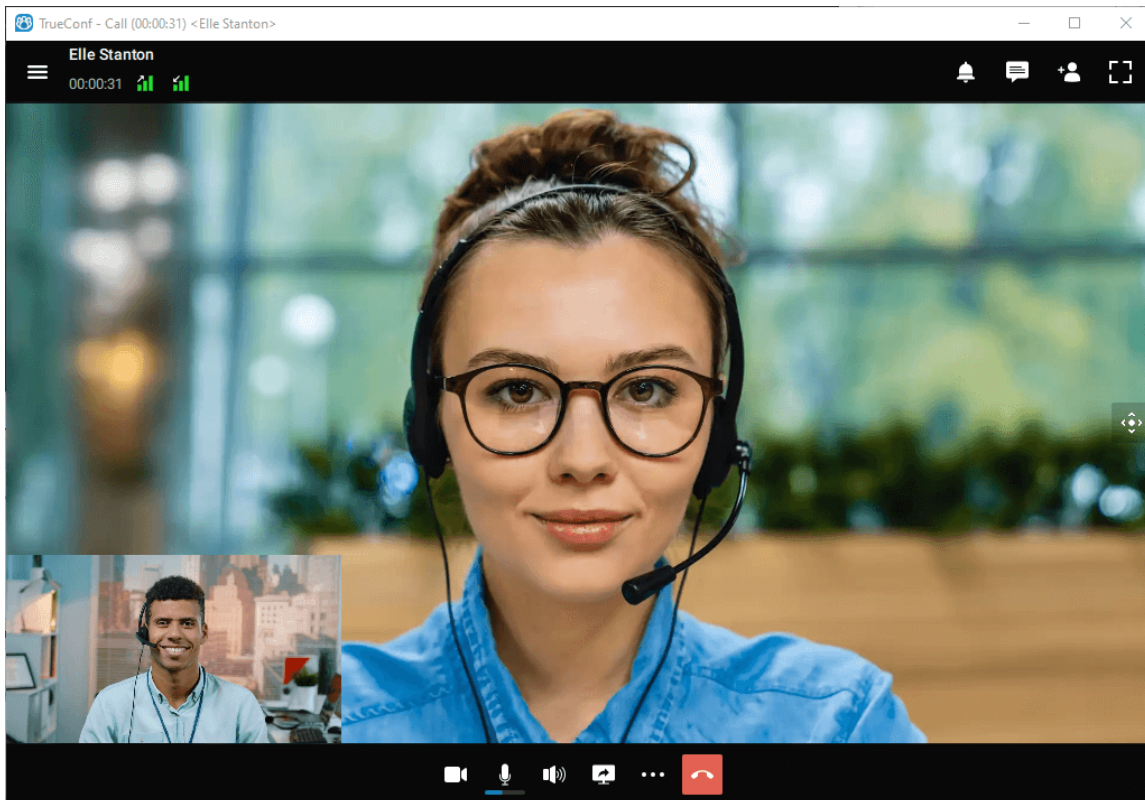
- **TrueConf Server Security Admin** on Windows
- **tcsecadmins** on Linux.

3. Types of Conferences

TrueConf Server supports various video conferencing modes that you can utilize depending on your current business needs.

3.1. What is a video call

A **video call** is a video communication session between two users who can see and hear each other.

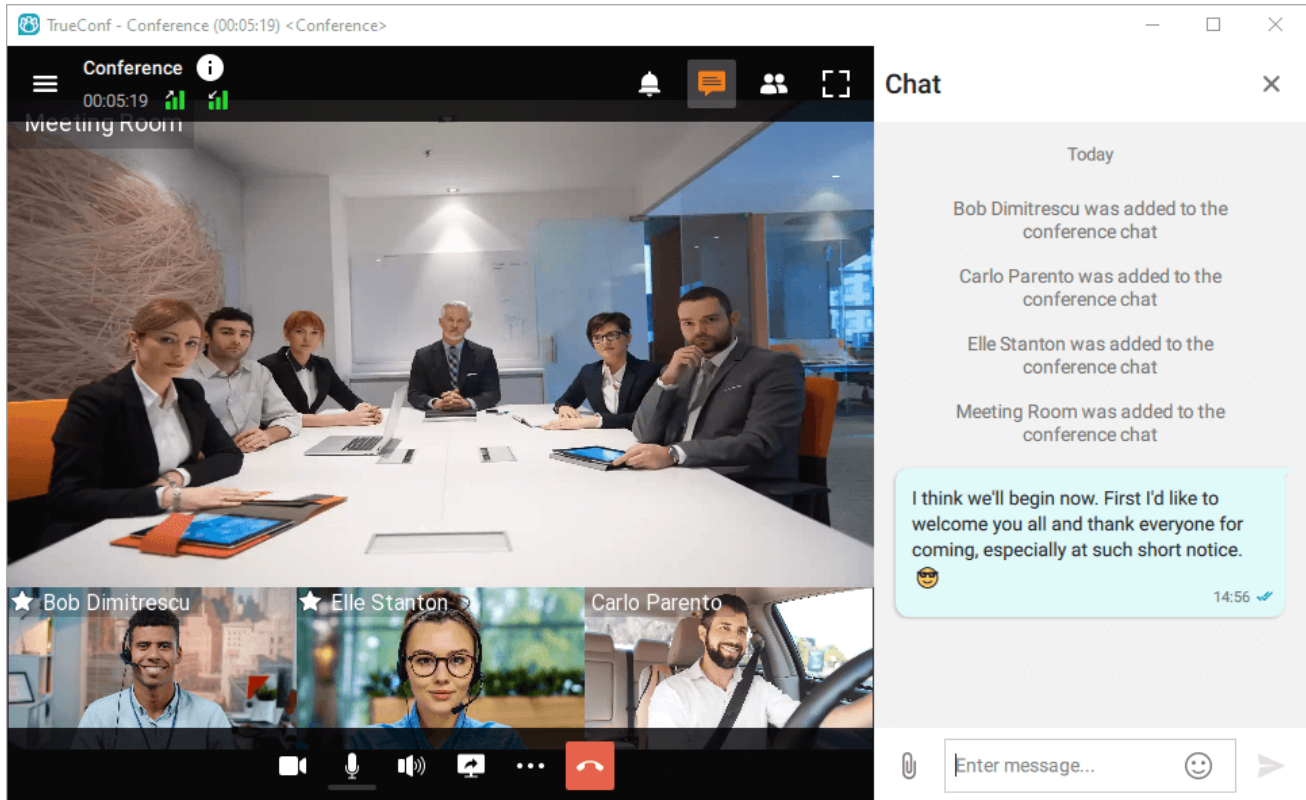


TrueConf provides a number of additional options during video calls: chat, file sharing, content sharing (e.g. sharing screen or separate application windows) and other collaboration tools.

For more information on video calls, visit [our website](#). You should also review the [system requirements](#) and materials on how to make video calls in client applications for various operating systems: [Windows / Linux / macOS](#), [Android](#), [Android TV](#), [iOS / iPadOS](#).

3.2. What is a video conference? Types of video conferences

Video conference is a video conferencing session between more than two users.



TrueConf Server enables holding video conferences of the following types:

- **Private.** Secure conference available to users authorized on your TrueConf Server instance or on a federated instance. Private conferences can also be accessed by third-party SIP/ H.323 and RTSP devices if they have received a conference ID (e.g., in an email invitation).
- **Public (webinar).** Public conferences are organized for guests (users that do not have an account on your VCS server instance) and can be easily accessed by anyone with a link or by following an email invitation. If you do not have **Public Web Conferences** extension enabled on your server, this conference type will be unavailable.

Group conferences TrueConf also vary by launch type:

- **Scheduled.** Video conference with a specific start date and time and duration of the event. It is possible to schedule a conference to be launched weekly on certain days (e.g., on Tuesdays and Fridays).
- **Virtual room** – an unscheduled conference with no duration and start time settings. Participants can join and leave this meeting at any time by using its ID up until the moment when this meeting is deleted from the server.

The maximum duration of an active virtual room is 240 hours, after which it will automatically end. However, users can reconnect to this event.

Detailed step-by-step instructions on how to join a conference are described in the [article in our knowledge base](#).

The administrator of TrueConf Server can create a group conference of any type and view information about ongoing or scheduled conferences in the control panel (admin panel). Registered users can do it in the [scheduler](#) of their client applications and in their personal area.

System requirements for client PCs for different video conferencing modes are available [here](#).

3.3. Video Conference Modes

TrueConf Server supports the following video conferencing modes:

- **All on screen** – all participants are speakers which means that they can see and hear each other.
- **Smart meeting** – participants are automatically given the role of a speaker if their voice activity is detected or when they start sharing content.
- **Moderated role-based conference** – speakers are selected by the moderator.
- **Video lecture** – the lecturer is the only participant given the role of a speaker; he/she can also see and hear all other participants.

Read more about the advantages of each mode [on our website](#).

3.4. Conference ID

Conference ID (CID) is the unique identifier assigned to each video conference on TrueConf Server. If you need to join a conference on a different server (federation has to be configured with this server), you should specify the full CID along with the server address in order to make a direct call. To join a conference on your corporate video conferencing server, you can simply specify the ID without the server address.

Examples:

```
\c\interview
```

```
\c\12345
```

```
\c\interview@video.example.com
```

 — the full CID, including the server address.

If this identifier is not set explicitly, it will be generated automatically when a meeting is created and will consist of digits. However, it is possible to create an arbitrary identifier for both private and public conferences. In this case, CID may include digits, Latin letters, underscores, and hyphens.

Manual assignment and editing of conference IDs can be disabled for all events by [server administrator](#).

If this action is not forbidden by server settings, you can set the ID before the conference start:

- in the server control panel
- in the [client application's scheduler](#);
- in the personal area.

It is also possible to change the ID of an ongoing conference in the [real-time meeting management section](#).

To join a video conference, a user only has to know its ID. The conference ID is used to generate a link to the conference page.

3.5. What is a waiting room

The **waiting room** is a preliminary queue of participants who try to join a conference. When this option is enabled, certain participants will be automatically put in the waiting room when they try to join the meeting, if they were selected on the **Advanced** tab when the event was created. The use of the waiting room is available in both private and public conferences of any mode.

There is a participant in the waiting room:

- cannot be seen in the list of participants by anyone except moderators
- is unable to receive video and audio from other conference participants and cannot send his/her own audio and video streams
- cannot see the list of conference participants
- cannot access
 - chat
 - audio reply and the podium
 - collaboration tools (recording, content sharing, reactions, remote desktop control).

A participant can be moved from the waiting room to the conference by any [moderator \(including the owner\)](#).

When a user is invited to the conference from the waiting room, he/she can take advantage of all features available to participants.

4. Enhancements

The core features of TrueConf Server can be enhanced with various extensions. Many of these extensions are available in all versions of the server, including the free version. However, some of them can be activated only after purchasing the specific technical support package.

4.1. SIP / H.323 / RTSP gateway

Thanks to this extension, it will be easy to connect to TrueConf Server:

- Video conferencing terminals from third-party manufacturers and [PBX](#), as well as users of popular [cloud services](#) such as Zoom, Cisco Webex, LifeSize Cloud, and Skype for Business servers — via SIP/H.323 protocols;
- [IP cameras and video surveillance systems](#) as well as streams (e.g., streams of other conferences) — via the RTSP protocol.

With TrueConf Server Free, you can have one SIP/H.323/RTSP connection for free.

The gateway acts as a gatekeeper or SIP registrar for third-party devices that will be displayed as regular TrueConf users in the address book.

The configuration of the TrueConf Server multigateway is detailed in the [section "SIP/H.323/RTSP Gateway and Transcoding"](#) of the documentation.

4.2. Integration with LDAP and Active Directory

With this extension, you can synchronize user information between the TrueConf Server address book and your company's [LDAP directory service](#) (e.g., Active Directory). Administrators can centralize and automate user account management operations, such as adding new users or removing ex-employees, resetting passwords, or keeping user data up to date.

This extension is available in any version of the server, including the free TrueConf Server Free.

The settings for integration with LDAP/AD directories is described in the [section "Users and groups. Integration with LDAP/Active Directory"](#) of the documentation.

4.3. Public Web Conferences

With this extension you can organize public web conferences available to users that do not have an account on your TrueConf Server instance. This feature is typically used for conducting [webinars](#).

Each public web conference has an external web page that contains a conference description and provides information on how to connect to it. You can also [embed a public web conference](#) to your website with a widget.

With TrueConf Server, you can organize public web conferences with 1 guest connection. If you would like to add more guest connections to your license, please [contact us](#) to request a free trial or purchase the extension.

For more details on creating a conference with guest connections, refer to the description in the [“Group conferences and streams”](#) section.

4.4. Live Streaming

This extension allows you to [broadcast video conferences](#) through external platforms or content delivery services such as CDNvideo, YouTube, Facebook or Wowza. The number of viewers is limited only by the capabilities of your chosen streaming solution and can exceed 1 million users!

This extension is available with the purchase of the [extended or full technical support package](#).

4.5. Simultaneous Interpretation

Let us suppose that an international conference is to be held and presenters will speak multiple languages. In such a case, one has to make sure that all participants can fully understand the speakers. Such a task can be easily done with the **Simultaneous interpretation** extension: just [select simultaneous interpreters](#) who will translate all presentations into required languages on the fly. In your video conference, there will be the list of audio tracks with different languages and every participant will be able to select a track in a client application or browser.

If server-side recording is activated for an event with simultaneous interpretation, multiple audio tracks will be created: the main track and a separate track for each language into which the conference was translated.

This extension is available on request, just [contact us in any convenient way](#) to specify the terms of activation.

4.6. Federation

To enable calls between users of multiple TrueConf Server servers located in different branches within your network, use the **Federation** extension. You can also connect with other companies using TrueConf server or cloud products. Federation allows users on your server to call and invite any TrueConf subscribers to conferences, and vice versa.

Another important advantage is that participants' media streams are processed on the servers where these users are authorized. This helps to reduce traffic between distributed networks and decrease the load on the hardware of the TrueConf Server instance where the conference is created.

This option is included in the standard functionality of TrueConf Server and to activate it, [you just need to have *any* paid license](#).

For a detailed description of federation and its settings, refer to the [section "Network and federation settings, email notifications"](#).

4.7. Integration with DLP

This extension is part of [TrueConf Enterprise](#) and allows you to connect TrueConf Server to a third-party DLP system using the [ICAP protocol \(RFC 3507\)](#).

DLP system (Data Leak Prevention) is a specialized software solution that follows certain security policies to prevent the leakage of confidential information, for example, it is needed to ensure that data cannot cross the borders of the corporate network.

Thanks to the integration with such a system, every message (including a file) sent in private and group chats is automatically directed to a DLP system before it could be directed to the recipient. This message will be checked and if it does not meet security requirements set on the side of the DLP system, it will not be sent. On the side of TrueConf Server, you can choose if the recipient should see a notification that the message was blocked or simply receive no message.

To learn about integration with DLP systems, refer to the ["Configuration of extensions" section](#).

4.8. Support for SDK applications

[TrueConf SDK](#) allows you to develop custom applications with the corporate features you need and incorporate communication based on TrueConf technologies. For example, if you have an application with news about companies and promotions for clients, you can use a widget from the SDK to connect with your representative (operator). We offer libraries for all popular desktop (Windows, Linux, macOS) and mobile (iOS, Android) platforms.

An example of an application developed using the TrueConf SDK is the [TrueConf Kiosk](#) information kiosk – a software solution for self-service systems.

In addition to SDKs for various platforms, you can use API calls for several of our products: [TrueConf Server](#), [TrueConf MCU](#), [TrueConf Room](#), [TrueConf Group](#). The API allows you to remotely execute a range of commands and retrieve data from these solutions, for instance, from external code based on certain triggers.

You can [find code examples for working with our SDKs and APIs on GitHub](#).

4.9. Integration with AI server

TrueConf offers [a standalone solution TrueConf AI Server](#). It is based on AI (machine learning) and intended for creating conference transcripts. This AI server automatically recognizes audio streams from conferences and generates transcripts with speakers' names included. A single AI server can be integrated with multiple video conferencing servers. It is also possible to configure flexible user access settings for transcripts and audio recordings.

To use the AI server within your video conferencing infrastructure, activate the separate **TrueConf AI Server** extension. For more details on how to configure this solution, refer to the description of the [corresponding section](#) in the control panel.

4.10. Integration with a corporate calendar

In large companies, employees often use Microsoft Exchange corporate mail and schedule various events in Outlook. The TrueConf Calendar Connector solution is intended for such organizations. It supports automatic import of all events created in Outlook into the calendar of TrueConf client applications. So, users will see all events in a single interface: those that include TrueConf conferences and regular events that are not linked to any conference.

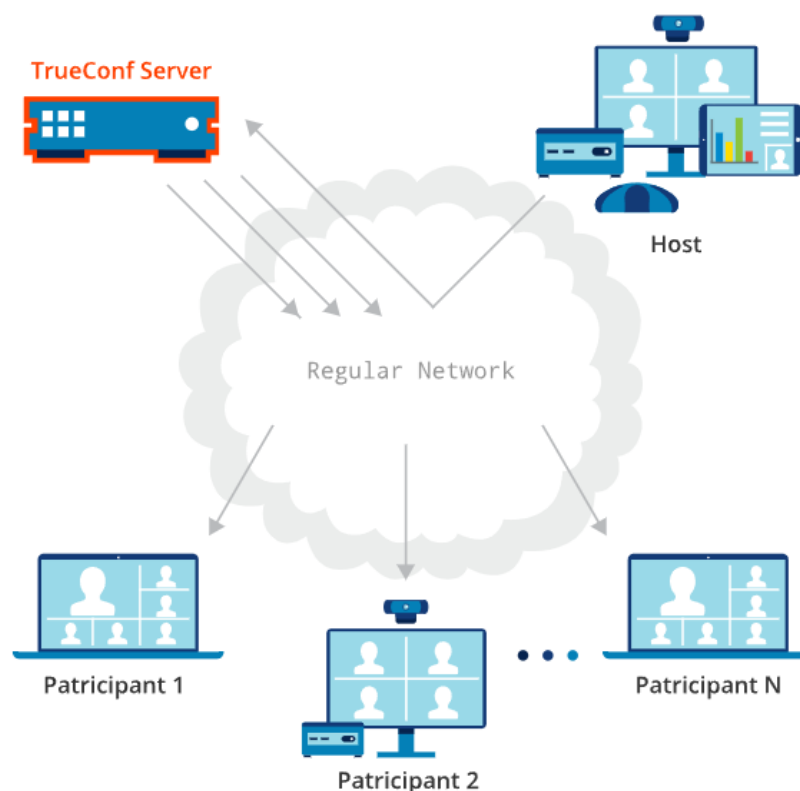
To integrate the corporate calendar with the video conferencing system, you only need to purchase a license for TrueConf Calendar Connector. Additionally, some features are available even in the free version. For more details on how to set up integration with TrueConf Calendar Connector, refer to the description of the [corresponding section](#) of the control panel.

4.11. Using UDP Multicast

UDP (User Datagram Protocol) Multicast is a data transmission protocol under which a signal is transmitted through the Multicast switch, bypassing the server.

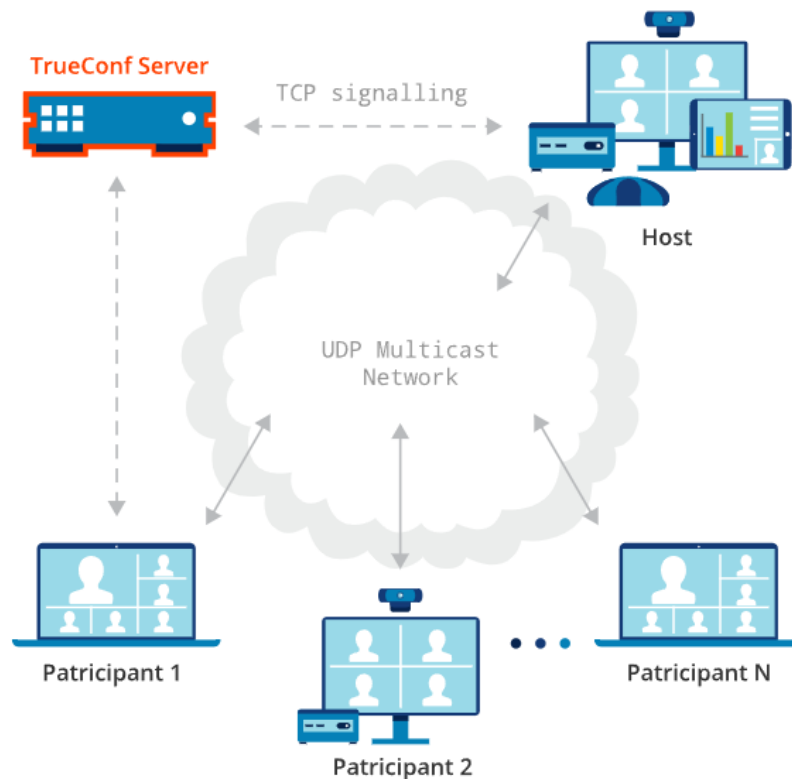
This extension is available with the purchase of [any paid license](#).

During a standard group video conference (without UDP Multicast mode) data are transmitted through a TrueConf Server instance to each participant. Data traffic during such a conference can substantially load the server channel.



The use of [UDP Multicast mode](#) during a group conference allows meeting participants to exchange data directly with each other without the server which, in turn, decreases the network load on the server. Audio and video streams are transmitted only inside the UDP Multicast

domain. These domains can be used in LAN or VPN. By default, data transmission via the UDP Multicast protocol is possible only inside a closed corporate network.



Please note that in UDP Multicast mode, some features are not supported; this includes conference recording, connections via SIP/H.323/RTSP, browser-based conferences via WebRTC, and streaming to third-party services.

4.12. TrueConf Directory

This extension will enable the users of your TrueConf Server to search for users/groups on all TrueConf servers synchronized with it and add them to the address book. As a result, your users will have a unified address book available in [client applications](#).

TrueConf Directory is part of [TrueConf Enterprise](#).

For information on configuring TrueConf Directory, refer to the [“Extension Setup” section](#).

4.13. TrueConf License Manager

This extension is part of [TrueConf Enterprise](#) and is designed to balance the license pool used by group TrueConf Server. Detailed documentation for configuring the balancing is provided by our technical support team upon request from enterprise customers.

4.14. TrueConf Border Controller

TrueConf Border Controller (border controller) is an extension for [TrueConf Enterprise](#) designed for installation in the corporate network's DMZ (demilitarized zone) to protect video conferencing servers from malicious external traffic.

For more information on how this extension works and how to set it up, please refer to [its documentation](#).

4.15. TrueConf Enterprise

When using TrueConf Server in large enterprises with over 500 employees, one may find it necessary to deploy additional servers. This approach is convenient for companies with geographically dispersed branches.

For such clients, TrueConf offers a **TrueConf Enterprise** – a turnkey solution with a unique configuration designed to meet the customer's requirements.

Main benefits:

- The complete replication of key nodes ensures 99.99 % availability of all system components across the entire enterprise.
- Users of TrueConf Enterprise have access to an exclusive premium technical support package.
- The ability to balance server load (by connecting additional TrueConf Server instances along with dynamic license borrowing on the main server).
- Branding client applications.

You can learn more and order this solution on [our website](#).

4.16. Advanced monitoring of video conferencing servers

In the TrueConf Server control panel, there is a [monitoring page](#) with basic information about the server's operation. Additionally, the company TrueConf offers [a separate solution TrueConf Monitor](#) for advanced performance monitoring and data collection. This solution allows you to track statistics across multiple servers and offers several other benefits:

- Track active conferences, their participants, and online users from each connected server, as well as the total number of ongoing conferences.
- Monitor server hardware performance metrics: average disk wait time and performance in IOPS, swap file usage, detailed RAM and CPU information.
- View conference history.
- Advanced analysis of data about participants' connection and errors during a video conferencing session.

5. Licensing

Access to different features of TrueConf Server collaboration platform is determined in two ways:

1. The presence of [extensions](#).

Title	Terms of Provision
LDAP/Active Directory	Free
SIP / H.323 / RTSP gateway	Purchase the required number of gateway connections (1 connection is available for TrueConf Server Free).
Public conferences (webinars)	Guest connections are purchased guest connections (1 guest connection is available for TrueConf Server Free)
Simultaneous interpretation	Free
Integration with a corporate calendar	The solution TrueConf Calendar Connector is licensed separately (a free version is available)
Integration with AI server	Licenses are required for both the integration module and TrueConf AI Server itself (for more details, see the integration description).
Federation	Purchase of any paid license
Ability to set a watermark for the conference video layout	Purchase of any paid license
Live streaming	Purchase of a extended or full technical support package
UDP Multicast conferences	Purchase of any paid license
Integration with DLP	Included in TrueConf Enterprise
TrueConf Directory	Included in TrueConf Enterprise
TrueConf License Manager	Included in TrueConf Enterprise
TrueConf Border Controller (border controller)	Included in TrueConf Enterprise
Support for SDK applications	Available upon request

You can learn more about the levels of technical support TrueConf by following this [link](#).

2. Licenses that set the number of connections for each of these types:

License Type	Who can use it	Features
Online users	Authorized users on TrueConf Server	All capabilities of the video conferencing server, except for participation in group conferences
PRO users	Authorized users on TrueConf Server	Participation in group conferences
Guest users	Users without an account on TrueConf Server	Participation in public conferences (webinars)

License Type	Who can use it	Features
SIP/H.323/RTSP connections	Connections using SIP, H.323, RTSP protocols (terminals, PBX users, IP cameras)	Participation in conferences via SIP, H.323, RTSP protocols

In TrueConf Enterprise, there is no difference between PRO and online users which means that all authorized accounts can participate in conferences.

The server administrator can track the number of available connections for each of the listed types in the **Summary → License info** tab.

The free version of TrueConf Server Free has limitations on the number of connections for each type. For details, please refer to the [product solution page](#).

Additionally, TrueConf Server Free **requires** a constant connection to the TrueConf Server Free registration server via the TCP port **4310**. This connection is necessary for continuous license verification, which involves frequent transmission of small data packets; this is a normal behavior.

Comparison of features available to PRO users, online users, and guests (assuming that all of them connect via client applications):

		PRO user	Online user
Point-to-point video calls	V	V	X
Using collaboration tools (screen sharing, local recording, etc.) during point-to-point video calls.	V	V	X
Messenger features include personal and group chats, file sharing, and more.	V	V	X
Access to the conference chat after it ends	V	V	X
Using the address book and personal area	V	V	X
Creating scheduled conferences and virtual rooms in the scheduler	V	V	X
Preparing slides for presentations before a conference or call	V	V	X
Participation in a public group conference (webinar)	V	X	V
Using the chat during a public conference (webinar)	V	X	V
Collaboration tools in a public conference (webinar) include content sharing, local recording, and more.	V	X	V
Ability to be a moderator in a public conference	V	X	V
Using the internal group conference chat during the meeting	V	X	X
Participation in an internal group conference	V	X	X
Opportunity to be a moderator for an internal conference	V	X	X
	V	X	X

		PRO user	Online user
Collaboration tools in internal conferences: content sharing, local recording, and more.			
Starting an instant conference from the application menu, as well as from the chat and address book.	V	X	X

Below we will closely discuss the licensing of each connection type.

5.1. Online users

Online users are the users who are authenticated under their account on your TrueConf Server. An online license is linked to the device, but not to the TrueConf ID of a user. So, if a person is signed in on a smartphone and PC at the same time, 2 online licenses will be taken.

If the OS run on a user's device puts TrueConf client application to sleep mode or closes it (e.g., if the PC was put to sleep mode), TrueConf Server will not count such connections as online users. For example, if a user is authenticated on a mobile device and has the status  (recently active), no online licenses will be taken. Such a person is technically offline, even though he/she can receive push notifications.

When purchasing a license, 3 online users are provided for every 2 PRO users to ensure they can connect to the system from different devices. It is also possible to buy additional online licenses as packages for 50, 100, 200, 300, 400, and 500 users at the price which is much lower than the price for PRO licenses.

Thus, the competitive advantage of separate licensing for online users on TrueConf Server is that it allows company employees to stay connected via messenger and occasionally make [video calls](#). In other words, authorized users have access to all features of the TrueConf system, except for participation in [group conferences](#).

5.2. PRO Users and Conference Participation

The rules described in this section apply to the registered users of your video conferencing server. They can connect from:

- client applications TrueConf for desktops (Windows, macOS, Linux);
- client applications TrueConf for mobile devices on Android, iOS/iPadOS;
- client applications TrueConf for Android TV;
- software terminal TrueConf Room;
- hardware endpoint TrueConf Videobar;
- software solution for kiosks and self-service terminals TrueConf Kiosk;
- Browser (via WebRTC), in other words, the user joins a conference with a link (this does not include guests who are licensed separately).

PRO users (can also be called PRO licenses) are the users, who are authenticated on your TrueConf Server, and are allowed to participate in group conferences. The user, who is authenticated on the server from a single device, takes only one online license without taking a PRO license until he/she starts to participate in a group conference.

The number of available PRO licenses for participating in conferences is regulated by the **PRO users** parameter, which the server administrator can view in the control panel under the **Summary** section, on the **License info** tab:

The screenshot shows the TrueConf Server control panel interface. The top navigation bar includes the TrueConf logo, the address 'video.example.net#vcs', and a 'System' dropdown menu. The left sidebar contains a list of navigation items: Dashboard, Summary (selected), PRO Licenses, Settings, Network, Network Settings, SMTP, Federation, Gateways, SIP, H.323, RTP, WebRTC, Transcoding, Web, Settings, Security, HTTPS, Users, User Accounts, Groups, Aliases, Authentication, LDAP / Active Directory, Settings, Group Conferences, Conferences, Templates, Streaming, Settings, API, and OAuth2. The main content area is titled 'Summary' and has a 'Help' link. Below the title bar, there are tabs for 'Dashboard' and 'License info' (selected). The 'License info' section is divided into three panels: 'Registration details', 'License details', and 'Extensions'. The 'Registration details' panel shows 'Server ID: kk123', 'Organization name: Great Company', and 'Contact person: Joe Smith, smith@example.com'. It also indicates 'Registered' status, 'Expires in 162 days', and a 'Register' button with a 'License agreement' link. The 'License details' panel contains a table with the following data:

Item	Value	Action
Server license	Annual	
Connection to the registration server	Not required	
User accounts	196	
Active conferences	100	
PRO users	20	Add
Online users	1000	Add
H.323/SIP connections	5	Add
Guest users	4	Add
Technical support	Basic	Upgrade
License expiration date	31.01.2024	

The 'PRO users' row is highlighted with an orange border. The 'Extensions' panel lists various features and their status: SDK application support (Add), SIP/H.323 Gateway (Enabled), LDAP/Active Directory (Enabled), Public conferences/Webinars (Enabled), Streaming/YouTube integration (Enabled), Federation (Enabled), Integration with DLP (Enabled), TrueConf Directory (Enabled), UDP Multicast conferences (Enabled), File sharing (Enabled), Screen sharing (Enabled), Conference recording (Enabled), Slideshow (Enabled), and Improved Security (Enabled).

5.2.1. Features of using PRO connections

The administrator of TrueConf Server can distribute the common pool of PRO licenses which can be of two types: **permanent** and **temporary**.

Permanent licenses are given without any time restrictions to the users from the groups selected by the administrator. The users with permanent PRO licenses can join conferences at any moment without waiting for licenses to be released into the common pool. Distribution of permanent licenses is not available in the free version of the video conferencing server.

Temporary licenses are taken from the remaining pool of available PRO licenses and are given to other users based on the common rules described below:

1. If a user, who is not included in the group with permanent PRO licenses, tries to join a group conference, the application will check if PRO licenses are available. If there are available licenses, the user will automatically receive a **temporary** PRO status. This status will be reserved for this user for 24 hours. If the user joins the same group conference or any other during this period, the countdown will be reset to zero. While a user is staying in a conference, the PRO status is automatically renewed.
2. An administrator of TrueConf Server can instantly revoke a temporary PRO status from an existing (non-deleted) user by clicking the ✕ button next to their name (see the description in [section PRO licenses](#) of the control panel).
3. A PRO status of an account deleted from the server will be released 24 hours after deletion, and it cannot be manually revoked from such a user.

4. The server administrator can allow users to request a PRO license manually before participating in a conference (this status will also be active for 24 hours after reception).
5. The number of devices used by a person for participating in conferences does not affect the number of PRO licenses available on the server since the PRO status is linked to a specific user account (TrueConf ID). It is not tied to the device on which the user is authenticated. So, if the user, who is simultaneously signed in on two devices, joins two conferences from these devices, two online licenses and one PRO license will be taken.
6. When the number of PRO licenses available on the server becomes equal to 0 and a user tries to join a group conference, his/her status will be checked:
 - If this person has a permanent PRO status, he/she will be allowed to participate in the conference.
 - If this user previously received a temporary PRO status, and this status is still valid (check Step 1), he/she will be able to participate in the conference.
 - In other cases, the user will be unable to participate in a conference. At the same time, this person will still be able to participate in one-on-one calls and chats or make use of other features.
7. Permanent PRO licenses will be redistributed right after the manual restart of TrueConf Server. They can also be redistributed automatically every 24 hours (the countdown starts from the latest launch of the main server service):
 - If the pool of available PRO licenses is not sufficient for the users with permanent licenses, the licenses will be taken away from the users with temporary licenses (starting from the users whose temporary PRO status has the shortest expiry period).
 - If a user is removed from the group with permanent PRO licenses after the redistribution, this person will be given a temporary PRO license (if it is available). This step will be performed after Step 5.1.
 - If there are ongoing conferences, only the participants, whose PRO licenses were taken away after the automatic redistribution (Steps 5.1 and 5.2) will be removed from meetings.

Licenses are redistributed automatically so that one does not have to restart TrueConf Server manually to apply changes in the lists of user groups for which permanent PRO licenses are reserved. Besides, when licenses are redistributed automatically, ongoing meetings are not ended as it is the case when the server is restarted manually.

The administrator TrueConf Server can view the duration of temporary PRO connections and allocate permanent ones in the [section of the PRO Licenses control panel](#).

5.2.2. Using PRO connections in federation

If external participants connected via [federation](#) are joining a conference on your TrueConf Server, they do not use up PRO connections from your server's license.

Alternatively, if your users participate in conferences hosted on a federated server, only your PRO licenses will be taken.

5.2.3. Examples of PRO connections

Let us discuss some examples to get a better idea of this question.

Case 1

1. There are 10 PRO licenses on the server.
2. No permanent licenses were given to users which means that 10 PRO licenses are available.
3. In total, four users are authorized on the server (each one is authorized on a single device).
4. A user (this person's login will be **user**) takes part in a single group conference.
5. In the **PRO Licenses** control panel, the administrator can see that 1 PRO license (assigned to **user**) and 4 licenses for online users were taken.
6. The PRO license will be released by the **user** in 24 hours after he/she leaves the conference.

Case 2

1. There are 10 PRO licenses on the server.
2. Permanent PRO statuses are given to the **IT** group which includes 3 users.
3. In total, there are 2 users authorized on the server and they do not belong to the **IT** group.
4. One of the users from part 3 is taking part in a conference.
5. In section **PRO Licenses** of the TrueConf Server control panel, the administrator can see that 4 PRO licenses and 2 online user licenses have been used. This occurs because permanent connections are always reserved (allocated to three users from the **IT** group), and one temporary license is granted to the actual conference participant mentioned in item 3.
6. In this case, 6 PRO licenses will be available to other users. These licenses will be given automatically as it was [described above](#).

Case 3

1. There are 10 PRO licenses on the server.
2. Permanent PRO licenses were not given to users which means that 10 PRO licenses are available.
3. In total, 4 different users are authorized on the server with 3 of them being authorized from one device each.
4. A user (this person's login will be **user**) is authenticated on 2 different devices, and is participating in two group conferences from these devices.
5. In the **PRO Licenses** section of the TrueConf Server dashboard, it shows that the following have been used: 1 PRO license (by user **user**, due to the PRO license binding rule to TrueConf ID rather than to devices) and 5 online user licenses (2 by user **user**, and 3 by other authorized users mentioned in item 3.).
6. The PRO license will be released in 24 hours by the **user** after he/she leaves the last conference on any of the applications.

5.3. SIP/H.323/RTSP connections

The number of participants who can join your conferences via SIP/H.323/RTSP is regulated by the licenses needed for connections via the built-in gateway. TrueConf Server Free provides 1 connection via the SIP/H.323/RTSP gateway.

Connections via SIP/H.323/RTSP do not require PRO licenses. If the endpoint is authenticated with the user account, an additional online license is used. SIP/H.323/RTSP devices are always allowed to connect to a conference.

Case 1

1. 150 online licenses, 100 PRO licenses, and 5 SIP/H.323/RTSP licenses are activated on the server.
2. A server user invites 2 SIP endpoints (none of them is authorized on TrueConf Server) and 1 RTSP surveillance camera to a conference.
3. In the TrueConf Server control panel, the administrator will see that 1 online license and 3 SIP/H.323/RTSP licenses are used.

Case 2

1. There are 150 licenses for online users, 100 PRO licenses and 5 SIP/H.323/RTSP licenses.
2. A server user invites 2 SIP endpoints to a conference. One of the endpoints is authorized on TrueConf Server.
3. In the TrueConf Server control panel, the administrator will see that 2 online licenses and 2 SIP/H.323/RTSP licenses are taken.

5.4. Guest connections

[Public conferences \(webinars\)](#) can be joined by guests or the users who are not registered on your server. The number of such participants is determined by the number of guest connections supported by your license. TrueConf Server Free supports 1 guest connection.

Guest connections do not require PRO or online licenses. Guests are always allowed to join conferences. However, you need to keep in mind that one cannot send a text message to a guest user outside a conference or make a one-on-one call.

Example

1. There are 150 online licenses, 100 PRO licenses and 5 guest licenses on the server.
2. A server user invites 3 guests to a public conference.
3. In the TrueConf Server control panel, the administrator will see that 1 online license, 1 PRO license, and 3 licenses for guest connections are being used.

6. Preparing for Installation and System Requirements

Minimum steps to achieve a working corporate communication system:

1. *Choose a machine (PC, physical or virtual server) with suitable hardware.* **You are here!**
2. [Install TrueConf Server](#).
3. [Log in to the control panel](#).
4. [Register the server](#).
5. [Configure HTTPS](#) (it is used for many key features such as integration with the AI server, conference scheduling, etc.) and [specify the external server address](#) (the address of the guest page).
6. [Configure access to the server for users within the corporate network](#) and, if necessary, from an external network (outside the corporate network).
7. [Create user accounts](#) or [integrate the server with a directory service](#) via the LDAP/LDAPS protocol.
8. Install client applications for users and show them how to connect to your server (check the [documentation for the desktop application](#)).

After taking these steps, you will have a basic functional messenger with TrueConf video conferencing. However, this system should be thoroughly configured in various parts of the control panel, depending on your needs. For more information, refer to other sections of this documentation.

For testing purposes, you can install TrueConf Server on a consumer edition of Windows, but make sure that it is **not Home! Windows 10 / 11 Pro or Enterprise** versions are required because they provide user group management. Additionally, regardless of the operating system (Windows or Linux), the OS user account under which you are installing the server, **must** have a password.

6.1. Helpful explanations

TrueConf Server has several peculiarities that should be considered when selecting equipment for a specific setup. Understanding these features will help you in choosing the right components.

1. **IMPORTANT:** If you plan to use Intel® Xeon® 6 or newer, keep in mind that there are two versions of CPUs: one with only E-cores (energy-efficient) and one with only P-cores (high-performance). The main differences are that P-cores include Hyper-Threading, AVX-512 and AXM instructions, larger cache memory, and higher frequencies. So, in most cases, it is preferable to use VMs or VPS based on P-cores. In other situations, it is **essential** to consult with [technical support provided by TrueConf](#). In any case, desktop hybrid Intel CPUs should NOT be used.
2. **Only x86-64 CPU architectures** are supported (also known as x64, x86_64, AMD64, and Intel 64).
3. Different types of connections create varying loads on the CPU and network. For example, when TrueConf client applications for desktops and mobiles are connected, the server mainly uses CPU resources for transmitting media streams over the network, instead of

stream management, thanks to the [SVC technology](#). There is no need to transcode streams (as in the case of recording for mixing the resulting video). We can assume that processing 200 Mbps of traffic requires one physical core of a typical server CPU with multi-threading (Hyper-Threading or SMT). This means that if TrueConf Server is installed on a physical server, 1 core is needed to process 200 Mbps, when the server is installed on a virtual machine (VM), 1 vCPU is required to process 100 Mbps.

4. In practice, all users rarely participate in conferences at the same time. This is why the video conferencing server engine does not impose limitations on the bandwidth of corporate or Internet networks. However, in our estimates, we **recommend that you do not exceeding 3 Gbps** for the machine running a single TrueConf Server, regardless of the number of participants, types of conferences, etc. This is the maximum value that has been observed and tested in practice. If your usage exceeds this value and some problems arise, please contact our [technical support](#). You should also take into account the capabilities of the adapter installed on the machine running TrueConf Server.
5. TrueConf Server works equally well on Intel and AMD CPUs from approximately the same release year (family). It also supports multithreading technologies: Intel's Hyper-Threading and AMD's SMT.
6. CPUs released at different times (different generations) vary in per-core performance even if they have the same clock speed.
7. TrueConf Server Works the same on Linux and Windows.
8. In practice, we recommend making sure that CPU load on the machine with TrueConf Server does not exceed 80%. If your use-case scenarios involve higher loads, you should either allocate more resources to the virtual machine (VM) or physically upgrade the hardware.
9. The software can be installed on both physical and virtual machines (including VPS), so the system requirements are the same.
10. When a virtual machine is used, it is necessary to configure the CPU topology to have the minimum number of sockets. Please review the instructions for your hypervisor, but general recommendations are as follows:
 - If we allocate N threads and this number does not exceed the number of cores in a single CPU, then there will be 1 socket, N cores, and 1 thread per core.
 - If we allocate N threads and this number is greater than the number of cores but less than the number of threads in a single CPU, then we have 1 socket, N/2 cores, and 2 threads per core.
 - If we allocate N threads and this number exceeds the number of threads in a single CPU, we need to evenly distribute N among sockets, cores per socket, and threads per core. The product of these three numbers must equal N. The priority is to have the minimum number of sockets, with no more than 2 threads per core. For example, if there are 2 CPUs, each with 24 cores/48 threads, and we want to allocate 56 threads for a VM, we would configure 2 sockets, 2 threads per core, resulting in $56/2/2 = 14$ cores.

6.2. Requirements for Administrators

The administrator, who will have full access to server settings (check [role descriptions](#)), is expected to have basic knowledge and skills related to OS and networking:

- Understanding the basic file system structure of the server OS (Windows or Linux) and the ability to work with it
- Knowledge of the difference between regular and administrative (root) access, and the ability to run commands or installation files as an administrator
- Ability to create users in the OS and add them to specific groups
- Knowledge of basic networking concepts: IP, DNS, NAT, router, firewall
- Understanding the basics of SSL/TLS certificates and their role in securing website access
- If the server has to be integrated with third-party services and protocols (e.g., email, LDAP/AD, SIP, etc.), a basic understanding of their work is also needed.

6.3. Detailed system requirements

	Initial Configuration	Recommended Configuration
CPU	x86-64 architecture (also known as x64, x86_64, AMD64, and Intel 64): Intel Core i3-8100 (3.6 GHz) Intel Core i5-7400 (3.0 GHz) Intel Xeon E-2234 (3.6 GHz) Intel Xeon W-2223 (3.6 GHz) or any other processor with at least 4 logical cores and a PassMark® score of over 7000 points.	x86-64 architecture (also known as x64, x86_64, AMD64, and Intel 64) Intel Core i7-10700 (2.9 GHz) AMD Ryzen 7 2700 (3.2 GHz) Intel Xeon E-2288G (3.7 GHz) Intel Xeon W-2245 (3.9 GHz) or any other processor with at least 16 logical cores and a PassMark® score of over 14000 points.
Features of standard configurations	• Up to 200 online users connected through client applications	• Up to 1000 online users connected through client applications • Recording or broadcasting a single video conference of any type
	<i>And also...</i>	
	• 1 conference in all-on-screen mode with 36 participants connected via applications TrueConf <i>or</i> • Up to 6 smart meetings or moderated role-based conferences with 20 participants connected through TrueConf applications, including 4 on the podium <i>or</i> • 1 smart meeting or moderated role-based conference with 240	• Up to 3 all-on-screen conferences with 36 participants connected via applications TrueConf <i>or</i> • Up to 15 smart meetings or moderated role-based conferences with 20 participants connected through TrueConf applications, 4 of which can be on the podium <i>or</i> • Up to 2 smart meeting or moderated role-based conferences with 240

	Initial Configuration	Recommended Configuration
	participants (60 WebRTC connections + 180 client applications), including 2 WebRTC participants on stage and 3 through client applications <i>or</i> • Up to 25 WebRTC participants displayed in conferences of any type <i>or</i> • Up to 10 SIP or H.323 endpoints displayed in any type of conference	participants (60 WebRTC connections + 180 client applications), with 2 WebRTC participants and 3 client application participants on the podium. <i>or</i> • Up to 36 WebRTC participants can be displayed in conferences of any type <i>or</i> • Up to 20 SIP or H.323 endpoints can be displayed in any type of conference
	Examples of other typical configurations →	
GPU Hardware Acceleration Capabilities	Adding an NVIDIA Quadro P2000 graphics card increases the number of individual video layouts for SIP/H.323 participants by 20 without the need to change other equipment.	
Operating system	Dedicated or virtual 64-bit operating system: • Microsoft Windows Server 2012/2016/2019/2022/2025 (including Core editions) with the latest updates installed • Debian 11 / 12 / 13 • CentOS Stream 9 • • • When deploying TrueConf Server on a VM, it is not recommended to use CPU oversubscription (i.e., the number of vCPUs should not exceed the number of processor threads on the host machine). For more detailed VM recommendations, refer to this article. As part of our commissioning service, we can offer the deployment of TrueConf Server on corporate OS distributions that are not officially supported, such as Oracle Linux, RedHat Enterprise Linux, Rocky Linux, etc. For more detailed information, please contact us using any convenient method.	
RAM (Random Access Memory)	16 GB	32 GB and above
	When installing memory modules, follow the motherboard vendor's recommendations for achieving maximum performance (these are usually provided for server components). Otherwise, we generally recommend using all available memory channels on the motherboard, meaning at least one memory module should be installed per channel.	
Hard drive	20 GB of free disk space	

	Initial Configuration	Recommended Configuration
	To calculate the required storage space for recordings, information on how video compression works during recording can be helpful.	
Network	Ethernet 1 Gbps	
Ports	• 443 (can be changed in the control panel) — the default HTTPS port used for transmitting service information between the server, client applications, and browsers. If the HTTPS port is closed, the conference scheduler and real-time meeting management from the client application will not function. • 4307 (can be changed in the control panel) — port for media data exchange with client applications. Learn more →	
IP	A static IP address is required for the server to function properly.	
Supported hypervisors	Microsoft® Hyper-V, Xen, KVM, Oracle VM VirtualBox, VMware Workstation, and ESXi	
Compatible Cryptographic Gateways	Contact our support for details	

6.4. Optimizing swap file usage

General recommendations for swap size on Windows and Linux:

Installed RAM size	Minimum swap size	Recommended swap size without hibernation	Recommended swap size with hibernation
2-8 GB	1-2 GB	1 x RAM	1.5 x RAM
8-64 GB	4-8 GB	0.5 x RAM	1 x RAM
64-256 GB	4-16 GB	4-16 GB	1 x RAM
>256 GB	4-32 GB	4-16 GB	1 x RAM

If swap files are heavily used on a virtual or physical machine where TrueConf Server for Linux is installed, and there is plenty of available RAM, you can configure the OS settings for using swap files. As a general rule, Linux-based operating systems use swap files in the following way:

- There is no single parameter for using swap depending on the percentage of RAM which is being used.
- One should not rely on the mistaken belief that having a lot of RAM (e.g., 128 GB) means that you can do without swap: this file is an important part of memory management logic in the OS.

- The use of swap is determined by the `vm.swappiness` parameter in the system file `/etc/sysctl.conf`. This parameter essentially represents the ratio between anonymous and physical memory pages. Physical pages correspond to files and their parts in the file system (typically, the code of running programs). Anonymous pages are dynamically created data (for example, variable values).
- Reduction of `vm.swappiness` prioritizes anonymous memory over physical memory which decreases the use of swap.
- By default, the value `vm.swappiness = 60` works well on standard machines (with 8-16 GB of memory). However, machines, where TrueConf Server is installed, have more RAM, so it makes sense to choose a different value.

You can read more about how swap works in Linux [on the Red Hat website](#).

So, to reduce the use of swap, take these steps:

1. Open the `/etc/sysctl.conf` file with the administrator account in any text editor, for example, by executing the following command in the terminal:

```
sudo nano /etc/sysctl.conf
```

sh

2. If the file already contains a line like `vm.swappiness = 60`, change the value 60 to a smaller number, for example **10**. If this value is not included in the file, just add a new line `vm.swappiness = 10`.

Track the results under different loads (e.g., with a different number of conferences, etc.) and adjust the value, reducing it from 10 to 1. **Do not set it to 0** under any circumstances. The final value may vary depending on the amount of RAM and the load on TrueConf Server during your test cases.

7. Installation and Update

Here are the minimum steps needed to set up a working corporate communication system:

1. [Select a machine \(PC, physical or virtual server\) with suitable hardware.](#)
2. *Install TrueConf Server.* **You are here!**
3. [Log in to the control panel.](#)
4. [Register the server.](#)
5. [Configure HTTPS](#) (it is used for many key features such as integration with the AI server, conference scheduling, etc.) and [specify the external server address](#) (the address of the guest page).
6. [Configure access to the server for users within the corporate network](#) and, if necessary, from an external network (outside the corporate network).
7. [Create user accounts](#) or [integrate the server with a directory service](#) via the LDAP/LDAPS protocol.
8. Install client applications for users and show them how to connect to your server (check the [documentation for the desktop application](#)).

We recommend carefully planning your setup, starting with the [selection of hardware](#) suited to your use cases.

Also, **if you have the Free version** (no purchased licenses), you will need to connect to the registration server `reg.trueconf.com` via TCP port 4310 to complete the registration process (more details about [ports here](#)).

7.1. Checking the registration key

Before installing TrueConf Server, make sure you have a **registration key**. You most likely received it when downloading the server installer from our website or when purchasing it from one of [our partners]. If so, you can skip this step and proceed to [installing TrueConf Server](#). Otherwise, you will need to obtain the key as shown in the "[Registration](#)" section.

7.2. Server Installation

TrueConf Server It is provided as a distribution package that includes the server component and client applications for the Windows operating system. Client applications TrueConf for other popular operating systems are available on the website TrueConf (download links can be found on [the guest page](#) [TrueConf Server](#)).

If you are installing TrueConf Server Free behind the firewall, in order to complete the registration process you should open TCP port `4310` to allow access to our registration server located at `reg.trueconf.com`.

If you purchased a paid license, there is no need to open the port, and you will be able to [register the software in offline mode](#).

7.2.1. Which services will be added to the OS after installation

7.2.1.1. Windows

- **TrueConf Server** is the main service. It is responsible for the core functions of the video conferencing system: point-to-point calls, video conferences, messenger, etc.
- **TrueConf Database** — the database server service. It stores chats and logs. The operation of TrueConf Server Manager depends on the TrueConf Database service.
- **TrueConf Web Manager** is responsible for the operation of the TrueConf Server control panel, guest page, personal area, scheduler, web application (connecting to a conference through a browser via WebRTC). It also manages HTTPS settings. If this service is disabled, you will not be able to use the listed functions.
- **TrueConf Server Manager** — manages Windows registry and settings files. It is required for displaying certain data in the TrueConf Server control panel.
- **TrueConf Bridge** is a service that receives websocket messages (commands) from web applications and converts them into transport messages understandable by TrueConf Server.

7.2.1.2. Linux

- **trueconf** — the main service, the server engine. It is responsible for the core functions of the video conferencing system: point-to-point calls, video conferences, messenger, etc.
- **trueconf-db** is the database service. It stores all data for TrueConf Server, including chats, user lists, conferences, groups, web server settings, etc.
- **trueconf-web** is responsible for the control panel of TrueConf Server, the guest page, the personal area, the scheduler, the web application (WebRTC), and HTTPS settings. If this service is disabled, you will not be able to use the listed features.
- **trueconf-manager** — a manager for handling databases and configuration files. It is required for displaying certain data in the TrueConf Server control panel.
- **trueconf-php** — this service is responsible for processing specific scripts and is an internal system service.
- **trueconf-bridge** is a service that receives websocket messages (commands) from web applications and converts them into transport messages understandable by TrueConf Server.

7.2.2. Installation on Windows OS

On the page that opens [after completing the form](#), go to the **Windows** tab and click the **Download TrueConf Server** button.

Thank you! What's Next?

Choose your operating system:

Windows

Linux

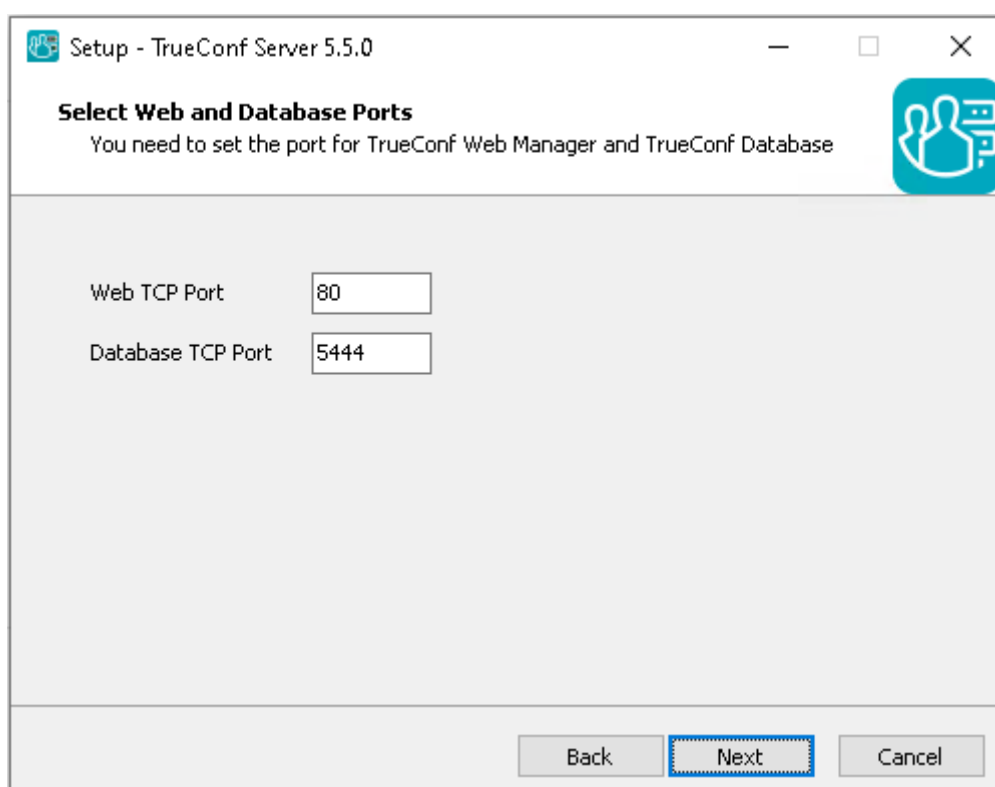
- ✓ **Fill in this form and get a registration key**
- 2 **Download and install TrueConf Server for Windows**
[Download TrueConf Server 5.0.0.10357](#)
- 3 **Register TrueConf Server with your key**
Your registration key has been sent to your email address `stalker.shoc@gmail.com`.
- 4 **Follow our installation guide**
Deployment will take only 15 minutes, simply [follow our short guide](#).

Скачать TrueConf Server

Download and run the distributive to start the installation. The installation process will take not more than a minute.

During the installation you can specify:

- Web TCP port for accessing control panel over HTTP
- TCP port of the database for server reports.



Database port for server reports is set to `5444` by default. It is selected during the installation process and cannot be changed afterwards (to change it you will need to re-install TrueConf Server). The control panel is given port `80` or `8888` (if port `80` is unavailable). If both port `80` and `8888` are unavailable, you will need to specify it manually during the installation process.

If after installation, the control panel cannot be opened via the specified port, it means that this port is probably used by another process. In this case you will need to [select a different port manually](#).

If control panel port is not `80` (HTTP) or `443` (HTTPS), you need to specify it manually in the host name after the colon in the browser URL bar (e.g. `http://localhost:8080`).

Your browser will automatically open TrueConf Server control panel after installation.

To [access the control panel](#), you need to enter the OS username and password used during the server installation.

7.2.3. Installation on Linux OS

Next, we will show the main steps for installing the software on Linux from the file (downloaded package). It is also possible to install from the repository. This installation method is described in the corresponding section of the article about the installation on each operating system.

- [Debian](#)
- [CentOS Stream](#)
-
-
-

TrueConf Server contains its own web server. To prevent any possible conflicts or clashes, please deploy it on a computer running on Linux without a pre-installed web server.

Step 1.

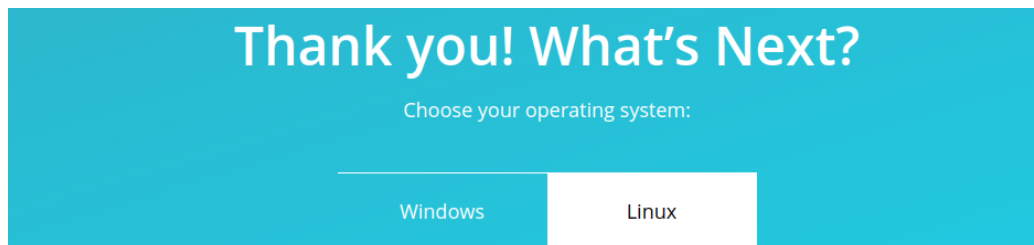
Add the user who will install TrueConf Server and get access to the TrueConf Server control panel to your OS. You can use the account that was created when installing your OS.

You cannot use **trueconf** as an OS username! This is because the OS will automatically create such a user to run certain TrueConf Server services. If such a user already exists, it needs to be removed.

How to create a user in Linux OS is explained later in the [initial server setup](#) description.

Step 2.

On the page that appears [after completing the form](#), go to the **Linux** tab for a description of the next steps.



- ✓ **Fill in this form and get a registration key**
- 2 **Download and install TrueConf Server for Linux**
You can find TrueConf for Linux installation packages in our [blog](#).
- 3 **Register with your key**
Your registration key has been sent to your email address mymail@example.com.
- 4 **Follow our installation guide**
Deployment will take only 15 minutes, simply [follow our short guide](#).

Click on the link in the second option to view the detailed guide in our blog on the installation of TrueConf Server for Linux.

Step 3.

Download the distribution for your operating system.

Step 4.

If you want to deploy TrueConf Server manually, open the directory with the downloaded installation package. Depending on your operating system, run one of the following commands as administrator, where `server-installation-file` is the file name.

For Debian:

First, update the system packages with the command:

```
sudo apt update && sudo apt upgrade -y
```

sh

Only then should you install the server:

```
sudo apt install -yq ./server-installation-file.deb
```

sh

For CentOS:

1. To make sure that TrueConf Server works correctly on CentOS, you will need to disable SELinux, the system can control the process access to the OS resources. To do it, run the following command as the administrator:

```
sudo sed -i 's/^SELINUX=.*SELINUX=disabled/g' /etc/selinux/config
```

sh

2. It is also necessary to connect the EPEL repository:

```
sudo dnf install epel-release
```

sh

3. Update the system packages with the command:

```
sudo dnf update -y
```

sh

4. Only after this can you install TrueConf Server:

```
sudo dnf install -y server-installation-file.rpm
```

sh

When you run the command to install the software from a file on Linux, you can use an additional parameter to enter the list of users, who will have access to the control panel without using the login window. To do it, add the parameter `TCADMINS_USERS=[users]` to the installation command with the list of required OS users, for example, on Debian:

```
sudo TCADMINS_USERS=main_admin,second_admin apt install ./server-installation-file.deb
```

sh

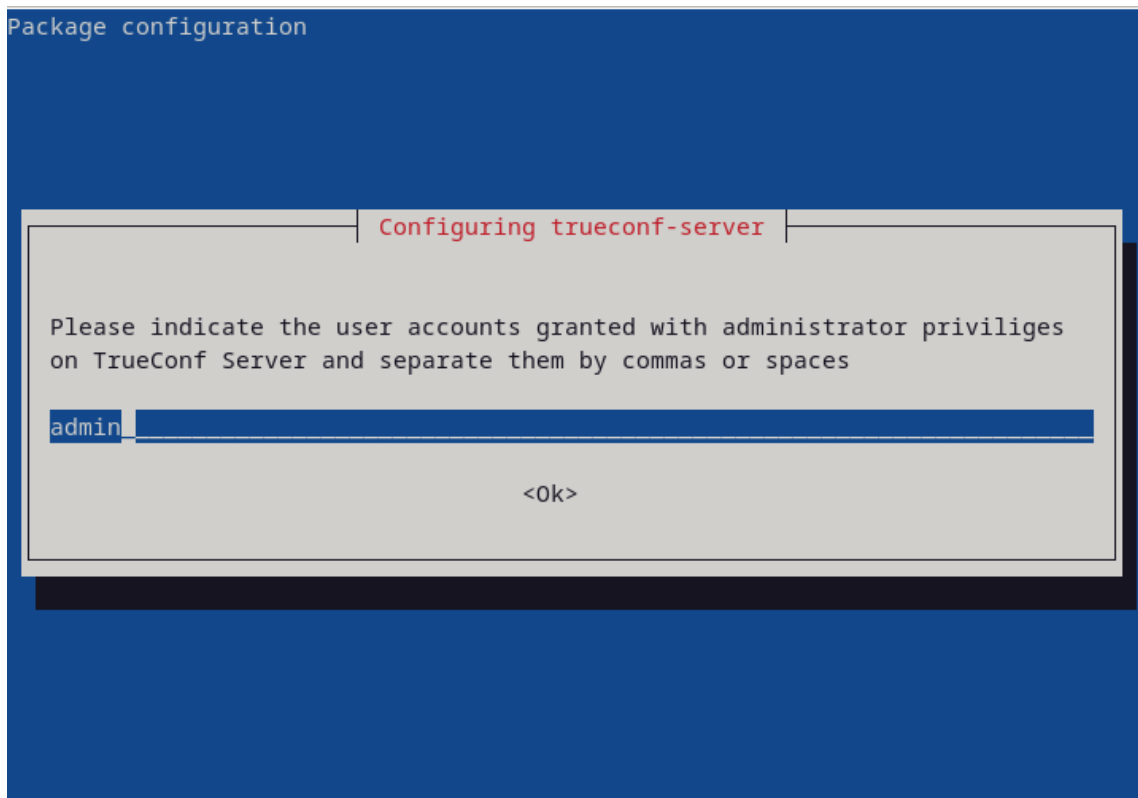
Or

```
sudo TCADMINS_USERS=main_admin apt install ./server-installation-file.deb
```

sh

Step 5.

During installation, you will see a field for entering the names of OS users who will be given administrator-level access to the control panel. Specify the name of the [user created earlier](#).



Step 6.

The OS will include the TrueConf services that were [described earlier](#). The web server and manager should start automatically after installation.

Use another computer in your LAN, open your web browser and type the IP address of the Linux-based computer with TrueConf Server installed. To find your IP address in Linux, run `ip a` command.

The control panel is given port `80` or `8888` (if port `80` is unavailable). If both port `80` and `8888` are unavailable, you will need to [specify it manually](#) during the installation process.

If control panel port is not `80` (HTTP) or `443` (HTTPS), you need to specify it manually in the host name after the colon in the browser URL bar (e.g. `http://localhost:8080`).

Refer to the [article in our knowledge base](#) to learn how to access the control panel when installing the software outside the local network (e.g., when installing on a cloud server).

Since the server is not registered yet, an admin login page will be displayed instead of the guest page. Sign in with the user account you have previously created to start [server registration](#).

7.2.4. How to change the port to access the control panel without reinstalling server

For Windows OS

1. Go to the TrueConf Server installation directory (`C:\Program Files\TrueConf Server` by default).

2. Open the `\httpconf\conf\listen.conf` file using a text editor (administrator rights required).
3. Change the port number in the `Listen <port number>` parameter (e.g. `Listen 8888`) and save changes.
4. Open the `\manager\etc\manager.toml` file as an administrator and specify the same port in the parameter:

```
[web]
connection = "http://127.0.0.1:80"
```

sh

For example, you can replace `80` port with `8888`:

```
[web]
connection = "http://127.0.0.1:8888"
```

sh

5. Restart the computer where TrueConf Server is installed.

For Linux OS

If you use Linux, you cannot specify ports to access the TrueConf Server control panel during the installation process. If necessary, you can only change this port after the installation.

1. Open the file `/opt/trueconf/server/etc/webmanager/listen.conf` with any text editor (as a superuser):

```
sudo nano /opt/trueconf/server/etc/webmanager/listen.conf
```

sh

2. Change the port number in the `Listen <port number>` parameter (e.g. `Listen 8888`) and save changes.
3. Open the file `/opt/trueconf/server/etc/manager/manager.toml` with any text editor (as a superuser):

```
sudo nano /opt/trueconf/server/etc/manager/manager.toml
```

sh

4. Specify the same port for the parameter:

```
[web]
connection = "http://127.0.0.1:80"
```

sh

For example, you can replace `80` port with `8888` :

```
[web]
connection = "http://127.0.0.1:8888"
```

sh

5. Restart the **trueconf-manager** and **trueconf-web** services using these commands:

```
sudo systemctl restart trueconf-manager
sudo systemctl restart trueconf-web
```

sh

7.3. Updating the video conferencing server

TrueConf Server is updated with the help of installation files or repositories (on Linux). Please note that when updating the **major version** (the first two digits are changed, e.g., from 4.5 to 4.7 or from 4.7 to 5.0), you will need to re-register TrueConf Server because the hardware key (HW key) will change. Registration will also be needed if some of the following hardware parameters are changed on the physical or virtual machine where TrueConf Server is installed:

- CPU model (please note that the number of virtual cores (vCPUs) does not affect the license)
- Storage size (SSD or HDD)
- Operating system.

For more information about updating TrueConf Server, refer to the [relevant article](#).

7.4. How to solve typical installation issues

7.4.1. gnupg error when installing from the repository on Debian

If the following error is displayed in the terminal, when the software is installed from the repository on Debian:

```
E: gnupg, gnupg2 and gnupg1 do not seem to be installed, but one of them is required
for this operation
```

sh

it means that the **gnupg** encryption solution is not installed on the OS.

In this case install the missing package with this command:

```
sudo apt install gnupg2
```

sh

7.4.2. Administrator login input error during installation

If you type an incorrect or non-existing login when [entering the administrator login during Step 5 of installation](#) on Debian, installation may end with the following error:

```
E: Sub-process /usr/bin/dpkg returned an error code (1)
```

sh

In this case, you will need to run this command on behalf of the superuser

```
echo PURGE | sudo debconf-communicate trueconf-server
```

sh

This will clear the package settings data stored in the OS. For more details, refer to the [official documentation](#).

Then [restart the installation process](#) from the first step.

7.4.3. Unable to access the control panel

If you are unable to access the TrueConf Server control panel after installation, this problem may occur due to multiple reasons:

- You are trying to access the control panel which is outside the local network (e.g., the server was installed on VPS).
- The user, on whose behalf you are trying to sign in, does not have required permissions (please note that it has to be the OS user added to the [corresponding group](#)).
- on CentOS Stream, if the password for the OS user (administrator TrueConf Server) has been changed, you will need to execute the command:

```
sudo setfacl -m u:trueconf:r /etc/shadow
```

sh

We have detailed instructions on how to resolve the issue with accessing the admin panel in [our knowledge base](#).

7.4.4. What is the default administrator login and password?

An existing system account is used for accessing the TrueConf Server control panel, no new accounts are created during installation. Access is controlled by adding the selected OS accounts to a specific group. To learn more, refer to the [description of control panel access settings](#).

8. Registration

Here are the minimum steps needed to set up a working corporate communication system:

1. [Select a machine \(PC, physical or virtual server\) with suitable hardware.](#)
2. [Install TrueConf Server.](#)
3. [Log in to the control panel.](#)
4. *Register the server.* **You are here!**
5. [Configure HTTPS](#) (it is used for many key features such as integration with the AI server, conference scheduling, etc.) and [specify the external server address](#) (the address of the guest page).
6. [Configure access to the server for users within the corporate network](#) and, if necessary, from an external network (outside the corporate network).
7. [Create user accounts](#) or [integrate the server with a directory service](#) via the LDAP/LDAPS protocol.
8. Install client applications for users and show them how to connect to your server (check the [documentation for the desktop application](#)).

8.1. What are a registration key and server ID?

Registration key – a unique secret combination of characters that uniquely identifies the licenses for your TrueConf Server instance. It is required to activate the video conferencing server after [installation](#). You may have received it earlier when downloading the server from the TrueConf website or purchasing through [company partners](#).

When contacting TrueConf technical support, employees may request you to provide your server ID (first five characters, e.g. **EB2MM**) but never the entire registration key.

Two servers cannot function simultaneously on two computers with the same registration key. If you try to register two servers on different computers with the same key, a [hardware key error](#) will occur.

Server ID is a unique identifier for the video conferencing server TrueConf Server. The server ID includes a series of characters that match the beginning of the registration key (up to the first dash), for example, **EB2MM**. It is displayed in the TrueConf Server control panel in the [section](#)

Summary:

Dashboard

Summary

PRO Licenses

Settings

Network

Network Settings

SMTP

Federation

Gateways

SIP

H.323

RTP

Summary

Help ?

Dashboard License info

Registration details

Server ID: **kk123**

Organization name: Great Company

Contact person: Joe Smith, smith@example.com

Registered

Expires in 162 days

Register

[License agreement](#)

If you don't have a key, you can use a free license by clicking the **Download free version** button on the [page TrueConf Server Free](#).

Registration TrueConf Server is required in order to:

- Make sure that your key is not used by anyone else, in other words, we need to protect your software license
- Ensure that the ID of each server is unique which is needed for the correct work of [federation](#).

A detailed comparison of the features of the free and paid versions is available on the [pricing page](#).

A page with a form will open, which you need to fill out to receive TrueConf Server Free:

Download TrueConf Server Free Language: English

TrueConf Server Free is available for Windows, Linux, and Docker environments. Once you **complete the form**, you will be able to select the appropriate installer for your platform on the **download page**. Please note that the free version **activation key** will be sent to the **corporate email address** you provide.

Company

Industry
-- Choose your business category --

Full Name

Corporate Email

Contact phone Format: +1(123)4567890 #123

Country
Russian Federation

☐ I accept the [Terms of Use](#) and [Privacy Policy](#).

We may use your email for sending automated notifications and product updates. [Learn more](#) about how TrueConf protects and uses your personal data.

Submit & Download

Useful links

- [How to install and set up your video conferencing server for Windows in 15 minutes](#)
- [How to install and set up your video conferencing server for Linux in 15 minutes](#)
- [What is the difference between TrueConf Server Free and TrueConf Server?](#)
- [What are the system requirements?](#)
- [Are you ready to buy? Then click here!](#)

Need help?
[Click here, we are pleased to help you](#)

A registration key will be sent to the email address that you provided.

You will receive the key within 15 minutes

If you did not receive the key, please [contact us](#) in any way convenient to you or check your **SPAM** email folder.

After filling out the form, select your operating system to get access to the corresponding installation guide. When TrueConf Server is deployed, you can register it.

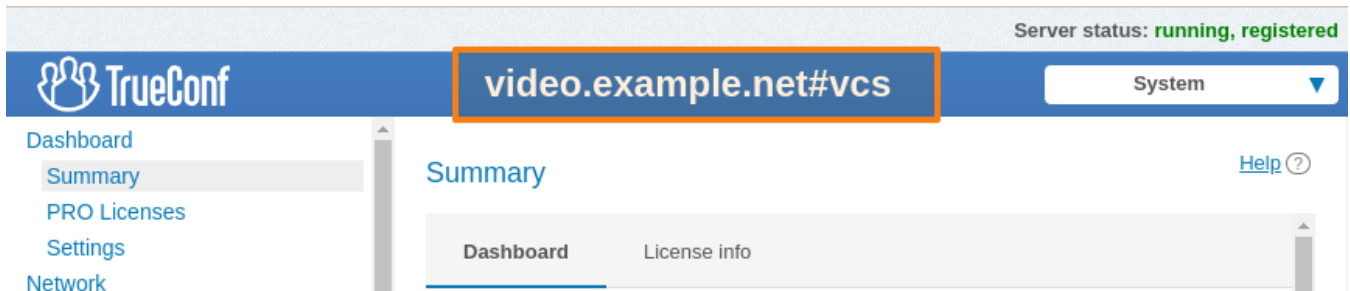
8.2. Server Name (Имя сервера)

Имя сервера TrueConf (Server Name) is the alphanumeric name used to identify TrueConf Server on the network. Knowing the server name is crucial for organizing conferences with

external TrueConf Server via [federation](#) and for integration with SIP and H.323 devices, such as Polycom terminals or TrueConf Group.

Server name is generated automatically in the control panel upon [TrueConf Server registration](#). Standard server name has the following format: `<server_id>.trueconf.name#vcs`, where `<server_id>` is server ID. Server name can be changed; instead, you can set domain name for your TrueConf Server instance.

After successful registration, the server name will be displayed at the top of the TrueConf Server control panel window:



An IP address cannot be used as the server name.

You can change the server name only when re-registering it. Please note that all previous chat messages will become unavailable. So, we do not recommend doing it without consulting our [technical support](#).

8.3. Server registration process online

Register the server. To do this, you will need to enter the [registration key you have received earlier](#).

1. Open your browser and go to the TrueConf Server settings page. By default, its address is identical to the address of the machine where the video conferencing server is deployed. If you do not know how to learn the address and port, check the [installation guide](#).
2. Enter your key in the appropriate field and click the **Registration** button:

TrueConf Server Registration

- 1 Enter the registration key that has been sent to your **email address**.

XXXXX-XXXXX-XXXXX-XXXXX

[Where do I get the key?](#)

Server Name *

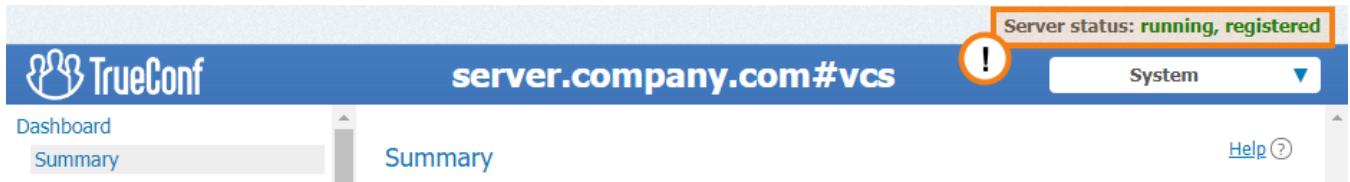
ruwu1.trueconf.name #vcs

- 2 **Registration**

See the [help](#) section or contact TrueConf support by phone +1 (833) 878-32-63 or write us at sales@trueconf.com

If you do not have a key, click the **Where do I get the key?** link on the server registration page and follow the [instructions described above](#).

3. Once the server is successfully registered, the corresponding message **running, registered** will appear in the upper right corner of the control panel window:



If the connection with the registration server (`reg.trueconf.com` via TCP port `4310`) is lost, your TrueConf Server Free will be disconnected after 12 hours. The scheduled disconnection time will be displayed on the **Summary** tab. The full version of TrueConf Server does not have such limitations, regardless of the registration method (online or offline).

8.4. Offline Registration

Offline registration is not available in a free license. It is supported only in premium licenses or in the servers with a temporary trial license provided by managers.

8.4.1. Registering a new server or after a clean reinstallation

To complete offline registration on a PC without an Internet connection, you'll need a device with access to an external network to get the registration key. Go to the [form page](#) on this device, and follow the instructions in the [Server Registration](#) section.

Once you receive an email with the registration key, enter it in the corresponding field **Registration Key** of the control panel on a PC that is not connected to the Internet, and click the **Registration** button:

TrueConf Server Registration

1 Enter the registration key that has been sent to your **email address**.

XXXXX-XXXXX-XXXXX-XXXXX

[Where do I get the key?](#)

Server Name *

ruwu1.trueconf.name

#vcs

2

Registration

See the [help](#) section or contact TrueConf support by phone +1 (833) 878-32-63 or write us at sales@trueconf.com

In the registration window, the **Create registration file** button will appear. Click it to generate a file with the registration information.

TrueConf Server Offline Registration. Step 1

To start offline registration process please click on **Create registration file** button to create offline key file. Once created it will downloaded automatically, please save it.

Please note: you won't be able to return and download this file again.



[Start registration process from the beginning](#)

See the [help](#) section or contact TrueConf support by phone +1 (833) 878-32-63 or write us at sales@trueconf.com

The created **offlinereg.vrg** file is automatically saved in the browser's **Downloads** folder. Send it to sales@trueconf.com. In return, you will receive a file that must be transferred to the PC where the server offline registration is being performed.

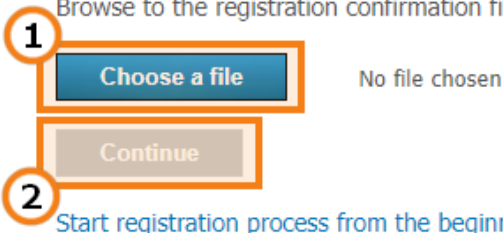
Please do not try to restart offline registration until you receive a respond to your request. If you restart offline registration, you will need to retry the whole process.

Click **Select file** and select the **offline2.vrg** file sent to your computer, then click the **Continue** button.

TrueConf Server Offline Registration. Step 2

Please send **offlinereg.vrg** file generated during step #1 to .

Browse to the registration confirmation file you've received from the sales department and click **Continue**.



If you close this page, the registration process can be resumed at any moment from here on.

See the [help](#) section or contact TrueConf support by phone +1 (833) 878-32-63 or write us at sales@trueconf.com

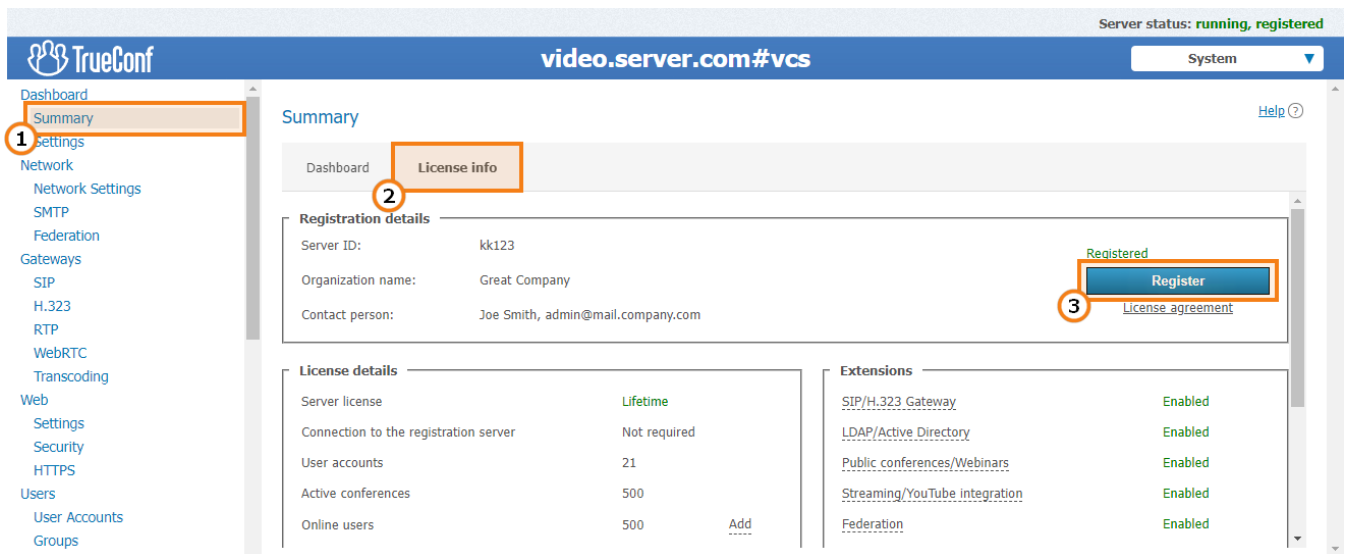
If the offline registration has been successful, you will be notified that TrueConf Server has been successfully registered in the control panel.

8.4.2. Re-registering the server in a closed network

If the server previously worked in a private network and you want to change the license composition, or if the server was stopped due to the error **CHECK CERT: HW key is failed!**, you

do not need to go through the full offline registration process again. Since you already have the registration key, there is no need to get a new key by filling out the installer download form.

1. Go to the **Summary → License info** section in the server control panel and click the **Register** button:



2. Enter **your existing registration key** in the appropriate field and click **Registration**:

TrueConf Server Registration

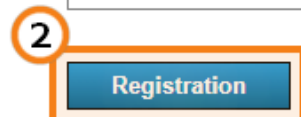
- 1 Enter the registration key that has been sent to your **email address**.

XXXXX-XXXXX-XXXXX-XXXXX

[Where do I get the key?](#)

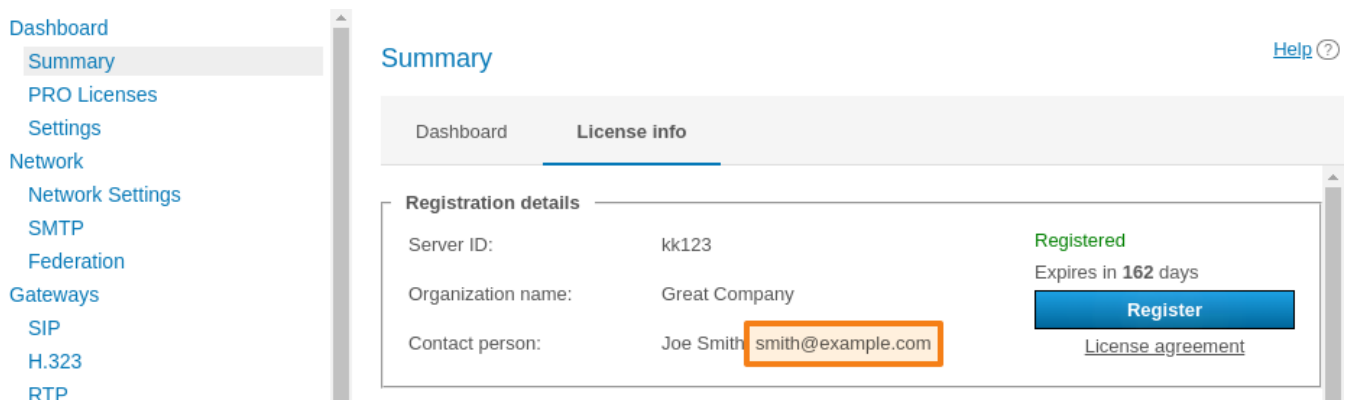
Server Name *

ruwu1.trueconf.name #vcs



See the [help](#) section or contact TrueConf support by phone +1 (833) 878-32-63 or write us at sales@trueconf.com

You can find your **registration key** in the email inbox you provided in the registration form when downloading the server. The email address is also displayed in the TrueConf Server control panel in the **Contact person** field:



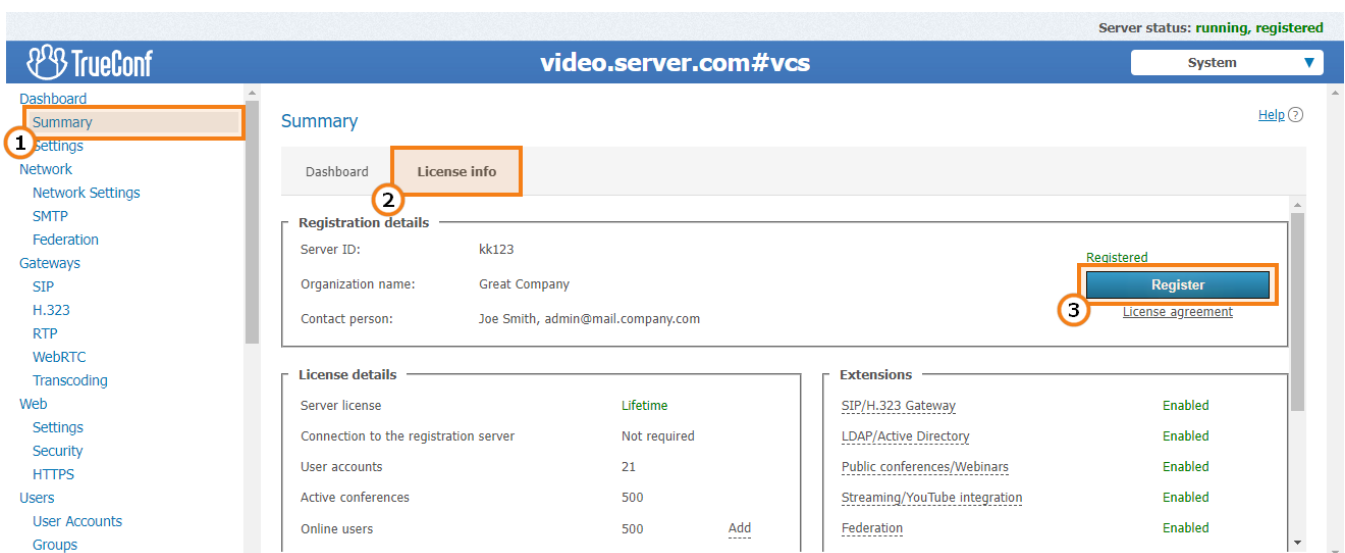
If the email was accidentally deleted, you can request the key from your manager. If you don't have your manager's contact details, just [contact us](#), provide your [server ID](#), and we will help you. However, this method will not work if you change the server hardware configuration: in this case, you will need to ask us to reset the hardware binding. Then, you will need to repeat the offline registration procedure described below.

8.5. How to re-register the server

To re-register TrueConf Server without changing the key (for example, to activate new features after purchase), simply go to the **Dashboard → Summary** section and enter your old key as [previously shown](#).

To change the registration key TrueConf Server:

1. Log in to the control panel and navigate to section **Dashboard → Summary**.
2. Go to the **License info** tab.
3. Click the **Register** button and enter the new key as [previously shown](#):



8.6. Re-registering with a previously used server name

Sometimes, it may be necessary to change the server name to the one which was previously used for a different registration key. For example, a trial version was used, and then, a new registration key for corporate use was obtained for TrueConf Server. In this case, you can use one of the two options:

1. Request your TrueConfmanager, who is assigned to your company, to release the selected domain name (please note that to release a name does not mean to reset the hardware binding).
2. First, register the server with the old (test) key using a different server name that has not been used yet. Then, register it with the new (production) key using the required server name.

8.7. Frequently Asked Questions about Registration

8.7.1. Is it possible to register the free version of the server without an Internet connection?

No, this feature is only available to users with an annual or perpetual license for the TrueConf Server product. If you need a trial version of TrueConf Server that operates without an Internet connection, just [contact us](#).

8.7.2. What should I do if I get the message "Computer change is not available for this server code"?

This means that your [key is "linked" to the computer](#) where the server was installed. To remove this link, [contact us](#) using one of the available methods.

8.7.3. How to reset the binding?

You need to reset the binding for TrueConf Server if something has changed on the machine where it is installed and the HW key (binding key) is "broken." The list of parameters that affect the HW key is detailed in [this article](#). Consequently, to reset the binding and restart TrueConf Server, [please contact TrueConf](#) using one of the methods provided.

8.7.4. What should I do if I get the message "The registered server doesn't have valid licenses"?

It means either that the key has expired or the time and date on your PC have busted. Make sure that time and date are specified correctly on your PC.

8.7.5. What should I do if I get the message "Server name is already registered"?

This notification means that the [server name](#) you specified during registration is already in use somewhere (by you or another organization) and is linked to a different key. Just specify a different name, or if you specify an external domain name in this field, and you are certain that you are the owner of this address, make sure that no other server with this name is registered in your company.

8.7.6. Why is it necessary to maintain connection with the registration server and what kind of data will be sent there?

TrueConf Server sends only service information to the registration server to protect your registration key and speed up the analysis of support requests. No data regarding settings, chats, users, etc., is sent. To learn more, read the [article on port usage](#).

9. Accessing the control panel and configuring preferences

Here are the minimum steps needed to set up a working corporate communication system:

1. [Select a machine \(PC, physical or virtual server\) with suitable hardware.](#)
2. [Install TrueConf Server.](#)
3. [Access the control panel.](#) **You are here!**
4. [Register the server.](#)
5. [Configure HTTPS](#) (it is used for many key features such as integration with the AI server, conference scheduling, etc.) and [specify the external server address](#) (the address of the guest page).
6. [Configure access to the server for users within the corporate network](#) and, if necessary, from an external network (outside the corporate network).
7. [Create user accounts](#) or [integrate the server with a directory service](#) via the LDAP/LDAPS protocol.
8. Install client applications for users and show them how to connect to your server (check the [documentation for the desktop application](#)).

9.1. How to access the control panel (admin area)

You won't be able to access the control panel if you install TrueConf Server on Windows Home (check [system requirements](#))! You need versions of Windows that support user group management (Server / Pro / Enterprise). Additionally, regardless of the OS (Windows or Linux), the user account you are trying to authenticate with, **must** have a password.

If you have installed TrueConf Server **on Windows**:

1. Open your browser and go to the IP address of the machine where the server is installed.
2. If you are accessing the control panel for the first time from the same machine where TrueConf Server is installed, you should be automatically authenticated on the registration page:

 TrueConf **FREE**

TrueConf Server Registration

Enter the registration key that has been sent to your **email address**.

[Where do I get the key?](#)

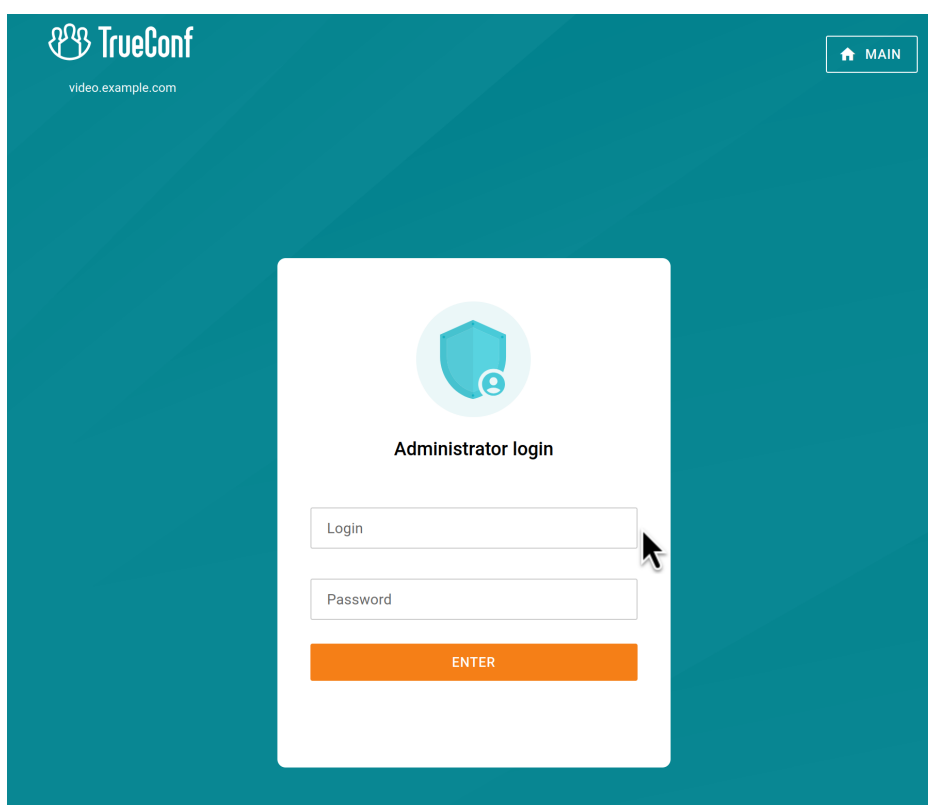
Server Name *

#vcs

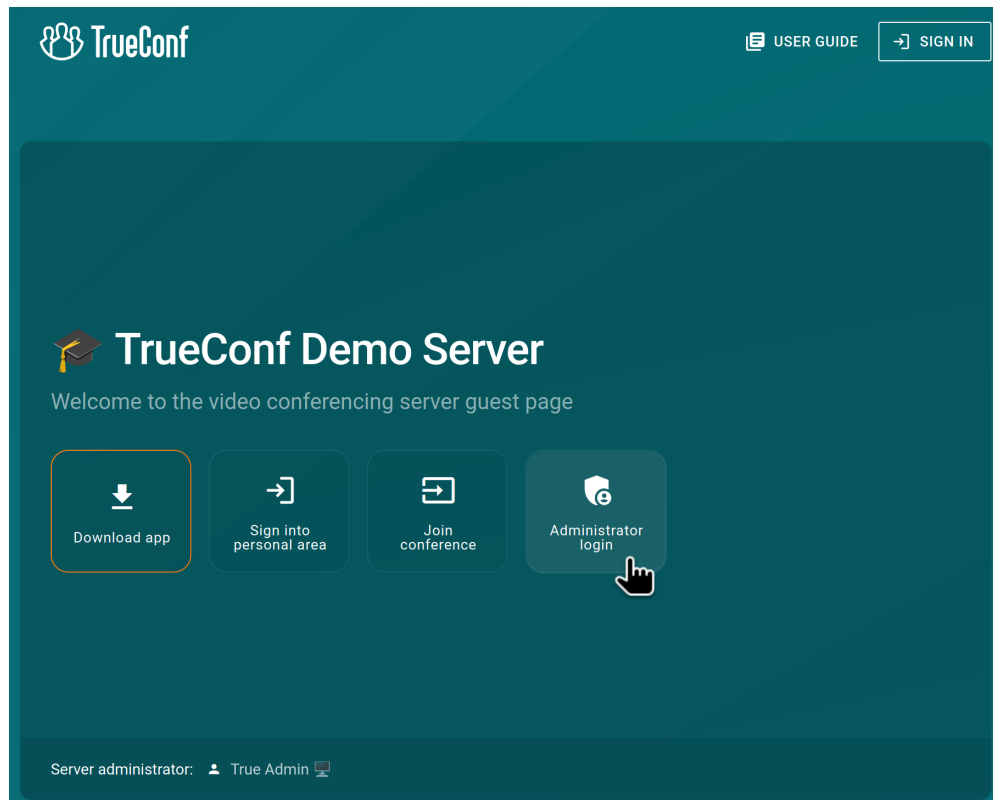
Registration

See the [help](#) section or contact TrueConf support by phone +1 (833) 878-32-63 or write us at sales@trueconf.com

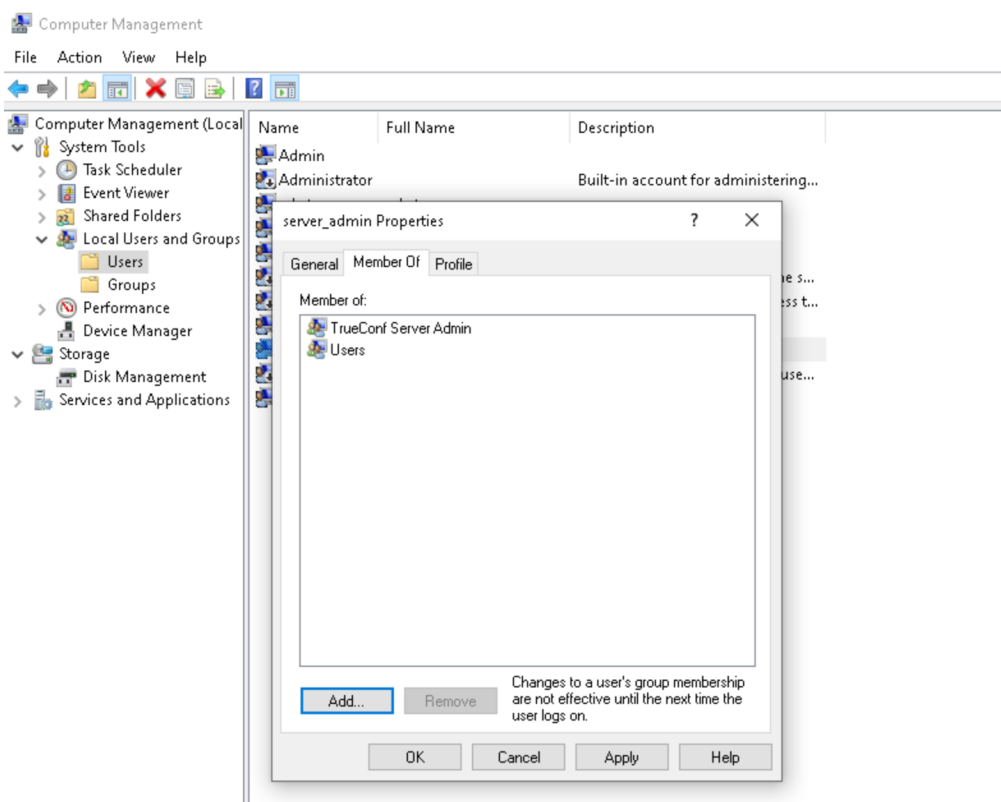
3. If the registration page opens, you may [activate the server](#).
4. If you access the control panel from another PC and subsequently open the server address from the same machine, a guest page will be displayed:



5. Press the **Administrator login** button and enter the OS user login and password used to install the server:



6. If you are unable to log in, make sure that the user on the Windows machine with the server is a member of the **TrueConf Server Admin** group:



On Linux OS, users are added to the **tcadmins** group [manually during the installation process](#). These users will have access to the admin panel.

There is no "universal" default login; you need to know the login and password linked to the account on the OS where the server was installed. Any type of access to the TrueConf Server

control panel requires authentication with the login information of a user who is included in one of these groups:

- **TrueConf Server Admin** on Windows (**tcadmins** on Linux operating systems) — for server administration;
- **TrueConf Server Security Admin** on Windows (**tcsecadmins** on Linux OS) is used for viewing reports and video conference recordings.

Important! There is no other way to add an account for administering TrueConf Server. Additionally, you cannot change another administrator's password or perform similar actions in the control panel; all access is managed through the OS user account.

By default TrueConf Server can be administered from any computer in the same local network where it was installed. In other words, by default access is limited to the following ranges of IP addresses: `10.*` , `192.168.*` , `172.16-172.31` , `127.*` .

Detailed access settings are discussed in the description of [section Web →Security](#).

How to create a new account in different operating systems and add it to the desired group is detailed [using the example of the TrueConf Server Security Admin administrator](#).

TrueConf Server there are no limits on the number of administrators of each type.

If an administrator wants to manage TrueConf Server from a remote computer, they need to make sure that the firewall allows incoming connections over the control panel access port (`80` by default) and that this option has been enabled in the [Security section of the control panel](#).

We explained how to manage TrueConf Server from a computer offline in the [relevant knowledge base article](#).

After access configuration, we recommend [setting up HTTPS](#) as soon as possible because it will be needed for frequently used features: application scheduler, real-time meeting management, and access to users' personal area. When HTTPS is configured, the port 80 (or any other port used to access the control panel) will no longer be needed for the work of TrueConf Server and can be disabled on the firewall for enhanced security.

9.2. Adding Administrators

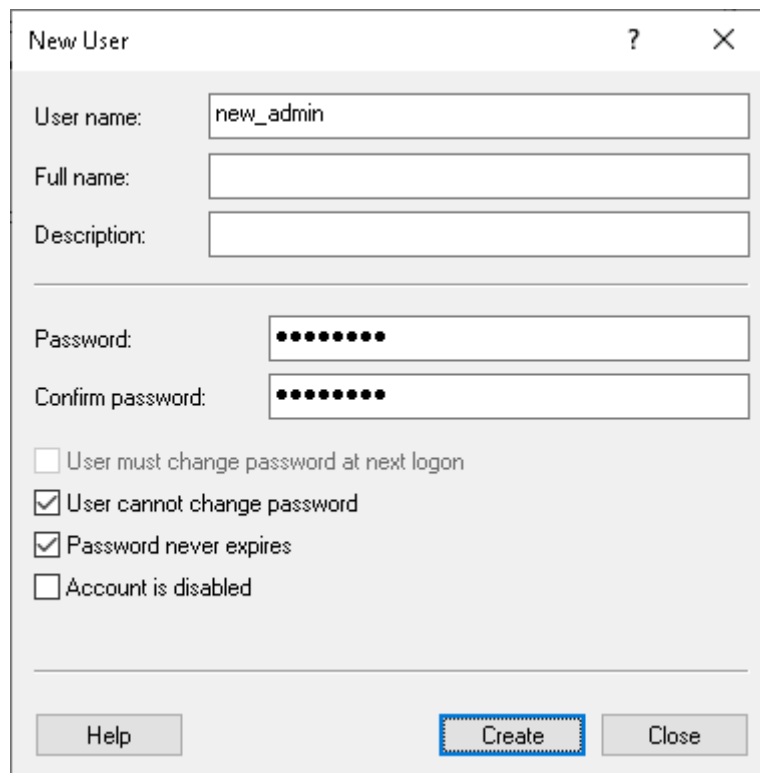
You can configure access rights for existing accounts or create new ones. Below, we will show how to create a user and immediately add this account to the appropriate group on Windows and Linux.

9.2.1. For Windows

To create a new local Windows account and add it to the TrueConf Server Admin group:

1. Go to the **Local Users and Groups** snap-in. To do this, press **Win+R** and run the `lusrmgr.msc` command in the window that appears.
2. Right-click on the **Users** list and select **New User...**

3. Fill in the required fields and configure the password change settings.

A dialog box titled "New User" with a question mark icon and a close button (X). It contains several input fields and checkboxes. The "User name:" field is filled with "new_admin". The "Full name:" and "Description:" fields are empty. The "Password:" and "Confirm password:" fields are filled with ten dots each. Below these fields are four checkboxes: "User must change password at next logon" (unchecked), "User cannot change password" (checked), "Password never expires" (checked), and "Account is disabled" (unchecked). At the bottom are three buttons: "Help", "Create" (highlighted with a blue border), and "Close".

New User

User name: new_admin

Full name:

Description:

Password:

Confirm password:

☐ User must change password at next logon

☒ User cannot change password

☒ Password never expires

☐ Account is disabled

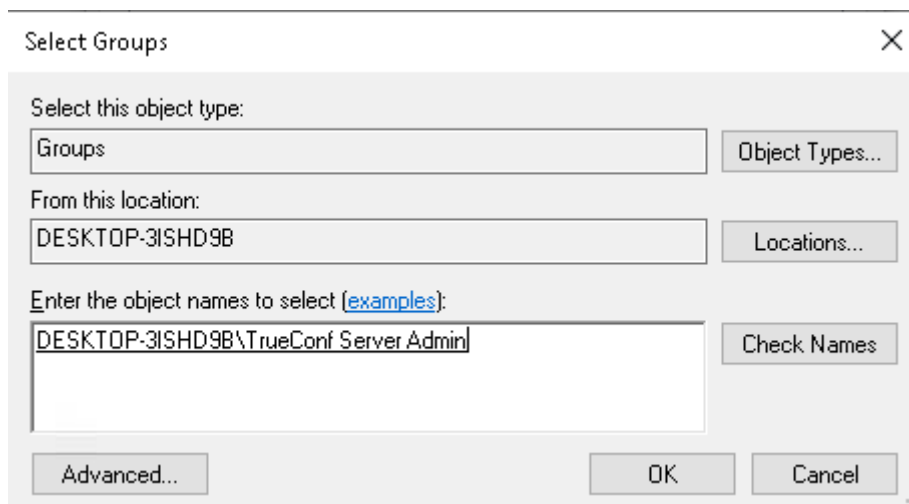
Help Create Close

4. Go to the **Users** list.

5. To grant access to the server control panel, right-click the created account and go to **Properties**.

6. On the **Member Of** tab, click **Add...**

7. Specify **TrueConf Server Admin** as the name of the object to be selected and click **OK**.

A dialog box titled "Select Groups" with a close button (X). It contains several input fields and buttons. The "Select this object type:" field is filled with "Groups". The "From this location:" field is filled with "DESKTOP-3ISHD9B". Below these fields is a text area labeled "Enter the object names to select (examples):" containing the text "DESKTOP-3ISHD9B\TrueConf Server Admin". To the right of the text area is a "Check Names" button. At the bottom are three buttons: "Advanced...", "OK", and "Cancel".

Select Groups

Select this object type: Groups

From this location: DESKTOP-3ISHD9B

Enter the object names to select (examples):
DESKTOP-3ISHD9B\TrueConf Server Admin

Object Types... Locations... Check Names

Advanced... OK Cancel

Accounts imported from Active Directory/LDAP can also be added to the local group TrueConf Server Admin.

9.2.2. On Linux OS

The commands listed below need to be executed with superuser privileges or using `sudo` (e.g., `sudo command`). Please note that **sudo** may be unavailable by default in your operating system. You can check its availability using the `sudo -V` command.

For Debian

1. Run the following command:

```
sudo adduser --ingroup tcadmins [new_admin]
```

sh

where `[new_admin]` is the username of the admin.

2. Enter your password in the corresponding field and confirm it.
3. Optionally, provide additional information for the admin (full name, phone number, etc.).

For CentOS

1. Run the following command:

```
sudo adduser -G tcadmins [new_admin]
```

sh

where `[new_admin]` is the username of the admin.

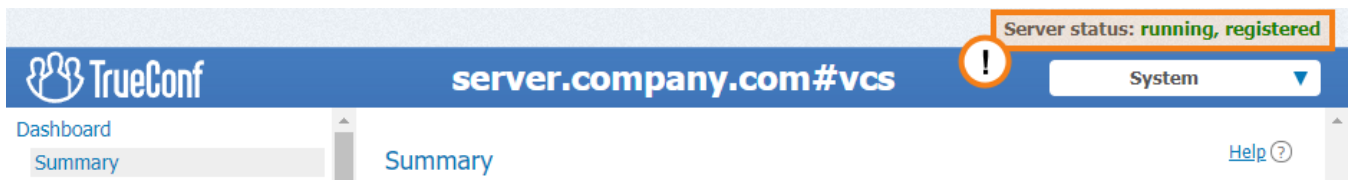
2. Set the password for the new user `[new_admin]` with the following command:

```
sudo passwd [new_admin]
```

sh

9.3. Server Status

The current status of TrueConf Server is displayed in line **Server status** as **green** text (if it is running) or **red** text (if it is stopped) in the upper right corner of the control panel:



What to do if server is not running?

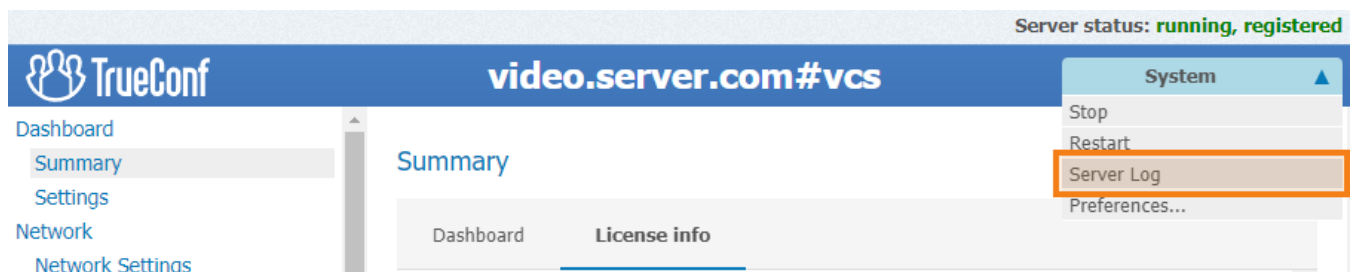
The text **Stopped** is displayed in line **Server status**.

There are three possible reasons for this:

- **Invalid license:** contact your system supplier to get a license.
- **Server files are missing or corrupted:** please reinstall the TrueConf Server server (see the section [Server Installation](#))
- **The server hardware key has malfunctioned:** please refer to the [guide for resolving the key issue](#).

9.4. Server log

If issues arise on the server, TrueConf support can assist you more quickly and efficiently if you [provide the server logs](#). The main server log can be viewed in the log accessible via the **System** → **Server log** button in the upper right corner.



To ensure the logs are as informative as possible, the option **Enable detailed logging** in [the Dashboard → Settings section](#) should be enabled. Technical support staff may ask you to do this to facilitate troubleshooting.

Do not enable detailed logging without a reason because it can unnecessarily occupy space with detailed log files.

Additionally, several supplementary log files are stored in the working directory TrueConf Server, which are discussed in detail in the [relevant knowledge base article](#).

9.5. Configuring Preferences

Some settings can be set up personally for each TrueConf Server administrator. e.g., control panel interface language, time zone, and reports export parameters.

video.server.com#vcs

System

- Stop
- Restart
- Server Log
- Preferences...

Preferences

In this section you can set preferences for your account (**anonymous**)

Settings

Language: English

Time zone: GMT+0:00 ☒ Use device time zone

Export to CSV

Encoding: UTF-8

Field delimiter: ;

Apply

1. Go to the **System → Preferences...** menu in the upper right corner of the control panel.
2. Select your language and time zone. Please note that the time zone will be applied to your meetings in all [server logs](#) and during the [scheduling process](#). You can use the time zone of the computer where your server is installed by checking the corresponding box.
3. In section **Export to CSV**, you can configure the [report export](#) settings, such as the encoding used and the delimiter character for representing table rows in text format.

After changing your preferences, click **Apply** to save them.

If version TrueConf Server is used on Linux OS and the time zone is changed with the **Use device time zone** checkbox selected, all server services need to be restarted.

10. Server Information and General Settings

TrueConf Server Control Panel is a web interface that allows you to manage TrueConf Server.

Thanks to the web interface, administrators can:

- View information about the status, registration, and server license, as well as track its performance
- Add and delete users
- Schedule video conferences
- Setup client applications and integration with Active Directory and LDAP
- Set connection rules for calls over SIP and H.323 gateways.

By default, the TCP port for accessing the TrueConf Server control panel is equal to **80**; however, when deploying the server on Windows, you can change the port number in the installation dialogue window.

However, you can [select any different port](#) after installation both on Windows and Linux. In this case, the port has to be specified in the browser address book right after the colon in the hostname, e.g., `http://localhost:8080`.

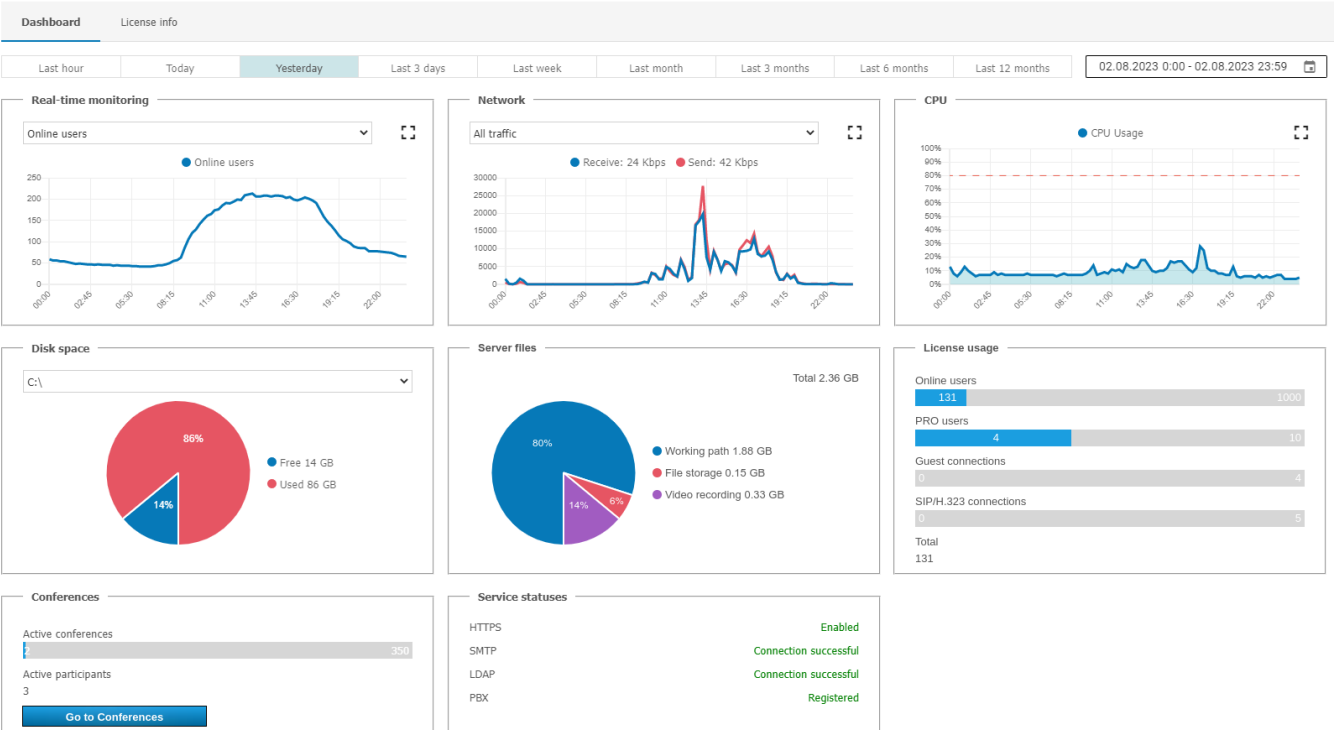
10.1. Server Information

When you navigate to the TrueConf Server control panel, it opens in the **Summary** section.

On the **Dashboard** tab, you will see the following data:

- Real-time performance graphs:
 - CPU usage
 - Network usage (according to the traffic type)
 - Numbers of active conferences and connections of all types
- Available disk space
- space occupied by the [working folder](#), [files transferred in chats](#), and [recordings of conferences and calls](#);
- Number of online users, reserved PRO licenses, guest connections and SIP/H.323/RTSP connections
- The number of active (ongoing) conferences and the total number of its participants
- The status of HTTPS, SMTP, LDAP, and SIP/H.323 gateways.

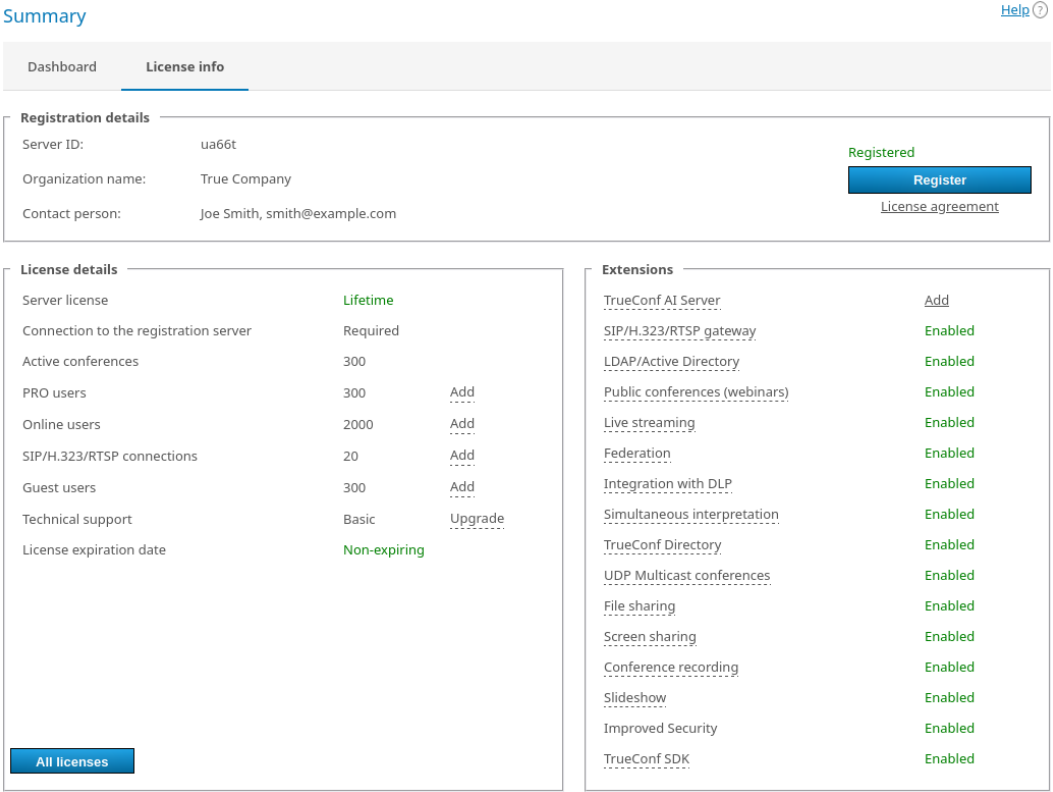
Summary



You can enlarge each chart using the button, and by navigating to the calendar with the button, you can select any date range to display the data.

The **License info** tab shows information about the license, registered contact person, and the extensions used on the server. Here, you can:

- by using the **Register** button to [renew or modify the server license](#);
- proceed to purchasing additional features from block **Extensions**.



By clicking the **All licenses** button, a window will appear with the full list of licenses associated with this instance of TrueConf Server, verified by [server ID](#). To obtain this information, a connection to the registration server `reg.trueconf.com` is required.

In case of any problems with server registration, the administrator may reach out to TrueConf technical support team via the contacts that will be displayed in case of an error.

In the event of a connection loss with the registration server (`reg.trueconf.com` on TCP port `4310`), your TrueConf Server Free will be disconnected after 12 hours. The scheduled disconnection time will be displayed on the **Summary** tab. The full version of TrueConf Server does not have these limitations, regardless of whether the registration is online or offline.

If the server is connected to the Internet, administrator will be able to receive notifications updates in TrueConf Server control panel. In the left menu of the control panel you will see a notification, while at the top of the page a message with the latest version download link will be displayed. After you have updates, the notification will disappear.

10.2. PRO licenses

In the **Dashboard → PRO licenses** section, the administrator TrueConf Server can configure the [distribution of PRO licenses](#) for conference participation and view data on their usage.

[PRO licenses](#) [Help](#)

To participate in group conferences, each registered user needs a PRO license.

- Permanent licenses are provided on an indefinite basis to the selected user groups
- Temporary licenses are provided automatically when a user connects to a conference if PRO licenses are available on the server at the moment.

User interface settings

- ☒ Display information about PRO license
- ☒ Allow users to request temporary PRO licenses

Client license management

Available PRO licenses: 0 2 users do not have a license [Add](#)

Permanent (10) **Temporary (0)**

EDIT

User	TrueConf ID	Groups
Kathryn Floyd	floyd	Developers
Daniel Reed	reed	Developers
Margaret Taylor	taylor	Developers
Abe Chester 2	chester	IT department
Bruce Hubbard	hubbard	IT department
Carla Devine	devine	Managers
Deborah Humphrey	humphrey	Managers
Albert Moore	moore	Managers
Ethan Nelson	nelson	Managers
Alice Campbell	campbell	Operators

1. Activate the display of information about a PRO license in the user personal area and in TrueConf client applications (enabled by default).
2. Enable users to request a PRO license in advance (before participating in a conference) either in the personal area and in the client application (enabled by default).

3. The list of users who are given permanent PRO licenses. Such users can be picked only by selecting groups. It is impossible to select users individually.
4. Click on the **Edit** button to select groups of users. To apply changes, you will need to restart TrueConf Server. If the number of selected users is larger than the number of licenses available on your TrueConf Server, the licenses will be distributed depending on the priority of groups. Within groups, the licenses will be first given to the users who are on top of the list (users are sorted by their display names).
5. The list of users who were given temporary PRO licenses, along with the validity period of each license. You can revoke a user's temporary license by clicking **X** next to the user's name. This will immediately return the license to the pool of available temporary PRO licenses. If a user is participating in a conference at the time when the license is revoked, he/she will be automatically removed from this meeting.
6. If there are users, who did not receive licenses, the corresponding notification will be displayed and the number of users without a license will be specified.

Users without a license



Permanent (2)

Temporary (0)



Search



Bruce Robertson

robertson@video.example.net



Amanda White

white@video.example.net

The current list of users was created on 23.08.2023 at 18.26

Two separate lists will be generated there:

- **Permanent** — users who couldn't obtain licenses during the distribution of permanent PRO licenses will be added there (the time of the last restart TrueConf Server will be displayed at the bottom of the list);
- **Temporary** — users who attempted to obtain a temporary PRO license but found none available on TrueConf Server. This list is not cleared when the TrueConf Server service or the computer itself is restarted. Each user is removed from the list 24 hours after being added.

Please note that the changes in the distribution of PRO licenses are applied either after the server restart or automatically once every 24 hours (check part 5 in the description of [license distribution](#)). For example, if a new user is added to the group with permanent PRO licenses, he/she will not receive a PRO license until you restart TrueConf Server.

10.3. Basic settings

In the **Dashboard → Settings** section, you can modify several operational parameters of TrueConf Server and adjust some client application settings.

10.3.1. Server settings

In section **Settings**, you can modify the following parameters:

Settings

[Help ?](#)

Work path

Path: Apply

Reports

☐ Enable detailed logging

Language settings

By default: ?
 Public pages and the personal area: Apply

1. **Work path** — the directory on the machine where the server is installed. Here, the server stores certain data needed for its work (e.g., logs, user avatars, etc.). We do not recommended using network drives for this directory as a way of saving space; it is better to use network storage separately for [recordings](#) and [files sent in chats](#).

In the TrueConf Server for Linux control panel, the working directory path is set to `/opt/trueconf/server/var/lib` and it cannot be changed. However, you can set up a symbolic link (symlink) as [shown in the corresponding section](#).

2. Check **Enable detailed logging** to collect more detailed information in the [server operation logs](#). These logs may be needed when contacting technical support. This setting is responsible for the `stdout.log` file.

In our knowledge base, you can find detailed information about the [purpose of the saved log files](#), and [which logs are needed in various situations](#) for analyzing and resolving server-related issues.

3. **Language settings** The text contains only colons and does not require translation.
 - The language from the **By default** list will be used for [email templates](#) (until you select a different language when configuring SMTP notifications), ICS files for adding

events to the calendar, web page previews on social media, and the connection menu for SIP/H.323 endpoints.

- In the **Public pages and the personal area** list, you can specify which languages supported by the server will be displayed on the [guest page](#), [event pages](#), and also in the user's [personal area](#). The language **By default** will necessarily be included in this list of languages.

10.3.2. How quickly will `stdout.log` fill up if detailed logging is activated?

Activation of detailed logging requires additional space on the SSD drive where TrueConf Server is installed because the size of the `stdout.log` file will increase much faster.

Path to `stdout.log` :

- Windows: `working directory\stdout.log`
- Linux: `/opt/trueconf/server/var/log/vcs/stdout.log`

By default, the maximum size of `stdout.log` is 1 GB. When this limit is reached, the file is automatically renamed to `stdout.old.log`, and a new file is created in its place. So, there can be at most 2 main log files of server operation with a total size of 2 GB. The rate at which the file fills up is not constant: it depends on the activity on TrueConf Server (number of meetings started, online users, etc.).

Remember, besides `stdout.log`, there are also [other log files](#) on the server.

You can increase the maximum size of `stdout.log` with the help of technical support.

10.3.3. Application Settings

In section **Application**, you can modify the following parameters:

Application

Application	Current version	Min. ver	Last ver	Authorization	Setup URL
TrueConf Android				☒	https://play.google.com/store/apps/details?id=com.trueconf.videochat&hl=en
TrueConf iOS				☒	https://itunes.apple.com/us/app/trueconf/id536475636
TrueConf Linux				☒	
TrueConf OS X				☒	
TrueConf Windows	8.5.0	7.2.1	8.5.0	☒	https://10.140.0.33/downloads/trueconf_windows_client.exe

Application settings

User connections authentication key

iMhrzdXv2uyEfe1VnsGFt_P8OEckKpELy

Generate a new key

Guest connections authentication key

j_BNw2Fqd3LHyuHa3CTp7aIzayrJHxCR-

Generate a new key

Authorization token lifetime on a device

60

days

Push notification content

Show name and message content

Display the Reactions panel in multipoint conferences

☒

Save application settings

1. **Settings of the client applications TrueConf** from which users will connect to your conferences.
2. **User connections authentication key** — is used when creating session keys to identify users in a conference. To replace the key with a new one, click the **Generate a new key** button. Changing the key during a conference can enhance its security by making it more difficult for third parties to connect.
3. **Guest connections authentication key** — similar to the previous one, but it controls connections through guest accounts in public conferences.
4. **Authorization token lifetime on a device** indicates the duration for which the session will be maintained after the client application connects to TrueConf Server or the user logs into their personal area. After the specified time expires:
 - If a user has been signed in to a client application and then goes offline (either logs out or closes the application), he/she will need to authenticate again according to the [specified settings](#) when the application is launched.
 - If a user has been signed in to the personal area, he/she will be logged out after clicking on any button or going to a different section; this person will need to re-authorize according to the [current settings](#).
5. In the drop-down list **Push notification content** you can select the content that will be sent to push notification services (Google, Apple, etc.) and displayed on a user's mobile device. Available options: the message and the sender's name, only the name, or an anonymous notification (both the name and content will be hidden).
6. If you check the box **Display the Reactions panel in multipoint conferences**, users will be able to use [special statuses](#) (reaction icons) during events.

Don't forget to save settings after changing them.

10.3.4. Transferring server settings

You may need to save the backup copy of settings if it is necessary to reinstall the operating system or migrate the server to a different physical machine without having to re-configure the server from scratch. To learn more about saving and restoring settings, refer to our knowledge base:

- [migrating TrueConf Server from one Windows server to another](#) ;
- [migrating TrueConf Server from one Linux server to another](#);
- [migrating TrueConf Server from Windows to Linux](#);
- [migrating TrueConf Server from Linux to Windows](#).

10.3.5. Configuring client application connections

Further down the page, there is a section for configuring restrictions on TrueConf client applications used to participate in calls and conferences held on your TrueConf Server. It is also possible to set separate restrictions for different operating systems: Windows, macOS (previously OS X), Linux, Android/Android TV, iOS/iPadOS.

Here, one can also disable authorization and joining conferences (including guest connections) from the applications for certain operating systems. For example, you may need to prevent employees from using corporate video communication on smartphones, and allow it only at workstations. To do it, uncheck the **Authorization** box for the selected application in the **Application** table.

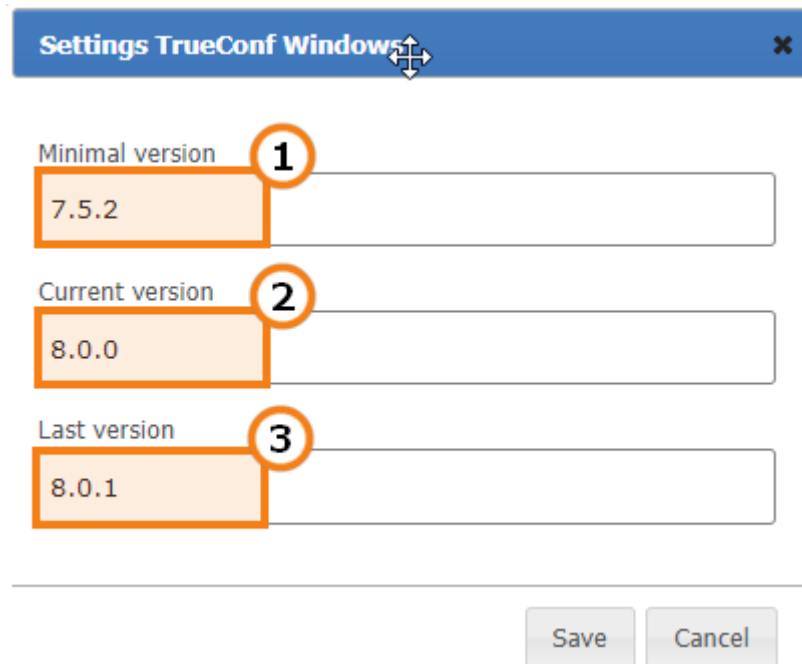
When TrueConf Server is updated, the installation files for TrueConf for Windows client applications, available for download on the guest page and already embedded with links to connect to your server, are automatically updated as well. Other applications need to be installed from other sources, with all links also provided on the [guest page](#).

To choose allowed versions of the application, click on the application name in the first column of the table. Here, you can choose the latest version of the application to which users will be allowed to update. Besides, you can choose which updates should be mandatory and which should be only recommended when users connect to your server:

Application

Application	Current version	Min. ver	Last ver	Authorization	Setup URL
TrueConf Windows	8.3.1	7.5.2	8.4.1	☒	https://10.140.2.195/downloads/trueconf_windows_client
TrueConf Android				☒	https://play.google.com/store/apps/details?id=com.trueconf.videochat&hl=en
TrueConf iOS				☒	https://itunes.apple.com/us/app/trueconf/id536475636
TrueConf Linux				☒	
TrueConf OS X				☒	

Here, you can edit the following parameters:



Settings TrueConf Windows

Minimal version 1
7.5.2

Current version 2
8.0.0

Last version 3
8.0.1

Save Cancel

1. In the **Minimal version** field, you can specify the oldest version of the client application that can be connected to the video conferencing server. If the client application version is lower than the one specified here, a user will be required to update the application. A user will be unable to continue working with the application without updating it. A warning window will prompt the user to update to the version specified in the **Last version** field. If the user connects to a different video conferencing server, the application version will be compared with the version from the new server. The warning window will include the button for downloading the update if a link is provided in the **Setup URL** column for the configured application.
2. In the **Current version** field, specify the preferred client application version. If a user's application version is lower than the one specified in this field, but equal to or higher than the version in the **Minimal version** field, the user will be prompted to follow a link to the appropriate resource and update the application. The user will also be allowed to close the notification window and continue working.
3. In the **Last version** field, specify the version of the client application to which the user will be prompted to update.

You can install TrueConf for Windows client application on multiple machines in the corporate network with the help of group policies (GPO). To do it, you can use an msi package that can be downloaded from our website. To learn more about this feature, read the [corresponding article in our knowledge base](#).

10.3.6. Updating applications for Windows without reinstalling the server

The next version of the client application may be released independently of the update for TrueConf Server. In this case, you can also manually configure the transition to it for TrueConf for Windows users of your video conferencing server.

To do it:

1. Go to the [page TrueConf for Windows](#) and download the latest release versions.
2. Rename the downloaded file according to its bit version in the following way:
 - Rename the **x64** file (for 64-bit OS) to `trueconf_windows_client_x64.exe`
 - Rename the **x86** file (for 32-bit OS) to `trueconf_windows_client_x86.exe`.
3. Move the renamed files to the following directories depending on the OS used on your server:
 - TrueConf Server for Windows – to the `ClientInstFiles` directory at the server installation path (by default `C:\Program Files\TrueConf Server\ClientInstFiles`)
 - TrueConf Server for Linux – to the `/opt/trueconf/server/srv/clients/` directory.
4. Go to the **Settings** section of the server control panel.
5. Open the TrueConf for Windows settings window and specify the version of the previously downloaded application in fields **Current version** and **Last version**, as [shown above](#).

10.4. How to use other folders on Linux with symlink

If you plan on storing many conference recordings or expect a large number of files to be sent in chats, you might find it convenient to change their storage path. For instance, you could move them to a larger SSD to avoid taking up space on the system storage. On Linux, you cannot change the path through the server control panel, but it is possible to use **symbolic links (symlink)**.

To run the commands listed below, use the **sudo** program, or switch to the administrator mode by executing the `su -` command in the terminal and entering the root password.

To change the storage location for TrueConf Server on Linux, follow these steps:

1. Create a new directory for the required files. Below are the examples of console commands for working with new directories at the `/var/server/` path:
 - creating a directory for storing conference recordings:

```
mkdir -p /var/server/recordings
```

sh

- creating a directory for storing files:

```
mkdir -p /var/server/files
```

sh

2. Give the **trueconf** user owner permissions for the created directory.
 - for recordings

```
chown -R trueconf:trueconf /var/server/recordings
```

sh

- for files

```
chown -R trueconf:trueconf /var/server/files
```

sh

3. If you need to keep the existing files, move them to the new directory:

- copying recordings

```
cp -aRT /opt/trueconf/server/var/lib/recordings /var/server/recordings
```

sh

- file copying

```
cp -aRT /opt/trueconf/server/var/lib/files /var/server/files
```

sh

4. Delete the directory that you want to replace with all its files since we will create a symbolic link instead:

- deleting the directory with recordings

```
rm -r /opt/trueconf/server/var/lib/recordings
```

sh

- deleting the directory with files

```
rm -r /opt/trueconf/server/var/lib/files
```

sh

5. Create a symbolic link to the new directory:

- for recordings

```
ln -s /var/server/recordings /opt/trueconf/server/var/lib/recordings
```

sh

- for files

```
ln -s /var/server/files /opt/trueconf/server/var/lib/files
```

sh

6. Restart the server main service:

```
systemctl restart trueconf
```

sh

7. If you need to remove a symbolic link, use the following command:

```
unlink [symlink_path]
```

sh

where `[symlink_path]` is the path to the directory created at step 2, for example, `/var/server/recordings`. Please note that this command does not delete the directory itself. To do this, run:

```
rm -r [symlink_path]
```

sh

10.5. Mounting a network storage on Linux

You can also create a symbolic link to any mounted directory, such as an external network storage.

To run the commands listed below, use the **sudo** program, or switch to the administrator mode by executing the `su -` command in the terminal and entering the root password.

For example, to mount an external network storage available via the [SMB protocol](#), follow these steps:

1. Install required tools on your system:

On Debian

```
apt-get install -y cifs-utils
```

sh

2. Create a directory where you will mount the network storage (see [step 1 in the section about creating symbolic links](#)). For example, to mount the directory with chat files:

```
mkdir -p /var/server/files
```

sh

3. Create the file `credentials.ini` with the data required to access the remote storage. It should include the following lines:

```
username=[login]
password=[password]
domain=[domain]
```

sh

where:

- `[login]` — login
- `[password]` — password
- `[domain]` — the domain to which the network storage belongs (this line is optional).

For example, with this command in the terminal:

```
echo -e 'username=[login]\npassword=[password]\ndomain=[domain]' > credentials.ini
```

sh

The `-e` parameter of the `echo` command enables correct interpretation of special characters that are escaped with `\`. In the example above, this is the newline character `\n`.

4. Mount the network storage to the created directory using the `credentials.ini` file:

```
mount -t cifs -o credentials=[credentials_path] [remote_path] [local_path]
```

sh

where:

- `[credentials_path]` — the full path to the `credentials.ini` file created during the previous step
- `[remote_path]` — the path to the mounted storage, for example, `//10.100.2.120/files`
- `[local_path]` — the path to the local directory used for mounting (see step 2), for example, `/var/server/files`.

You can now create a symbolic link to the mounted directory, as [shown earlier](#).

To unmount a directory, run the following command (as administrator or using `sudo`):

```
umount [local_path]
```

sh

where `[local_path]` is the path to the local directory for mounting (see step 2), for example, `/var/server/files`. After that, you can delete the directory with the command:

```
rm -r [local_path]
```

sh

10.6. Configuring access to network storage in Windows

TrueConf Server for Windows will be able to access network drives, only if its three services are allowed to read and write to network paths. However, by default, these services are launched under the Local System account, which does not have access to network resources. So, you need to configure the services to run under a user account with required permissions (e.g., OS administrator):

1. Open the list of Windows services. To do it, launch the command prompt (terminal) or PowerShell and run the command `services.msc`.
2. Locate the **TrueConf Server** service in the list (the main service of the video conferencing server).
3. Go to the service properties by double-clicking on the name or from the context menu.
4. On the **Log On** tab, activate the **This account:** toggle.
5. Enter the username and password for the required account, for example, a Windows administrator, and click **OK**.
6. Repeat steps 2-5 for the **TrueConf Web Manager** and **TrueConf Server Manager** services.

10.7. File storage

When the location for the working directory is selected, one can immediately configure other parameters related to the allocation of space for various video communication needs: paths for chat files and video recordings of events.

When the path to chat files is changed, the files will not be automatically moved to the new location. To make sure that these files are available in chats, you should first move them to the new directory, and only then change the path in the control panel. The same applies to recording files: they will be unavailable in the built-in player of the control panel and in users' applications until they are copied to the new directory.

In the **File storage** section, you can specify the file storage settings for user exchanges:

File storage

[Help ?](#)

Settings

Path: **1**

Available space on the hard drive: **14.54 GB**.

☐ Set disk quota for file storage (GB): **2**

☒ Set file expiration date (days): **3**

☒ Limit download speed 10847 kbit/s **4**

☒ Limit upload speed 16581 kbit/s **5**

Apply

1. Select the location of the file directory. By default, recordings are stored in the `files` folder inside the [server working directory](#). It is possible to use network paths (see above to learn how [services can be configured on Windows](#)).

In the control panel of TrueConf Server for Linux, one cannot change the path to the directory where conference recordings are saved. However, you can set up a symbolic link (symlink) as [shown in the corresponding section](#).

2. The maximum storage allocated for chat files. The decimal counting system is used, where 1 KB = 1000 bytes. Keep this in mind, as the OS may display it differently; for example, Windows Explorer shows sizes in multiples of 1024.
3. File lifetime (specified in days): the period after which files will be automatically deleted. The countdown starts from the time when the file was first uploaded. By default, automatic deletion of files is disabled. Available values range from 1 to 99999 days (almost 274 years, which is clearly sufficient for any business task).
4. Use the slider to set maximum download speed limits to download the files from the server.
5. Use the slider to set maximum upload speed limits to upload the files to the server.

Below you can **set restrictions** on the size and extension of files sent in chats. These restrictions apply to files sent between users of your server and incoming files from users of other (federated) servers:

File upload restrictions

☒ Restrict file uploads by size (MB):

☒ Restrict file uploads by extension

Blacklist

File extension list

BAS BAT CHM CMD COM CPL DLL EXE EXE HLP JAVA JS LNK PIF PY REG SCR SHS SSH VBS

Separate extensions with a space and do not include the leading dot

Text message to replace blocked file

The file (%file_name) cannot be uploaded due to the server policy

Apply

- The file size (from 1 to 99999 MB), the decimal system is used where 1 KB = 1000 bytes. Keep this in mind because the operating system may display it differently; for example, in Windows Explorer, sizes are shown in multiples of 1024.
- Extension (for example, due to security reasons, you can block the sending of executable files such as `.exe`, `.bat`, `.sh`, etc.). Separate the values with a space as shown in the screenshot above:
 - When selecting option **Blacklist** (default value), only explicitly specified extensions will be blocked.
 - When selecting option **Whitelist**, all extensions will be disabled except for those specified in the list;
- You can also specify the message that will be displayed instead of the blocked file if it violates one of the restrictions on size or extensions.

The notification replacing the blocked file will be displayed exactly as you specify it, in all languages, it will be the same for all users regardless of locales, etc. If you have a multilingual audience working with chats, keep this in mind when writing the text (e.g., you may write the text in English).

10.8. Call and Conference Recordings

In section **Recordings**, you can adjust the server settings for automatic conference recording.

If a conference is simultaneously translated into one or multiple languages, its recording will include all the audio tracks that were translated, and as a separate track with the main audio, where one can listen to both the speakers and attendees who made audio remarks. This will work regardless of the selected video recording format.

Recordings

[Help ?](#)

The screenshot shows the 'Settings' panel for 'Recordings'. It contains the following fields and controls:

- Path:** A text input field containing 'C:\TrueConf\Recordings', highlighted with an orange box and labeled with a circled '1'.
- Record video calls:** A dropdown menu set to 'disabled', highlighted with an orange box and labeled with a circled '2'.
- Record multipoint conferences:** A dropdown menu set to 'on demand', highlighted with an orange box and labeled with a circled '3'. To its right is the text 'Determined by settings when scheduling a conference'.
- Recording indicator:** Two checkboxes, both checked. The first is 'Show indicator in client applications' and the second is 'Show indicator in mixed video stream'. This section is highlighted with an orange box and labeled with a circled '4'.
- Recording downloading by the owner:** A dropdown menu set to 'enabled', highlighted with an orange box and labeled with a circled '5'.
- Video container:** A dropdown menu set to 'MP4', highlighted with an orange box and labeled with a circled '6'.
- Set video records expiration date (days):** A checkbox followed by a text input field containing '7', highlighted with an orange box and labeled with a circled '7'.

At the bottom left of the settings panel is a blue 'Apply' button.

1. Path to the folder where all recordings will be saved. By default, recordings are stored in the `Recordings` folder inside the [server working directory](#). The [list of recorded conferences](#) displays video recordings from the specified folder. If the path is changed, the list will also be changed accordingly. A network path can also be specified in this field, in this case check above to learn how [services can be configured on Windows OS](#).

When the storage path is changed, the recording files **will not be automatically moved**. Due to this reason, the owners of conferences will be unable to download video recordings in the personal area. However, if recordings are manually moved to the new location, everything will work as intended.

In the TrueConf Server for Linux control panel, one cannot change the path to the directory with conference recordings. However, you can set up a symbolic link (symlink) as [shown in the corresponding section](#).

2. Enable/disable point-to-point video call recording. This option is similar for all calls: either all are recorded, or none are recorded. Please note that if you enable this option, you will not be able to use direct connection between users (to be recorded, all information between subscribers is transferred through the server).
3. There are three options to set up group conference recordings: either all are recorded, or none are recorded, or recording is set [separately for each conference](#) ("on demand" mode).
4. Visibility settings for the indicator showing that a conference is being recorded on the TrueConf Server side (enabled by default). With these checkboxes, an administrator can disable the display of this indicator separately for:
 - participants in client applications TrueConf;
 - mixed video for recording, WebRTC users (from a browser), or connections via SIP/H.323 protocols (from endpoints).

5. Making it impossible for the conference owner to download meeting recordings stored on TrueConf Server. In this case the conference owner will see the list of recordings in the personal area or in the client application, but will be unable to download them.
6. The video format in which recordings will be saved. Supported formats are MP4, MKV, and WebM.
7. Time (in days) after which conference recordings should be deleted automatically. Click the checkbox next to the field to activate the text field. If you don't check this box, recordings will be stored indefinitely (recordings are not deleted automatically).

10.8.1. Frequently asked questions about recordings

10.8.1.1. What will happen if I run out of space in the directory selected for storing recordings?

New recordings will no longer be saved, but the recordings that had been made previously will remain.

10.8.1.2. What happens to the recording if storage space runs out during a conference?

Recording will end and the file will be saved at the moment when the directory is filled.

10.8.1.3. How much space does a call or conference recording take?

To estimate the storage space required for storing the recordings of TrueConf calls and conferences, you need to know the approximate bitrate (number of bytes per unit of time). However, due to the use of VBR (variable bitrate), video is optimally compressed, so it's impossible to predict in advance how much space, say, 10 minutes of video will take up. The size may depend on many factors:

- recording quality (selected in the [section Gateways →Transcoding](#));
- The number of movements in the frame, for example, the video of a speaker, who is sitting without any movements, will be compressed better than the video with some dynamic content
- The quality of the camera given that the resolution of the captured video is the same.

Generally, the storage requirements for recording a video conference in FullHD 1080p can range from approximately 50 MB to 500 MB, depending on the factors mentioned above. It's advisable to plan for the higher end of the range to make sure that there is enough space.

10.9. Connecting Users

To learn how to configure access for users outside your VCS server's network, refer to [our knowledge base](#).

TrueConf client applications can send DNS queries to simplify the initial connection of users to your server. Here is how this feature can be used:

- for automatic [search of available servers](#);
- for [corporate email authentication](#) instead of entering a username (TrueConf ID).

Additionally, users and guests of your server can go to a convenient [guest page](#) with links to client applications.

10.9.1. Where can I find client applications

To enable users of your server to connect to the video conferencing system, share the link to the guest page where they can download client applications for all supported platforms.

The guest page is available at `http[s]://<server>[:<port>]` where:

- `<server>` — the address of the computer with TrueConf Server;
- `<port>` - port used to access the control panel (if you are using default `80` port, you don't need to specify it)

For example:

- `https://videosever.com`
- `http://100.120.12.12:7777`

You can configure the link to the guest page in the [Web →Settings](#) control panel menu.

10.9.2. Configuring automatic server discovery

You need to specify the server address in the network settings of your client application so that your client application can connect to your TrueConf Server instance and your users can authorize. You can either do it manually or let your client application find the server automatically via DNS.

After connecting to the desired server, the user must authenticate by entering their [username and password](#).

10.9.2.1. Manual configuration of the client application

Users can configure connection to TrueConf Server manually. In order to do it, you need to specify the TrueConf Server address and connection port manually in the application network settings menu (or upon the first application launch). You can find detailed instructions on how to connect an application to the server on the guest page.

10.9.2.2. Automatic server discovery with mDNS

The TrueConf client application sends a broadcast message at startup, asking the host (TrueConf Server) to identify itself. This request is sent via the UDP port `5353`. In response, the application receives server data, including its IP address. All other host machines in the network record the information about the identified host in their mDNS cache. This allows the user to get the list of the servers available for connection without manually specifying the address. Typically, there is one server in a corporate network.

More details about mDNS operating conditions are covered in the basic administration course for TrueConf Server at the [certification center TrueConf](#).

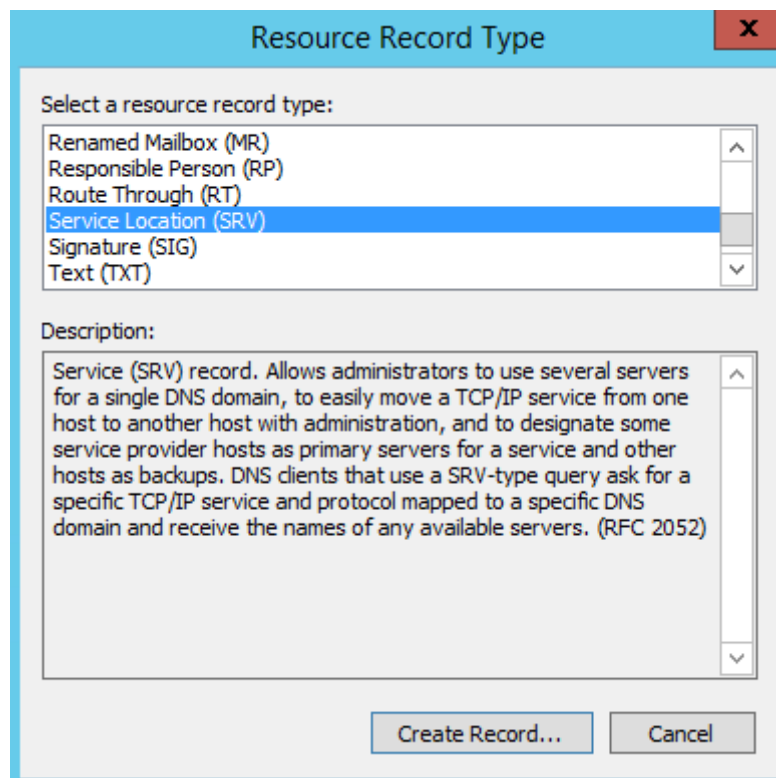
10.9.2.3. Additional DNS Configuration for Discovery

If mDNS is blocked in the corporate network, the client application within the domain will still be able to automatically discover TrueConf Server. To enable this feature, specify the server address in the DNS domain, which is the **primary DNS suffix** for the client computer. Create an SRV record for the `_vcs._tcp` service in the required domain and specify the server address and port in this record.

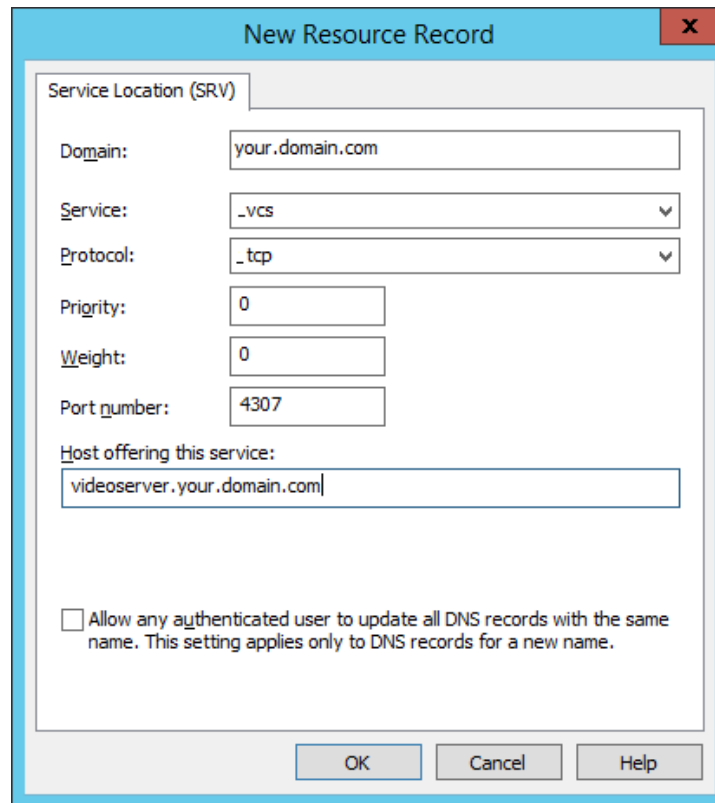
If your server version is 5.5.1 or older, use the SRV record in the format `vcs2.tcp`. Starting from the version 5.5.2, the format with underscores is required.

The following example shows how to do this using DNS utility in Microsoft Windows 2022 Server:

1. Go to **DNS Manager**.
2. Right-click on the desired domain, select **Other New Records**, and choose **Service Location (SRV)** from the list:



3. Configure the following settings:



In this example the TrueConf Server instance has **videoserver.your.domain.com** address and port 4307.

10.9.3. Configuring automatic server connection using corporate email

To authenticate on TrueConf Server, you can use not only your login (TrueConf ID) but also your corporate email. This option can be useful if SSO is not used and the email server address does not match the address of the video conferencing server, for example, `mail.example.com` and `video.example.com`. In this case, instead of remembering the login, the user only needs to remember his/her email address and enter it in the login field when signing in to the application. The application will then find the video conferencing server address by the mail server address and try to connect to the video conferencing server.

Please note that this corporate email must also be specified in the [user profile](#).

This feature is not dependent on the server version but requires client applications of a specific version:

- TrueConf for desktops (Windows, Linux, macOS) version 8.5+
- TrueConf Room versions 5.0+
- TrueConf for Android versions 3.1+
- TrueConf for iOS/iPadOS versions 3.9+

However, this feature does not work out of the box; **preliminary configuration is required**. An SRV record of a specific type has to be added on the DNS server accessible to client applications:

```
_vcs._tcp.[mail-server]. 3600 IN SRV 10 0 4307 [video-server].
```

sh

where:

- [mail-server] — address of the corporate mail server
- [video-server] — the address is TrueConf Server.

For example:

```
_vcs._tcp.mail.example.com. 3600 IN SRV 10 0 4307 video.example.com.
```

sh

For more information on configuring this feature and SRV records, refer to the **basic administration course** in the [certification center](#) TrueConf.

11. Network and federation settings, STUN/TURN servers

Here are the minimum steps needed to set up a working corporate communication system:

1. [Select a machine \(PC, physical or virtual server\) with suitable hardware.](#)
2. [Install TrueConf Server.](#)
3. [Log in to the control panel.](#)
4. [Register the server.](#)
5. [Configure HTTPS](#) (it is used for many key features such as integration with the AI server, conference scheduling, etc.) and [specify the external server address](#) (the address of the guest page).
6. *Configure the server availability for the users within the corporate network and, if necessary, for the users from an external network (outside the secure corporate network).* **You are here!**
7. [Create user accounts](#) or [integrate the server with a directory service](#) via the LDAP/LDAPS protocol.
8. Install client applications for users and show them how to connect to your server (check the [documentation for the desktop application](#)).

In section **Network**, you can configure certain TrueConf Server settings related to the network:

- connecting client applications and third-party devices (SIP, H.323, etc.)
- sending email notifications for users and administrator
- connection with other instances of TrueConf Server.

11.1. Network Settings

In section **Network → Network settings**, you can specify the IP addresses and ports that the client applications downloaded from TrueConf Server will use to try to connect. By default, only the IP address of the machine where TrueConf Server is installed is used for this purpose.

Client applications always connect to TrueConf Server over the only TCP port (4307 is used by default). It is the only port used for signalling, sending authentication data and audio or video streams. An HTTPS port (443 selected by default) is used for displaying the scheduler, accessing real-time meeting management and for API calls. To learn more about this topic, check out the [article in our knowledge base](#).

You can specify a different port when editing the list of IP addresses.

No UDP port can be used for communication between TrueConf Server and a client application.

Network settings

[Help ?](#)

Internal addresses	External addresses
☐ Listen on all IP addresses	☒ Specify
10.120.1.141:4307 192.168.56.1:4307	5.100.101.102:4307
Add Reset Apply	Add Reset Apply

The **Internal addresses** list contains the addresses and ports that the server will monitor for client application connections. These should be the network interface addresses of the machine where TrueConf Server is installed, or its internal DNS name that resolves to one of the network interfaces by IP. When the **Listen on all IP addresses** checkbox is selected (it is checked by default), the list is automatically compiled from all such addresses, including virtual ones.

To edit the **Internal addresses** list:

1. Clear the checkbox **Listen on all IP addresses**.
2. To change the parameters for the specific connection, just click on the line with the selected address.
3. Use the buttons at the end of the list to add a new address and to save or discard changes.

Addresses from the **External addresses** list are added in an encrypted form to the name of TrueConf for Windows installer downloaded from the server guest page (refer to [application settings](#)). These addresses will be used when the application is launched for the first time. Users of your server and guests, who try to join a webinar, will be unable to connect to the server if the external address will be unavailable to them (however, they will be able to connect, if they specify a correct address in application settings). So, we suggest that in the **External addresses** list, you should specify the addresses accessible to all users both within the corporate network and from outside. This list can include addresses configured for forwarding to internal addresses, the IP address of your NAT, DNS name, or addresses to which you plan to migrate TrueConf Server in the future (so that the applications which were downloaded before, could connect to the server via the new IP address). If the server will be used only within a local network, this list will not be needed.

If you plan to migrate the server to another IP address, all you need to do is to add the new IP address to the **External addresses** list beforehand. This will help client apps to store the new address right after the next connection to the server in advance.

To edit the **External addresses** list, check the **Specify** checkbox.

After you have changed the address to an external one, go to the [section Web →Settings](#) of the server control panel and change the external website address to the public IP (which you

specified in the list **External addresses**). Then, restart the server to allow external users to connect from outside.

This guide does not cover TCP port forwarding or DNS names. You can learn more about these topics in your network equipment manuals.

11.2. Federation

Federation mode enables users TrueConf Server to make calls and join conferences with users from other TrueConf Server, as well as exchange chat messages. Federation is available only in the full version of TrueConf Server (for example, when purchasing additional [licenses of any type](#)). There is no limit to the number of servers that can be federated. The limitations on conducting group conferences will correspond to the limitations of the TrueConf Server initiating the connection.

Federation

[Help ?](#)

Allowed for all but blacklisted servers ▼

Blacklist

video.some-company.com

video.other-company.com

Add

Reset

Whitelist

Add

Apply

Requirements for the correct work of federation:

1. The server has to be [registered](#) with an existing DNS name or you have to specify the real server address with the help of DNS SRV records.
2. Each federated server has to be accessible to another server by its DNS (FQDN) name, specified during registration, via the main port for the TrueConf protocol (**4307 is selected by default**). Moreover, it has to be accessible via an HTTPS port (**443 is used by default**). If a different HTTPS port is [configured on one of the servers](#) or [a different port is selected for the communication protocol](#), access to this server should be configured via the selected port instead of the standard one.
3. Each federated server has to be available to all users of both servers (whose participation in calls and conferences is expected). Each server has to be accessible via an HTTPS port (**443 is selected by default**) by its domain name which should match the external server name specified during the registration.

4. **IMPORTANT!** If you are using a server which is **below 5.4.0**, it also has to be accessible to all federated users via the main port for the TrueConf protocol (**4307 is used by default**).

For more details on how the client application can locate the server, refer to the section on [configuring automatic connection](#).

Federation has to be configured on both servers to ensure that they are accessible to each other according to the rules mentioned above. To do it:

1. In the drop-down list, select the federation mode:
 - **Disabled;**
 - **Allowed for whitelisted servers** – meaning federation is available to all servers specified in the list, and only to them;
 - **Allowed for all but blacklisted servers** – Federation with the server is available to any servers not listed here.
2. Enter the IP addresses or domain names (FQDNs) of the required servers into one of the lists (depending on the federation mode) and click **Add**.

IP addresses do not have to be specified for federation; only DNS (FQDN) names are needed. Besides, the masks containing an asterisk ***** are supported, for example, `*.example.com`, `v*.example.com`, `example.*`, `*.example.*`.

3. Click the **Apply** button to restart TrueConf Server and save the changes.

11.2.1. Examples of federation in operation

Federated users can access the chat of a virtual room if they were added as participants when the room was created or edited, but not if they were added "on the fly" after the event had already started.

Let us take a look at some examples.

Case 1

To configure federation with a different TrueConf Server instance, e.g., `videoserver.example.com`, you will need to:

1. Add `videoserver.example.com` to the white list
2. Activate federation on the side of `videoserver.example.com` in one of the following ways:
 - Add the domain name of your server to the its white list
 - Allow federation with all the servers that have not been added to the black list (make sure that your server is not added to the black list).
3. Make sure that both servers and client applications connected to them, are accessible to each other by domain names.

Case 2

If the server `videosever.example.com` is added to the blacklist, you will block all calls between users of your server and all users whose ID takes this form `id@videosever.example.com`.

Connection to a conference in federation mode

Connection to a conference (including the cases when federation is used) is fully described in the ["Conference page"](#) section.

11.3. TURN/STUN servers settings

If needed, specify the addresses of the STUN/TURN servers in section **Network →TURN/STUN** for fine-tuning NAT traversal.

You can find more information about how WebRTC works in the [article on the website](#).

When adding STUN/TURN, one should consider how this mechanism works:

1. TrueConf Server acts both as an authorization server and a WebRTC client (a conference participant) at the same time.
2. For a STUN or TURN server, different parameters can be set for **Assigned for**: for TrueConf Server, for the browser (WebRTC client), and for client applications TrueConf.
3. Depending on the role of STUN/TURN, its use will yield different results:
 - If STUN/TURN is assigned for TrueConf Server, it will allow TrueConf Server to obtain an external IP address;
 - If STUN/TURN is assigned for a WebRTC client, participants using browsers will be able to get an external IP address.
 - If STUN/TURN is assigned for the native TrueConf application, then participants using desktop applications, mobile applications, TrueConf Room software terminal, and TrueConf Kiosk application will be able to obtain an external IP address.
4. STUN/TURN can be assigned simultaneously for TrueConf Server and for the WebRTC client (both options are selected in the **Assigned for** dropdown list).
5. Only one configuration can be added with assignment to TrueConf Server.
6. There is no limit on the number of STUN/TURN servers assigned to a browser and TrueConf client applications.

If the STUN/TURN server role is assigned to users (a browser or a native application), these users will connect to the server in the following way:

1. Initially, an attempt is made to connect using local addresses TrueConf Server.
2. If the attempt is unsuccessful, the browser client or native app tries to use external addresses obtained with the help of STUN servers.
3. If Step 2 also fails, the browser client attempts to establish a connection using TURN servers to proxy secure DTLS traffic.

12. Configuring email notifications (SMTP)

12.1. Integration with a mail server via the SMTP protocol

TrueConf Server TrueConf Server does not include a built-in mail system and can only use an external SMTP server or service to deliver email notifications to users. In the **Network → SMTP** section, you can select the SMTP server that should be used. It is also possible to edit the templates of emails that will be sent to users.

The email address that has already been used or may be used in a [user profile](#) should not be specified in the settings of the mail server for sending notifications from TrueConf Server. A separate mailbox should be created for the server.

To configure an SMTP connection:

SMTP

[Help](#) ?

Outgoing Mail Server

Host	Port	Connection security
mail.example.com	465	SSL
Authentication Type	Login	Password
simple password	smith	
Sender email	Sender name	
smih@mail.example.com	Admin	

Status: **successfully connected**

[Check connection](#)

Admin e-mail

E-mail
smih@mail.example.com

☐ Notify administrator about the server restart due to internal issues.

1. Specify the host (the address of the mail server).
2. Select a secure connection type: SSL, STARTTLS, or none.
3. Specify the port for your connection type if it is not default.
4. Select the authentication type (**no authorization** or **simple password**), and in the second case, specify the username and password to connect TrueConf Server to the SMTP server.
5. Fill in the email address fields (full mailbox address, including login, @ and domain) and sender's name in the SMTP **From** field. In this case, the address should match the login and host specified above.
6. Verify the settings using the **Check connection** button. The **Status:** field shows the current connection status with the mail server: **successfully connected** if the connection to the SMTP server is successful and **invalid server** if there is a connection error.

7. Enter your TrueConf Server administrator email to be displayed in the outgoing emails. Enable the checkbox below the input field so that the administrator is notified when TrueConf Server restarts due to internal errors.
8. Click **Apply** at the bottom of the page to save the changes.

12.2. Configuring email templates

Below the [parameters for connecting to an SMTP server](#), you can set the templates for different email notifications.

To restore the default templates for all emails, click the **Set default** button in the **User mails** section. This will apply the templates in the language [selected in the preferences](#) by the administrator.

12.2.1. Missed Call Notifications

To receive missed call notifications, check **Notify users about missed calls**. If users are offline during a call or conference call, TrueConf Server will attempt to send a notification to the address specified in the **E-mail** field in the [user profile settings](#) or in the corresponding field [imported via LDAP](#).

Notifications about missed calls will be sent to unregistered users, if a user from your video conferencing server did not know their TrueConf ID and tried to call them by email. Such calls have to be made with the `#mailto:` prefix, for example, `#mailto:user123@example.com`. This prefix has to be included, because the format of TrueConf ID is identical to that one of an email address; so, a special prefix in the call string is needed to distinguish between them.

When participants are added to a public conference (webinar) by email, the `#mailto:` prefix will be included automatically; no additional actions will be needed.

12.2.2. Conference invitations

To enable invitation sending for all newly created conferences, check the **Send invitations to participants of the group conference** box. In this case, when scheduling a conference, all invited participants will receive notifications with the date and time of the event (if specified).

You can enable or disable sending invitations for each conference individually on the [Advanced tab](#) when creating or editing it.

12.2.3. Registration confirmations for a public conference

To send confirmations of successful webinar registration (if the [appropriate settings](#) are configured), use a separate template **Conference registration notification**.

12.2.4. Reminders for upcoming conference

You can set up email reminders for upcoming events. All participants added to a scheduled conference will receive an email reminder before it begins. The reminder template can be customized in section **Reminder about upcoming conference** below.

Select the time period before the event starts for which you want to receive a reminder from the **Reminders** list:

- If the **Send users reminders about upcoming conference** checkbox is not selected, you will not be able to enable reminders for conferences
- If the checkbox is selected but nothing is selected in the list, then when [creating any scheduled conference](#), the administrator or owner can enable reminders on the **Advanced** tab by manually specifying the desired time period
- If, for example, you select “1 day” and “5 minutes,” the event will already be set up to send reminders at those intervals when you schedule it. However, you'll still be able to add your own reminder intervals.

If the administrator checks **Send users reminders about upcoming conference** and selects periods from the list **Reminders**, then notifications with these periods will be automatically added to previously scheduled conferences without reminders.

12.2.5. Conference Rescheduling Notifications

To notify participants of a scheduled event about a change in its start time, check the box **Notification of start time change for scheduled conference**.

An email notification will also be sent if the repetition type of a scheduled conference is changed, for example, a one-time conference becomes a recurring conference or the other way around.

If a new start time is set for a one-time scheduled conference which has already ended so that this event can be started once again, this email will not be sent. Instead, users will receive an [invitation to the new event](#).

12.2.6. Conference cancellation notifications

To notify participants of a scheduled event that it has been canceled, check the box **Notification of conference cancellation**. This notification will be sent if:

- A scheduled conference was deleted before its start time.
- The launch type of a conference was changed to a virtual room.

12.2.7. Notifications about removal from a conference

To enable notification for participants about their removal from the invitation list, select the checkbox **Notify users if they are removed from the participant list**. This setting applies to all conference modes. For webinars with registration enabled, notifications will be sent to both self-registered participants and those invited during the event creation.

12.3. List of parameters used in email templates

Use the following syntactic structures to customize the templates of emails sent by TrueConf Server:

- For notifying users about missed calls:
 - `%caller_display_name` — display name of the caller

- `%caller_call_id` — ID of the user who made the call (e.g. `user@server.trueconf.name`)
- `%recipient_display_name` — display name of the caller (the user who missed the call)
- `%missed_call_time` — time and date of the call.
- additional variables for missed call notifications sent to unregistered users:
 - `%recipient_call_id` is the ID of a user who missed the call.
 - `%tcs_guest_page_url` — link to [the guest page of your TrueConf Server](#).
- For inviting to a conference:
 - `%conf_name` — name of the conference
 - `%conf_id` — ID of the conference, e.g. `\c\df0a2adebe`
 - `%owner_name` — display name of the [conference owner](#);
 - `%owner_email` — contact email of the conference owner
 - `%owner_mobile_phone` — mobile phone number of the conference owner
 - `%owner_work_phone` — the work phone number of the conference owner
 - `%owner_home_phone` — the home phone number of the conference owner
 - `%owner_sip_number` — the conference owner's SIP number
 - `%user_display_name` — display name of the user who is invited to the conference
 - `%start_time` is the time and date of the conference start. The time corresponds to the server time zone which will be specified in the email. Participants should take into account time zone differences to join the conference at the correct time.
 - `%conf_description` — a description of the conference that is [set](#) in section **Advanced →Description** during its creation;
 - `%conf_url` — link to the [conference page](#), for example:
`https://example.com/c/CID`
 - `%conf_url_app_join` — a link for quick one-click connection via a client application without having to open the conference page. It works as follows: if the link is clicked, when the conference has already started and [connection via client applications is allowed](#), the application installed on the user's device will be launched, and an attempt will be made to connect to the conference. Essentially, it is similar to visiting the conference web page and clicking the button for joining the meeting from a client application. The link looks in the following way:
`https://[server_address]/c/CID#app=1`

The anchor `#app=1` triggers the JS script that initiates the connection from the installed application.

A link like `https://[server_address]/c/CID#app=1` can be used not only in emails from TrueConf Server but also in other emails or messages to simplify user connection to a conference.

- For notifications about webinar registration:
 - `%conf_unique_link` — the unique conference link provided to each participant.

Server administrator contacts parameters:

- `%admin_name` — display name
- `%admin_email` — email address
- `%admin_phone` — phone number.

13. SIP/H.323/RTSP gateway and transcoding

TrueConf Server It includes a built-in gateway for SIP 2.0, H.323, and RTSP protocols, which can be configured in the **Gateways** section of the control panel.

With the gateway you can:

- [configure the integration of TrueConf Server and Asterisk](#);
- [configure the integration of TrueConf Server and Cisco UCM via SIP](#);
- [register TrueConf Server on an external H.323 gatekeeper](#) by adding the necessary configuration;
- Send [DTMF commands](#) to perform certain actions during a conference.

Built-in gateway is necessary only if you need to call the devices connected to a third-party server (e.g. H.323 gatekeeper, PBX, MCU). Otherwise you can use the call string for SIP 2.0/H.323 devices.

If your PBX and TrueConf Server are integrated with an LDAP directory (such as Microsoft Active Directory), additional fields can be used for convenient user dialing. For instance, you can retrieve aliases from LDAP and use them for calling. For more details, read the [LDAP fields description](#).

13.1. SIP Gateway

This section helps to configure TrueConf Server built-in SIP 2.0 gateway parameters. The number of rules created using these settings is unlimited.

TrueConf Server Free version provides only one **active** connection through the gateway, including SIP 2.0, H.323 and RTSP protocols.

To call devices through the SIP gateway in TrueConf Server, a [special call string format](#) is provided.

SIP Gateway

[Help ?](#)

Network settings

☐ Listen on all IP addresses

[10.120.1.141:5060 \(tcp\)](#)

[10.120.1.141:5060 \(udp\)](#)

Add

Rules for SIP connections

Name	Role	Host	Status
SIP connections list is empty.			
Add a configuration			

13.1.1. Block "Network Settings"

This list contains the addresses where the gateway will await incoming SIP 2.0 connections. By default, it is pre-filled with IP addresses provided by the operating system. To edit the list, uncheck the box **Listen on all IP addresses**.

13.1.2. Section "Rules for SIP Connections"

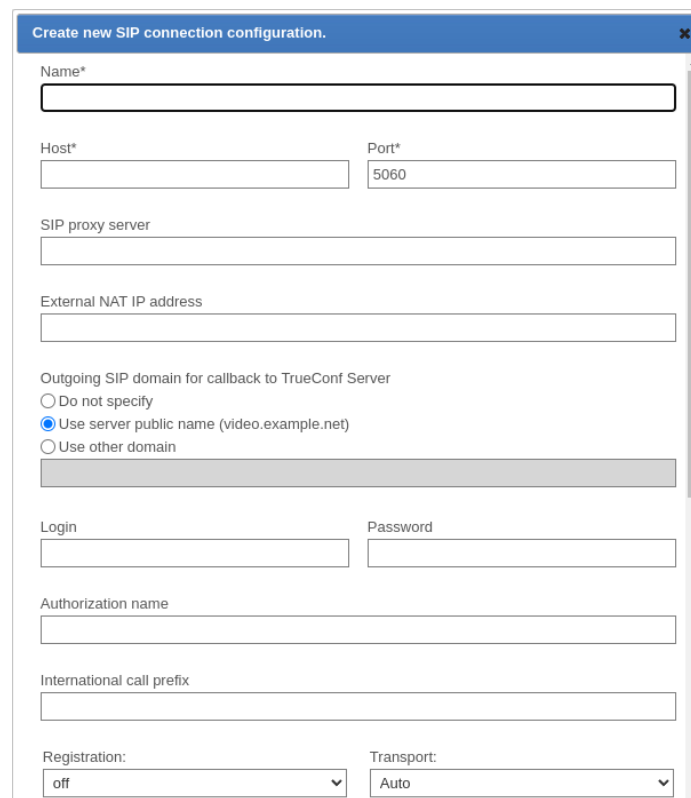
In this section you can create specific rules for certain SIP addresses or call directions. For example, you can use special set of settings to connect to Skype for business servers and another one for PBX connectivity. Every rule is relevant only for target address specified in **Host** field. Every rule redefines global settings for SIP 2.0 connections.

Gateway can also authenticate on and maintain active connection with SIP devices for which the rules have been created. This option can be useful to maintain permanent connection with PBX or VoIP services. You can find the connection status in the rules for SIP Connections table.

To create a new rule, click the **Add a configuration** button. You will be prompted to choose from two templates: [manual setup](#) and [server connection setup Skype for business](#). The Skype for business template sets certain properties needed for its correct operation, such as the port in use, protocol, video codec, and registration mode.

13.1.3. Form for creating a new rule

The first group of settings affects the forwarding of SIP connections and authorization (if needed):



Create new SIP connection configuration. [X]

Name* [text box]

Host* [text box] Port* [5060]

SIP proxy server [text box]

External NAT IP address [text box]

Outgoing SIP domain for callback to TrueConf Server

☐ Do not specify

☒ Use server public name (video.example.net)

☐ Use other domain [text box]

Login [text box] Password [text box]

Authorization name [text box]

International call prefix [text box]

Registration: [off] Transport: [Auto]

Name field is only displayed in the table for rules. **Host** and **Port** fields are more important and also mandatory. They are required to determine call direction applied to this rule. If you are using an SIP proxy server, enter its IP address or domain name in the corresponding field. If the port for connecting to the proxy is different from the **5060** default port, enter the required port after the address and separate it with a colon. Please note that it isn't possible to set different rules for one host but different ports.

In the **External NAT IP address** field, you can specify the server's IP address to be listed in the SDP for receiving and sending media streams when calling users behind NAT.

The field **Outgoing SIP domain for callback to TrueConf Server** is used to create a SIP URI in the format `user@server` for outgoing calls to SIP devices, where `server` is the entered IP address or FQDN, and `user` is replaced with the ID of the user initiating the call. It is typically displayed as the caller's address on SIP devices. Possible values:

- **Do not specify**, then only TrueConf ID will be in the address;
- **Use server public name**, then the external server address specified in [section Web → Settings](#) is substituted;
- **Use other domain**, specifying the desired domain name in the input field.

The next set of fields is intended for configuring authentication on a SIP device for which a rule is being created. If **Authorization name** is the same as the login, it can be left blank. Specifying **International call prefix** allows you to replace the `+` symbol, which users input when calling phone subscribers, with another value, such as `810`. If this field is left empty, the `+` in phone numbers will not be replaced.

The **Registration** mode determines how registration will be conducted in this direction:

- **off** — the REGISTER request is not sent, and registration or authorization on the external SIP device does not occur;
- **permanent** — registration occurs automatically each time TrueConf Server is launched;
- **before call** — Registration occurs immediately before each call and remains active only during the call.

You can manually specify the connection protocol (TCP, UDP or TLS) if necessary.

Please note that each active gateway connection reserves one SIP 2.0/H.323 connection from TrueConf Server license.

Next, you can find the settings for the transfer of data and other advanced parameters:

Reduce SIP messages size

- ☐ Remove optional SDP attributes for static RTP payload types
- ☐ Use compact form of SIP headers

Advanced setting

- ☐ Enable ICE support
- ☐ Enable SRTP support
- ☐ Enable forward error correction (FEC)
- ☒ Enable content sharing via BFCP
- ☒ Enable far end camera control via Q.922/H.224/H.281
- ☐ Enable timers support (RFC4028)

Max session refresh interval (seconds)

1800

Available codecs

- | | | |
|--|--|--|
| ☐ H.265 | ☒ G.722.1C 32 kbit/s | ☒ G.711 ulaw |
| ☒ H.264 High Profile | ☒ G.722.1C 48 kbit/s | ☒ G.711 alaw |
| ☒ H.264 Main Profile | ☒ G.722.1C 24 kbit/s | ☒ OPUS |
| ☒ H.264 Baseline Profile | ☒ G.722.1 32 kbit/s | ☒ Speex |
| ☒ X-H264UC | ☒ G.722.1 24 kbit/s | |
| ☒ H.263++ | ☒ G.722 | |
| ☒ H.263+ | ☒ G.723 | |
| ☒ H.263 | ☒ G.728 | |
| ☒ H.261 | ☒ G.729A | |
| ☒ VP8 | | |

Role

- ☐ Default SIP trunk
- ☐ Default VoIP server

Use block **Reduce SIP messages size** to compress SIP message packets and headers, preventing issues related to exceeding their maximum allowable size (MTU).

The checkbox **Enable ICE support** (Interactive Connectivity Establishment) determines whether the gateway will be available if TrueConf Server is located behind NAT.

When the checkbox **Enable SRTP support** is enabled, it ensures the encryption of media data transmitted in this direction. Some SIP devices require this (for example, Skype for business servers).

The checkbox **Enable forward error correction (FEC)** enables control over error correction when the connection deteriorates on a configurable SIP route. It is enabled by default, but some devices or server MCUs may not function correctly with this setting, in which case it should be disabled. If you are configuring rules for connecting to TrueConf Group or TrueConf MCU, we recommend keeping the checkbox **Enable forward error correction (FEC)** enabled.

The checkbox **Enable content sharing via BFCP** determines whether the server can [exchange content sharing with SIP devices in this direction](#) by transmitting content as an additional video stream. For example, this could be used to share the desktop screen from a computer connected to a SIP terminal or to send slides from applications TrueConf to a SIP terminal.

When content is shared from SIP/H.323 devices in the secondary stream, it is sent with a reduced frame rate to reduce traffic (similar to the transmission of the secondary stream from TrueConf client applications).

The checkbox **Enable far end camera control via Q.922/H.224/H.281** determines whether remote control of SIP device cameras will be available from the TrueConf client application.

Please note that this parameter has the same name in the SIP and H.323 gateway configuration menus, however, these are two different checkboxes responsible for different permissions.

The checkbox **Enable timers support (RFC4028)** is used to disconnect the SIP terminal from the conference if the connection is lost. It is disabled by default.

You can manually set **Max session refresh interval (seconds)** (default is 1800 seconds).

The list of **Available codecs** contains codecs that the gateway can use in this direction. Disabling some codecs may resolve compatibility issues with certain SIP devices. You can learn more about this from our [technical support service](#).

SIP device for which the rule is created can take **special roles**:

- **Default SIP trunk** . This role allows users to avoid entering full SIP URI for calls with `#sip:` prefix. For example, all calls in the `#sip:Endpoint` format will be automatically replaced with `#sip:Endpoint@Host` , where `Host` is taken from the properties of this rule and `Endpoint` is a username specified during the call.
- **Default VoIP server** . This role is required for treating an SIP device as a VoIP server or a PBX and activating the dialers built in TrueConf client applications. All the calls made from application dialers or with the help of `#tel:` prefix will be automatically forwarded to this SIP endpoint. For example, `#tel:Phone` will be automatically replaced with `#sip:Phone@Host` , where `Host` parameter is automatically taken from the properties of this rule and `Phone` is replaced with the phone number entered by user.

Please note that each of these roles can be assigned only for one SIP 2.0/H.323 connection rule.

13.1.4. Setting up integration with Skype for Business

This integration is designed to work with Skype for business 2015 Server or Lync 2013 Server on-premises deployments and cannot be used for their cloud versions.

To connect successfully, you will need to receive a trusted root certificate from the Skype for business administrator and install it in the system where TrueConf Server is installed.

1. Create a new account for TrueConf Server on the Skype for business server.
2. Use Skype for business template to create a new rule for SIP connections. Enter username and password of this freshly created account in the appropriate fields.
3. In the **Host** field, enter the IP address or domain name of the Skype for business server.
4. Check the box **Default SIP proxy**.
5. Save the rule and check if the connection status has changed to successful in the table for rules. Please note that TrueConf Server service must be running.

To call Skype for business subscribers from TrueConf client applications, use the format `#sip:<user>` , where `<user>` is the login of the Skype for business user. An incoming call to this user will be displayed as coming from the account created for TrueConf Server. Similarly, Skype for business subscribers can be invited to conferences or added to the address book.

To call TrueConf users from Skype for business client application, send the following message to the user created for TrueConf Server authentication: `/call <USER_ID>`, where `<USER_ID>` is any valid TrueConf Server user ID including SIP / H.323 devices registered on TrueConf Server. You can use `/conf` command to create a multipoint conference, etc. After the message has been sent, TrueConf Server will call Skype for business user and connect him/her to a TrueConf user or a conference. If you try to call this user directly, the call will be rejected and you will receive a help message with a list of available commands in chat. However, if default call destination is set in global SIP settings, you will be connected to this default destination address.

Please note that you can also create a group conference on TrueConf Server and invite into the conference the endpoints connected via any protocols the gateway supports. For example Skype for business users and various SIP/H.323 devices or RTSP IP cameras.

13.1.5. Global SIP settings

Settings in this section automatically apply for all SIP 2.0 connections for which there are no rules.

Global SIP settings

Action on incoming call to the TrueConf Server IP address

☒ Reject call

☐ Forward to menu for entering a conference ID

☐ Forward to a user or conference by the specified ID

SIP proxy server

An outbound proxy that will receive SIP requests from TrueConf Server.

External NAT IP address

This address will be used in SDP to send and receive audio and video when calling external users.

Action on incoming call to TrueConf Server IP address — this parameter allows you to select the behavior for a SIP call to any of the addresses from [block Network settings](#) using the SIP 2.0 protocol:

- automatically reject such a call;
- transfer the call to the conference ID input menu using DTMF;
- Transfer the call to [TrueConf ID user](#) or [conference ID](#). You should then enter this ID in the field below.

The remaining settings are identical to those used when [creating rules for connections](#).

13.1.6. Invitation of the SIP endpoint to the conference on your server

There are several ways to invite a SIP terminal to a conference: the conference owner can call the terminal during the conference using the client application TrueConf, employing a [special call string format](#), or an administrator can add the terminal to the conference from the server control panel.

To add an SIP endpoint to the conference via control panel you need to:

- select a conference on the [conference list page](#);
- Add the SIP terminal as a conference participant if it hasn't started yet, or invite it to an ongoing conference. To do this, use the call string format.

13.1.7. How to join a conference with its CID (conference ID) from an SIP endpoint

To connect to a conference from the endpoint **registered** on TrueConf Server, enter **CID (Conference ID)** into the endpoint address field. Please note that you need to replace `\c\` in CID with `00` (two zeroes) when calling from external endpoints. In our case, you need to enter `00e22a39ba2a@<server>` if CID is equal to `\c\e22a39ba2a`.

To connect to the conference from the endpoint **unregistered** on TrueConf Server, use the following format:

```
CID@<server>:<port>
```

where:

- **CID** is a conference ID with two leading zeroes instead `\c`
- **<server>** — the IP address of the TrueConf Server gateway (for example, `00e22a39ba2a@192.168.1.99`);
- **<port>** — connection port (in case it is different from the standard 5060 port).

Additionally, in the case of SIP it is possible to specify the protocol name explicitly (UDP is used by default):

```
CID@<server>:<port>;transport=<protocol>
```

For example, `00e22a39ba2a@192.168.1.99:5061;transport=TCP`.

You can also find an instruction on how to connect to a conference held on TrueConf Server from an SIP endpoint on the conference web page.

13.2. H.323 Gateway

This section explains how to configure built-in gateway parameters for H.323 connections. The number of rules for H.323 connections created using this section of control panel is unlimited.

TrueConf Server Free version provides only one **active** connection through the gateway, including SIP, H.323 and RTSP protocols.

Connections using the H.323 protocol are primarily used for calls to third-party hardware video conferencing terminals. TrueConf Server also allows configuring integration with MCU, H.323 gatekeeper, and PBX. This can be useful for addressing devices and subscribers registered on them using H323-ID or E.164 format numbers without specifying the terminal's IP address in the call string. For calling devices via an H.323 gateway in TrueConf Server, a [special call string format](#) is provided.

H.323 Gateway

[Help ?](#)

Network settings

☐ Listen on all IP addresses

[192.168.234.1:1719 \(tcp\)](#)

[192.168.234.1:1719 \(udp\)](#)

[192.168.88.181:1719 \(tcp\)](#)

[192.168.88.181:1719 \(udp\)](#)

Add Reset Apply

Rules for H.323 connections

Name	Role	Host	Status
H.323 connections list is empty.			
<button>Add a configuration</button>			

13.2.1. Block "Network Settings"

This section contains a list of addresses where the gateway will wait for incoming H.323 connections. By default, it is pre-filled with the IP addresses of the operating system. You can edit the list by unchecking **Listen on all IP addresses**. The list of ports used for H.323 connections can be [found in our blog article](#).

13.2.2. Section "Rules for H.323 Connections"

Here you can create specific rules for certain H.323 devices or call directions. Each rule is relevant only for specific destination address indicated in the **Host** field and redefines [global settings for H.323 connections](#).

The gateway can also register on H.323 devices and maintain an active connection, which might be useful when connecting to an MCU or H.323 gatekeeper. The status for such connection is displayed in the rules table. To create a new rule, click **Add a configuration** button.

13.2.3. Form for creating a new rule

The field **Name** is used only for display in the rule list. **Host** and **Port** are also required and are used to determine the direction of calls to which this rule will apply. Note that it is not possible to create two rules with the same host but different ports.

Create new H.323 connection configuration. ✕

Name*

Host*

Port*

1719

External NAT IP address

H323-ID

Password

DialedDigit

Registration:

off

Advanced setting

☐ Enable H.235 encryption
 ☒ Enable content sharing via H.239
 ☒ Enable far end camera control via Q.922/H.224/H.281

Available codecs

☒ H.264 High Profile
 ☒ H.264 Main Profile
 ☒ H.264 Baseline Profile
 ☒ H.263++
 ☒ H.263+
 ☒ H.263
 ☒ H.261
 ☒ G.722.1C 32 kbit/s
 ☒ G.722.1C 48 kbit/s
 ☒ G.722.1C 24 kbit/s
 ☒ G.722.1 32 kbit/s
 ☒ G.722.1 24 kbit/s
 ☒ G.722
 ☒ G.723
 ☒ G.728
 ☒ G.729A
 ☒ G.711 ulaw
 ☒ G.711 alaw

Role

☐ Default H.323 gatekeeper
 ☐ Default VoIP server

Create

Cancel

In the **External NAT IP address** field, you can specify the server's IP address to be listed in the SDP for receiving and sending media streams when calling users behind NAT.

The fields **H323-ID** and **Password** are meant for authentication on the H.323 device for which the rule is created. To maintain a constant connection with the device, you need to select the appropriate option from the drop-down list **Registration**.

After successful registration, the H.323 device TrueConf Server will also be available for dialing using the E.164 number format, provided it was specified in the **DialedDigit** field. This feature is beneficial when used in conjunction with the **Default call destination** field in the [global H.323 settings](#). In this case, all calls to this **DialedDigit** number originating from a connected H.323 device will be redirected to a specific user or conference on TrueConf Server.

Please note that each active gateway connection reserves one SIP/H.323 connection from TrueConf Server license.

The checkbox **Enable H.235 encryption** is designed to enable encryption of media data transmitted to H.323 devices according to ITU-T H.235 version 3, which is necessary for the proper functioning of certain terminals.

Enabling the checkbox **Enable content sharing over H.239** allows [the sending and receiving of content from an H.323 device](#) as an additional video stream. For example, it can be used to share the desktop screen from a computer connected to an H.323 terminal or to send slides from TrueConf applications in the reverse direction.

When content is shared from SIP/H.323 devices in the secondary stream, it is sent with a reduced frame rate to reduce traffic (similar to the transmission of the secondary stream from TrueConf client applications).

The checkbox **Enable far end camera control over Q.922/H.224/H.281** determines whether remote camera control via **Q.922, H.224, H.281** protocols will be available through client applications TrueConf.

Please note that this parameter has the same name in the SIP and H.323 gateway configuration menus, however, these are two different checkboxes responsible for different permissions.

The list of **Available codecs** displays the codecs which gateway is allowed to use in this direction. Disabling some of the codecs can solve compatibility issues with certain H.323 devices.

H.323 device for which the rule is created can take **special roles**:

- **Default H.323 gatekeeper** — allows not specifying the full address of the called device when making [H.323 device calls](#) through the `#h323:` prefix. For instance, all calls made by server users in any direction in the `#h323:Endpoint` format will automatically be replaced with `#h323:Endpoint@Host`, where the `Host` parameter is taken from the properties of this rule, and `Endpoint` is the username specified during the call.
- **Default VoIP server**. This role is required for treating an H.323 device as a VoIP server or a PBX and activating the dialers built in TrueConf client applications. All the calls made from application dialers or with the help of `#tel:` prefix will be automatically directed to this H.323 endpoint. For example, `#tel:Phone` will be automatically replaced with `#h323:Phone@Host`, where `Host` parameter is automatically taken from the properties of this rule and `Phone` is replaced with the phone number entered by user.

Please note that each of these roles can be assigned only for one H.323 rule.

13.2.4. Global H.323 Settings

Most of the settings in this section are identical to the settings described above. However, they automatically apply for all H.323 connections for which there are no rules.

The **Action on incoming call to TrueConf Server IP address** parameter allows you to select the behavior for a SIP call to any of the addresses from the [block Network settings](#) using the SIP 2.0 protocol:

- automatically reject such a call;
- transfer the call to the conference ID input menu using DTMF;
- Transfer the call to [TrueConf ID user](#) or [conference ID](#). You should then enter this ID in the field below.

13.2.5. Methods for calling subscribers and conferences on your server using H.323 devices

Depending on the H.323 endpoint model there are two different methods to call TrueConf Server users and conferences: using SIP URI or hashes (##) notation. Please try both to find the one suitable for your H.323 equipment. The call strings provided below should be entered as a string or number to call in the endpoint's interface. TrueConf Server IP address mentioned below could be an any address specified in H.323 network settings section:

- `Server##User` , where `Server` is the IP address of TrueConf Server, and `User` is the ID of the user or device registered on TrueConf Server;
- `Server##00CID` , where `Server` is the IP address of TrueConf Server, and `CID` is the conference ID on TrueConf Server;
- `User@Server` , where `User` is ID of the user or device registered on TrueConf Server and `Server` is TrueConf Server IP address
- `\c\CID@Server` , where `CID` is the conference ID on TrueConf Server, and `Server` is the IP address of TrueConf Server;
- `00CID@Server` , where the first two characters are zeros, `CID` is the conference ID on TrueConf Server, and `Server` is the IP address of TrueConf Server.

For more details, [H.323 call formats](#) examples are described in the user documentation.

13.2.6. Registering H.323 devices on the video conferencing server

TrueConf Server can act as a gatekeeper or MCU for third-party H.323 devices and simplify their addressing. From the TrueConf Server user perspective an H.323 device registered on the server does not differ from any other user: you can see its status, call it from the address book or invite to the conference without using call strings notation. Similarly, calls using H323-ID names from a registered H.323 device interface will be interpreted by the server as a call to specific TrueConf ID to entered H323-ID.

Registering an H.323 device on TrueConf Server is similar for most endpoints available on the market. Basically, to do so, you will need to specify TrueConf Server address as a gatekeeper or MCU address and use username and password of any TrueConf Server account to authenticate.

13.2.7. Sending DTMF Commands

Thanks to the ability to process DTMF signals, during a conference in the “moderated role-based conference” mode, you can send the following DTMF commands from your SIP/H.323 terminal:

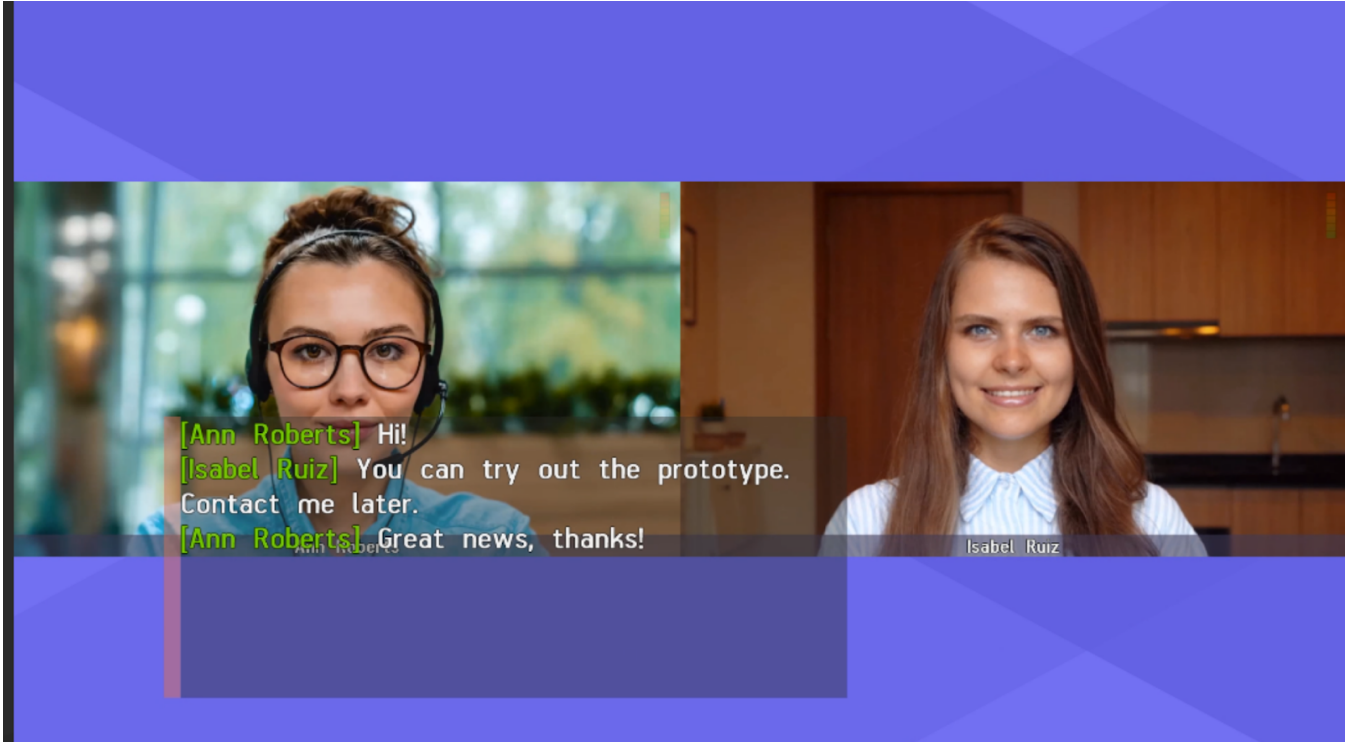
- **1** – request to take the podium.
- **2** – to leave the podium.

To do this, use the supplied remote control or keypad. For more details, read the manuals for your specific device.

In our knowledge base, we have covered the use of TrueConf Server with [Polycom HDX series terminals](#), including sending DTMF commands from them.

13.3. Chat during calls on MCU

When meeting participants make calls from TrueConf client applications to conferences created on TrueConf MCU, they will be able to make use of chats that work via H.323 / SIP. This means that users who have signed in to TrueConf Server are not only able to make calls to TrueConf MCU, but can also send messages. The text of such messages will overlay the video layout, and all conference participants will see it regardless of their connection method:



13.4. RTP

In section **Gateways → RTP**, you can configure the UDP port range used for media exchange during SIP/H.323 calls (default is 50000-51999).

RTP

[Help ?](#)

UDP port range	
From	To
50000	51999
Apply	

13.5. WebRTC

In this section, one can configure parameters for connecting conference participants via WebRTC (from a browser):

WebRTC

[Help](#) ?

UDP/TCP port range

53000 - 56000

Protocols
UDP,TCP

Apply

Public IP address

Public IP address is added to SDP as an extra ICE candidate.

Protocols
UDP,TCP

Apply

TURN/STUN servers

The use of custom TURN and STUN servers will disable the default TrueConf servers.

Host	Port	Role	Protocols	Assigned for
stun.example.com	3478	STUN	UDP	TrueConf Server, WebRT...

Add Reset Apply

- Set up [UDP or TCP port range for WebRTC connection](#) (the ports 53000-56000 are used by default). You can also choose the protocol for working with WebRTC: TCP, UDP or both.
- In the **Public IP address is added to SDP as an extra ICE candidate** field, you can specify the IP address to be used for NAT traversal if automatic detection fails for any reason. You can choose the protocol for NAT traversal at this address: TCP, UDP, or both.

13.6. Transcoding

In the **Gateways → Transcoding** section, you can set the background and watermark for the video layout, as well as video quality for different types of connections and recording.

13.6.1. Adjusting Quality

In the section **Restrictions for modules**, one can configure conference video quality for WebRTC users (joining from a browser), H.323/SIP/RTSP devices, and recording. In other words, here you can set the quality of video streams **outgoing** from the server in these directions.

These settings do not apply to the transcoding of the second stream for SIP/H.323 participants, in other words, they do not affect content sharing via BFCP/H.239: protocols:

- If BFCP/H.239 content is transmitted from one endpoint to another, it will be delivered in its original quality, for example, 720p @ 60 fps.
- If participants connected through TrueConf client applications receive BFCP/H.239 content from an endpoint, the content will be delivered to them in its original resolution (up to 1080p) at 0.5 fps (1 frame every 2 seconds). This behavior is similar to when content is shown in the second stream from a client application.

The video quality settings from conference participants to TrueConf Server are selected in the [conference settings](#).

Transcoding [Help ?](#)

Restrictions for modules

FPS: 30 ▼

Recording 720p ▼

SIP/H.323 720p ▼

RTSP 1080p ▼

WebRTC 1080p ▼

Advanced

☒ **Do not display self-view in video layout for H.323 and SIP endpoints**
Enabling this option can significantly increase CPU load

☐ **Do not display self-view in video layout for WebRTC participants**
Enabling this option can significantly increase CPU load

☐ **Do not display content from the second stream to SIP/H.323/WebRTC participants**
CPU load can significantly increase if this option is enabled

☐ **Use GPU to reduce CPU load**

☐ **Automatically spotlight active speaker window**

Enabling the checkbox **Do not display self-view in video layout for H.323 and SIP endpoints** allows you to create a conference video layout for each SIP and H.323 terminal without the video window of that particular device. This means that an individual video layout is generated for the SIP/H.323 participant, excluding the image from the camera connected to it.

Enabling the checkbox **Do not display self-view in video layout for WebRTC participants** will create a conference video layout for each browser connection without including the participant's own video window. This means an individual layout is created for the WebRTC connection, excluding the browser's camera feed.

The checkbox **Do not display content from the second stream to SIP/H.323/WebRTC participants** allows you to exclude the mixing of the second stream (which transmits content or a slideshow) from the final video layout for all SIP/H.323/WebRTC connections to conferences. However, if the server-side video recording of the conference is enabled, a separate mixing process will be initiated, and the second stream will be included in the recording.

Please note that if a video layout is set at the conference level (either in advance or in the real-time meeting management tool during the session), the settings for excluding the self-view (which were discussed earlier) will no longer apply to the current conference. In other words, the settings of a specific conference have priority over general settings.

By creating individual video layouts for each SIP/H.323 and WebRTC endpoint or excluding the content stream, you can significantly increase CPU load on the physical machine where TrueConf Server is installed.

If the box **Use GPU to reduce CPU load** is checked, conference video will be processed by the GPU of the physical machine where the server is installed. NVIDIA graphics cards with CUDA support are suitable, preferably server versions (such as Quadro P2000). The graphics card will process the video of individual layouts which are generated for SIP/H.323/WebRTC protocols according to the settings discussed earlier:

- **Do not display self-view in video layout for H.323 and SIP endpoints;**
- **Do not display self-view in video layout for WebRTC participants;**
- **Do not display content from the second stream to SIP/H.323/WebRTC participants.**

GPU can be used for transcoding only in TrueConf Server for Windows. Not all models may be suitable, so please contact our [technical support](#) before estimating the possible encoding acceleration.

The parameter **Automatically spotlight active speaker window** activates automatic speaker window enlargement based on voice activity. Note that the settings for hiding your video in the layout and automatic speaker enlargement will only work if a layout is not explicitly set for SIP/H.323/WebRTC participants during [conference scheduling](#) or in [real-time meeting management](#).

13.6.2. Adding Background and Watermark

In section **Gateways → Transcoding → Visual settings**, you can select the global background and watermark settings for the video layout of all conferences. Once you choose a watermark image, you can specify its position in the layout.

Visual settings

Background

Do not use

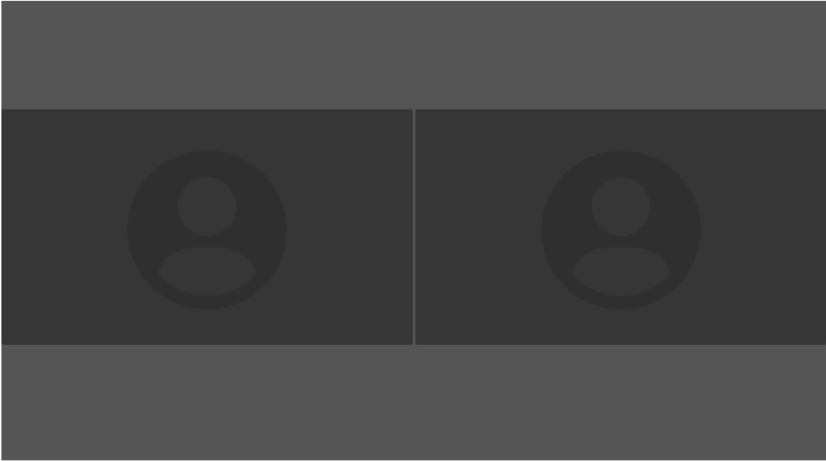
Watermark

Custom settings

Position

[+ Upload file](#)

PNG image, 400x100 resolution (maximum), no more than 1 MB



Apply

Adding a watermark is not available in version TrueConf Server Free; a paid license is required.

14. Web and HTTPS Settings

Here are the minimum steps needed to set up a working corporate communication system:

1. [Select a machine \(PC, physical or virtual server\) with suitable hardware.](#)
2. [Install TrueConf Server.](#)
3. [Log in to the control panel.](#)
4. [Register the server.](#)
5. [Configure HTTPS](#) (it is used for many key features, such as integration with the AI server, conference scheduling, etc.) and [specify the external server address](#) (guest page). **You are here!**
6. [Configure access to the server for users within the corporate network](#) and, if necessary, from an external network (outside the corporate network).
7. [Create user accounts](#) or [integrate the server with a directory service](#) via the LDAP/LDAPS protocol.
8. Install client applications for users and show them how to connect to your server (check the [documentation for the desktop application](#)).

Section **Web** contains the settings for the guest page and access parameters for the control panel. It is recommended to configure HTTPS first, followed by the other parameters.

14.1. HTTPS

In section **Web →HTTPS** of the control panel, you can configure the data transmission security settings between the browser and TrueConf Server.

A secure connection with your TrueConf Server instance is necessary for capturing media devices [using WebRTC technology in all modern browsers](#). Thus, users won't be able to join your meeting from their browsers if you haven't enabled HTTPS connection.

Additionally, HTTPS is required for users connected to your server from TrueConf client applications to use the [conference scheduler](#), [presentation sharing](#), [real-time meeting management](#), and to work with polls and transcripts.

TrueConf strongly recommends that you should configure HTTPS even if you are not intending to use TrueConf Server for holding public conferences and connecting participants via a browser (via WebRTC). Using HTTPS is one of the best practices for web services and helps to enhance the security of video communication.

After configuring HTTPS, update the external server address in the [Web →Settings](#) section. Make sure that it starts with `https`, for example, `https://video.company.com`. Alternatively, if an external service is used to proxy the traffic, specify its address in this section.

14.1.1. Block "HTTPS Configuration"

In this section you can select your certificate and set other HTTPS parameters. The web server applies HTTPS settings at startup. If invalid certificate port and parameters are entered, the web

server will not start and administrator will lose access to the control panel. Therefore it is required to carefully check the parameters beforehand.

HTTPS Settings

[Help ?](#)

HTTPS configuration

HTTPS mode: Use self-signed certificate ▼ [Why HTTPS is important and how to properly configure it](#)

HTTPS port: 443

Usable TLS protocol versions: ☒ TLSv1.2 ☒ TLSv1.3

Test configuration Apply

1. In the **HTTPS mode** dropdown list, select one of the three operating modes:
 - **Disable HTTPS** — the HTTPS protocol will not be used;
 - **Use self-signed certificate** — using a certificate automatically generated by the server (this certificate is not suitable for connecting external users via WebRTC);
 - **Use custom certificate** — using the certificate uploaded by the administrator TrueConf Server.
2. In the **HTTPS port:** field, specify the TCP port that will be used by the web server for HTTPS protocol (use numbers). Port 443 is set by default.
3. Specify which versions of the [TLS protocol](#) your TrueConf Server will use for HTTPS operation.
 1. Click **Test configuration** to check the HTTPS configuration settings without restarting the web server. This action does not modify the web server's configuration file.
5. Click **Apply** to save the web server configuration file with the specified parameters. You will see a dialog box notifying you that this action will automatically lead to your server instance restart.

14.1.2. Self-signed and complete certificates

There are two certificate types available in TrueConf Server. If you are using a trusted certificate, no additional actions are required, as browsers trust certificate authorities who signed it. To configure an uploaded certificate, the server administrator requires an X.509 certificate and the correct private key.

As an alternative you can also use a self-signed certificate:

- a self-signed certificate is valid for 365 days and can be generated from control panel
- this certificate can be renewed for unlimited period of time
- with a self-signed certificate, you can test WebRTC without purchasing a trusted certificate

In our knowledge base, you can find information on how to create a free Let's Encrypt certificate [on Windows](#) or [on Linux](#), depending on which OS your TrueConf Server is deployed.

14.1.3. Block "Self-signed Certificate"

If you have previously created a self-signed certificate, this section will display the main parameters of the root certificate and the certificate that will be used by the web server and TrueConf Server, in addition to the generation button:

Self-signed certificate

Root Certificate Authority (Download ca.crt ↓)		
Subject	Valid after	Valid until
commonName=TrueConf Server CA countryName=AU stateOrProvinceName=Some-State organizationName=Internet Widgits Pty Ltd	Tue, 27 Apr 2021 15:11:55 +03:00	Wed, 27 Apr 2022 15:11:55 +03:00

Certificate for server		
Subject	Valid after	Valid until
countryName=AU stateOrProvinceName=Some-State organizationName=Internet Widgits Pty Ltd subjectAltName=IP Address:192.168.56.1, IP Address:192.168.88.181	Tue, 27 Apr 2021 15:11:55 +03:00	Wed, 27 Apr 2022 15:11:55 +03:00

Create a new SSL certificate

The **Create a new SSL certificate** button allows you to generate a new self-signed server certificate. This feature is required to extend the certificate's validity by another 365 days or to update the company information in the certificate when it changes. Through the **Download ca.crt** link, the administrator can download the root certificate file for distribution among client devices.

14.1.4. Block "Uploaded Certificate"

If the certificate is uploaded, this section will contain the basic certificate's parameters. If it's not, you will find the buttons for uploading the certificate:

Custom certificate

Subject	Valid after	Valid until
commonName= countryName= stateOrProvinceName= organizationName=	Fri, 25 Dec 2020 17:04:24 +03:00	Sat, 25 Dec 2021 17:04:24 +03:00

Certificate:

Choose a file

 No file chosen

Private key:

Choose a file

 No file chosen

Upload

Use the **Choose a file** buttons to select the certificate and key files. Then click **Upload**.

The certificate format, key format and key correspondence to certificate are checked during download. Should just one check fail, the certificate and key files will not be saved.

In our knowledge base, you can find information on [how to convert an existing commercial certificate](#) into a format supported by the server.

14.2. Web Settings

14.2.1. Guest Page Settings

To change the guest page URL and its appearance, you can use the following options:

The screenshot shows the 'Web Settings' interface with the following elements highlighted by numbered callouts:

- 1:** The 'External address of TrueConf Server web' field, which contains the URL 'https://10.140.2.195' and an 'Apply' button.
- 2:** The 'Guest page' section header.
- 3:** The 'Link to the guest page' field, which contains the URL 'https://10.140.2.195'.
- 4:** The 'Contact details of the server administrator' section, which includes fields for 'Contact name' (Joe Smith), 'Email' (admin@example.com), and 'Phone' (+8080899999), along with an 'Apply' button.
- 5:** The 'Company logo' section header.
- 6:** The 'Choose a file' button, which is part of the logo upload interface.

1. The TrueConf Server address which is used to generate links to the guest page and conference pages. Make sure that it is accessible to all users of your TrueConf Server. If a non-standard port (other than HTTP 80 or HTTPS 443) is used, it has to be specified in the address field after a colon, for example, `https://video.server.com:4433`. When an external service is used to proxy traffic, the external address of TrueConf Server will be its address. Such a service could be, for example, NAT or [TrueConf Border Controller](#). The specified `address:port` will be used by client applications to receive the widget for real-time conference management, conference scheduler, content shared in the second stream and presentation (slideshow).
2. Link to the [guest page](#), which contains instructions for connecting new users to TrueConf Server. It matches the external server address.
3. Your company's name which will be displayed on the guest page.
4. Server administrator contact details which are published on the guest page and web conference pages.
5. Don't forget to save guest page settings because settings in each block are saved independently of each other.

6. Upload a logo to be displayed on the guest page and conference webpages.

If some users in your organization install MS Outlook web plugin from your TrueConf Server (check the “Mail plugins” section) and the external address of the server is changed, they will need to delete the plugin and reinstall it. This issue can be explained by the fact that the external address is specified in the xml file of the plugin downloaded from the server.

14.2.2. Additional documents

In section **Personal data processing**, you can add texts for the following rules:

- Cookie Policy
- Privacy Policy
- Terms of Use

The size of each document can be up to 100,000 characters.

Document links will be displayed at the bottom of your TrueConf Server guest page and conference webpages.

Personal data processing

To comply with local regulations, you can display additional legal documents describing data processing policies of your company on TrueConf Server public webpages. Please note you will need to add these documents on your own.

☒ Display cookie notification
You can edit the document text in the table below

These documents will be displayed on public web pages

Document title	Display link	Action
Cookies	☒	Edit
Privacy Policy	☒	Edit
Terms of Use	☒	Edit
Agreement	☒	Edit Delete document

[Add document](#)

To add or edit rules:

1. Choose a document you would like to edit and click **Edit** to change the title and content of your document. The Cookie Policy already contains default text; however, you can also change it.
2. Check the box in field **Display link**.
3. Check the box **Display cookie notification** if you need to display a pop-up alert with a link to the cookie usage policy for each new visitor on the guest page and public conference pages.

4. Click the **Add document** button if you need to display a link to an additional agreement (up to two additional agreements, allowing for a total of five documents). To ensure the document appears on the page, remember to check the **Display link** checkbox for it as well.
5. Click **Delete document** to remove special rules from the list. Please note that standard agreements cannot be deleted, but you can hide them from the guest page and public conference pages by unchecking the **Display link** box.

You can also add extra information or a manual for your guest page visitors, which will be displayed once you click on the **Help** button at the bottom of the page. Please note that **Help** is optional and it does not replace the default manual that opens by clicking on the **User guide** button.

Additional information

☒ Display the **Help** button on the guest page to show additional information from the administrator.

B ***I*** **U**      Normal   

It is additional information for VCS users.

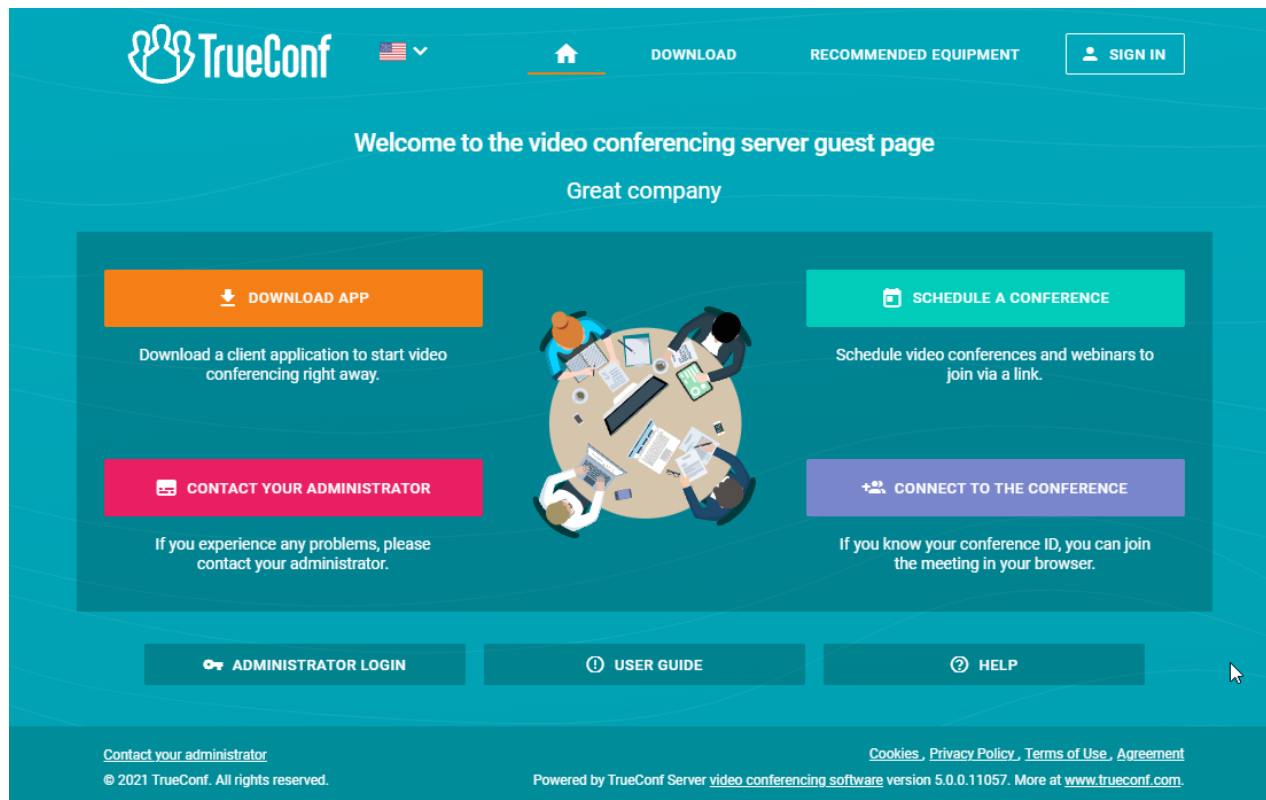
This text is available on the guest page.

Apply

To display additional information:

1. Check the box **Display the Help button**.
2. Enter your information in the field below.
3. Click **Apply**.

Below you can see an example of a guest page with three default documents, one additional document and a custom **Help** button:



14.3. Security

Use this section to configure access to the TrueConf Server control panel and API.

Details about [who has access to administrate the VCS server](#) on different operating systems and the reasons for it are explained in the server setup section.

Web Security [Help ?](#)

Dashboard

Give admin access to:

☒ members of **TrueConf Server Admin** local security group

☐ all Windows users on **localhost**

☒ Limit access to admin area by IP

10.0.0.0/8

192.168.0.0/16

172.16.0.0/12

Add

API

Please indicate the secret key for TrueConf Server API. Read more in [API documentation](#)

Secret key

0SGKjUnlqFnTlk44LM5TkCBDQznitfrt

Generate a new secret key

Apply

1. Select the users of your operating system who will be granted access to your TrueConf Server control panel.

If the machine with TrueConf Server is added to the domain and you grant access to all users on **localhost**, then all domain users will have access to the control panel. Use this option with caution!

2. Check this box to make sure that your server is available for control only to the IP addresses specified in the list. In such a case the **Administrator login** button will be displayed only if the [guest page](#) is opened from the IP address added to this list. If the guest page is opened from the IP address which is not included in the specified ranges, the button for administrator login will be hidden.

3. Click this button to add a subnetwork with access to the control panel. Enter the address in the **Network address** field (allowed characters are numbers and dots, admissible format is 4 octets in decimal representation without leading zeros from 0 to 255, separated by dots, e.g. 192.168.11.10). To open a drop-down list in **Subnet mask** field click the arrow on the right side and choose the appropriate option. The mask 32 – 255.255.255.255 is used by default.

4. The secret key to access your TrueConf Server API.

With a secret key, you can access APIs with no time limits or verifications until the key is changed. This is why we recommend that you use the secret key only for [testing purposes](#) or for TrueConf Server admin with privileges that cannot be specified when creating an OAuth application (e.g., viewing logs). For regular operation, please use [OAuth2 technology](#).

5. Click to generate a new secret key. It is impossible to revert to the previous key or set a custom key.
6. Click to apply the changes.

15. Users and groups. Integration with LDAP/Active Directory

Here are the minimum steps needed to set up a working corporate communication system:

1. [Select a machine \(PC, physical or virtual server\) with suitable hardware.](#)
2. [Install TrueConf Server.](#)
3. [Log in to the control panel.](#)
4. [Register the server.](#)
5. [Configure HTTPS](#) (it is used for many key features such as integration with the AI server, conference scheduling, etc.) and [specify the external server address](#) (the address of the guest page).
6. [Configure access to the server for users within the corporate network](#) and, if necessary, from an external network (outside the corporate network).
7. [Create user accounts](#) or [integrate the server with a directory service](#) via the LDAP/LDAPS protocol.
You are here!
8. Install client applications for users and show them how to connect to your server (check the [documentation for the desktop application](#)).

15.1. Accounts

In section **User Accounts**, you can add new user accounts, as well as edit and delete existing ones.

You cannot edit user details in [LDAP mode](#). User data entry form is available only in [Registry mode](#).

In the free version of TrueConf Server Free, there are limitations on the maximum number of accounts, which are detailed on the [page of this solution](#).

The screenshot shows the 'User Accounts' management page. It includes a top navigation bar with a 'Help' link. Below the title, there is an 'Add a user' button (1), a search bar (2), a 'Groups' toggle switch (3), and an export button (4). The main area contains a table of users (5) with columns for User, TrueConf ID, and Email. Each user row includes an avatar with a status indicator and a delete icon.

User	TrueConf ID	Email
Leila Olson	olson	olson@company.com
Mary Humphrey	humphrey	humphrey@company.com
Sara Baros	baros	baros@company.com
Terry Reed	reed	reed@company.com
Wayne Moore	moore	moore@company.com
William Hubbard	hubbard	hubbard@company.com

1. Click the **Add user** button to start creating a [new account](#).
2. The **Search** field allows filtering users by TrueConf ID, first name, last name, display name, and email.
3. The **Groups** toggle allows you to display the list of user groups available on the server. You can expand each group to view its members. The groups have to be [configured separately](#).
4. Use the button to export the user list to a CSV file for subsequent import into the TrueConf Group address book. The import itself is performed in the [section of the Maintenance terminal control panel](#). This button is available only in [Registry mode](#). The CSV file is saved in UTF-8 encoding, using ";" as the delimiter, thus ignoring [preference settings](#).
5. Below you will find the list of users registered on the server. The status of each user is displayed at the bottom of the avatar:
 - - online;
 - - offline;
 - — is in a conference or video call;
 - — is the [conference owner](#);
 - — The account has been deactivated by the administrator (see [field Status](#) in the profile).

To modify user information, click on their name. To delete a user, press the button.

15.2. Endpoint authentication under the user's account

It is possible to register an SIP/H.323 endpoint on the server under a user's account. This can give you several advantages when working with this endpoint:

- automatic export of the address book for codec TrueConf Group (detailed configuration is [described in the terminal documentation](#));
- Tracking the status of the endpoint as a regular user in the address book (online, busy, offline).

Please take into account that when each of the endpoints is authenticated, one online license is taken in addition to the gateway license (for more details, refer to the [licensing section](#)).

We do not recommend registering the endpoint on the same server using both SIP and H.323 protocols.

15.3. User Profile

If you create a user or click on any existing user in the list, you will be redirected to the page for entering or editing information about this person:

[Edit user](#)

Account information	
Status	☒ Active Disconnect
History of devices	View
TrueConf ID	chester @video.example.net
Password	•••••••• Confirm •••••••• ?
Email	chester@company.com
Display name	Abe Chester
First name	Abe
Last name	Chester
Middle name	
Organization	Real Meetings
Branch	Chats
Address	Meetings City
Department	IT
Job title	Developer
Manager	brown
Groups	selected item(s): 1 ▼
Mobile	+123123112
Work	
Home	
SIP number	

1. Using the checkbox **Active**, you can set the user to an "active" or "inactive" state ([see below](#)). These users will be displayed in the [general list](#) with a semi-transparent appearance and a grey status.
2. Use the **Disconnect** button to disconnect a user from TrueConf Server in all client applications. This feature may come in handy if you need to quickly connect a different user and the maximum number of connections is already reached (according to the license).

3. Click the **View** link next to the **History of devices** item to view information about the user's connections to the server ([more details below](#)).
4. **TrueConf ID** is the unique identifier used for authentication in client applications and making calls. The user's login (the part of TrueConf ID before `@`) can include only Latin and Cyrillic letters, digits, underscores, hyphens, and periods. The full TrueConf ID with the [server name](#) specified after the login (the extra part in the format `@server` next to the input field) is needed for making calls to a user from a different server. The login is set when a user account is created and cannot be changed later.
5. Enter the user's password. This password cannot be viewed when the account is created or edited, but it can be changed. Use the  button which is next to the password confirmation field to view the [password requirements](#).
6. Next, specify the email address for sending notifications to the user, distributed TrueConf Server [via the SMTP linked to the server](#).
7. **Display name** is another required field which will be displayed in the address book of other users. This field is pre-filled with the username entered during Step 3. However, its value can be changed.
8. Next, comes a group of fields for various data about a user and his/her position in an organization. These fields are optional.
9. In the **Groups** drop-down list, you can add a user to the [selected groups](#). Click on the arrow icon to view the list of groups available on the server. To add a user to one or more groups, just check the box to the left of a group name.
10. If necessary, you can specify the user's phone numbers. When you access the [user profile](#) in the client application TrueConf, you can call any of these numbers by simply clicking on it.
11. If SIP telephony is used, it is possible to specify a SIP call number in the corresponding field. If you do it, this field will be displayed in the [user profile](#) in TrueConf client application. When a user clicks on this field, the call will be started in the format `#sip:<number>`. The number can be specified as `<number>`, `sip:<number>` or `#sip:<number>`.

If the user enters the wrong password consecutively as many times as specified in section **Users → Settings**, web application login will be blocked for 24 hours. You can manually enable login access by clicking the **Unlock** button on the user's profile page.

Edit user

[Help](#) 

Account information

Authentication is locked for this user (IP address: 10.140.2.166) until 2022-05-26 00:22:44 due to a number (5) of failed login attempts

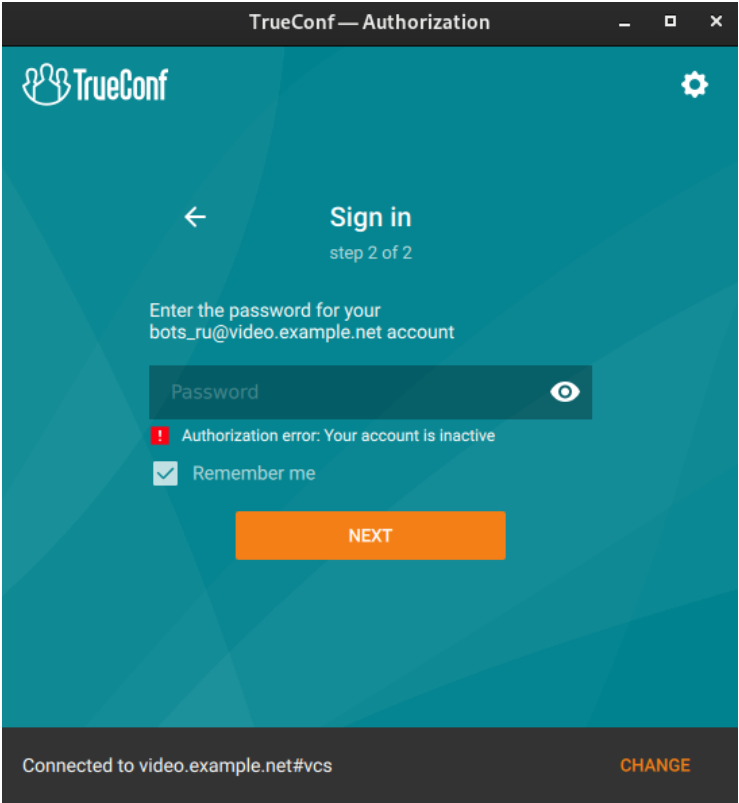






15.3.1. User Deactivation

The **Active** checkbox in a user's account can determine if this user should be able to authorize. If the user account is inactive, it will not be deleted, but one will not be able to use it for authorization. The following message will be displayed in all client applications:



15.3.2. User device history

In the **History of devices** list, you can view a table of each user's active and completed authorizations on your server. Essentially, this list represents information from the [Reports → Endpoints log](#), filtered for a specific user:

History of devices: Jane Flowers (jane@video.example.com) Help ?

Application	Authentication status	Last authenticated ▾	IP address	Endpoint	Auto login	
TrueConf Linux 8.5.3.749	Authenticated	18.03.2026 00:05	10.100.2.241	C606B86D348754AF5A8AEA64878622	✓ Disable	
TrueConf Linux 8.5.3.749	Not authenticated	17.03.2026 22:43	10.100.2.241	2A7215524BAF290FC4616850775CFB3	✓ Disable	
TrueConf Windows 8.5.2.3	Not authenticated	12.02.2026 15:27	10.111.13.124	5B57E53469232E06A0E3FA88B3699AEI	✓ Disable	
TrueConf Windows 8.5.2.3	Not authenticated	11.02.2026 18:08	10.140.2.119	9071A97FD4CE4D6595C80445FAE9FFB	✓ Disable	

The list displays all active connections, with the application version shown in the first column **Application**. For browser connections, variant **TrueConf WebClient** will be displayed.

You can forcibly terminate a specific active connection which will effectively log out the user. For instance, you may log out the user on a lost smartphone for security purposes. To do it, click the button next to the selected device in the list. A confirmation pop-up will be displayed. Here, you can also disable auto-login; as a result, the user will be required to enter his/her password during the next authentication. Additionally, you can disable auto-login without logging the user out from the server by clicking the **Disable** link in the corresponding row.

15.3.3. Calls and Conferences

If you are editing a previously created user account, you will see a block **Calls and conferences** with links for navigation right below the user's information.

- Call history of the selected user

- The [general list](#) of scheduled conferences and virtual rooms created on this server and filtered by this user. It will include only those meetings where this user is one of the participants.



The call history will include all user sessions in one-on-one calls and conferences:

Call history: Abe Chester <chester@video.example.com>

10.05.2023 0:00 - 11.05.2023 12:32 | All types | Search

User / Conference	Type	Duration	Date and time ↑
C Conference	★ Conference	3 min 52 s	11.05.2023 12:01:46
W Webinar	★ Conference	53 min 22 s	11.05.2023 11:58:01
Carla Devine	✓ Incoming call	2 min 29 s	11.05.2023 11:55:18
Carla Devine	✗ Outgoing call	0 s	11.05.2023 11:53:47
Bruce Hubbard	✗ Outgoing call	0 s	11.05.2023 11:52:31

Total: 5

3

Conference Webinar

Conference ID \c\webinar

Owner Albert Moore

Type Conference

Duration 53 min 22 s

Date and time 11.05.2023 11:58:01

Session ID 0000003e507a6b34@video...

Conference page https://10.110.2.242/c/webi...

1. General UI for working with the table (check the [description of the reports section](#)). Events can be filtered by the following types:
 - **All types** (by default);
 - **Incoming call**;
 - **Outgoing call**;
 - **Missed call**;
 - **Conference**.
2. 2. To view full information, select session (communication session) in the list on the left, Recurring conferences and virtual rooms may have multiple sessions depending on the number of times these conferences were started.
3. 3. When selecting a session linked to the specific conference, you will see the following information in the card on the right:
 - Conference name and ID
 - The owner's display name
 - Current session duration
 - Session start and end time
 - a link to detailed session information in section **Call history**;
 - Link to the web page of a conference linked to the session. It will not be available for the meetings created ad hoc in TrueConf client applications.

15.3.4. Application Settings

On the page where a user account is either edited or created, the administrator can set special parameters that will be activated in the client application when a user authorizes on the server.

These parameters can determine the restrictions for incoming and outgoing bitrate and can be found in the **Application settings** section.

If such settings have not been configured, group settings (if any) are applied to the user (the member of the group). User group settings are displayed next to the user settings field. They are displayed for preview only and cannot be changed. If a user is a member of multiple groups, the scope of the user rights will be defined by the group with fewer rights.

Application settings

User's group settings are formed by the following groups: Developers, IT

	User	Group settings
Inbound bandwidth limit (kbit/s)	☒ 1024	2048
Outbound bandwidth limit (kbit/s)	☐	4096

Apply

If bitrate restrictions are set at the user or group level, users will not be able to change them in TrueConf client applications, but will be able to see what parameters were selected.

User application settings have higher priority than group settings: if you put user restrictions lower than group restrictions, user restrictions will be applied.

15.3.5. User's Address Book

At the bottom of the page you can find the address book and edit buttons. The address book contains all the users who are located in the address books of the user groups where the user belongs.

You can add individual entries to the list, which will be displayed only to the user being edited. Please note that you can add not only TrueConf Server users, but any call string, such as conference ID, SIP/H.323 or RTSP in the address book. Subsequently, you can delete them using the  button. The user can delete them in the address book of the client application or in the personal area.

If address book editing is allowed at the [group level](#), a user will be able to add contacts and organize them into groups in the client applications. Such groups are displayed only for the current user and are not included in the list of groups displayed in the control panel. However, the contacts added by the user will be displayed in the address book for his/her [account](#) in the control panel and the administrator will be able to edit this list.

Address book

1. Add user:

Enter user ID

Display name

Add

2. User will have address book of these groups combined: Developers, IT

3. Search

4. List of users:

User	TrueConf ID	Email
Bill Bush	bill	bill@mail.company.com
Bob Ice	bob	bob@mail.company.com
Ann Branson	ann	ann@mail.company.com
Alonso Lopez	alonso	alonso@mail.company.com
SIP endpoint	#sip:id@some-si...	
Elle Linn	elle	elle@mail.company.com

1. Add a user to the address book. To add a user, start typing the username or display name. From the drop-down list, select the user that matches your search (if the user is registered on your TrueConf Server instance).
2. The list of groups that the user belongs to, as well as the address books which are included in the user's contact list and cannot be removed.
3. Search for users.
4. The list of users displayed in the address book. Click on the user registered on your TrueConf Server instance to edit their profile.

For examples of call strings that can be added to the address book, refer to the [documentation for the user's personal area](#).

15.4. Groups

In **Groups** tab you can create, rename, edit and delete groups. You can also add or remove users from the group, set up their address book and configure individual settings for the users of any group.

Manual editing of the user list and settings (e.g., group name) is not available in [LDAP mode](#). You can only import groups from the LDAP directory as shown below.

Regardless of the data storage mode (Registry or LDAP), the following groups are included in the list by default:

- **Users without group** — it automatically includes users who have not been explicitly added to any groups either during [account setup](#) or in this section as [shown below](#);
- **Federated users** for users who make calls to users and conferences of your TrueConf Server through [federation](#);
- **Guest users**, where guests who join your public conferences (webinars) are placed.

It is impossible to rename or delete the default groups.

Each user group has specific permissions for using your video conferencing server.

15.4.1. List of rights for the user group

Please note that certain permissions cannot be given to the groups created by default. This restriction is set for security considerations (e.g., to make sure that operator rights are not available to everyone) and due to application logic reasons (e.g., since guests do not have a permanent account on your server, they cannot create conferences).

Federated users will have the same calling rights that are configured on their server. For example, if a user on a federated server is added to only one group, and this group is not allowed to make calls, this person will not be able to make calls to your users.

Below is a list of permissions that [can be configured](#) for user groups TrueConf Server:

-  Editing address book. By checking this field, administrator allows users to change users display names of the users, delete/add users and perform any other changes in the group's address book. If the box is not checked, group users will not be able to perform the actions mentioned above. In this case, all changes are performed by administrator in TrueConf Server control panel and extend to all address books of the users from this group.
-  Making point-to-point calls. Users will be able to answer incoming calls.
-  Creating group conferences.
-  Display your desktop or individual application windows.
-  The ability to send a request to control the interlocutor's desktop.
-  Providing the ability to control your desktop.
-  Presentation of slides can be imported from files or assembled from images by the user. This function does not depend on the right to share the desktop or applications.
-  File transfer in chats of any type: both personal and group.
-  Downloading files in chats. If this permission is not granted, the user will see a message in the chat indicating that this option is unavailable instead of the file and download option.
-  Recording conferences in the client application. This does not affect the ability to enable recording when creating a conference in the application scheduler or in the personal area.
-  Creating polls and distributing them across campaigns.

-  Viewing and managing available transcripts. This permission grants access to the transcripts of a user from this group in the server's AI personal area and their TrueConf Server. In this context, a user's transcript is one that can be accessed through the following settings:
 - by the administrator in the general settings of TrueConf Server, see [general settings in the control panel](#). For instance, by default, all participants have access to the conference transcript (moderators have full access, while others have read-only access);
 - by manually managing the settings from other users, see more in the [description of working with transcripts in the personal area](#).Restricting access does not remove the ability to manage audio recording for transcripts (see below).
If this checkbox is unchecked (the right is revoked), users will not see the **Transcripts** section in the app and in their personal area TrueConf Server, and when attempting to log in to the AI server, they will receive an access denied message.
-  Full access to all event transcripts of this TrueConf Server. In this case, a user from this group will be able to view and manage any transcripts, including those of conferences they did not participate in. To enable this right, both checkboxes must be selected: this one and  to view and manage available transcripts.
-  The ability to enable audio recording for transcription when creating a conference and during real-time meeting management.
- ☆ Operator privileges. This right allows group members to act as moderators and access [the real-time meeting management tool](#) in any event they join.

15.4.2. How permissions restrictions work

If a user is a member of two groups: the permissive settings will override restrictive ones. For example, the user account is included in such groups as **IT** and **DevOps**. If the members of the **IT** group are allowed to show slides, the user will be allowed to show slides even if this feature is not permitted for the members of the **DevOps** group.

Group-level user rights can also be redefined by [restrictions for authentication zones](#).

The persons who make a call to the users of your TrueConf Server via federation, will have the rights specified on your side (for the **Federated users** group) and on the side of their own server. For example, if you have disabled file sharing for federated users, they will not be able to send files when participating in the conferences hosted on your server, even if this right was given to them on their own TrueConf Server. Similarly, the federated user will be unable to send files if you have allowed this feature for federated users; but this right is denied to the group of this user on the side of his/her video conferencing server.

15.4.3. Configuring Groups in Registry Mode

Below, you can find an example of group settings for Registry mode, while [some parameters will differ for LDAP mode](#).

Groups

[Help](#) ?

Group list

Group Name **Create**

	Group Name	Address Book	Application	Group call pickup	User rights													
☐																		
☐	Developers	Customize	Customize	Change	☒	☒	☒	☒	☒	☐	☒	☒	☒	☒	☐	☐		
☐	HR	Customize	Customize	Customize	☒	☒	☒	☒	☒	☐	☒	☒	☒	☒	☐	☐		
☐	IT	Customize	Customize	Change	☒	☒	☒	☒	☒	☐	☒	☒	☒	☒	☒	☐		
☐	Lawyres	Customize	Customize	Customize	☒	☒	☒	☒	☒	☐	☒	☒	☒	☒	☐	☐		
☐	Managers	Customize	Customize	Change	☒	☒	☒	☒	☒	☐	☒	☒	☒	☒	☐	☐		
☐	Meeting rooms	Customize	Customize	Customize	☒	☒	☒	☒	☒	☐	☒	☒	☒	☒	☒	☐		
☐	Operators	Customize	Customize	Customize	☒	☒	☒	☒	☒	☐	☒	☒	☒	☒	☒	☒		
☒	Sales	Customize	Customize	Customize	☒	☒	☒	☒	☒	☐	☒	☒	☒	☒	☒	☐		
☒	Terminal room	Customize	Customize	Customize	☒	☒	☒	☒	☒	☐	☒	☒	☒	☒	☒	☐		
	Users without group	Customize	Customize		☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☐		
	Federated users	Customize	Customize		☐	☐	☐	☒	☒	☒	☒	☒	☒	☒	☒	☐		
	Guest users	Customize	Customize		☐	☐	☐	☒	☒	☒	☒	☒	☒	☒	☒	☐		

Delete selected

1. To add a new group, click the **Add** button, enter its name in the pop-up window, and press **Create**.
2. At the group level, you can enable or disable certain features by using checkboxes in selected columns. These settings allow you to delineate the rights of different server users. A [complete list of these permissions is provided above](#), and you can also check the [description of how rights work](#) when a user belongs to several groups. Rights management is also available when you are [editing the settings of a group](#) on the **User rights** tab.
3. Click on the desired group in the list to [edit it](#). Clicking on the column **Group Name** allows you to sort the list alphabetically.
4. To delete one or more groups, check their boxes and click **Delete**. The accounts of group participants will not be deleted from the server.

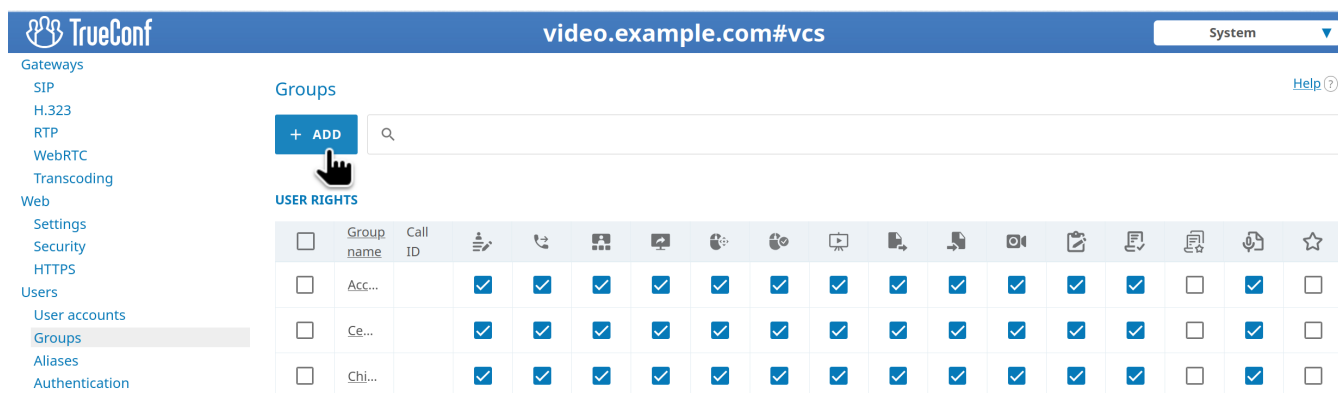
15.4.4. Configuring Groups in LDAP Mode

Manual editing of the user list and settings (e.g., group name) is not available in [LDAP mode](#). You can only import groups from the LDAP directory as shown below.

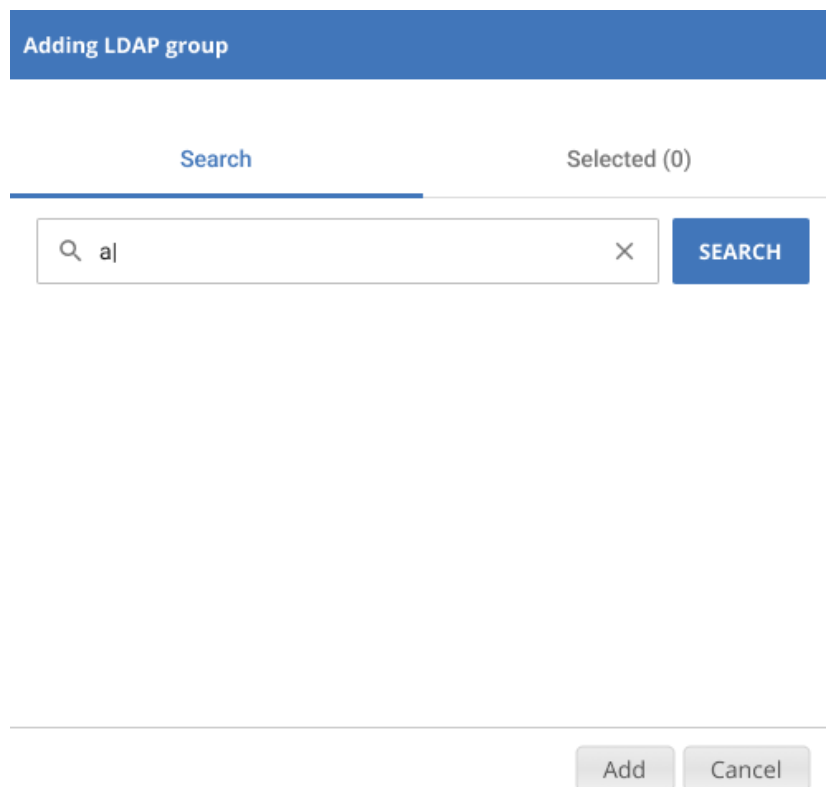
If you would like to centrally manage user information and enable [LDAP synchronization](#) on your TrueConf Server instance, the list of users and groups is imported from the LDAP catalog (e.g., Active Directory). Note that your designated user search catalog object must contain all necessary user groups. For instance, if when configuring LDAP you indicated in the **Group** field the string `cn=UsersGroup,ou=People,dc=example,dc=com`, on the LDAP side the `UsersGroup` object must contain the necessary account groups:

In this case, system administrators will not be able to create user groups and add group members in the TrueConf Server control panel. Instead, they can be imported from the LDAP catalog. To do it, follow the next steps:

1. In the server control panel, navigate to section **Users → Groups**.
2. Click **Add** above the group list:



3. In the window that opens, enter part of the group name you want to add and click the **Search** button:



4. In the list of filtered groups, click on the names of the ones you want to add to the list. They will appear in the **Selected** list:

Adding LDAP group

Search

Selected (2)

Development
devs

Sales and SEO
marketing

Add

Cancel

5. Click **Add** to apply the changes.

For groups imported from LDAP, as well as in Registry mode, settings for [user rights](#), [address book](#), [client application restrictions](#), and [group calls](#) are available.

15.4.5. Editing a group

By clicking on a group name in the list, you will open the menu for editing information about the group:

Groups / Group editing

Help ?

Sales



Participants

Address book

User rights

Application settings

Call settings

ADD

 Search



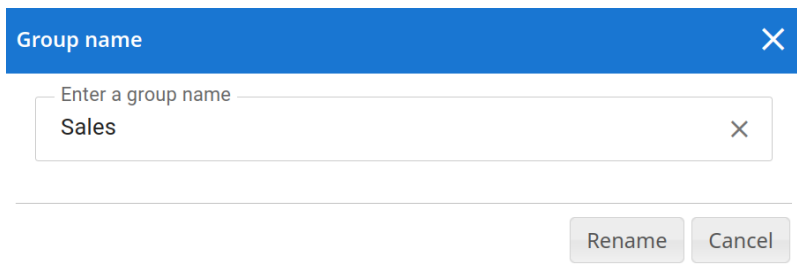
User	TrueConf ID	Email	
 James Wolf	wolf_active	wolf_active@company.com	×
 Amanda White	white_active	white_active@company.com	×
 Bruce Robertson	robertson_active	robertson_active@company.com	×
 Alice Campbell	campbell_active	campbell_active@company.com	×
 Cliff Brown	brown_active	brown_active@company.com	×
 Jane Flowers	bots_en	bots_en@company.com	×
 Jane Flowers	bots_active_en	bots_active_en@company.com	×

Here you can do the following actions:

- Rename the group

- [edit its participant list](#);
- [configure the address book](#) for all group members;
- select available permissions for the group on the **User rights** tab (all permissions are detailed [above](#));
- [specify application settings](#);
- [configure a group call](#).

To change the group name, click the  button to the right of the name. In the window that opens, enter the new name and click **Rename** (or **Cancel** if you want to close the window without saving changes):

A screenshot of a 'Group name' dialog box. The dialog has a blue header bar with the text 'Group name' and a close button (X). Below the header is a text input field with the placeholder text 'Enter a group name'. The field contains the text 'Sales'. To the right of the input field is a small 'X' button. At the bottom of the dialog are two buttons: 'Rename' and 'Cancel'.

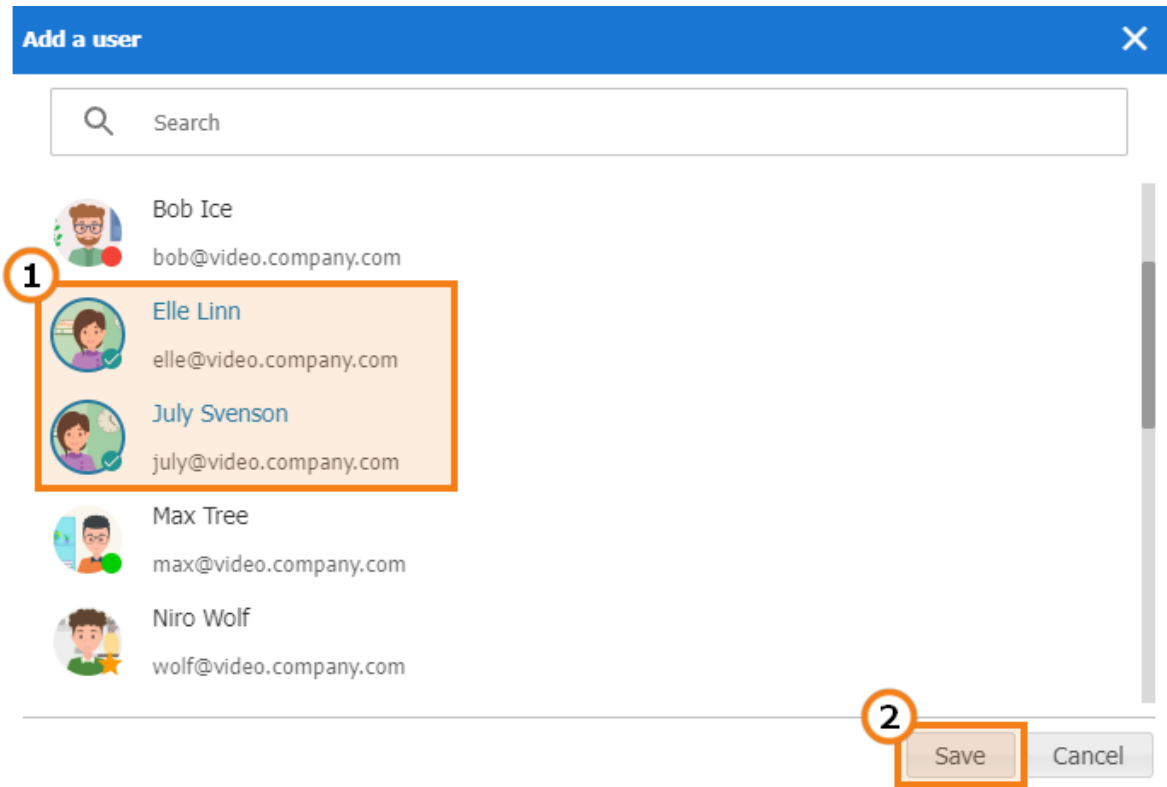
You can also click the  button to export the list of users from a specific group to a CSV file for subsequent [import into the TrueConf Group](#) address book.

15.4.5.1. Editing the group participant list

In [LDAP mode](#), the add button is not displayed on the **Participants** tab. In this case, the entire group is imported as [shown above](#).

To add participants to the group:

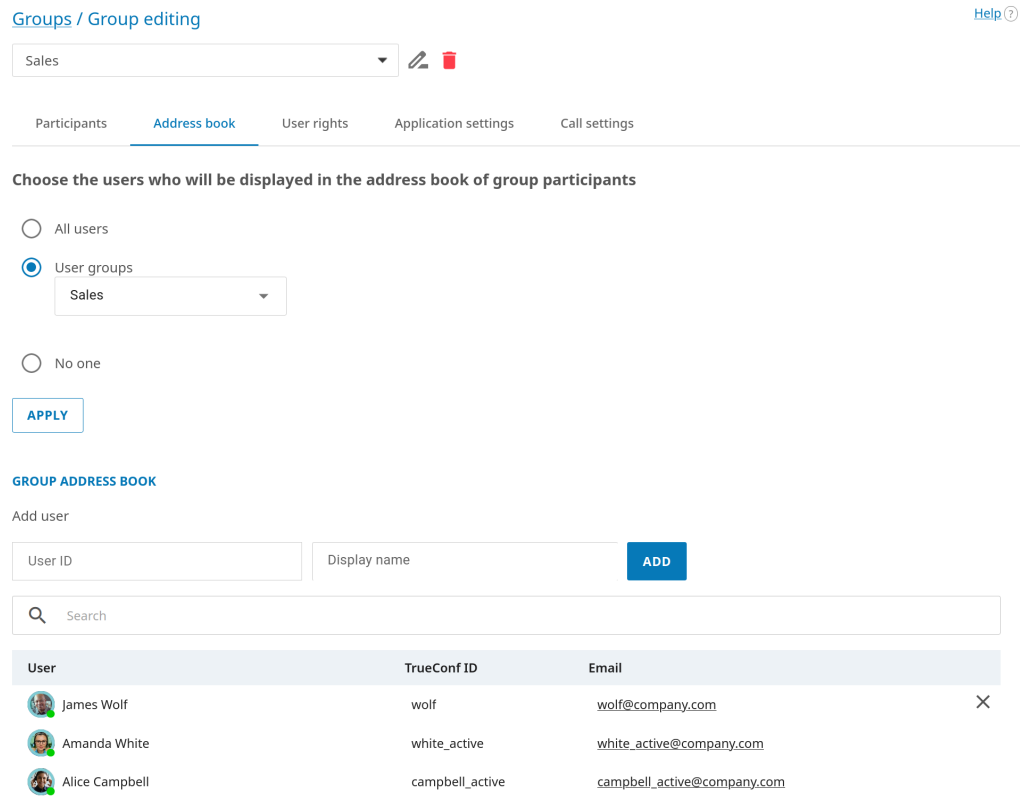
1. Open it in the [general list](#).
2. Go to the **Participants** tab.
3. Click the **Add** button.
4. In the window that opens, select the users you want to add to the chosen group (a filter by name or TrueConf ID is available). Once all users are selected, click **Save**:



To remove a user from the group, click the  button on the right side of the line with their name.

15.4.5.2. Configuring the address book for group users

In the **Address Book** tab of each group, you can set a contact list that is shared among all users of that group:



Participants can also add new contacts to the address book on their own, but only if the box **Address Book Editing** is checked in the permissions settings. Please note that adding contacts to the address book by the administrator and manually by a user are applied independently of each other.

You can add all users from another group to the address book of the selected group (i.e., to the address book of each participant) at once. To do it:

1. In section **Choose the users who will be displayed in the address book of group participants**, select item **User groups**.
2. Click on the drop-down list next to it and select groups.
3. To save the settings, click the **Apply** button.

In the **Group address book** section, you can also manually add users of various types, similar to [adding them to the address book in a user profile](#). However, a group member will not be able to delete them independently because these contacts are added for the entire group, not to their personal address book.

15.4.5.3. Configuring application settings for user groups

By clicking the **Customize** link in the **Application** column of the group row in the main table, a menu will open where you can set bandwidth limitations for users belonging to that group.

Please note that the [user application settings](#) take precedence over group settings.

If bitrate restrictions are set at the user or group level, users will not be able to change them in TrueConf client applications, but will be able to see what parameters were selected.

[Groups / Group editing](#)

Sales



Participants

Address book

User rights

Application settings

Call settings

BANDWIDTH LIMITATION

☒ Inbound bandwidth (kbit/s)

32 - 10240

2048

☒ Outbound bandwidth (kbit/s)

32 - 10240

1024

APPLY

Please note that if [channel limits for the application](#) are set for a specific user, these settings will take precedence over the group settings.

15.4.5.4. Configuring Group Calls

The administrator can enable group calls for a user group. When this feature is activated, it will be possible to make calls to the entire group, rather than an individual user, so all group participants will see an incoming call. As soon as someone answers this call, it will be automatically declined for other users.

To activate group call pickup:

1. Select the desired group from the [general list](#) and go to the **Call settings** tab:

[Groups / Group editing](#)

Sales



Participants

Address book

User rights

Application settings

Call settings

☒ Enable group call pickup

Incoming call ID:

[RESET TO DEFAULT](#)

APPLY

2. Check the box **Enable group call pickup**.
3. To start a call, specify an ID, which has to be unique within the server, meaning that it cannot match the IDs of other group calls or TrueConf ID of user accounts. To start a group call, use this ID in the format `id@example.com`, where `example.com` is your server address, for instance, `001@video.example.com`. You can use letters, numbers, and characters `. _ -` in the ID. This call string can be added to the address book for future use. By default, the group ID is filled in, but you can specify your own (e.g., a short string for convenience).

To save the settings, don't forget to click the **Apply** button.

15.5. Alias

15.5.1. Description of operation

Aliases allow you to find a contact by entering a short string (a kind of filter) instead of the full string. Such a contact can be:

- A user from the same server
- A user from a federated server
- A call string via SIP, H.323, RTSP protocols (endpoint, IP camera, etc.)
- A conference (including a conference held on a different server).

By adding an alias, you essentially create a new filter for quick searches in client applications. In the control panel, the administrator CANNOT use an alias as a full-fledged ID; for example, you cannot add an alias for a user or group in the address book.

This feature is especially useful when [making calls to TrueConf Server from mobile devices with a digital keyboard](#). Shorter aliases help users to quickly find a contact or add it to the address book. The contact can be of any type which was mentioned previously.

Aliases

[Help ?](#)

☐	Alias	User
☐	123	bill@server.company.com
☒	124	bob@server.company.com
☐		
☐		

Create an alias:

Alias

User

1. An alias may contain numbers, letters, hyphens `-` and underscores `_`. The maximum number of characters is 32.
2. Call string (including a server user's login). Calls to this alias will be redirected to the user. To specify a conference, use the format `\c\ID@server`.
3. Press the button to add a new alias to the list.
4. To delete one or more aliases, select them using the checkboxes and click **Delete selected**.

Examples of call strings for alias configuration:

- `ceo_user` — a user of your current server with the login `ceo_user`
- `other_user@example.com` — a user from a [federated server](#) with the address `example.com`
- `\c\webinar` — a conference on your current server. To copy the conference ID in this format, select the event in the [general list](#) and open the card of this event.
- `\c\webinar@example.com` — a conference held on a federated server with the address `example.com`
- `#sip:@10.110.8.217` — an SIP endpoint with the address `10.110.8.217`. If you need to call an [endpoint registered on the server](#), when setting up the alias, you can specify the login of the user under which the endpoint is authenticated.

15.5.2. Using in Federation

In [federation mode](#) aliases can be used to make calls just like TrueConf ID. An alias will be resolved on the server which is specified after `@` in the full `alias@server` alias, e.g., `122@video.server.name`.

We will now discuss two examples of using aliases on federated TrueConf Server instances, `one.name` and `two.name`.

Case 1

Each of TrueConf Server instances has its own aliases. We have created an alias `111` for the user `userA` from the `one.name` server.

To make a call to `userA` from the `two.name` server, the following string should be entered in the address line:

`111@server` where `server` is the DNS name or IP address of the `one.name` server.

Case 2

Create an alias `111` on the `two.name` server for the user `userA` from the `one.name` server. It will correspond to the following call format:

`userA@server` where `server` is the DNS name or IP address of the `one.name` server.

In this case the users from the `two.name` server will be able to call users from the `one.name` server without its IP or DNS name. They will just have to enter aliases in the address line of their client application. For example, they can use `111` which we have discussed before.

The second option is more transparent for users, but in this case, it will be more difficult to configure a convenient system of aliases.

15.6. Authentication

In the **Users → Authentication** section, you can configure the authentication methods for your TrueConf Server.

Authentication is the process by which the service verifies the identity of a user/application. In other words, this process essentially has to confirm that the entity is what it claims to be. For example, authentication can confirm that the user is indeed who he/she claimed to be when connecting to the server. After the identity is verified, **authorization** takes place. At this stage, the user or application is granted permissions to perform certain actions on the service according to the settings.

TrueConf Server supports the following authentication methods:

- With a login and password, in Registry mode (when accounts are stored on the server), you can [set your own password complexity rules](#)
- [NTLM SSO](#)
- [Kerberos SSO](#)
- [Microsoft Outlook SSO](#)
- [Microsoft Active Directory Federation Services, AD FS](#)
- [Keycloak](#)

- [Custom provider settings via OAuth / OpenID Connect protocols.](#)

Authentication may occur in two different security zones: **trusted** (or **Trusted network** as it is called by default) and **external (untrusted)** (called **Internet** by default). They are included from the very beginning and cannot be deleted. However, one can configure them as it will be described below.

Everyone, who does not get into the trusted zone, will automatically be moved to the external zone. A user's IP address will determine the zone to which this person will belong.

Authentication

[Help ?](#)

Zones		
Name	Authentication meth	State
Trusted network	Login and password	☒
Internet	Login and password	☒

Authentication methods		
Name	Status	State
Login and password	Enabled	☒
NTLM SSO	Connection to an LDAP server is required (Active Directory)	☐
Kerberos SSO	Connection to an LDAP server is required	☐

[Add](#)

1. Security zones. To open the settings of the security zone, click on it.
2. Authentication methods specified for each zone.
3. Zone activation or deactivation. When a zone is deactivated, the users, who belong to this zone, will receive a notification that authorization is currently unavailable when they try to connect to your TrueConf Server. The users, who were connected previously, will be able to interact with the system up until the moment when the [authorization token](#) expires.
4. Verification methods that can be configured. The **Login and password** and **NTLM SSO** methods do not require configuration; they are simply activated with the toggles on the right side. For other added providers, you can edit the settings by clicking on the provider name. You can also remove unnecessary providers, but it is not possible to remove NTLM and Kerberos methods; they have to be disabled if needed.
5. The configuration and work status of each method.
6. Activation of authentication options.
7. Adding two-factor authentication providers: AD FS (Active Directory Federation Services), Keycloak, manual settings for adding a different provider.

For methods **Kerberos SSO**, **NTLM SSO**, **AD FS**, and **Microsoft Outlook SSO** to be available, the [LDAP account storage mode](#) must be selected and configured. For other authentication methods (Keycloak, manual settings), this is not necessary.

15.6.1. Access Zone Settings

Click on the name of a **trusted zone** to open its settings:

1. You can change the zone name, e.g., to “Corporate network”.
2. In the **Subnet masks** section, specify the network segments that are included in the current zone. By clicking on any entry, you will open the pop-up window for editing the address and subnet mask. Here, you can also delete the subnet. At least, one zone has to be specified for the trusted zone.
3. To add a new subnet to the list, click the **Add** button.
4. In the **Authentication methods** section, select required parameters by checking corresponding boxes. The list of zones is generated from the following options: login and password, NTLM SSO, Kerberos SSO, and other authentication providers which were [added manually as shown below](#).

Below is the **Available rights** section where you can select the available permissions for each area. The list of available permissions is the same as in the [group settings](#), and any restrictions are added to those for groups. In other words:

- The right is **given** to a user if he/she is in a zone where this right is allowed, **and** belongs to at least one group that was granted this right.

- The right is **denied** to a user if he/she is in an area where this right is prohibited **or** belongs to groups that were not given this right.

Don't forget to save changes to apply them on the server.

It is possible to specify the name of the **external zone**, its authentication methods, and available rights, but one cannot specify subnets.

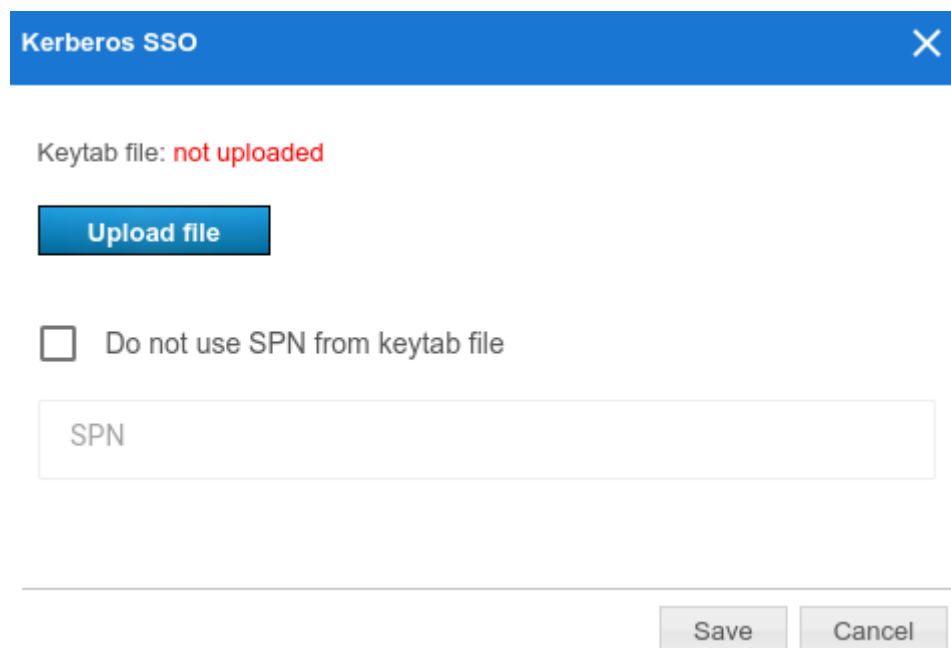
15.6.2. SSO Settings

Single sign-on (SSO) technology integrated with an LDAP server enables users of your TrueConf Server to be automatically authenticated on it after logging into the OS on their PCs and launching the TrueConf client application. You can use one of the following options for this: **Kerberos**, **NTLM**, or Outlook SSO (when integrated with Microsoft Exchange Server).

To make sure that SSO authentication works correctly via NTLM, add the machine, where TrueConf Server is installed, and users' PCs to the domain. In the case of Kerberos, only users' PCs have to be registered in the domain, but this is not mandatory for the machine with TrueConf Server.

To activate **NTLM**, simply enable it in block **State**. There are no additional settings required.

To configure the connection using the **Kerberos** protocol, click the link **Kerberos SSO** in the **Authentication methods** section (on the **Authentication** page with the list of security zones):



Kerberos SSO

Keytab file: not uploaded

Upload file

☐ Do not use SPN from keytab file

SPN

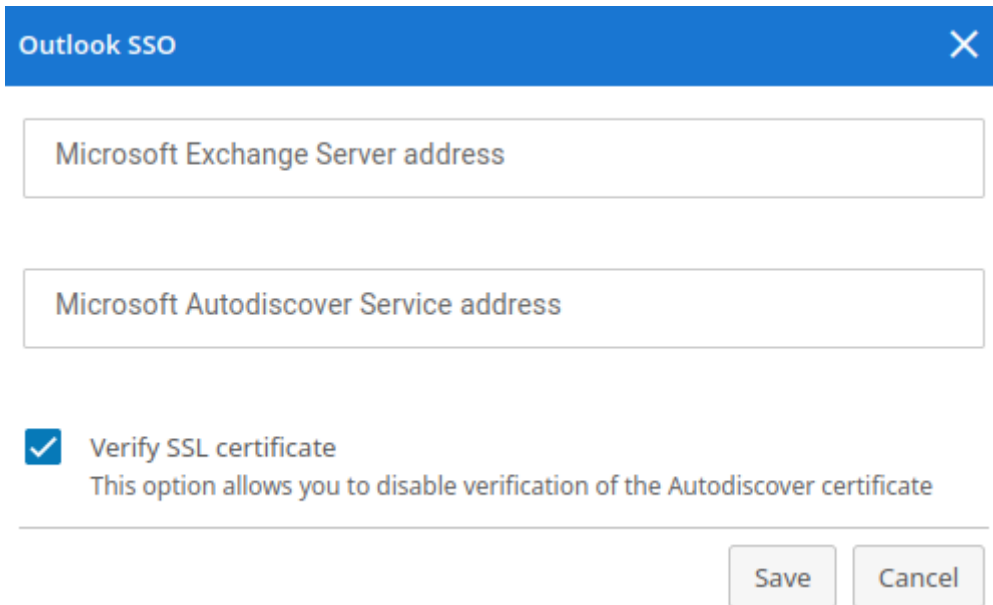
Save Cancel

In the pop-up window, select:

- The keytab file that will be used for authentication
- If necessary, click **More** and enter your value **ServicePrincipalName (SPN)** in place of the one saved in the file.

To configure SSO in the Outlook mail plugin, click on the **Outlook SSO** link. Specify the addresses in the pop-up window:

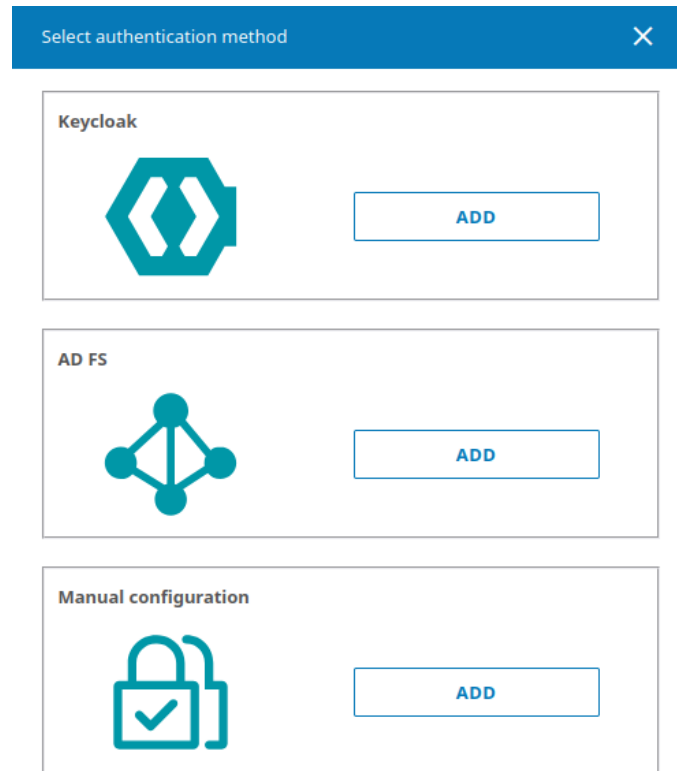
- **Microsoft Exchange Server host** for authentication token verification, it should be in the form of `{host}` without the protocol prefix (i.e., **without** `http/https`);
- **Microsoft Autodiscover Service host**, appears as `{host}` without specifying the protocol prefix (meaning **without** `http/https`);
- Additionally, you can disable SSL certificate verification for the Autodiscover server.



The screenshot shows a dialog box titled "Outlook SSO" with a close button (X) in the top right corner. Inside the dialog, there are two text input fields. The first field is labeled "Microsoft Exchange Server address" and the second field is labeled "Microsoft Autodiscover Service address". Below these fields, there is a checkbox labeled "Verify SSL certificate" which is currently checked. To the right of the checkbox, there is a line of text: "This option allows you to disable verification of the Autodiscover certificate". At the bottom right of the dialog, there are two buttons: "Save" and "Cancel".

15.6.3. How to add two-factor (2FA) authentication providers

You can add one or more two-factor authentication methods (AD FS or OAuth 2.0 / OpenID Connect providers) to be selected later for the desired [zone](#). There is no limit to the number of providers you can add. To do this, in the **Authentication methods** section, click **Add** and select the desired option:



Active Directory Federation Services (AD FS) is the software component of Windows Server which acts as the authentication provider needed for accessing the resources outside the Active Directory corporate system, for example, it may be used for accessing web applications.

To configure integration with the selected authentication provider, click on the **Add** button in the corresponding section and specify the following parameters in the settings window:

1. The identifier (Client ID) of the OAuth application created on the side of AD FS for receiving the access token.
2. URI set on the side of TrueConf Server used for receiving the response from the provider. This URI also has to be specified on the provider side.
3. **Authorization form URL** on the provider side.
4. **Request token URL**, is used when connecting users to TrueConf Server upon successful authentication.
5. **Logout URL**.
6. Scope (**Scope**). Specify the `scope` selected when configuring the rule on the provider's side. For example, for AD FS, see [Microsoft documentation](#) for more details. You can specify multiple scopes by listing them separated by commas without spaces.
7. The authentication provider name displayed in the list of authentication options on the [page where access zones are configured](#) and in TrueConf client applications when two-factor authentication is used.
8. You can disable SSL certificate verification on the TrueConf Server side from the provider.
9. To make it easier to distinguish one authentication method from another, you can set a custom image, by uploading it in the SVG format.

In addition to AD FS, other solutions such as Keycloak can be used to implement two-factor authentication via OAuth 2.0. The configuration settings will be the same as for AD FS.

15.7. LDAP / Active Directory

Two modes for storing user data are supported TrueConf Server: Registry and [LDAP](#). You can switch between them at any time by clicking the **Switch** button:

User Storage

[Help ?](#)

Current status: Server is in registry mode.

Registry

☒ Enable

Description: Local data storage is the source of user account information.
In this mode, the server administrator is allowed to create user accounts.
If TrueConf Server is moved to another computer, user accounts can be exported from the settings file.

LDAP

☐ Enable

Description: A third-party LDAP directory service such as Microsoft® Active Directory or 389 Directory is the source of user account information.
User accounts will be organized and processed with the help of LDAP tools. TrueConf Server automatically synchronizes all changes made in the LDAP directory.
You can import user accounts from LDAP to a local data storage when switching to Registry Mode (please note that passwords cannot be imported).

[Switch](#)

15.8. Registry Mode

Registry mode is used by default. In this mode, the server contains information about the users on the local server. You can add or remove users via control panel. If the server has been switched from Registry to LDAP data storage mode, existing user records will not be used anymore.

When switching to LDAP data storage mode, user records stored on the local computer will not be removed, so switching to another data storage mode will not damage saved information.

When the server is switched from LDAP to Registry mode, it is possible to import users from the directory service into the server local storage. This ensures you won't lose account data if you choose to stop using AD/LDAP or no longer need to synchronize accounts. To transfer accounts from the directory service to the Registry storage, check the box **Import user information**:

How transfer works:

User Storage

[Help](#) (?)

Current status: Server is in LDAP mode.

Registry

☒ Enable

Description: Local data storage is the source of user account information.

In this mode, the server administrator is allowed to create user accounts.

If TrueConf Server is moved to another computer, user accounts can be exported from the settings file.

LDAP

☐ Enable

Description: A third-party LDAP directory service such as Microsoft® Active Directory or 389 Directory is the source of user account information.

User accounts will be organized and processed with the help of LDAP tools. TrueConf Server automatically synchronizes all changes made in the LDAP directory.

You can import user accounts from LDAP to a local data storage when switching to Registry Mode (please note that passwords cannot be imported).

☒ Import user information

Switch

1. Data will be saved for the fields that were in LDAP/AD and are available in Registry mode (check [the profile description](#)).
2. The password will not be transferred, and a new one will not be created. This field will remain empty, and the administrator will need to manually set a new password.
3. Accounts will be deactivated.

15.9. LDAP Mode

In this storage mode, the server takes user information from a remote or local LDAP directory. This approach offers a number of advantages when the server is used in the corporate environment:

- Automatic syncing of user information
- No need for authorization within the network at the workplace
- Transparency, speed, and ease of administration
- Administration security
- Support for various directory services: Microsoft Active Directory, FreeIPA, OpenLDAP, 389 Directory Server, etc.

In LDAP mode, you cannot edit the list of users and group settings in the server control panel. By default, the configuration settings for LDAP correspond to Microsoft Active Directory. User information is edited with the Active Directory management tools. However, when a user is deleted from the directory service, the avatar locally stored on the machine with TrueConf Server will also be deleted.

Additionally, in this mode a user will be able to set an avatar and change the display name in the application or personal area. This information will also be updated on the directory service side, but the following conditions have to be met:

- **Display Name** and **Allow Avatar Propagating** fields are correctly set in [additional LDAP settings](#)

- The account under which TrueConf Server connects to the LDAP directory has the permission to write these fields for objects.

To learn more about the LDAP protocol and the Microsoft Active Directory service, [read our website](#).

In LDAP mode, user rights are determined by their membership in a particular Active Directory group. To activate this mode, check the box in field **LDAP → Enable** and click the **LDAP settings** button that will appear at the bottom. This will open the LDAP settings form:

LDAP

[Help ?](#)

The screenshot shows the LDAP settings form with the following fields and callouts:

- 1**: Server Type dropdown menu (set to Active Directory).
- 2**: Secure connection checkbox (checked).
- 3**: Auto detect radio button (selected).
- 4**: Domain text input field (ldap.example.loc).
- 5**: Server text input field.
- 6**: Port text input field (636).
- 7**: Authentication dropdown menu (set to NTLM).
- 8**: Name text input field (admin).
- 9**: Password text input field (masked with dots).
- 10**: Apply button.

Below the authentication section, there is a section titled "Group allowed to authorize" with a description: "This group restricts the list of users allowed to authorize on TrueConf Server." It contains a text input field for "Path (distinguishedName):" with the value "cn=users,dc=ldap,dc=example,dc=loc" and a "Browse" button.

At the bottom, there is an "++Advanced" button.

1. In the dropdown list **Server Type**, select your directory service, supported options are: **Active Directory**, **OpenLDAP**, **389 Directory Server**, **FreeIPA**. This selection determines the default attribute names read by the server from the LDAP directory. You can also choose **Custom** to manually set the attribute names. After selecting the server type, to switch to its corresponding attribute names, [expand the Advanced block](#) below and click the **Default** button. You will see that the attribute names in the **Value** column have changed. If necessary, you can enter the required values and then click the **Apply** button, which is located in the same **Advanced** block.
2. Use the **Secure connection** option to connect to the LDAP server in protected mode (via LDAPS protocol) to ensure secure transfer of user data over the network.
3. Switches **Auto detect** define the mode for specifying the server address and port.
4. Specify your domain in the **Domain** field. In the automatic mode the LDAP server can be chosen among the servers by default of the DNS domain, specified in this field. Default servers are being chosen according to the relevant DNS-notes of SRV type. For Active Directory DNS domain name AD can be indicated here.

5. Specify the LDAP server address/port for manual configuration in the **Server** and **Port** fields. You can use the global directory to connect to the directory service. To do it, specify **3268** as the connection port for LDAP or **3269** for LDAPS.
6. Specify the directory object for user search in the **Base DN** field (Base Distinguished Name), for example, `ou=People,dc=example,dc=com`.
7. In section **Authentication**, select the authentication mode TrueConf Server on the LDAP server. The supported options are:
 - **Simple** — by the specified login/password;
 - **NTLM** — using a login and password, but via [NTLM protocol](#);
 - **Current NT user (available only when installed on Windows)** — the server will attempt to connect to the directory service using the account under which its services are running (more details [described below](#));
 - **GSS** — using a login and password, but through the [GSS protocol](#);
 - **Kerberos Keytab** — is detailed [below](#).

In Active Directory, outdated NTLMv1 and LM protocols are disabled, so when using TrueConf Server on Linux OS, **NTLM** authentication may not work.

1. If necessary, specify the LDAP server authorization settings in fields **Name** and **Password**.
2. In the **Path (distinguishedName)** field, you can specify the LDAP user group that is allowed to authenticate on TrueConf Server, for example, `cn=TC_Users,ou=People,dc=example,dc=com`. You can select a group using the **Browse** button. To enable this button, you must correctly fill in the LDAP server connection fields (in blocks **Server settings** and **Authentication**), including the **Base DN** field.

10. You can fine-tune the [additional LDAP settings](#) in block **Advanced**.

When switching server types (for instance, from Active Directory to OpenLDAP), the additional LDAP settings are not reset automatically. To revert to the default parameter values for the new server, expand block **Advanced** and click the **Default** button.

When switching from LDAP mode to Registry, you can import user records. To do this, on the **User storage** tab, select Registry mode and check the **Import user information** box, then click the **Switch** button.

User passwords are not imported. After import, the accounts remain in an "inactive" state (see the description in section [User accounts](#)).

In LDAP mode, only the digest password will be available for editing in the user profile. This digest password **must** be specified when [registering an SIP/H.323 endpoint on TrueConf Server](#). The same password should be specified in the authorization settings for the endpoint:

Edit user

[Help ?](#)

Account information

Status: Active Disconnect

TrueConf ID: room@server.name

Digest password: Confirm: ? Apply

E-mail:

Display name: Huddle room

First name:

Last name:

Company:

Groups: Users without group

Back

Directory of groups and users registered on TrueConf Server. This tab allows to create and manage the user's groups. User Accounts tabs allows creating groups and managing rights. In the Registry mode a user can belong to one (or more) created groups. This parameter can be edited in the edit user information window. In the LDAP mode this window allows you to define rights for several LDAP groups. User attribute can be defined in the LDAP folder.

To import user groups from LDAP, go to section **Users → Groups**. Click the **Change** button and select the desired groups from the list that appears. For more details, refer to the [article on configuring user groups](#).

When groups of users are imported from LDAP, the list will include only the groups that are included in it by default.

If you have several TrueConf instances connected to a common LDAP directory, users can log in to the personal area from a guest page of any of the connected servers. In addition, users can participate in private meetings hosted on a different TrueConf instance connected to a common LDAP directory using an auto-generated login.

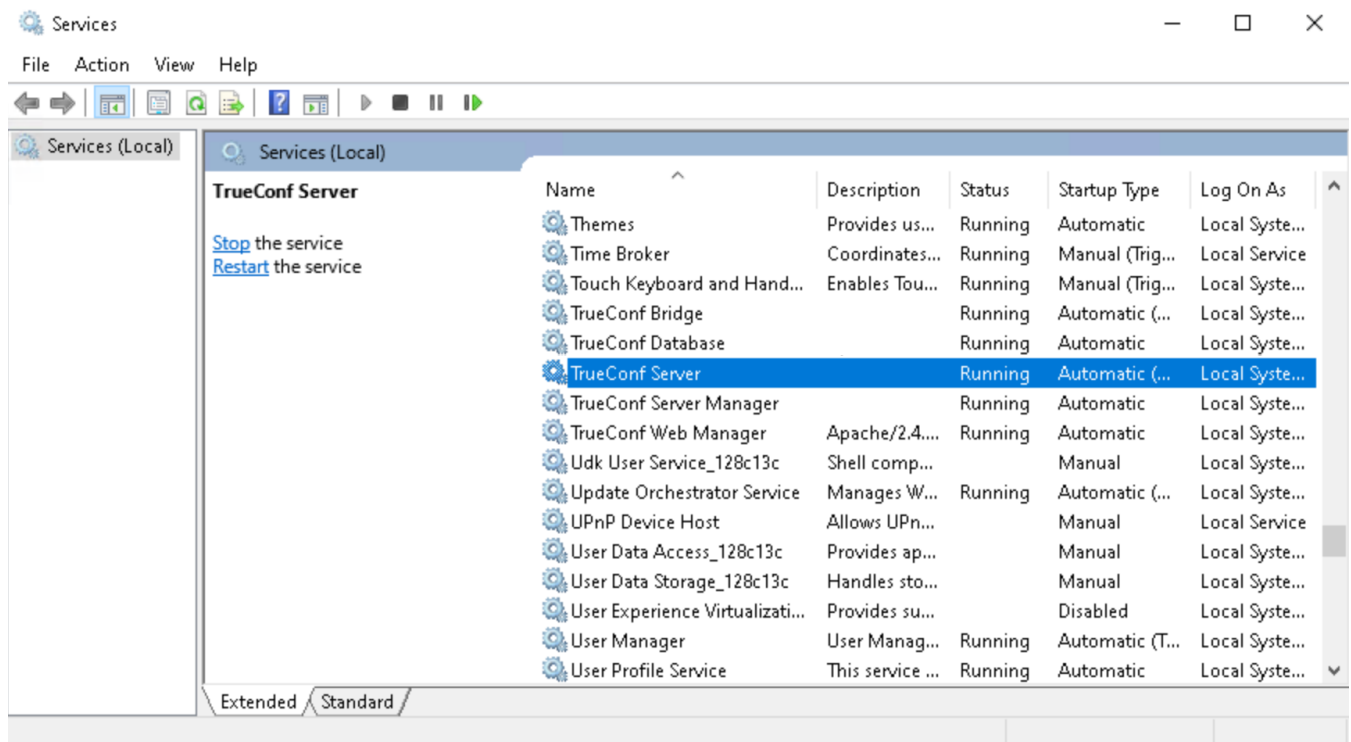
15.9.1. Authorization as an NT user on Windows

If TrueConf Server is installed on Windows and you prefer not to provide authentication details in the control panel for LDAP directory integration, you can use the credentials specified in the OS. In this case, TrueConf Server will use the login under which its services are running:

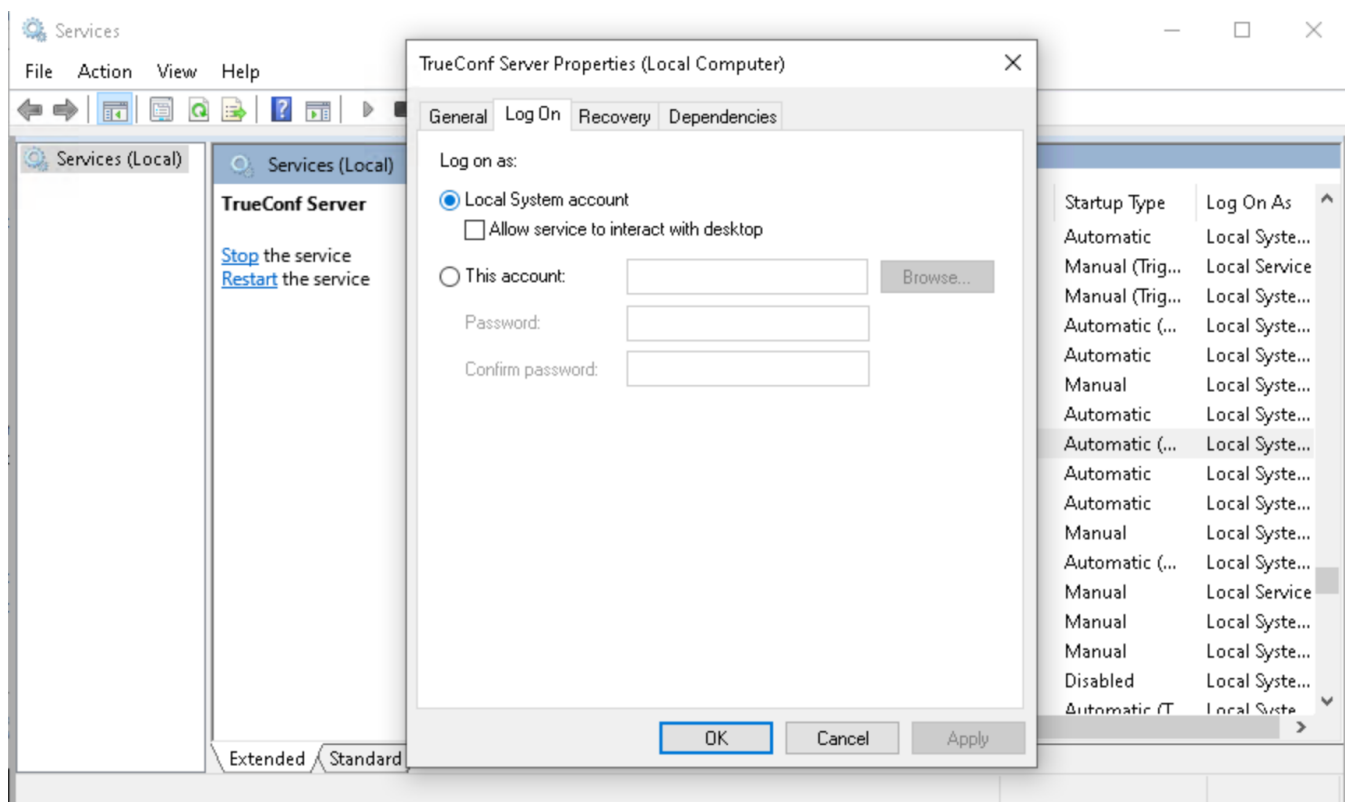
1. Make sure that the machine with TrueConf Server is within the same domain with the required LDAP directory (e.g., AD). By default, AD objects (including PCs registered in it) are allowed to read the list of objects, which would be enough for getting the list of users/groups. However, if you want avatars to be updated on the directory side, when they are changed in TrueConf, you will need to create a new user account and give it required

permissions. You should also make sure that `Allow Avatar Propagating: 1` is set in [additional parameters](#).

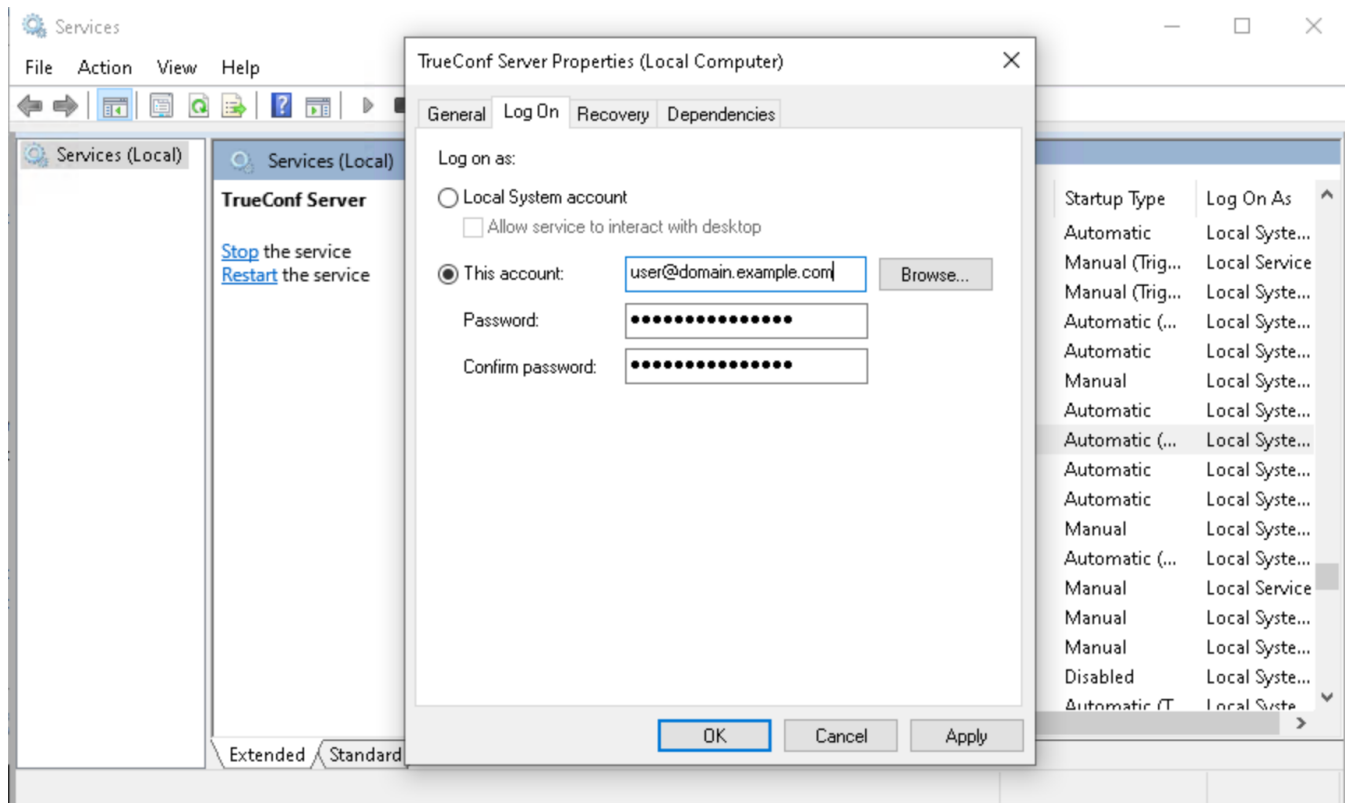
- Go to the OS service management (for example, by executing the `services.msc` command in the terminal/PowerShell):



- Double-click on the **TrueConf Server** service to open its properties and navigate to the **Log On** tab:



- Select option **This account** and enter the required login/password:



5. If you need to specify a particular user explicitly (when the default system account is not suitable), repeat steps 3-4 for the **TrueConf Web Manager** and **TrueConf Server Manager** services.

15.9.2. Generation of a keytab file for Kerberos server authentication

If the Kerberos protocol is used for connecting to the directory service via LDAP/LDAPS, a keytab file has to be uploaded for the connection of TrueConf Server. This file needs to be generated on the directory service side.

The keytab is issued for the user account (UPN) under which TrueConf Server will access the directory service, rather than for the SPN. So, such a user must be created on the directory service side.

Do not confuse generation of a keytab file for connecting a video conferencing server to a directory service with [generating a keytab for user connection to the server](#). These are different tasks! Even if the server receives data via Kerberos, you can still use any convenient [authentication methods](#) for user connections.

15.9.2.1. Generation of a keytab file for Active Directory

If you are setting up integration with MS Active Directory (MS AD), you will need to take these steps to generate a keytab file:

1. Run PowerShell on the machine where AD is installed.
2. If a user has not been previously created for accessing the directory service, add one by running the command:

```
New-ADUser -Name "[user]" -SamAccountName "[user]" -Path
"OU=example_ou,DC=example,DC=com" -AccountPassword (ConvertTo-SecureString "[pass]"
-AsPlainText -force) -Enabled $true
```

where:

[user] — the login of the new OS user

OU=example_ou,DC=example,DC=com — the user's LDAP group

[pass] — the new user's password.

3. For convenience, you can set a password policy for the user so that the password does not expire (has an indefinite validity period) and cannot be changed. Replace [user] with the login of the user which was created previously:

```
Get-ADUser [user] | Set-ADUser -PasswordNeverExpires:$True -CannotChangePassword:$true
```

4. Execute the command to generate the keytab file:

```
ktpass -princ [user]@example.com -mapuser [user] -crypto ALL -ptype KRB5_NT_PRINCIPAL
-pass [pass] -target example.com -out c:\ldap.keytab
```

where:

[user] — the login of the previously created OS user

example.com — domain name

[pass] — user password

c:\ldap.keytab — the path to save the file on the machine with AD; if necessary, you can specify a different path.

After that, transfer the file to any PC from which you administer TrueConf Server, and upload it when [configuring LDAP mode](#).

15.9.3. Additional LDAP Parameters

Below you can find additional LDAP parameters and their purpose (user fields, filter rules, etc.). Depending on the chosen provider type, some parameters may contain pre-filled values (which can be reset if necessary).

If both the PBX and TrueConf Server are integrated with the same LDAP directory (such as Microsoft Active Directory), you can use additional fields to make user dialing easier. For instance, you can configure aliases in the LDAP directory and specify a field from the directory in **Additional → User Alias List**. During the import of users, their aliases will be retrieved and immediately available for use in the TrueConf system. So, it will be possible to make direct calls to users by their aliases without an additional mapping configuration. This option may be helpful

when a person has to use numeric aliases for quick dialing from SIP phones and SIP/H.323 endpoints.

- **Login** - username;
- **Display Name** - full display name;
- **First Name** — name;
- **Middle Name** - middle name / patronymic;
- **Last Name** - last name;
- **Email** — email;
- **Company** — organization name;
- **Branch** - branch name;
- **Department** - department;
- **Job Title** — position;
- **Manager** — manager's name;
- **Address** - user address;
- **Max Results** — the total number of pages returned in the search results (5000 is selected by default for all templates of LDAP providers)
- **Max Request Limit** — the number of pages returned by a single request (default for all templates is 1000), meaning this is the number of pages the server requests data from the LDAP directory until it accumulates **Max Results** results;
- **Filter Disabled** — indicates whether the user is enabled or not;
- **Group Member** — specifies which participants are in a specific group;
- **memberOf** — (*for Active Directory only*) the parameter which is responsible for linking an object to groups. It includes the list of group DN entries for each user (needed for filtering users by groups).
- **Filter Login** — search filter by login;
- **Filter CallID** — not used, retained for backward compatibility;
- **Filter Group** — the filter for searching by groups which prevents other objects with matching names from being loaded
- **Attr primaryGroupId** — (*Active Directory only*) group ID parameter;
- **Attr primaryGroupToken** — (*Active Directory only*) group token parameter;
- **Attr objectSid** — (*Active Directory only*) object ID parameter;
- **Attr SIP Phone** - SIP number for contacting the user;
- **Mobile Phone** — mobile number for contacting the user;
- **Work Phone** - work phone number for contacting the user;
- **Home Phone** — home (personal) phone for contacting the user;
- **User Status Attr** — an attribute that determines a user's absence status across different servers simultaneously;
- **User ID Attr** — an attribute that identifies the user's absence across different servers simultaneously by their ID;
- **Full ID Attr** — the attribute that determines the user's absence status across different servers simultaneously with the help of the full user ID (with the domain name included)
- **DetailedUserInfo Attribute** — overriding fields to be displayed in user information;
- **User Alias List** — the list of attributes that will serve as user aliases after authentication (they have to be separated with commas ,)

- **TrustPartner Attr** — *(for Active Directory only)* the filter that allows you to combine multiple domains into a trusted domain
- **FlatName Attr** — *(for Active Directory only)* the display name for the trusted domain, when multiple domains are combined into a trusted domain
- **TrustedDomain Filter** — *(for Active Directory only)* the filter that allows you to combine multiple domains into a trusted domain
- **ForeignSecurityPrincipal Filter** — *(for Active Directory only)* the filter that allows you to combine multiple domains into a trusted domain
- **Trust Enabled** — *(for Active Directory only)* the filter that allows you to combine multiple domains into a trusted domain
- **FilterClientSearchByLoginGroup** — (`boolean`) used for searching contacts in a client application. If this attribute is not specified explicitly, it defaults to `true` . Moreover, only the users who belong to the login group will be found. If set to `false` , it allows finding other users in the LDAP directory who, for some reason, are NOT yet part of the login group.
- **Use Avatars** — should be set to `1` for correct avatar loading in applications;
- **Allow Avatar Propagating** — should be set to `1` for correct avatar loading in applications;
- **AddressBook Refresh** — a timer (in seconds) for periodic caching of relationships between groups and regeneration of address books. When the timer expires, it is assumed that the request did not yield any search results.
- **Filter AddressBook** — a filter that can be used to create a user's address book;
- **TimeOut** — the time allowed for connection/request execution (in seconds). When this time elapses, it is assumed that the request did not yield any search results.
- **thumbnailPhoto Attr** - avatar;
- **jpegPhoto Attr** — avatar storage location;
- **Meeting Room Filter** - filter to obtain a list of conference venues (such as meeting rooms), used in conjunction with **Meeting Room Search Filter Attr**;
- **Meeting Room Search Filter Attr** — LDAP attribute that contains conference locations;
- **Meeting Room BaseDN** — not used;
- **LDAP Login with subdomain** - Allow users from subdomains to log in, where their login will be in the format `sub.domain\user` .

15.9.3.1. Additional phone numbers

For integration with Microsoft Active Directory (AD), it may be useful to specify multiple attributes for a single field. The thing is that AD can store several pieces of data under different attribute names, such as `mobile` and `otherMobile` . In such cases, to display multiple contact details of the same type in a contact card, you need to enumerate the required attributes separated by commas in the field under the **Additional** list.

For example, to display multiple phone numbers in a subscriber's card, specify the value `mobile,otherMobile` in the **LDAP Property Name** column for the **Mobile Phone** field.

For providers of a different type, this is not necessary because the directory service can already store multiple values separated by commas.

15.9.4. How to upload user accounts from different domains

1. The account used by TrueConf Server for authentication on the directory service should be given the right to read "Foreign Security Principals" objects from other domains and the right to authenticate on them.
2. You should use authentication type **GSS** or **Kerberos Keytab**.
3. On the primary domain that TrueConf Server will connect to, create a group with the scope (range) of **Domain Local**.
4. Move to this group the accounts of users (or user groups with the universal range; nested groups are supported only within a single forest) that you want to upload on the server.
5. Complete the steps 1 and 2 for all domains that will be used for uploading accounts.
6. In the LDAP settings, specify this group in the field **Path (distinguishedName)**.
7. Ensure that the **Advanced** block in the LDAP settings has the **Trust Enabled** parameter set to **1** (default value).

15.9.5. Certificate installation for LDAPS connection

To ensure connection via LDAPS, one may have to upload the root SSL certificate on the physical or virtual machine where TrueConf Server is deployed. This certificate should correspond to the domain where the domain controller server operates. To do it, copy the root SSL certificate of the domain to any directory on the machine with TrueConf Server.

Please note that the certificate has to be in the **.crt** format. So, if a different format is used, you will need to convert the certificate as it is described in [this article](#).

Next, install the **.crt** certificate depending on your OS:

For Windows OS

1. Double-click on the certificate.
2. In the certificate installation window that appears, click the **Install Certificate** button.
3. In the storage location selection window, specify **Local Machine**.
4. In the next storage setup window, select **Place all certificates in the following storage** and click **Browse**.
5. In the list of repositories, select **Trusted Root Certification Authorities** and click **OK**.
6. To complete the setup, click the **Next** and **Finish** buttons.

On Debian:

1. Run the following command in the terminal as the administrator:

```
sh  
cp /home/$USER/cert.crt /usr/local/share/ca-certificates && update-ca-certificates
```

where `/home/$USER/cert.crt` is the absolute path to the **.crt** certificate copied to the machine with TrueConf Server.

2. Restart the machine with TrueConf Server.

CentOS:

1. Run the following command in the terminal as the administrator:

```
cp /home/$USER/cert.crt /etc/pki/ca-trust/source/anchors/ && update-ca-trust
```

sh

where `/home/$USER/cert.crt` is the absolute path to the **.crt** certificate copied to the machine with TrueConf Server.

2. Restart the machine with TrueConf Server.

15.10. How to address typical issues when using LDAP

When LDAP is configured, some errors may occur while connecting to the directory service. In such cases, after you click on the **Apply** button which is in the connection parameters block, the corresponding notification will be displayed in the upper part of the screen. Below you can find some typical issues:

Error LDAP error 81 (Server Down)

No connection with the directory service. Most likely, TrueConf Server cannot access this service via the specified address and TCP port (**389** for the standard connection and **636** for the secure connection via LDAPS). To test the connection, you can use the console application **telnet** (available on Windows and Linux):

```
telnet [ldap-server] [port]
```

sh

where `[ldap-server]` is the address while `[port]` is the port of the server that acts as the domain controller. For example, if you need to test access via LDAPS, you need to run:

```
telnet ldap.example.com 636
```

sh

If there is no connection, it is necessary to check the network equipment settings or network-to-network software. One should also make sure that the server acting as the domain controller has been started.

Error LDAP error 49 (Invalid Credentials)

Unable to authorize on the LDAP server. Make sure to provide the correct service account data used for connection to the directory service (go to LDAP settings, the **Authentication** section).

Error LDAP error 53

This issue is typically due to policy restrictions set on the side of the directory service, for example, NTLM may be disabled for AD. You should also make sure that the **Base DN** field is correctly specified.

Error LDAP error -1

This error may occur when connecting to the directory service via the secure LDAPS connection. This problem may occur due to various reasons.

1. It is necessary to make sure that [the root SSL certificate](#) of the domain, which includes the domain controller server, is uploaded on the physical or virtual machine where TrueConf Server is deployed. When the certificate is uploaded, you can test the connection with the **openssl** program: run the following command in a Windows or Linux terminal:

```
openssl s_client -connect [ldap-server]:[port]
```

sh

where `[ldap-server]` is the address while `[port]` is the port of the server acting as the domain controller.

2. If TrueConf Server is deployed on Linux, and connection to Microsoft Active Directory has to be configured, make sure to specify the fully qualified domain name (FQDN) of the machine, where the domain controller server is deployed, in the **Domain** field. It should include the name of this machine, for example, `server-name.ldap.example.com`. In this case, FQDN should be used in the command testing SSL connection (check the previous step).

Connection has been established, but the list of accounts is empty

Make sure that the set of filters in the **Advanced** tab corresponds to the selected server type (Active Directory, OpenLDAP, 389 Directory Server). To switch to the corresponding attribute name after the server type is changed, click the **Default** button and configure required filters.

The users from the main domain are displayed, but the users from trusted domains are missing

Make sure that:

1. In section **Advanced** of the LDAP settings, parameter **Trust Enabled** is set to **1**.
2. The account used to connect to the domain controller server has read rights for the **member of** attribute from the **ForeignSecurityPrincipals** container.

15.11. Password and Lock Settings

15.11.1. Password Requirements

When using Registry mode in block **Password requirements**, you can specify the minimum password length (from 2 to 64) and the mandatory presence of certain characters (uppercase and lowercase letters, numbers, special characters) for your TrueConf Server users. These parameters will be checked when adding a new account and when changing the password for an existing one, including when the user edits it in their personal area:

Settings

[Help ?](#)

Password requirements

Minimum number of characters:

☒ Letters in upper and lower cases (A – Z, a – z)

☒ Digits (0 – 9)

☐ Special characters (` ^ ' ? ! * @ # % \$ & + . _ - = ~ , ; () [] < > { } / \)

Apply

Additionally, the password may include characters that cannot be set as mandatory, including emojis, such as: 🍷.

If the password does not meet the requirements, an error message will be displayed. Click on the [?](#) button (which is next to the input field) to view the password requirements:

Account information

Status ☒ Active **Disconnect**

TrueConf ID @video.server.name

Password Confirm [?](#)

The password does not meet the requirements

Password requirements ✕

The password has to contain:

- At least 5 characters
- Letters in upper and lower cases (A – Z, a – z)
- Digits (0 – 9)
- Special characters (` ^ ' ? ! * @ # % \$ & + . _ - = ~ , ; () [] < > { } / \)

OK

15.11.2. Automatic Lock

In the **Account lockout policy** section, you can enable the account lockout policy for those cases when a user enters an incorrect password during authorization.

Lockout settings are available both in [Registry](#) and [LDAP](#) modes. The lockout should be configured on the side of the video conferencing server; it is not related to AD/LDAP settings.

Account lockout policy

☒ Lock automatically

Account lockout duration:

Maximum number of failed login attempts:

Reset account lockout counter after:

Apply

Here, you can specify:

- account lockout period (a user can be [manually unlocked at any time in his/her profile](#))
- maximum number of failed login attempts
- time interval between unsuccessful login attempts (if the interval is larger than the specified value, the counter for unsuccessful login attempts will be reset to zero).

Let us consider the following example. Here, we will use these settings:

- **Account lockout duration** = **6:00**, meaning 6 hours;
- **Maximum number of failed login attempts** = **5**
- **Reset account lockout counter after** = **00:10**, which is 10 minutes.

If a user with an existing server login (TrueConf ID) makes five failed attempts to enter a password with less than 10 minutes between each attempt, the account will be locked for 6 hours. However, if there is a 10-minute gap after any attempt (e.g., after the 4th attempt), the counter will be reset to 1.

15.11.3. Display of fields from a user card

In section **Fields visibility**, you can select which profile fields of any user on your server can be viewed by different user types. Independent settings are available in the following columns:

- **Users of your server** — specify what your users can see when they view a contact card (information about another user) in the application or personal area;
- **Federated users** — what data participants of the [federated server](#) can view when accessing user contacts on your server;
- **Guest users** — what information about your users is disclosed to guests of public conferences (webinars).

In this case, the display name is always shown.

Fields visibility

Choose which fields of user accounts from your server will be visible to the following groups

☒ Users of your server	Federated users	Guest users
☒ TrueConf ID	☒	☒
☒ Email	☐	☐
☒ Name	☒	☐
☒ Last name	☒	☐
☒ Middle name	☒	☐
☒ Company	☒	☐
☒ Branch	☐	☐
☒ Address	☐	☐
☒ Department	☐	☐
☒ Job title	☐	☐
☒ Manager	☐	☐
☒ Mobile phone	☐	☐
☒ Work phone	☐	☐
☒ Home phone	☐	☐
☒ SIP number	☐	☐

Apply

In the case of [directory service integration via LDAP/LDAPS](#), this data is retrieved from the relevant attributes described in [section Advanced](#).

After configuring settings for users, you can install client applications for them and teach them how to connect to your server (read the [desktop application documentation](#)). This will conclude the [essential steps](#) required to launch the corporate messenger with TrueConf video conferencing!

16. Group conferences and broadcasts

This section enables server administrators to schedule conferences, invite participants, and set other parameters.

Such conferences can be launched automatically (at a specified time or according to a schedule) or manually by server administrators.

The free version of TrueConf Server Free has limitations on the number of simultaneous group conferences, which are detailed on the [solution page](#).

16.1. List of group conferences

This list includes the following events:

- events created by administrator in this section of the TrueConf Server control panel
- events added by users in the application or personal area
- created in the email plugin TrueConf;
- added with API commands from third-party scripts/applications
- active conferences created ad hoc in the client applications (they will disappear from the list when they end).

The screenshot shows the 'Conference List' interface. At the top, there is a 'Create' button (1) and a 'Help' link (2). Below these are search filters for 'Topic / CID', 'Owner', 'Participant', 'All modes', 'All types', and 'All sources'. The main table lists conferences with columns: Topic, Start time, Owner, Mode, Type, and CID (3). A 'Hide' button (4) is next to the CID column. The first row is highlighted in orange, indicating an ongoing meeting. To the right of the table, there is an 'Information' tab (5) showing details for the selected 'Meeting'. The details include Conference ID, PIN, Owner, Start time, End time, Recurrence, Reminders, Type and Mode, Recording, Meeting location, Source, and Integration (6). Below the details is a 'Conference Manager' section with buttons: Launch (7), Go to the conference page (8), Edit (9), View history (10), and Delete (11).

Topic	Start time	Owner	Mode	Type	CID
Brainstorm	Without sch...	Amanda W...	All on screen	🔒	\c\3662477...
Meeting	25.08.2023 ...	Jane Flowers	Role-based	🔒	\c\meeting
Webinar	29.08.2023 ...	Abe Chester	Role-based	🌐	\c\0699653...

Meeting Details:

- Conference ID: \c\meeting
- PIN: 453861
- Owner: Jane Flowers
- Start time: 25.08.2023 18:25:00
- End time: 25.08.2023 19:25:00
- Recurrence: Occurs every week: Fri
- Reminders: 15 min before
- Type and Mode: Private, Role-based 6x290
- Recording: Scheduled
- Meeting location: Main office
- Source: TrueConf
- Integration: Available options

Conference Manager:

- Launch
- Go to the conference page
- Edit
- View history
- Delete

Ongoing meetings are **always** displayed in the upper part of the list and are highlighted in orange.

Here you can do the following actions:

1. [Add a group conference](#).

2. Filter the list by the name (or ID) of the selected conference, as well as by its owner, any participant, mode, access type, or source ([more about sources](#)).
3. The conference card can be minimized; in this case, the control panel with multiple buttons will be displayed instead (the buttons on the panel will vary depending on the conference status, either active or inactive). The actions available for each scenario will be described below in more detail.
4. View information about the selected conference: its name, [ID \(unique identifier\)](#), PIN code (if set), owner's name, link to its web page, email reminders (if added), location (if specified), mode and launch type, source of its creation (TrueConf or mail plugin), and whether video recording is scheduled.
5. Open the list of invited participants.
6. Click on the link to get the HTML code of the widget needed for [embedding the conference on external websites](#). It will be available only for webinars (public online events). If you have [set a streaming configuration](#) for the webinar, the corresponding link will be displayed below the widget code:

Integration ✕

Use this code to embed the conference in external website:

```
<iframe allowfullscreen="allowfullscreen" width="720" height="405"
allow="microphone; camera; autoplay; display-capture"
src="https://server.company.com/c/webinar"></iframe>
```

Copy stream URL:
`rtsp://server.company.com/c/webinar/`

Ok

7. Start the conference manually. Before the start you will be offered to invite all the participants to the conference or select particular users. At conference forced start, only online users will be invited to the conference. Email invitations will not be sent out.
8. Go to the [conference page](#).
9. Edit the selected conference (unavailable for an ongoing meeting). In the conference editing menu, you can use almost the same group of features that are available when a [conference is created](#).
10. View the launch history of this conference in the [Call History section](#).
11. Remove selected conference.

16.1.1. Conference Sources

To make searching for events easier, we introduced a special filter based on the source of a conference. Conferences can be created in various ways, and accordingly, there are the following options for filtering the list of events by source:

- **TrueConf** — events created:
 - In the control panel, in the user personal area, in the application scheduler
 - "On-the-fly" in a client application (quick conferences)
 - using the secret API token from section **Web →Security**;

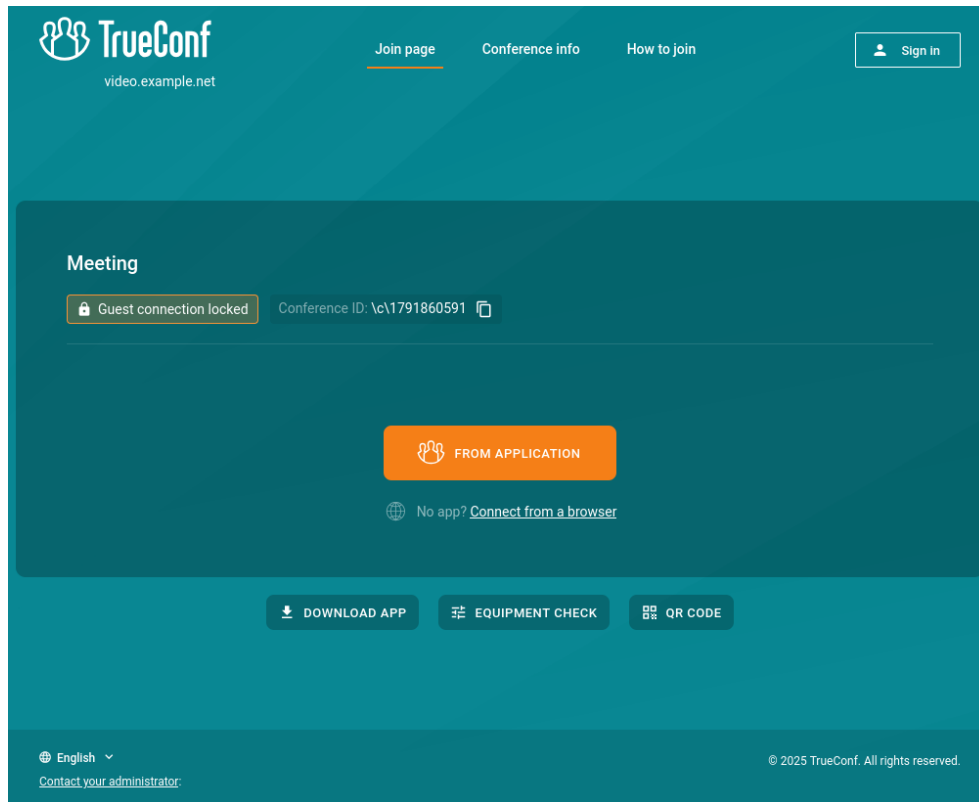
Please note that we do not recommend using this API token. It is safer to create [OAuth applications](#) with the necessary permissions for each task.

- **Email client** - conferences created through [email plugins](#);
- **OAuth applicayion** — conferences created using OAuth applications (see [API documentation](#)).

16.2. Conference Page

The conference page contains the main information about the event and some additional elements depending on the settings:

- Registration button if the conference is public (a webinar) and participants are allowed to sign up for the event on their own
- If the event is scheduled for a specific time, a countdown timer will be displayed along with a button to add the conference to the calendar
- Buttons for joining the conference from a browser or application if this event has already started or if it is a [virtual room](#).



Please take into account the specifics of [joining a webinar with registration](#) for SIP/H.323 endpoints, server users, and federated participants.

If the client application has already been installed, it will connect to the conference in the following way:

1. The application will try to connect to the conference with the authenticated user account (regardless of the name entered on the conference web page).
2. If the conference was created on a different TrueConf Server instance, the application will try to connect to the conference via federation.
3. If there is no connection via federation, the user will join the conference as a guest and then, when the conference is over, authorize automatically on the local server.

For more details on the ways to connect to a conference, refer to the [relevant article](#).

16.3. Saving guest connection data

There are several convenient features available to the guests who join webinars:

- The temporary internal ID (login) created for a guest is bound to the browser and client application (this ID may be displayed, for example, in the connection list on the [page of a session](#)). The guest ID will change if a different application is used (e.g., if a user signs in on a different device), if a different browser is used, or when connecting in incognito mode in the browser.
- Since the ID is saved, it is possible to gather accurate data about the number of participants and other metrics for reports and analytics.

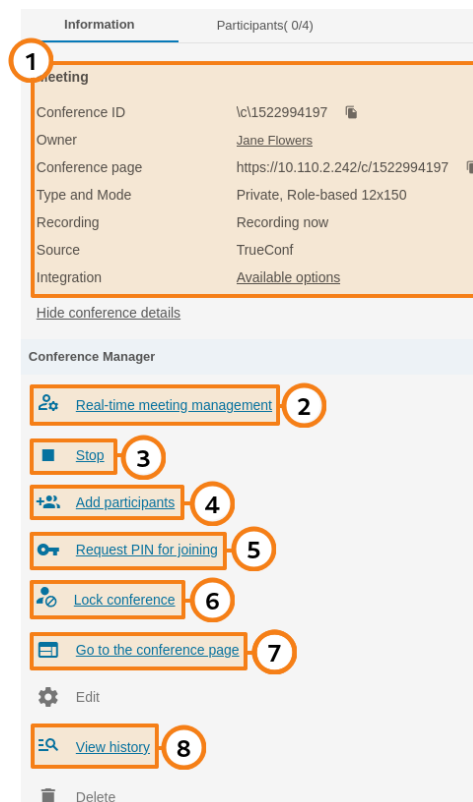
- If a user is suddenly removed from a conference (e.g., if connection is lost) or if the user leaves the conference and then decides to join the meeting again, he/she will see all chat messages, even though these messages were sent when the user was not connected to the conference.
- Thanks to saving the ID, you can leave the conference, quickly change the display name, and join the meeting again (for example, if a typo was made or the name which was entered previously does not meet the requirements set by the administrator). All messages sent under the previous name will also be displayed to all other participants with the new sender's name.

16.4. Managing an ongoing conference

When selecting an ongoing conference, the administrator can view information about it or change some of its parameters (e.g., the layout or PIN code). Standard editing and deletion options will be unavailable.

16.4.1. The "Information" tab

Display conference information and the control buttons:



1. A section with basic information and options for [integration with external websites](#).
2. Switch to [real-time meeting management](#).
3. Stop the meeting for all participants.
4. Clicking the **Add participants** link will open the user selection dialog:

Select participants X

Users Aliases Emails Selected (0)

Q Enter user's name, ID or phone number

 Max Tree max@server.company.com	 Sarah Nelson nelson@server.company.com
 Ann Branson ann@server.company.com	 Bill Bush bill@server.company.com
 Joe Smith joe@server.company.com	 Niro Wolf wolf@server.company.com

Select All Call Cancel

To add participants to the conference, select them on the **Users** tab. You can select all server users at once by clicking the **Select All** button. On the **Aliases** and **Emails** tabs, you can add a participant using their [alias](#) and [send](#) an invitation via email by specifying the email address and the name that will be displayed in the conference. The resulting list is displayed on the **Selected()** tab. After forming the list, click the **Call** button at the bottom of the window.

5. Changing or disabling the PIN code for conference entry. If secure entry is disabled, it can be activated by clicking **Request PIN for joining**.

6. Locking a conference. In this case, a conference can be joined only by moderators (including the owner) and the users invited after the conference was locked. If a regular user was added to the list of invited participants, but could not join the meeting before it was locked, he/she will be unable to join. If a public conference is held, guests will be unable to join and it will be impossible to send email invitations.

Each time when a conference ends, its access status is switched to **unlocked** which is the default value.

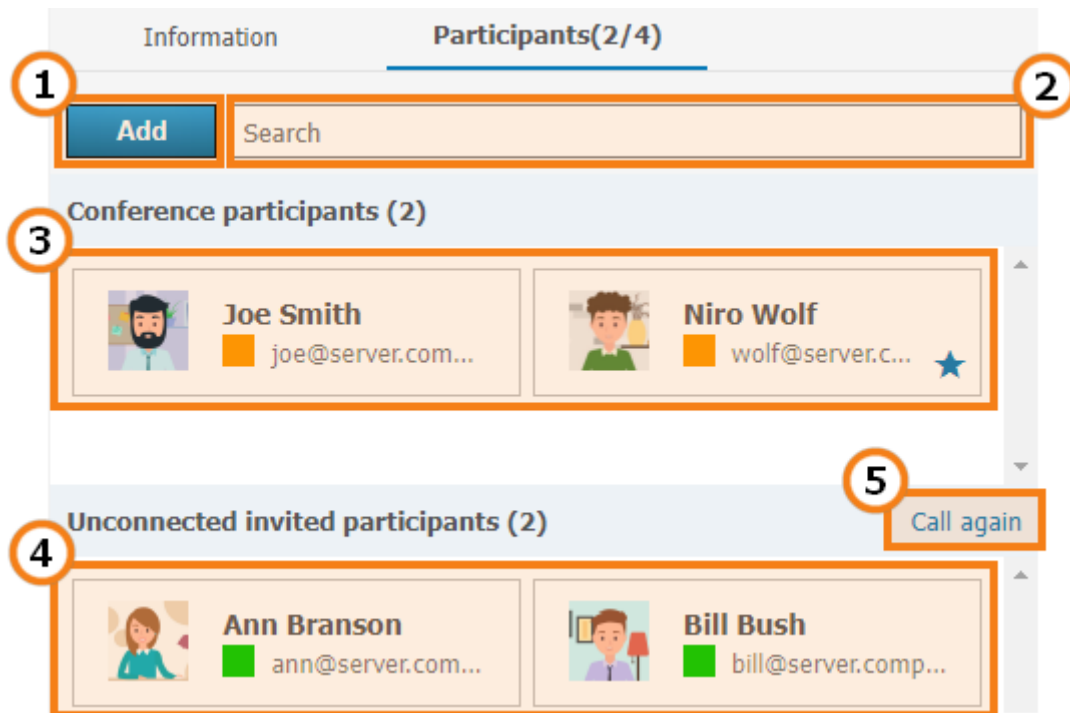
7. Go to the [conference page](#).

It is also possible to set a PIN for a conference or lock it in the real-time meeting management tool.

8. View the history of this conference's launches in the [section Call History](#).

16.4.2. The "Participants" Tab

Information about invited participants and those who have already joined the meeting:



1. Opening the [user selection dialog](#).
2. Quick search for participants.
3. The list of participants who have successfully joined and are present in the current meeting.
4. Users who have been invited to a meeting, but have not joined it yet.
5. To invite all participants who have not yet connected to the conference, click on the link **Call again**, and in the window that opens, click the **Invite** button.

16.5. Editing a conference

When selecting any non-started conference from the [general list](#), the server administrator can go to edit it. The options for modifying conference parameters will depend on whether [integration with corporate email through TrueConf Calendar Connector](#) is used:

- If there is no integration with the corporate calendar or the conference was not linked to an event (for example, the meeting was created before the integration was set up), you can set the same parameters that are available when [an event is created](#).
- If the server is run in integration with the corporate calendar and the conference was created as part of an event (refer to the TrueConf Calendar Connector documentation), editing capabilities will be limited:
 - it will be impossible to turn this meeting into a scheduled conference (calendar interaction supports only virtual rooms)
 - the sections related to conference ID, email invitations and reminders, time extension, and meeting location will be hidden
 - you will not be able to add or remove anyone from the participant list
 - it will be impossible to change the conference owner.

Server status: **running, registered**

clndr2111.trueconf.name#vcs

System

Dashboard
Summary
PRO licenses
Settings
Network
Network settings
SMTP
Federation
Gateways
SIP
H.323
RTP
WebRTC
Transcoding
Web
Settings
Security
HTTPS
Users
User accounts
Groups
Aliases
Authentication
LDAP / Active Directory
Settings
Group Conferences
Conferences
Templates
Streaming
Settings
Chats
Surveys
API
OAuth2
Reports
Events
Call history
Chat messages
Configuration changes
Conference recordings
Endpoints
File storage
Recordings
Manage add-ons
TrueConf Directory

Conference

General Participants(1) Layout Media Interpretation Advanced

You are editing the conference linked to a calendar event

Conference name
CEO speech

Owner
Joe Smith CEO
joe_smith_chief@clndr2111.tr...

Conference mode
Smart meeting
Everyone can see and hear participants when they start speaking 16x100

Date and Time
Virtual room
A conference available to participants at any time

☐ Guest participants
Anyone can join the conference via the link

☒ Waiting room
Participants will join the conference only after approval by the owner or moderator
Who is put in the waiting room?
Uninvited participants

☐ PIN when joining
PIN will be required for joining the conference

☐ Conference video recording
Video recording will be turned on automatically when the meeting starts

☐ Conference transcript
Transcription is activated when the conference starts.

Save as a template

CANCEL SAVE

You can set other parameters for scheduled event conferences just like for regular ones, for instance, enable [recording](#) or [audio transcription](#) in the **General** tab.

16.6. Creating a New Conference

By clicking the **Create** button in the **Conference List** menu, you will access the configuration of the most frequently used settings on the **General** tab.

It is also possible to create a conference from one of the [templates saved earlier](#).

In addition to the conference settings listed below, a background and/or watermark can be added to its video layout. These are selected for all events in section **Gateways → Transcoding → Visual settings**.

16.6.1. The "General" tab

The **General** tab at the top contains the parameters required to create a conference:

Conference [Help ?](#)

General Participants(0) Layout Registration Media Interpretation Advanced

Conference name

Owner

[SELECT](#)

Conference mode

 **Smart meeting**
Everyone can see and hear participants when they start speaking 16x110 >

Date and Time

[Scheduled](#) Without schedule

Start  25.07.2025 09:30

Duration  01:00 Ends at 10:30

☐ Weekly recurring meeting

 Athens (UTC+02:00) ▾

1. **Conference name** — for example, "Marketing Department Meeting".
2. **Owner**, [see detailed role description](#).

When scheduling a conference, the administrator selects the owner (who is automatically given the moderator role) and other moderators. The remaining roles are given to users during the conference.

3. **Mode conferences**: everyone on screen, smart meeting, moderated role-based conference, video lecture. Simply click on the line with the current option to select a new mode.

The logic of filling the video layout in [smart meeting](#) mode with various connection types is explained in detail in the [client application documentation](#) TrueConf.

For moderated role-based conferences and smart meetings, you can specify the number of [speakers](#).

The maximum number of participants in a [moderated role-based conference](#) and smart meeting depends on your license type. The number of participants can reach **2000**. The maximum number of [speakers](#) in a smart meeting or moderated role-based conference is **49**.

4. In section **Date and Time**, specify the [conference launch type](#): either unscheduled (virtual room) or scheduled. If scheduling is selected, specify the time for a one-time or recurring conference launch. On the [tab Additional](#), you can also configure extension settings for the scheduled conference.

Below you can find access settings, server-side recording settings, and the parameters for speech recognition (available if the [integration with the AI server is configured](#)):

☒ **Guest participants**
Anyone can join the conference via the link

☐ **Waiting room**
Participants will join the conference only after approval by the owner or moderator

☐ **PIN when joining**
PIN will be required for joining the conference

☒ **Conference video recording**
Video recording will be turned on automatically when the meeting starts

☐ **Create a conference transcript**
Transcription is activated when the conference starts.

Select a language for transcribing the recording:

English ▼

To make the conference [public \(create a webinar\)](#), check the box **Guest participants**.

The maximum number of webinar guests is determined by your license (within the overall limit depending on the conference mode). There are specific [guest number limitations](#) for TrueConf Server Free.

Learn more about webinars in our articles and videos:

- [What is a webinar?](#)
- [Tips for organizing secure webinars](#)
- [Webinar Guide](#)
-
-

To activate the [waiting room](#) for an event, check the corresponding box. You will be able to select which category of participants will be directed to this room. The list of participants, who can be put in the waiting room, varies slightly for private and public conferences.

SIP/H.323/RTSP connections are always treated as the participants from other servers. For example, if an endpoint makes a call to a conference or is invited to this meeting, it will be directed to the waiting room if all the settings are activated except **Guests only** for a webinar.

It is not possible to select the participants who will be directed to the waiting room, if [registration is allowed](#) for a public conference (webinar). In such a case, all participants except the owner and moderator will be directed to the waiting room if it is enabled.

Categories that can be selected for public conferences:

- **All participants (except the owner and moderators) – *everyone except the moderators and the owner***, including registered participants, will be placed in the waiting room;
- **Uninvited participants and guests** (selected by default) – the following ***will enter*** the waiting room:
 - all users from your server, who were ***not invited in advance*** before the start of the conference and are now calling the conference/owner or are invited after the start of the event
 - all users from a [federated](#) server who were ***not invited in advance*** before the start of the conference
 - all guests.

The following participants ***will not be moved*** to the waiting room:

- users from your server who were ***invited in advance*** before the start of the conference
- users from a [federated server](#) who were ***invited in advance*** before the start of the conference
- users who signed up for the conference (since they have already been added to the list of invited participants)
- users from your server and federated server who were ***invited in advance***, but did not join when the conference started and are now trying to join during a conference or receive another invitation call.
- **Uninvited participants from other servers and guests** – Only guests (except those who registered) and ***not pre-invited*** users from the federated server are placed in the waiting room.
- **Guests only** – Only guests are directed to the waiting room (except for those who have registered).

Categories that can be selected for private conferences (the rules are similar to the ones set for webinars except guests and unregistered participants):

- **All participants (except the owner and moderators);**
- **Uninvited participants** (selected by default);
- **Uninvited participants from other servers.**

If necessary, you can save conference settings as a template so that you could later create an event with the same settings in one click. To do it, check the box **Save as a template** at the bottom of the conference editing window.

Check the box **PIN when joining** to enable the use of a PIN for joining the conference. This will enhance security by protecting against unauthorized participants even if they have the link, such as during a webinar. When the checkbox is selected, a PIN will be automatically generated, but

you can change it in the field below or regenerate it using the button . PIN protection is not available when registration for a public conference (webinar) is enabled.

To directly connect from an SIP/H.323 endpoint to a PIN-protected event, add the PIN code separated by a comma after the conference ID in the call string:

```
00<conf_id>,pin@<server_address>:<port>
```

Check the **Enable conference recording** box to save a recording of the event on the server side (see the description in [section Recordings](#)). If this feature is enabled, the information will be displayed on the [event page](#), and the owner can manage the recording (pause and resume) in real-time during the conference. To ensure all participants (including those on SIP/H.323 terminals and in the browser) see that the event is being recorded, activate the indicator in section **Recordings**.

If your TrueConf Server [is integrated with the TrueConf AI Server solution](#), you will be able to override certain settings for a specific conference:

1. If the "on demand" recognition option is set in the [general inclusion settings](#), you can use the checkbox **Create a conference transcript** to save the audio track of this event for AI processing.
2. Below you can select the main language of the event, which will help the AI server in difficult speech recognition situations. The language is detected automatically, but some languages may be similar in terms of pronunciation, and under such circumstances, it is useful to explicitly specify the main language of the conference.

16.6.2. The "Participants" Tab

The **Participants** tab displays the number of participants added to the conference (the maximum possible number of participants depends on the conferencing mode and your TrueConf Server license. You can add participants to the conference from the list of users, by ID, by call string (for SIP/H.323/RTSP devices), and by email (for public conferences).

Add by ID or call string

Enter the user ID or call string for a SIP/H.323 or RTSP device in the search field on the **Contacts** tab and click **Select ID** to add it as a conference participant.

Adding email notification recipients

This feature is available only in public conference mode.

To invite participants via email, create a list of meeting guests:

1. Go to the **Email** tab.
2. Fill in fields **Name** and **Email** with the participant's information.
3. Click **Select** to add a user to the list being created.

After selecting all users, click **Add** to add them to the conference participant list.

Add participants (3 / 450)

×

Contacts

Selected(3)

Enter a user's name/ID or an endpoint ID

[How to add endpoints](#)

Groups

Ann Smith

ann@server.company.com

Bill Bush

bill@server.company.com

Bob Dimitrescu

bob@server.company.com

Carlo Parento

carlo@server.company.com

Elle Stanton

elle@server.company.com

CANCEL

ADD(3)

16.6.2.1. How to assign a newly added participant as a moderator

1. Select a user from the list of added conference participants and click three dot button.

2. Click **Assign as a moderator**.
- Conference

[Help](#) ?

General

Participants(4)

Layout

Media

Advanced

Number: 4 / 160

+

Search

Abe Chester

chester@video.example.com

Albert Moore

moore@video.ex...

Alice Campbell

campbell@video.example.com

Ana Bai

baros@video.example.com

×

Assign as a moderator

A participant designated as a moderator is marked with a star icon: .

A moderator can be selected not only from the users of your server but also from the users registered on [other servers \(federated\)](#). Guests cannot be appointed as moderators.

© 2010-2026 TrueConf LLC. All rights reserved. www.trueconf.com

178

16.6.2.2. Resend email invitations

Sometimes it's necessary to resend the invitation for a scheduled event to only certain participants. To do this, go to tab **Participants**, hover over the desired participant, and click on them with . In the menu that appears, select **Resend invitation email**.

Emails are not sent immediately; they are sent **only when conference settings** are saved. So, if you change your mind, you can select the participant again and click  to cancel the email invitation for this person.

16.6.3. "Interpretation" Tab

TrueConf Server supports conferences with simultaneous interpreters. Thanks to this feature, the users, who speak different languages, can take full part in an event without missing any important details. Each participant can select the language of the presentation [in a client application](#) or in a browser (depending on the preferred connection method). The number of interpreters is limited only by the number of participants.

Check the box **Language interpretation mode** to create a conference that can be assisted by simultaneous interpreters. When a conference with simultaneous interpretation is recorded, several audio tracks will be created: a general track and separate tracks for each of the languages selected for interpretation.

Interpreters are selected either from the users, who were previously added to the list of participants, or from registered guests (in the case of a webinar). Just click the **Add interpreter** button and select the language pair for translation. In the example below, the **English - Spanish** pair is selected. The interpreter will be able to change the translation direction during the event in his/her TrueConf application:

Conference

[Help ?](#)

General	Participants(4)	Layout	Registration	Media	Interpretation	Advanced
☒ Language interpretation mode						
Source language volume in interpreter channels						
30%						
Interpreters						
+ ADD INTERPRETER						
 Amanda White white@video.example.net Language 1 English Language 2 Spanish						
 James Wolf wolf@video.example.net Language 1 Chinese Language 2 English						

As an interpreter, you can add a user from your TrueConf Server, a user from a [federated video conferencing server](#), or guests of a scheduled public conference who manually signed up for this

event if [registration was required](#). Other participants, such as guests added manually via email, cannot be appointed as interpreters. Interpreters are not displayed in the video layout, and their video cannot be turned on during a conference (video settings are unavailable).

In this way, you can select several interpreters, including for the same language pairs (for example, one of the interpreters can rest while the other one works with the same languages). At any given time, only one person can interpret the selected language pair in one direction. For instance, only one person will be able to translate from English to Hindi, however, the second person can translate from Hindi to English.

In interpreter channels, participants will be able to hear the original audio track: its volume level will be set at 30 % by default. However, you will be able to reduce the volume level to 0 % (i.e. mute the track).

Please note that you can organize "relay translation" so that multiple interpreters can translate language pairs sequentially one after another for a wider audience. Read more in the [client application documentation](#).

16.6.4. The "Video Layout" Tab

In addition to the settings specified in the **Layout** tab, a background and/or watermark can be added. These are configured for all events in the **Gateways → Transcoding → Visual settings** section.

Keep in mind that to optimize screen space usage, TrueConf mobile client applications disregard video layout settings and display the layouts in their own style on multiple screens (more details on this topic can be found [here](#)).

16.6.4.1. General list of video layouts

In the **Layout** tab, you can set up one or more [conference layouts](#) (arrangement of participants' video windows). For more details about the types of video windows and their functionality, refer to the [user documentation](#) TrueConf Server.

The video layout can be one of three types depending on the category of participants for whom it is created: general (for all participants), individual for a specific participant (including a separate SIP/H.323 endpoint), or the common layout for [SIP/H.323 devices](#) and browsers (WebRTC).

Configuring the video layout is not available for the [video lecture](#) mode. In [smart meeting](#) mode, there must be at least 2 video windows of the "active speaker" type.

The list of layouts will be displayed if you previously created layouts for the event. When the mouse is hovered over any of them, you will see the buttons for editing the layout name  and deleting the layout . The checkbox on the left side of each layout will determine whether this layout should be selected as the main one in its category at the start of the event:

Conference

[Help](#) ?

GeneralParticipants(8)LayoutRegistrationMediaInterpretationAdvanced

+ ADD LAYOUT

Filled podiums: 9 out of 49 ?

⚙

For all +

Layout #1

8 video slots

Layout #2

8 video slots

For SIP/H.323 and WebRTC +

Layout #1

8 video slots

In the general list of conference layouts, you can configure display settings for video windows of the **Time-based shuffling** type. To do it, click the button  in the top right corner of the list. These settings will apply to all windows of this type in all layouts of the conference. You can choose the order of displaying participants who were not added to the layout. Besides, it is possible to select the type of shuffling (rotation) and set its speed.

Shuffling settings

×

Shuffling order

From 1 to 36From 36 to 1

Participants get shuffled from smaller to larger slot numbers

Shuffling type

ReplaceMove

1

2

3

4

5

6

Shuffling interval (sec)

30

CANCEL

APPLY

© 2010-2026 TrueConf LLC. All rights reserved. www.trueconf.com

181

16.6.4.2. Video Layout Editor

If the list is empty, you will first need to choose the category of participants for whom the layout will be created: a general layout (for all participants), an individual layout for a specific participant (including an SIP/H.323 endpoint), or the layout for all [SIP/H.323 devices](#) and browsers (WebRTC).

Conference

[Help ?](#)

General	Participants(8)	Layout	Registration	Media	Interpretation	Advanced
---------	-----------------	--------	--------------	-------	----------------	----------

Create the first layout

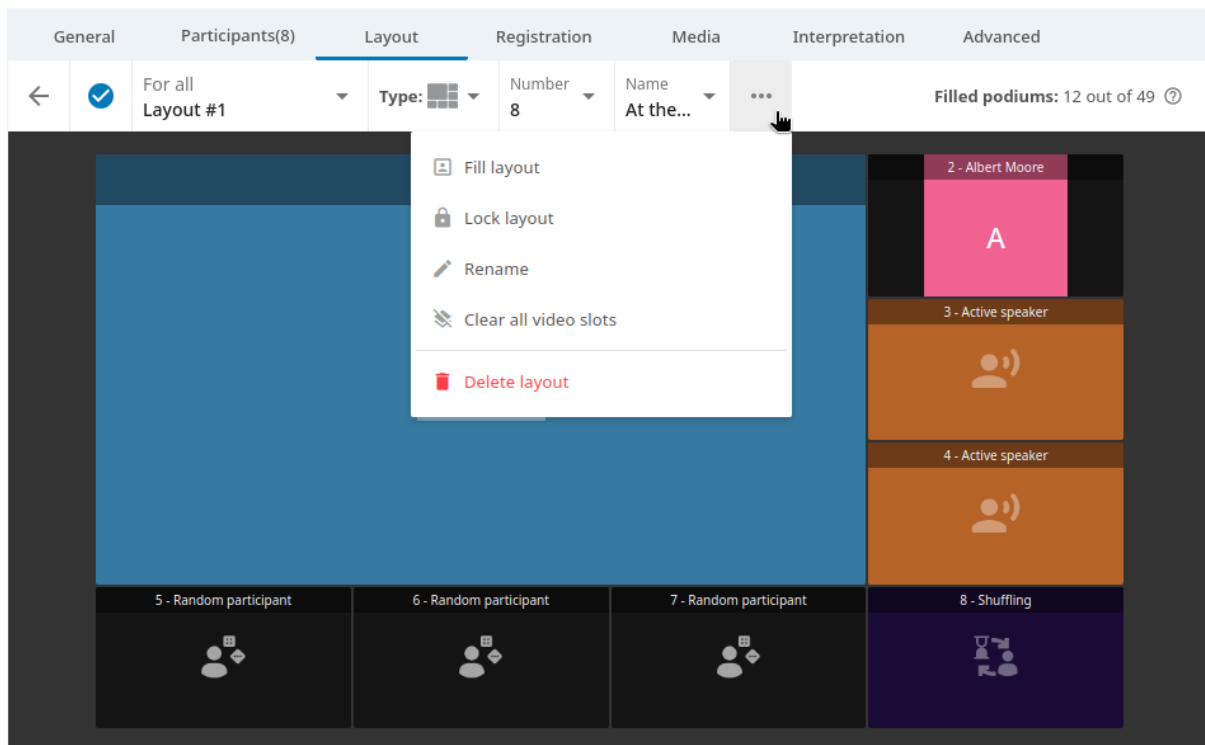
 **For all**
The layout will be displayed to all conference participants

 **For SIP/H.323 and WebRTC**
The layout will be displayed to IP telephony users, video conferencing endpoints, and participants who join from a browser.

 **For participants**
For an individual participant or a group of participants

After adding a video layout, you will see the pop-up window where the layout can be edited:

Conference

[Help](#) ?

1. Edit the conference video layout. You can move a participant's video window and select it as the priority window by double-clicking on it. Clicking on any video window allows you to choose its type: **Fixed**, **Random**, **Time-based shuffling**, **Active speaker**, **Content**.
2. If the box ☒ at the top of the editor is checked, this video layout will be used by default when the conference starts (this box is checked automatically for the first layout in each category). Click on this box to disable activation of this layout at the beginning of the conference.
3. You can add a new video layout directly from the editor by clicking the dropdown next to the layout name and selecting **Add layout**.
4. In the **Type** dropdown list, select the video window arrangement in the video layout.
5. In the drop-down list **Number**, select the number of windows in the video layout.
6. In the **Name** dropdown list, specify the position of the username in the video window.
7. Click the **...** button to proceed to the next items:
 - **Fill layout** — allows you to automatically fill slots in the video layout with invited participants; you need to clear the layout before using it.
 - **Lock layout** — in this case, participants will be required to use this layout when it is activated and will be unable to change it locally. This option is especially useful for connections via third-party SIP/H.323 protocols since endpoints often have fewer options for managing slots.
 - **Rename** — assign a convenient name to the video layout (up to 70 characters) for quicker identification in the [general list](#);
 - **Clear all video slots** — completely clear the video layout to start filling it again;
 - **Delete layout** — deletes the selected layout. If the deleted layout was set as the main layout for its category (e.g., for everyone), a different layout will not automatically become the main one after deletion. It has to be selected manually.

16.6.5. "Media" Tab

In this tab, you can set limits on video stream quality for different directions:

- in block **Limits for participants** — for incoming streams to the server from participants of all connection types;
- in block **Transcoding** — for outgoing streams from the server via third-party protocols.

Conference [Help](#)

General Participants(1) Layout Registration **Media** Interpretation Advanced

Limits for participants

Limits for video streams outgoing from conference participants

☒ Use custom settings

Video 720p

FPS (Video) 30

FPS (Content sharing) 30

Transcoding

☒ Use custom settings

FPS 30

Recording 720p

SIP/H.323 720p

RTSP 1080p

WebRTC 1080p

☒ Do not display self-view in video layout for H.323 and SIP endpoints
CPU load can significantly increase if this option is enabled

☐ Do not display self-view in video layout for WebRTC participants
CPU load can significantly increase if this option is enabled

☐ Do not display content from the second stream to SIP/H.323/WebRTC participants
CPU load can significantly increase if this option is enabled

☐ Automatically spotlight active speaker window

You can set custom quality parameters for video streams **incoming** to the server from all participants in a given conference: client applications, browser participants via WebRTC, and connections via SIP/H.323/RTSP. To do it, check the box **Limits for participants → Use custom settings** and select values in the drop-down lists. The frame rate limit for content sharing applies when content is displayed in a participant's window and not in a separate stream. So, the quality limit is the same for a participant's video window, but you can specify different frame rates depending on whether the speaker or content is being displayed.

The settings of block **Transcoding** mirror those in [section Gateways → Transcoding](#), except for the GPU acceleration option (it is configured once for the entire video conferencing server). Check the box **Use custom settings** to override resolution parameters at the conference level independently for each stream: SIP/H.323 terminals, WebRTC connections, recording, and streaming. The frame rate is set as a whole. Below are additional layout configuration settings, which are activated if explicit layouts are not specified for SIP/H.323/WebRTC participants when [scheduling a conference](#) or in [real-time meeting management](#).

16.6.6. The "Advanced" Tab

If necessary, you can set up additional conference settings in the **Advanced** tab.

The content of this tab will slightly differ depending on whether the conference is public or private (i.e., based on the state of the **Guest participants** checkbox on the [the General tab](#)):

- If a conference is private, you will be able to configure access for users who were not added to the list of invited participants.
- If a conference is public (webinar), you will be able to [set restrictions for guests](#).

16.6.6.1. ID, participant and broadcast management

Set the ID and security parameters for the conference:

Conference

General	Participants(2)	Layout	Registration	Media	Interpretation	Advanced
---------	-----------------	--------	--------------	-------	----------------	----------

Connection settings

Conference ID
5901667896

☒ Enable uninvited users to join the conference

Participant management

☒ Mute participants on entry

☐ Stop participants' video on entry

☐ Disable audio remarks

Streaming

☐ Enable streaming

Select a preset

1. Manually specify the conference ID to simplify participant connection. This option may be disabled for all conferences in the [section Group conferences →Settings](#).
2. Check the box **Enable uninvited users to join the conference** if you want to allow users not in the [predefined list of participants](#) to join the event (for internal conferences only).
3. Choose if it is necessary to automatically turn off the cameras and microphones of all participants when they join the conference. If needed, you can also disable audio remarks for participants (this option is available only in a moderated role-based conference).

On/off flag for camera and microphone is now ignored by SIP/H.323 endpoints when connecting to a conference to improve compatibility with smart meeting mode.

4. Below, you can enable conference streaming. To do this, select a pre-prepared streaming template from the dropdown list (see the description in section [Streaming](#)).

Please note that stream templates can be created only in the TrueConf Server control panel. In the scheduler users will only be able to select one of the predefined templates.

16.6.6.2. Connection methods, MCU mode, UDP Multicast

Configure the required parameters:

CONFERENCE JOIN OPTIONS

- ☒ Use custom settings
 - ☒ Client applications
 - ☒ WebRTC
 - ☐ QR code
 - ☐ SIP/H.323 endpoints

MCU MODE

- ☐ Enable MCU mode
 - Ensures the maximum video quality for SIP/H.323 and WebRTC participants.
 - Unavailable for connection from client applications**

UDP MULTICAST

- ☐ Turn on UDP Multicast

IP address
224.0.1.224:4000-6000

1. You can bypass [general settings](#) and select connection methods for the current conference. For example, if the license limits the number of connections through the gateway and no connections from endpoints are expected, this method can be completely disabled. Please note that this option will be unavailable when MCU mode is activated.
2. In regular conferences, SIP/H.323/WebRTC/RTSP streams from participants are transcoded on the server side into SVC streams for optimal distribution among other participants. If TrueConf applications will not be connected to the conference, this transcoding is not necessary and you can check the box **Enable MCU mode**. In this case, stream processing on the server will be optimized for handling streams without SVC support, and participants will not be able to choose a connection method. They will be able to join the conference **only** from a SIP/H.323 endpoint or browser; it will also be possible to connect an RTSP camera. Please note that if you activate MCU mode and then disable this option, the list of available connection methods will not be restored to its previous state. In other words, you will need to check the boxes for client applications and the QR code manually.
3. If necessary, enable UDP Multicast mode, more details on this mode are provided in the [description of extensions](#). This feature will allow you to increase the number of speakers regardless of the number of podiums. For example, you can create a moderated role-based

conference or smart meeting for 2000 participants and 36 podiums for speakers. However, there are many limitations listed below.

If UDP Multicast mode is enabled while you are trying to connect to the conference using third-party protocols (WebRTC, RTSP, SIP, H.323, etc), video conference recording and streaming will be unavailable.

Enabling this function is recommended **only** for those users who have hands-on experience in the sphere of network administration. Please note that it is your responsibility to check if this technology is available in your network.

If your network equipment is not configured to work in UDP Multicast mode, participants will see only a black screen during a conference.

4. If UDP Multicast mode has to be activated, specify the multicast/broadcast IP address. By default, this field is filled with the value **224.0.1.224:4000-6000**.

16.6.6.3. Sending invitations and extending the conference

It is possible to activate automatic email invitations to a scheduled conference and allow time extension for this event:

Conference

General	Participants(1)	Layout	Registration	Media	Interpretation	Advanced
Invitations						
☒ Send email invitations to conference participants						
Conference time extension						
☒ End the conference automatically according to the schedule						
☒ Enable conference time extension						
☒ Remind me 10 min before the conference ends						

1. Enable email invitations that will be sent to conference participants (activated by default). This option is available only for scheduled conferences if [integration with an SMTP server](#) is set up.

When editing a previously created conference, this checkbox will be cleared regardless of the settings used during its creation. This is done specifically to prevent accidental re-sending of invitations when editing the event. If you need to reactivate the sending of invitations for the conference (for example, when adding participants), manually check the box **Send email invitations to conference participants**.

2. By default, a scheduled conference will not automatically end when the [allocated time](#) expires. However, you can enable automatic termination of the event by using checkbox **End the conference automatically according to the schedule**. In this case, checkbox **Enable conference time extension** will become available to allow moderators to extend the event. This action will be available in the personal area, real-time meeting management within the applications, as well as through a button in the notification about the upcoming end of the event (if activated, see below).

1. You can configure notifications about the upcoming end of the event (see above) using checkbox **Remind me 10 min before the conference ends**. The notification time can be adjusted in the dropdown list. This option is available only for a scheduled conference. All moderators will see the notifications, not just the owner.

A scheduled conference without a time limit will automatically end when [certain conditions are met](#).

16.6.6.4. Conference setup

In section **Visual settings**, you can configure the conference background and watermark settings.

The same options are available as in the [section Gateways → Transcoding](#), with one difference: you can use the general settings or specify different ones for a particular conference.

16.6.6.5. Reminders and Description

Below you can find the settings for conference reminders and description:

Conference [Help](#) ?

General	Participants(8)	Layout	Registration	Media	Interpretation	Advanced
Reminders ☒ Send reminder emails about conference start 5 min before 15 min before SETTINGS Administrator-specified settings are used Meeting location Name Description B <i>I</i> <u>U</u> Normal						

1. With the **Send reminder emails about conference start** parameter, you can enable the sending of email reminders to event participants. This feature must first be enabled in the [SMTP settings](#). You can add up to 4 reminders for one conference using the **Settings**

button. To align notification settings with the global settings, click the **Use administrator specified settings** link.

2. You can fill in the **Meeting location** field with information that will be displayed under the **Information** tab on [its page](#) and in the [conference list](#). If integrated with an LDAP directory and the **Meeting Room Filter** and **Meeting Room Search Filter Attr** fields are configured (see [description of additional fields](#)), you will have the option to choose a location from a predefined list or manually enter your text.
3. In the **Description** field, you can add accompanying text for the planned event, such as descriptions of participants' presentations or the event program. This text will be displayed on the conference page.

16.6.7. Webinar Limitations

If the checkbox **Public conference (webinar)** was selected on the [tab General](#), then you can configure the following settings on the tab **Advanced**:

Conference

[Help](#) ?

General	Participants(10)	Layout	Registration	Media	Interpretation	Advanced
Guest permissions						
☒ Allow to send messages						
☒ Allow to send audio						
☒ Allow to send video						
☒ Limit the number of guests						
Number (from 1 to 300)						
100						

1. Permission settings for guest users
2. The **Number** parameter is used to restrict the number of guests in a webinar (by default they can join an event up until the moment when the license limit for guest connections is reached). This option may be helpful when multiple webinars are held at the same time, and it is necessary to distribute guest connections between them or if the rules of your event impose restrictions on the number of attendees (e.g., if it is a lecture).

Users of Mozilla Firefox, Safari, Google Chrome and other Chromium-based desktop and mobile browsers can participate in conferences via WebRTC. The number of guest connections is limited by your license.

16.6.8. Registration Tab

If a public conference (webinar) is created, you will be able to set the parameters on the **Registration** tab. Here, you can configure settings for self-registration of guest participants for your online event (available only for a scheduled conference).

Please note that registration for a webinar is not available for SIP/H.323 endpoints and RTSP devices (e.g., IP cameras). They will be able to participate in a public conference only if a moderator adds them to the list of participants when creating or editing the event, or invites them when the webinar has already started.

Registered users of the server also need to manually confirm their intention to participate in a webinar with registration. This means that even if you check the **Allow authorized users to join without registration** box, your users won't be able to simply join using the conference ID or link. They will first need to visit the event page and click the **Attend** button.

Direct calls via the conference ID/link are also unavailable for federated users until they are explicitly added as participants or register as guests.

Conference [Help](#)

General Participants(0) Layout **Registration** Media Interpretation Advanced

☒ **Enable conference registration**
All users, except invited participants, will be able to join the conference only after registration

Close registration

☐ At conference start

☒ **At conference end**

☐ Custom date and time
Set the registration start and end time

☒ **Close registration when the maximum number of participants is reached (depends on the selected webinar mode)**

☐ Allow authorized users to join without registration

☒ Request email confirmation [?](#)

Registration form settings

☒ Form editing will be available only when the conference is created

Field title	Required field
First and last name	☒
Email	☒
Company	☒
Job position	☐

[SETTINGS](#)

1. Check the box **Enable conference registration**.
2. In section **Close registration**, select when the option to join the webinar will no longer be available:
 - **Without limitation** — available only for recurring conferences, keeps registration permanently open for them;
 - **At conference start** - Registration will close after the webinar starts;
 - **At conference end** — Registration will be available until the end of the event;
 - **Custom date and time** — manually setting the registration availability period.
3. To ensure that the number of participants does not exceed the connection capacity, check the box **Close registration when the maximum number of participants is reached (depends on the selected webinar mode)**.

4. Check **Allow authorized users to join without registration** to allow users of your server to join the conference without filling out a registration form. In this case, any user of your server can log in on the conference page and add themselves to the list of invited participants by clicking the **Attend** button.

5. Settings for the input fields in the registration form. You can drag and drop input fields to create a custom registration form. Besides, you can mark the corresponding checkboxes to make sure that certain fields must be filled by participants. The customization of registration form is available only when a conference is created. This feature is not available when the conference is edited.

6. You can select the input fields that should be displayed during registration only when creating a conference. Click on the **Add field** button to specify both standard and custom fields (up to 10):

Registration form settings

☒ Name

☒ Job position

☒ Email

☐ Phone number

☐ Company

Custom fields

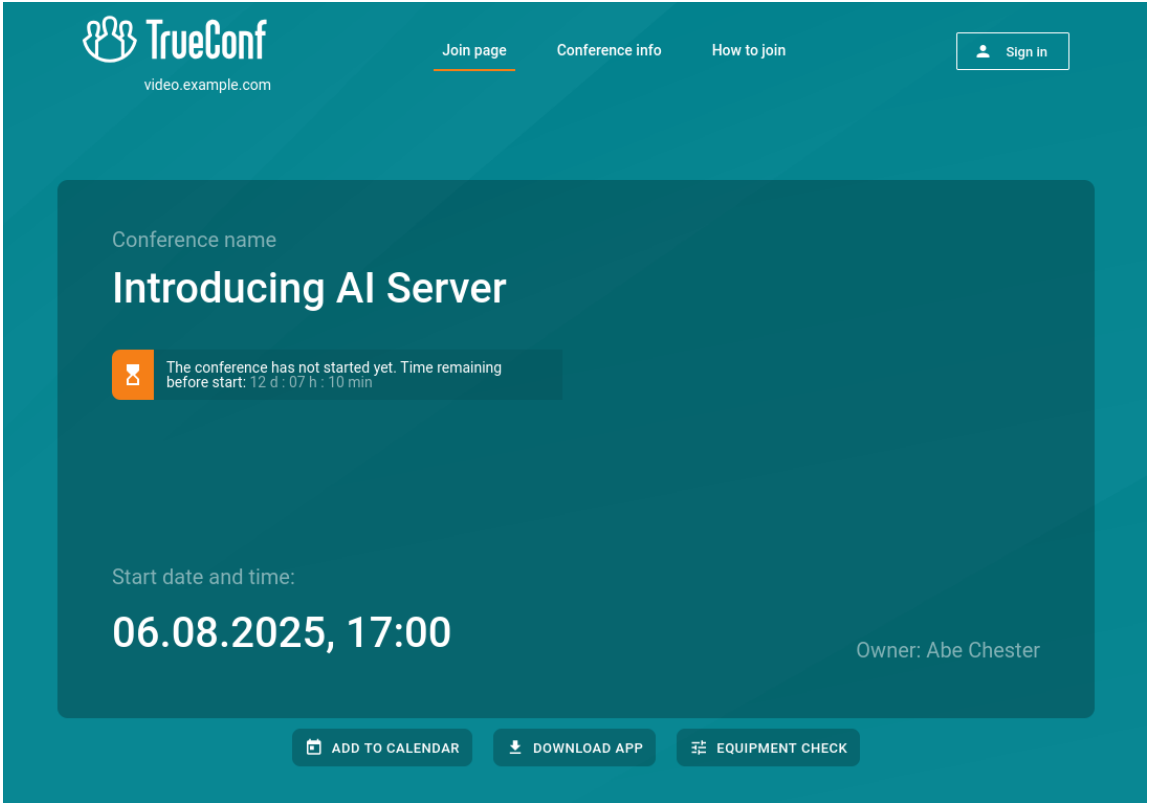
☒ Industry

ADD FIELD

CANCEL

SAVE

When the changes are saved, users will be able to sign up for a public conference on its web page. To learn more about this feature, check out the TrueConf Server user guide:



To view the list of participants who have signed up for the event, select your webinar in the list of conferences, and go to the **Participants** tab. The guest users' IDs will start with `#guest2:` :

Conference List [Help ?](#)

Create

Topic ↑	Start time	Owner	Mode	Type	CID
Brainstorm	Without sc...	Ann Smith	Role-based	🔒	\c\345720...
New version	31.05.2022...	Bob Dimitr...	Role-based	🌐	\c\247104...

Information **Participants(0/4)**

Add

Conference participants (0)

The list is empty

Invited participants (4)

Bob Dimitr...
bob@ruw... ★

Ann Smith
#guest2:0b1...

Boris Bronson
#guest2:120...

Jack Bee
#guest2:21b...

16.7. Automatic conference termination

By default, scheduled conferences do not end at the specified time, but this behavior can be changed in the [settings for each event](#).

To optimize the use of server resources, a scheduled conference will automatically end in two cases:

1. Time-based automatic conference ending is enabled. If it is possible to extend conference duration, but this option is never used, the meeting will also end.
2. Automatic conference ending is disabled, but only one participant remains and no one else joins the meeting for 15 minutes.

16.8. Templates

This section allows server administrator to create new conference templates and edit saved ones. Templates can also be saved while [editing conference](#).

When a conference is created from a template, its scheduling settings are cleared (it becomes a virtual room by default); however, the following parameters remain unchanged:

- Information about the name, mode, and owner
- List of participants
- Simultaneous interpretation settings
- settings from the **Additional** tab (except for the conference ID);
- Settings for saving conference video recordings on the server side and recording audio for transcription purposes
- PIN code settings
- Waiting room settings
- For a scheduled public conference (webinar) — registration settings saved in the template, except the time when participant registration will be closed.

Please note that the **Owner** field corresponds to the owner of the template (not the owner of the conference). In the example below, the administrator added two templates ("Meeting Template" and "Webinar"), while Ann Branson added the "Sales" template from the [scheduler](#) in her client application or from the personal area.

Creating and editing templates is very similar to [creating and editing conferences](#).

Template list [Help ?](#)

1 [Create a template](#)

Topic ↓	Owner	Mode	Type
Meeting Template	Administrator	Role-based	🔒
Sales	Ann Branson	All on screen	🔒
Webinar	Administrator	Video lecture	🌐

Information Participants(1)

Sales

Owner [Ann Branson](#)

Type and Mode Private, All on screen 49x49

Creation time 17.11.2021 14:07:47

Edition time 17.11.2021 14:07:47

[Hide conference details](#)

Template Manager

2 [+ Create a conference](#)

3 [⚙ Edit](#)

4 [🗑 Delete](#)

1. Create a new conference template.
2. Use a saved template to create a conference with typical parameters.
3. Edit saved conference template.
4. Delete unnecessary template.

16.9. Streaming

In this section, you can create and set streaming configurations that are used [when creating and editing conferences](#). You can also use templates for popular platforms which make configuration easier.

TrueConf knowledge base provides guides on how to organize streams to major platforms:

- [YouTube](#)
- [Wowza](#)
-
-
-

You can also manually [configure streaming to another video service](#), such as [or Facebook](#).

To create a configuration, click the **Add a configuration** button. In the window that appears, select the desired broadcast type:

Create a new configuration



Streaming via third-party services and products



We have prepared several templates to manage streaming through other popular solutions. Please select the option you need and follow the instructions.

ADD TEMPLATE

Manual setting

If you are not afraid of the abbreviations RTSP Push or RTSP Pull, then this is the place for you. The entire broadcast setup process is in your hands.

SETUP

16.9.1. Streaming on YouTube, Wowza, Rutube, VK, OK

Section **Streaming via third-party services and products** includes pre-configured templates for popular broadcasting solutions, suitable for both enterprise networks and the Internet. To proceed with further configuration, click the **Add preset** button.

In the configuration window select a required streaming service. Streaming service settings are listed below.

16.9.1.1. Wowza Streaming Engine

To broadcast a video stream to the [Wowza Streaming Engine](#) server, specify the following parameters:

Create a new configuration



Streaming server

Wowza Streaming Engine



This broadcast template can only be used in one of the simultaneously running conferences.

Template name

Host Server

Host Port



Application

☐ Authentication[Show advanced settings](#)[← Back](#)

CREATE

1. **Template name** Configuration name displayed in streaming configuration list on the conference edit page.

2. **Host Server** Address of the Wowza Streaming Engine.
3. **Host Port** Wowza Streaming Engine accepts connections on this port (e.g. 1935 or 1940).
4. **Application** — see the description of this field in the [Wowza Streaming Engine documentation](#).
5. When the checkbox **Authentication** is checked, you will be able to specify the login and password for accessing Wowza Streaming Engine.
6. Click the link **Show advanced settings** to expand the block of auxiliary parameters for the current configuration (see the section [Additional broadcast configuration settings](#) in the documentation).

Then click the **Create** button to save the changes.

16.9.1.2. Wowza Streaming Cloud

The following settings will be helpful when streaming a conference to Wowza Streaming Cloud:

Create a new configuration ×

Streaming server

Wowza Streaming Cloud ▼

 [Follow our instruction](#)

This streaming template can be applied only for one of the conferences running simultaneously.

Template name

Primary Server

Host Port ↕

Stream Name

☐ Authentication

[Show advanced settings](#)

← Back CREATE

1. **Template name** Configuration name displayed in streaming configuration list on the conference edit page.
2. In fields **Primary Server**, **Host Port**, and **Stream Name**, enter the broadcast settings you received from the Wowza Streaming Cloud service when creating the stream.
3. When you check **Authentication**, you can specify the login and password to access Wowza Streaming Cloud.
4. Click the link **Show advanced settings** to expand the block of auxiliary parameters for the current configuration (see the section [Additional broadcast configuration settings](#) in the documentation).

Then click the **Create** button to save the changes.

16.9.1.3. YouTube

Specify the following parameters for YouTube streaming:

[Create a new configuration](#)

Streaming server

YouTube

 [Follow our instruction](#)

Template name

Stream URL

Stream key

[Show advanced settings](#)

[← Back](#)

CREATE

1. **Template name** Configuration name displayed in streaming configuration list on the conference edit page.
2. **Stream URL** Server URL from the webpage where YouTube stream is created.
3. **Stream key** Stream name/key from the webpage where YouTube stream is created.
4. Click the link **Show advanced settings** to expand the block of auxiliary parameters for the current configuration (see the section **Additional broadcast configuration settings** in the documentation).

Then click the **Create** button to save the changes.

16.9.2. Manual configuration

Select option **Manual setting** to set up broadcasting manually with most existing solutions, including those mentioned above. TrueConf Server supports two methods for content delivery: RTSP Publish (also known as RTSP Push) and RTSP Pull. In the first case, your server notifies the broadcasting system about the stream's availability, while in the second case, the system retrieves it from your server.

RTSP Publish manual settings

Available parameters:

Create a new configuration



Streaming server

Manual settings - Publish ▼

Template name:

URL Publish:

☐ Authentication[Show advanced settings](#)[← Back](#)

CREATE

1. **Template name** Configuration name displayed in streaming configuration list on the conference edit page.
2. **URL Publish** The address which will be used to notify about available stream via RTSP ANNOUNCE protocol.
3. When the checkbox **Authentication** is selected, you can specify the login and password for accessing the service.
4. Click the link **Show advanced settings** to expand the block of auxiliary parameters for the current configuration (see the section [Additional broadcast configuration settings](#) in the documentation).

RTSP Pull manual settings

This method can be used to get an RTSP link to the conference stream and to specify this link directly on a third-party service or convert the stream with additional software, e.g., [OBS Studio](#).

Create a new configuration



Streaming server

Manual settings - Pull ▼

Broadcasting using this method must be configured individually for each conference. Here you can set additional settings.

Template name:

[Show advanced settings](#)[← Back](#)

CREATE

1. **Template name** Configuration name displayed in streaming configuration list on the conference edit page.
2. Click the link **Show advanced settings** to expand the codec parameters block for the current configuration (see the documentation section [Advanced broadcast configuration settings](#)).

Additional stream configuration settings

The availability of certain parameters depends on the selected template.

[Hide advanced settings](#)Videocodec
H264Audiocodec
MP3

Send outgoing RTP streams over TCP

Waiting time for a response from the.. ▾

Number of retries ▾

Delay before retry ▾

1. You can change video and audio codecs used for the stream encryption.
2. Check the **Send outgoing RTP streams over TCP** box if you need to send outbound RTP streams via TCP protocol. UDP is used by default.

3. In the **Waiting time for a response from the server** field, you can set the time (in seconds) to wait for confirmation from the external broadcasting system regarding the receipt of information about the broadcast conference stream.
4. The parameter **Number of retries** sets the number of reconnection attempts if the connection to the broadcasting system is lost, allowing TrueConf Server to attempt to restart the publication.
5. The parameter **Delay before retry** sets the delay (in seconds) between attempts to publish broadcast information.

16.10. Conference Settings

In section **Group Conferences → Settings**, you can configure automatic conference deletion and the available participant connection methods.

16.10.1. Automatic conference deletion

Sometimes, it may be helpful to delete events from the general list if they were held a long time ago, and are no longer needed. TrueConf Server allows you to configure automatic deletion of such conferences:

The screenshot shows the 'Settings' page with a 'Help' link. It contains three main sections:

- Deleting conferences automatically**:
 - ☐ Delete scheduled one-time conferences in days after their ending
 - ☐ Delete virtual rooms that have not been started for more than days
 -
- Limits for participants**:
 - Limits for video streams outgoing from conference participants
 - Video:
 - FPS (Video):
 - FPS (Content sharing):
 -
- Conference join options**:
 - You can configure the display of buttons and instructions on a conference page.
 - Private conferences**:
 - ☒ Client applications
 - ☒ WebRTC
 - ☒ QR code
 - ☒ SIP/H.323 endpoints
 - Public conferences**:
 - ☒ Client applications
 - ☒ WebRTC
 - ☒ QR code
 - ☒ SIP/H.323 endpoints
 -

The history of conferences launched in this manner from [the Reports → Call History](#) section is not deleted.

The following features are available:

1. Deletion of scheduled one-time conferences. You can specify a period from 1 to 10,000 days after the conference ending. Conferences with scheduled repetitions are not automatically deleted.

2. Delete [virtual rooms](#) that have not been launched for a certain number of days (from 1 to 10 000 days). The virtual rooms that were created, but were never launched during the specified period will also be deleted.

The list of conferences is evaluated for deletion once every 60 minutes. The countdown timer works in the following way:

- If a conference was created, but not started, the countdown will be based on the time when the conference was last saved (including after editing).
- If the conference had been started at least once, the countdown will start from the time of the last launch (even if the settings were changed after the conference start).
- If the start date of a scheduled conference is set beyond the expected deletion date, it will not be deleted (in other words, a scheduled conference that has never been started will not be deleted).

16.10.2. Limiting the quality of outgoing video from participants

You can set general quality parameters for video streams **outgoing** from all participants in all conferences. This includes client applications, participants, who join from a browser via WebRTC, and connections via SIP/H.323/RTSP. As a result, the server will explicitly instruct participant's devices/applications on the quality of the video to be sent. This will be the upper limit on the incoming video quality. The resolution limit applies only to the quality of the camera video, but not the content which is being shared in a participant's window. Content (screen/application window) is always shared with the resolution at which it is captured, with a maximum quality of FullHD 1080p. SVC works for fps/bitrate but not for resolution.

You can set the frame rate limit for two different scenarios: when a speaker is displayed in the video window or when this person is sharing content in the same stream. This limit does not affect content sharing settings for the second stream, where FullHD 1080p quality is always used with a low FPS, prioritizing resolution.

The server administrator can [set individual quality settings](#) for a conference when creating or editing this event.

16.10.3. Methods to connect to conferences

In this section, you can choose which ways of joining conferences should be available to all participants. These general settings will apply to the following conferences:

- to the pages of [smart meetings](#), which are created from the client application;
- Pages of scheduled conferences.

The parameters for private and public conferences have to be specified separately. Please note that quick conferences created in client applications are always private. Conferences can be joined from client applications, browsers (via WebRTC), by QR code from the event page, and from hardware or software SIP/H.323 endpoints.

16.10.4. Conference ID and participant call rules

In section **Conference ID**, you can set rules for the auto-generation of unique IDs when creating events. There is also an option to disable ID changes so that the administrator or user cannot alter it at their discretion on the **Advanced** tab.

Conference ID
Rules of automatic ID generation when creating a conference
☒ Digits (0 — 9)
☐ Letters (a — z)
Length: 10
☒ Allow conference ID editing
Apply

Automatic conference invitation
☒ Call participants when a scheduled conference starts
Apply

Below you can disable the automatic invitation of all added participants to the scheduled conference. To do this, uncheck the **Call participants when a scheduled conference starts** box (enabled by default).

17. Chat Settings

In section **Chats**, you can configure chat settings for the users of this TrueConf Server.

There is only one parameter in this section so far, but in the future versions of the video conferencing server other settings will be added.

17.1. Timeout settings for editing messages

Chats

[Help ?](#)

Settings

Prohibit users from editing their messages hours after sending

Apply

To limit the time for editing messages in chats, check the **Prohibit users from editing their messages** box (selected by default). In this case, after sending a message, the user on your server will have only the specified number of hours (48 by default) to edit it. Once this time has elapsed, the context menu in the TrueConf application, accessed by right-clicking on the message, will simply not include an edit option.

Limits apply to:

- Authenticated users of your TrueConf Server (their application will request the information about the restriction from the server and apply it)
- Guest participants of your conferences since a temporary user account is also created for them on the server.

Users of the external [federated server](#) will comply with the restrictions of the server where they are authenticated.

17.2. Automatic deletion of empty conference chats

In some cases when a conference ends, empty chats may remain, for example, if there was a meeting, but users discussed everything verbally without sending any messages to the chat. The developers of TrueConf Server made sure that such empty chats were not added to the chat list and were automatically deleted.

How it works:

1. You must have TrueConf Server version 5.5.0 or higher.
2. About once in 15 minutes, the system checks if a chat was automatically created for a one-time conference which has already ended (in other words, it is not the chat of a virtual room or the conference was started based on a group chat, but was unlinked from this chat). The system will also delete the chats of quick conferences created in a single click in TrueConf client applications. So, this chat will no longer be available to any user when the conference ends.

3. The system checks if the chats do not include any messages from users (however, a chat may include some service messages, e.g., notifications about a user's connection to the conference).
4. All the chats, which match these criteria, will be deleted; so, they will not be displayed in the list of chats in users' TrueConf client applications.

Please note that if some conference participants were from a federated server, the chat will be deleted depending on the settings of the server where the conference was created (for example, if the servers with different versions were used).

18. Surveys

Users of TrueConf video conferencing systems can create surveys to collect people's responses and examine their opinions. This feature does not require a separate license and is available even in TrueConf Server Free.

What features does the built-in polling (survey) module offer:

- Ability to configure survey access (available only to the users of your server or to everyone)
- Anonymous surveys
- Configuration of respondents' permissions to view the survey results
- Ability to retake the survey
- Permission to change responses
- Ability to use images as one of the response options for a multiple-choice question
- Add images to a question
- Ability to mark any questions as required which ensures that a user cannot skip these questions when completing the survey
- Create survey campaigns which will allow you to easily segment results by respondent groups
- Export results as a CSV file.

The server administrator can manage all surveys. The users, who were given the [right to create surveys](#) at the group level, can also manage them; however, such users can manage only the surveys that they created (in other words, they are the [owners](#) of these surveys). However, users cannot manage all surveys.

18.1. Types of questions and limits

Each survey may include questions of the following types:

- **Short answer** — a free-form response that is explicitly written by the user and not chosen from options (**up to 255 characters**);
- **Paragraph** — a variation of an open-ended response where you can write more text (**up to 4096 characters**);
- **Single answer** - a multiple-choice question where only one option can be selected; when creating the question, it's possible to add one answer option **Other**.
- **Multiple answers** — a multiple-choice question that allows the selection of several options; you can add one answer option **Other** when creating the question.

The following limitations also apply to polls TrueConf:

Maximum number of surveys — unlimited.

Maximum number of questions in one survey — 5000.

The maximum number of answer options for each question — 20.

The maximum length of a single response option — 255 characters.

The maximum length of a question — 255 characters.

Allowed formats for an image that may be uploaded for a survey — JPEG, PNG, GIF, BMP.

18.2. Creating and editing a survey

To manage polls, go to the **Surveys** section of the control panel TrueConf Server.

You will see the list of surveys (by default, it is empty):

Surveys [Help ?](#)

List Settings

Create

Name

Owner

Survey ID

Name	Last modifi... ↑	Owner	Survey ID	Hide >
 Employee Satisfaction Survey	17.06.2025 18:46	Jane Flowers	96faa5b3-5f6c-...	Employee Satisfaction Survey Survey ID 96faa5b3-5f6c-4b3b-bff8-8ad4fe80... Last modified 17.06.2025, 18:46 Owner Jane Flowers Questions 6 Survey page: 4 available campaigns Hide survey details Survey Manager  View responses  Edit survey  Campaign management  Create copy  End  Delete
 What we want?	04.07.2025 18:47	Not specified	6dd95770-c166...	

By clicking on a survey, you will open the card with general information about it: survey ID (which may be helpful when you need to find [its change history in the logs](#)), the last modified time, the owner's name, the number of questions, and a direct link to the campaign (if it was created).

Survey owner is a user of your TrueConf Server who has full access to manage the survey and its campaigns. A survey can be held even without the owner; however, in this case, it has to be created by the administrator. Moreover, only the administrator will be able to manage the survey and view its results.

A **campaign** is a specific survey session that allows you to segment participants for analyzing results across different groups. At least one campaign is **required*** for holding a survey since users essentially participate in a survey campaign. Each campaign includes all the questions created for the survey and differs only in terms of its link and access settings ([see below](#)). Multiple campaigns can be created for a single survey, and there are no restrictions on the number of active campaigns that can be held at the same time.

18.2.1. Creating a Survey

To create a survey, click the **Create** button in the general list. The **Questions** tab will be opened. Here, you should specify the survey name (required), description (optional, will be displayed to participants on the survey page). Plus, below you need to add survey questions:

Survey management

[Help](#) ?**Questions**

Settings

Campaigns (0)

Responses (0)

To start the collection of responses, create a campaign **CREATE**

Survey title

New survey

Survey description

+ ADD QUESTION

To create a question, click the **Add question** button and select [its type](#). Next, enter the question text and fill in the answer options, depending on the question type. If necessary, you can add an image to the question text and to any of the answer options. It may be necessary to give a better illustration of the question or to use images as answer options. Changes to the list of questions are saved automatically, so you don't accidentally lose your work when creating a survey with a large number of questions.

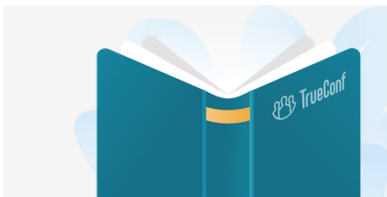
Below is an example of an added question of type **Single answer**:

Survey management [Help](#) ?

Questions Settings Campaigns (4) Responses (4)

Survey title
Employee Satisfaction Survey

Survey description
Thank you for participating! This confidential survey aims to understand your experience at work. Your feedback will help improve our workplace. Estimated time: 5-7 minutes.



1 Question *
How satisfied are you with your current role?

☐ Very Dissatisfied

☐ Dissatisfied

☐ Neutral

☐ Satisfied

☐ Very Satisfied

☐ Add option [or Add the "Other" option](#)

☒ Required

18.2.2. Settings

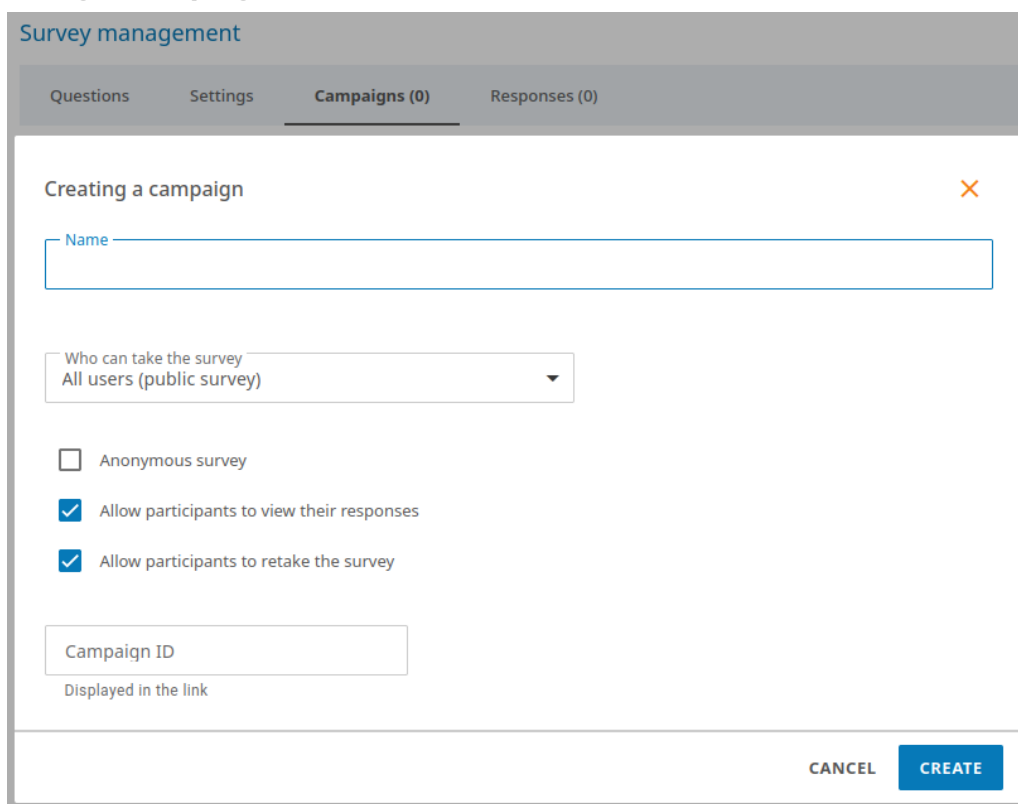
In the **Settings** tab, you can assign the owner to a survey. To do it, just click the **Select** button and choose one of the users on your video conferencing server. Other types of users such as guests or federated users cannot be selected as the survey owner. The user, who creates a survey in the personal area, automatically becomes its owner.

After adding the owner, you will be able to select a new one at any time (even when a survey campaign is running). However, you cannot remove the owner.

18.2.3. Polling campaigns

To hold a survey, you need to create and start at least one survey campaign. Go to the **Campaigns** tab to do it. By default, no campaigns are added, and they have to be created manually. If campaigns already exist, you will see [the list of campaigns](#).

18.2.3.1. Creating a campaign



The screenshot shows a 'Survey management' window with tabs for 'Questions', 'Settings', 'Campaigns (0)', and 'Responses (0)'. The 'Campaigns (0)' tab is active, displaying a 'Creating a campaign' form. The form includes a 'Name' text field, a dropdown menu for 'Who can take the survey' (currently set to 'All users (public survey)'), three checkboxes for 'Anonymous survey' (unchecked), 'Allow participants to view their responses' (checked), and 'Allow participants to retake the survey' (checked). There is also a 'Campaign ID' text field with the note 'Displayed in the link' below it. At the bottom right, there are 'CANCEL' and 'CREATE' buttons.

1. Click the **Create campaign** button.
2. Enter the campaign name in the **Name** field. It is not visible to participants and is used only for quickly finding campaigns in the list.
3. In the dropdown list **Who can take the survey**, select the campaign availability level for participants: everyone can follow the link and complete the survey (public campaign) or only users of your TrueConf Server.
4. Check the **Anonymous survey** box if you need to collect anonymized responses without participants' names. The results of an anonymous campaign will be displayed for each response option in each question, but without participants' names. No hidden analytics will be saved in the server database.
5. The checkbox **Allow participants to view their responses** will allow participants to review their answers once more after submitting the completed data.

6. Check the **Allow participants to retake the survey** option to allow participants to submit their responses again.
7. To provide participants with a neat campaign hyperlink, enter its suffix (the last part of the link added to your server address) in the **Campaign ID** field. For example, if you specify `office`, the link will look in this way: `https://example.com/s/office`. The ID must be unique within your server.

18.2.3.2. List of campaigns

If multiple campaigns have been created, they are displayed as a list with several available actions (public campaigns are marked with the  icon):

Survey management

[Help ?](#)

[Questions](#)
[Settings](#)
[Campaigns \(2\)](#)
[Responses \(1\)](#)

Campaigns will allow you to segment participants' responses [+ CREATE CAMPAIGN](#)

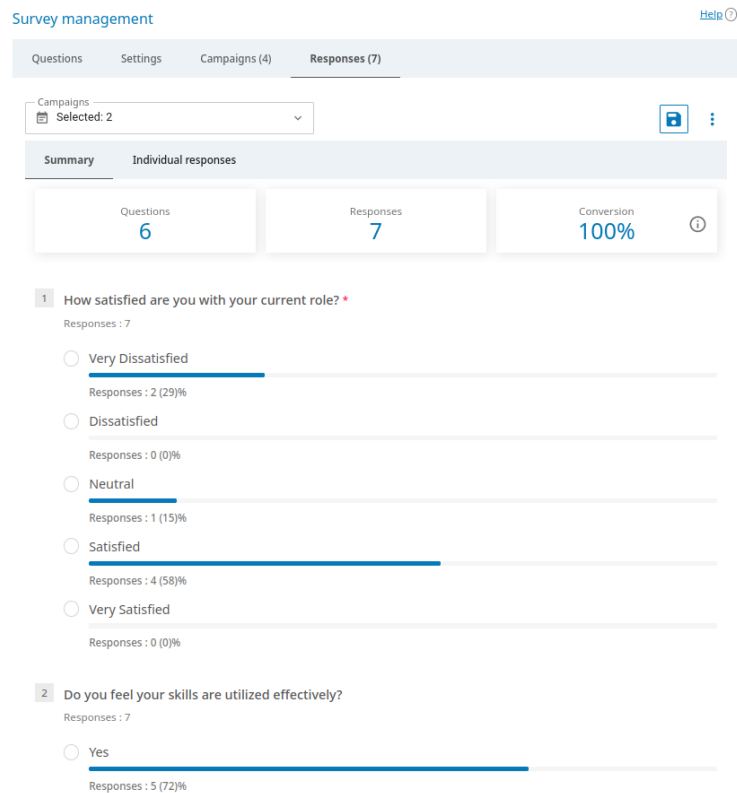
Name	Responses	Survey page	Status
Office managers	0	https://10.110.2.240/s/ifTkzmQ7s...	Not started  
Public survey 	1	https://10.110.2.240/s/fd4X2sZw...	Active  

 Copy link
 View responses
 Edit campaign
 Delete

1. To copy the campaign link, click the  button.
2. To launch an inactive campaign, click the  button.
3. To stop the campaign, click the  button. The survey will be paused and can be resumed later if desired.
4. To navigate to the [tab Responses](#) with the results of the desired survey campaign, click the  button in its row and select **View responses**.
5. Regardless of the campaign status (active or stopped), you can change its settings, for instance, to make it anonymous. To do this, click the  button and select the **Edit campaign** option.
6. You can delete a stopped campaign, and all responses left specifically for this campaign will also be removed. To do this, click the  button and select the **Delete** option.

18.3. Results of survey campaigns

To view the survey campaign results, go to the **Responses** tab while editing the survey, or click the **View responses** link in its card in the [general list](#). The opened tab will display the total number of responses for all campaigns:



1. In the dropdown list **Campaigns**, select the campaign you want to view the summary for and click **Apply**. You can select multiple campaigns at once to see their combined statistics.
2. The summary of results shows the number of responses, in other words, it shows how many users filled out the form and submitted responses. The conversion rate is also useful since it indicates the percentage of respondents who filled out the form after accessing the survey page.
3. To save responses for one or more campaigns selected in the list **Campaigns** to a .csv file, click the  button.
4. To clear the results of the selected survey campaigns, click the  button and select **Delete all responses**. This will delete all responses collected for the specified campaigns.

By default, results are displayed in the **Summary** tab, but you can switch to the **Individual responses** view, where you can select a participant to view their specific responses and test completion time:

Survey management [Help](#)

Questions Settings Campaigns (4) **Responses (7)**

Campaigns
Selected: 2

Summary **Individual responses**

<  Hailey Jones > Submission date
04.07.2025 18:55

Time to complete 00:00:20



1 How satisfied are you with your current role?*

☒ Very Dissatisfied

☐ Dissatisfied

☐ Neutral

☐ Satisfied

☐ Very Satisfied

If the campaign was launched as **anonymous** (see [campaign settings](#)), **Anonymous user** will be displayed instead of names in the participant list for option **Individual responses**.

19. Working with the server API

The features of TrueConf Server can be extended with the RESTful API available in all versions, including the free one.

19.1. How API and OAuth 2.0 work

Section **API → OAuth2** is designed for managing applications or services that work with the TrueConf Server API. Access management is conducted according to the OAuth 2.0 authorization protocol, which you can read more about in the [official RFC 6749 documentation](#), as well as in the inset below.

OAuth 2.0 is used to authorize certain applications (clients) to access protected resources with limited scopes and rights. With this approach, you can block a particular application or a user from the server resources at any given period of time. The protocol also allows you to authorize third-party applications and do actions on the server on behalf of the user via API. In this case, the user does not need to give their username or password to any third-party application (Authorization Code method).

After authorization on TrueConf Server using OAuth 2.0 protocol, every third-party application obtains an access token. Those applications with a valid access token can access TrueConf Server API. The list of API commands can be found in [API documentation](#). TrueConf Server administrator can manage third-party application permissions and access tokens obtained via this section.

Examples of working with the API can be found on our blog.

After successful authorization, the application receives *access token* with a limited lifespan and scope (server wide or limited to a specific user). For example, server wide scope gives information about any conference on the server, while user's scope provides the information only about those conferences where the user is the conference owner or a listed participant. The scope is defined by the authorization type selected by a third-party application developer, while permissions set (rights) are determined by TrueConf Server administrator for every application.

When requesting an access token, it is required to indicate Application ID and Secret. These parameters can be obtained and updated by creating or editing the application in this section. Application ID is created automatically and cannot be changed later. By contrast, application secret can be further regenerated.

OAuth 2.0 Authorization Method	Access Key Scope	Authorization Result
Client Credentials The application receives an access key whose scope is not limited by any specific user data. User authorization is not required. It is recommended to use only for trusted applications.	Unlimited.	An access token with a lifespan of 1 hour is issued.

OAuth 2.0 Authorization Method	Access Key Scope	Authorization Result
User Credentials (also known as <i>Resource Owner Password Credentials Grant</i>) To obtain the access token, you need to provide the user's login and password acquired on the application side.	Restricted to the visibility of the authorized user.	An access key is issued for 1 hour, along with a refresh token for 7 days.
Authorization Code The access token is issued after the user self-authenticates on the server side. The application does not have access to the user's login and password.	Restricted to the visibility of the authorized user.	An access key is issued for 1 hour, along with an access renewal key for 7 days.
Refresh Token This authorization method allows you to obtain a new access token based on the existing refresh token.	It is restricted to the visibility scope of the user who was issued the access renewal key.	A new access key is issued for 1 hour. It cannot be renewed using this method.

19.2. Permissions description

API capabilities of a third-party application depend on the permissions it obtained.

The list of permissions expands with each new version of the API as new features are added to the video conferencing server. Refer to the [API documentation](#) for the list of APIs available in each version.

In the [TrueConf Server API](#) documentation, each method specifies the set of permissions required for a successful call.

If an OAuth application requires both read and write access to a certain parameter, then you can specify a general permission `<permission>` instead of specifying `<permission>:read` and `<permission>:write` permissions, if it is available. For example, you don't need to click both `users:read` and `users:write` checkboxes to allow an application to read and edit TrueConf Server user accounts. Instead, you can select only the `users` checkbox.

19.3. Form for creating a new OAuth 2.0 application

To add an OAuth 2.0 application:

1. Click **Create a new application**.
2. Enter its identifier in the **Name** field. It is only displayed in the application list.
3. To authorize using the **Authorization Code** method, specify the URL to redirect the application to in the **Redirect URL** field. For other authorization methods please indicate the following address `https://localhost/`.
4. In the **Permissions** list, select the [permissions](#) required for your application.
5. Save the changes using the **Create** button.

19.4. Application Editing Page

On the application page you can not only edit its properties but also view access token list obtained by the application's users. You can remove user access tokens at any time to block particular user from accessing API data.

You can also **Regenerate** the application secret to block the application and its new users from accessing the server for security purposes. Please note that access tokens and refresh tokens obtained using previous application secret will still be valid within their lifespan.

19.5. Built-in API Documentation

The built-in documentation on API v4 is available starting from the server version 5.5.3 and later.

Your server installation already includes built-in documentation for easy API use (just like this administrator guide). Your developers won't need to search for any guides online. They will be able to create scripts and applications with TrueConf Server APIs even when working within a private network.

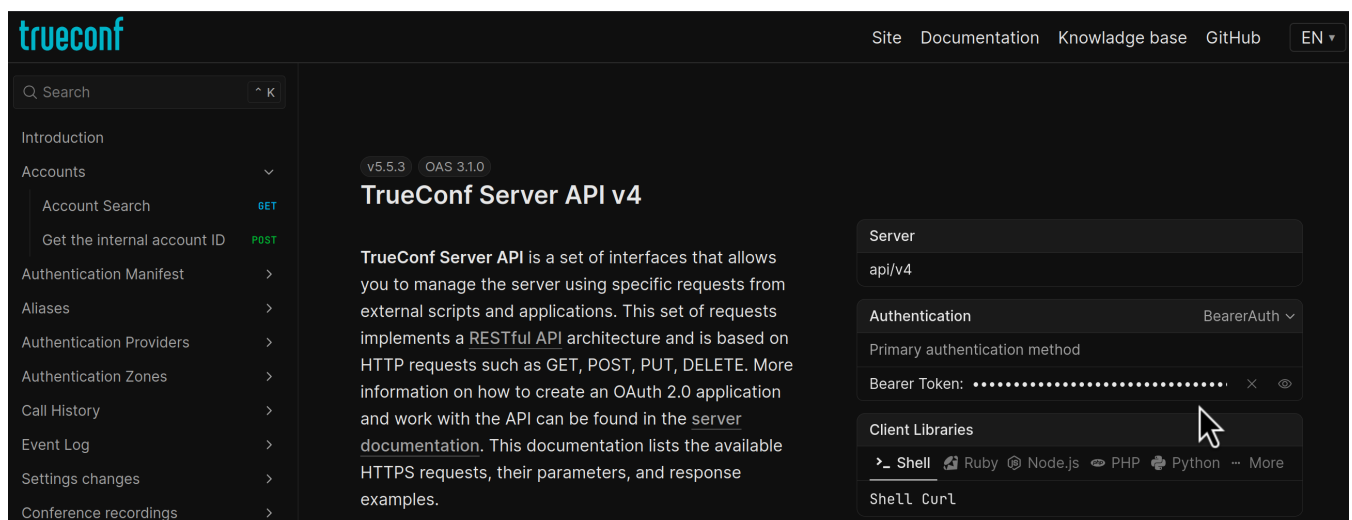
The built-in API documentation is available at:

`https://[server-address]/api/v4/docs/`

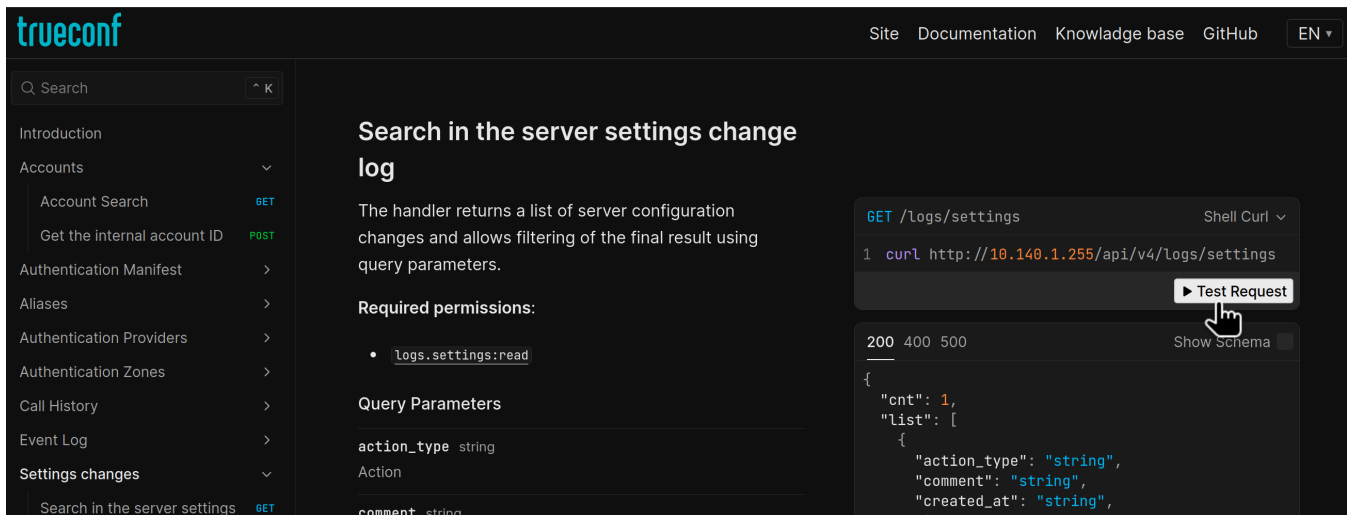
where `[server-address]` is the IP or FQDN address of your server.

The built-in documentation supports testing mode for any request. To use this feature:

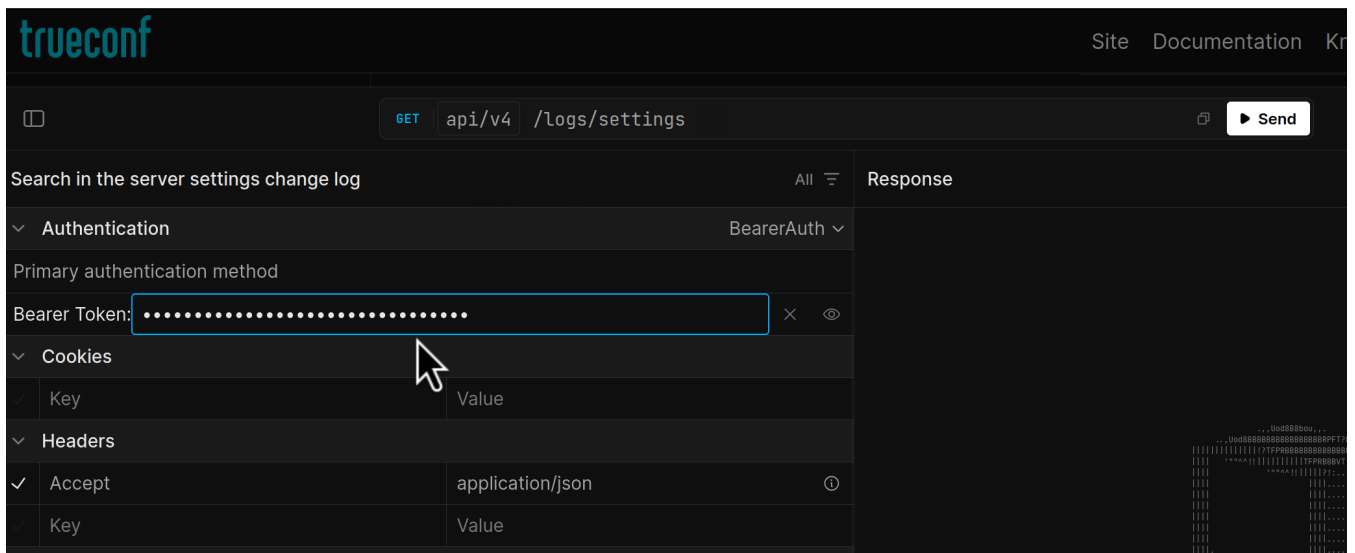
1. Generate a token for the OAuth 2.0 application with the required permissions (or use a token from section **Web → Security** for testing purposes).
2. Specify the token in section **Introduction** under block **Bearer Token**:



3. The token will now be remembered for the session duration of this page in the browser, allowing you to perform any request using the **Test Request** button:



4. The token from Step 1 will also be remembered for all requests if specified in any request before sending:



When the page language is changed or when the page is refreshed, the API token specified for testing will be forgotten and will have to be re-entered. This is done for security reasons, the token is not stored in cookies.

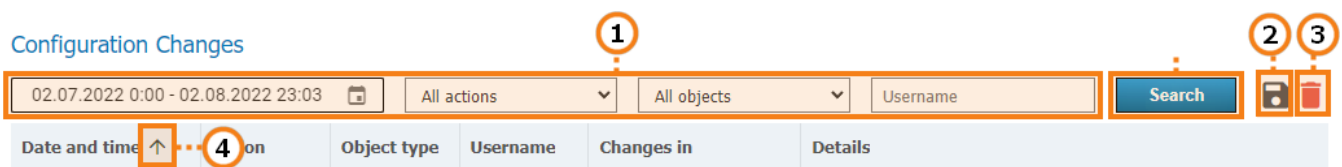
20. Conference recordings and logs (reports)

The **Reports** section stores all information about user connections, calls, messages, as well as video recordings of conferences. The data can be filtered by various parameters and downloaded in [CSV format](#). The time in the tables is displayed according to the time zone selected in the [preferences settings](#) menu.

We remind you that the main log TrueConf Server can be [viewed in the log](#), accessible from the **System → Server log** menu in the upper right corner of the control panel page.

On the right side of some tables you can find a dashboard containing detailed information about any event that is selected in the table.

The table reports have common functions:



1. Filter entries.
2. Saving the table in CSV format (the export format can be configured in the [preferences section](#)). This saves the selection obtained after setting the filters and clicking the **Search** button.
3. Delete the entries selected through filtering. Please note that you will delete only the entries that have been selected in the input fields, but not the ones that are currently displayed.
4. Sort entries by field values (click on any column name to change sorting order).

20.1. Differences between a session and a conference

Before describing the logs, we need to show what a session is.

Session is a specific communication instance of a conference. Each time the same conference is started, a new session (communication instance) is initiated with its own identifier. For example, this term can apply to scheduled events that are repeated multiple times, as well as to virtual rooms. Such conferences will have multiple sessions, one for each start event. The **session ID** should not be confused with the [conference ID](#), which can be changed by a moderator or server administrator.

20.2. Event Log

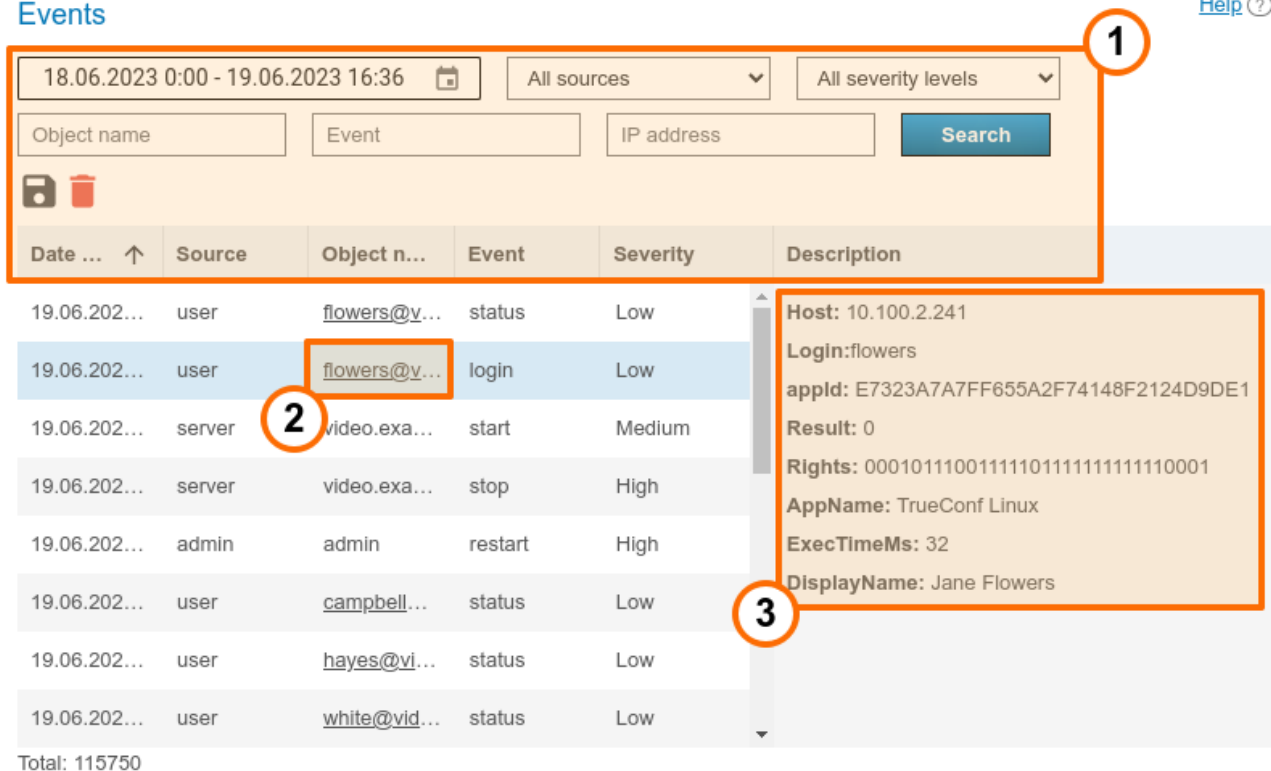
The event log includes consecutive records of:

- All changes in the user status (authorization, offline, and others) and changes in the server state (start, shutdown, connection to AD/LDAP)
- Results of the actions taken by OAuth applications (refer to the [server API description](#) for more details)

- Revocation of a user's PRO licenses due to one of these reasons:
 - No PRO licenses were available when a user tried to join a group conference.
 - Revocation of a user's PRO license (either permanent or temporary) as a result of [license redistribution after server restart or automatic revocation by timeout](#).
 - revocation of a temporary PRO license by the administrator from the user (in the [section Dashboard →PRO Licenses](#)).
- [deleting video recordings](#) using the  button from the control panel;
- removal of entries from logs in section **Reports**, where the event type from column **Event** indicates the corresponding subsection (see [description below](#)).

If you click on an event in the table, you will be able to check several details, for example, what client application or IP was used to authorize. Besides, you can track changes in the user status.

Events

[Help ?](#)


18.06.2023 0:00 - 19.06.2023 16:36 All sources All severity levels

Object name Event IP address Search

Date ... ↑	Source	Object n...	Event	Severity	Description
19.06.202...	user	flowers@v...	status	Low	
19.06.202...	user	flowers@v...	login	Low	Host: 10.100.2.241 Login:flowers appId: E7323A7A7FF655A2F74148F2124D9DE1 Result: 0 Rights: 000101110011111011111111111110001 AppName: TrueConf Linux ExecTimeMs: 32 DisplayName: Jane Flowers
19.06.202...	server	video.exa...	start	Medium	
19.06.202...	server	video.exa...	stop	High	
19.06.202...	admin	admin	restart	High	
19.06.202...	user	campbell...	status	Low	
19.06.202...	user	hayes@vi...	status	Low	
19.06.202...	user	white@vid...	status	Low	

Total: 115750

1. General UI for working with the table ([check the description above](#)). The **Event** drop-down list can be used to select one or multiple event types for more flexible search and analysis.
2. Link to the [user profile](#) who performed the action.
3. Event details. Contains detailed information required for the [technical support department](#) to solve possible issues you may face. The most common event details:
 - **Users:** list of [TrueConf ID](#) users (displayed, for instance, during an event of insufficient PRO licenses after distribution);
 - **IP address:** IP address of the connected user;
 - **Entered login:** The information specified during the authorization attempt [TrueConf ID](#) can help identify if the user made a mistake in the login details when the sign-in is unsuccessful.
 - **Real user ID:** existing [TrueConf ID](#) of the user under which authorization or another event occurred;
 - **Endpoint ID:** unique connection ID, reference it from the [section Endpoints](#);

- **Application name:** the name of the application used to authenticate on the server;
- **Authentication method:** authentication method, such as login and password in [Registry mode](#), and with [SSO login \(NTLM, Kerberos\)](#), the relevant method will be displayed;
- **User rights:** A binary sequence in which user rights are encrypted;
- **Display name:** display name of the user;
- **Previous status:** status of the user before the transition to the new value, takes one of the values: **-2** - inactive, **0** - offline, **1** - online, **2** - (busy) participating in a conference or video call, **5** - connected to the conference as its owner
- **New status:** the status the user transitioned to as a result of the event takes the same values as **Previous status**;
- **Description:** Detailed event description;
- **Administrator type:** The administrator access level when performing events on their behalf can be **sysadmin** (full access to the control panel) or **security** (restricted access, see [description TrueConf Server Security Admin](#)).
- When an administrator deletes entries from report tables, additional fields will be displayed showing the number of deleted entries and additional details about the deleted rows (depending on the table type).
- **User agent:** is the part of the HTTP request that includes information about the web application and the OS of the device which is being used to connect to the server.

20.2.1. Decoding event types

Below is a list of all event types that are recorded during the operation of TrueConf Server (some events can be either successful or unsuccessful, such as **login** authorization):

Event type	Explanation
authorize	User TrueConf Server authentication via SSO provider
login	Authorization: • user login with username and password in the client application or in the personal area in the browser • administrator in the control panel
logout	Deauthorization (logout) of a user or server administrator
lock	User account lockout upon entering an incorrect password
unlock	Unlocking a user's account by the server administrator or after the timeout specified in the lock settings .
activation	User account activation (see the checkbox in the profile description)
deactivation	Deactivation of a user account (see checkbox in profile description)
status	Changing the user status (online/offline, busy, owner, numerical values see details above)
connect	Connecting your TrueConf Server to an LDAP server

Event type	Explanation
disconnect	Loss of connection between your TrueConf Server and the LDAP server
delete_chat_messages	Deleting Entries from the Table Chat Messages
delete_chat_messages_cascade	Deleting records from the table Chat Messages when a conference is removed from the call history
delete_conferences	Deleting records from the Call History table
delete_connections	Deleting records from the Endpoints table
delete_events	Deleting records from the Events table
delete_logs	Deleting records from the Configuration Changes table
delete_video_recording	Deleting records from the Conference Recordings table
	Automatic deletion of entries from the table Conference Recordings after the timeout specified in the section Group Conferences → Settings .
start	Start TrueConf Server
stop	Stop TrueConf Server
restart	Restart TrueConf Server
pro_license_limit	Revocation of a user's PRO licenses due to one of these reasons: the user lacked a PRO license when attempting to join a group conference Revocation of a user's PRO license (either permanent or temporary) as a result of license redistribution after server restart or automatic revocation by timeout.
pro_license_revocation	Revocation of a temporary PRO license by the administrator from a user (in the section Dashboard → PRO Licenses)

20.3. Call History

This section contains history of video calls and conferences hold on the server.

Please note that each time you start the same conference, a new [conferencing session](#) with its own identifier is initiated. This is relevant for scheduled recurring events or for virtual rooms. For this reason, there will be several entries in the call history table with details of each independent conferencing session.

20.3.1. Call History List

On the main page of the section you can see the table where you can select a particular meeting. Besides the call history, the list also contains information about active sessions. The **End** field remains blank for current conferences.

When deleting data, the following records will be ignored and remain in the table:

- sessions that have not yet ended;
- communication sessions for which [server-side recordings](#) are available.

The remaining rows will be successfully excluded from the table.

Call History Help

02.07.2022 0:00 - 02.08.2022 23:24

Conference ID

Owner

All modes

Search

Session ID	Start	End	Duration	Participants	Owner	Mode	CID
0000009855057d39...	02.08.2022 16:57:21	02.08.2022 17:08:43	00:11:22	2	bronson@video.comp...	All on screen...	\c\19156941...
00000097b7c62da8@...	02.08.2022 16:21:01	02.08.2022 16:26:48	00:05:47	3	bronson@video.comp...	All on screen...	\c\brainstorm
00000096e9003773...	02.08.2022 16:18:39	02.08.2022 16:21:21	00:02:42	2	dawson@video.comp...	Video call	\c\04232061...
000000920367bc92@...	01.08.2022 18:33:28	01.08.2022 18:34:39	01:01:11	10	peters@video.compa...	All on screen...	\c\03860136...
000000902daa3a1e@...	01.08.2022 16:21:25	01.08.2022 16:59:38	00:38:13	5	smith@video.compan...	All on screen...	\c\10372891...
0000008ef5be8bc9@...	30.07.2022 17:50:53	30.07.2022 18:44:59	00:54:06	7	bush@video.compan...	All on screen...	\c\10372891...
0000008d2e1f0d28@...	30.07.2022 17:40:11	30.07.2022 17:41:51	00:01:40	3	bob@video.company...	All on screen...	\c\10372891...

Total: 23

1. General table interface (see the description above).
2. Link to the [page with detailed information](#) about the communication session.
3. Link to the [profile](#) of the conference owner or call initiator.
4. If this session has a parent server-side conference (not created ad hoc in the client application), you can find it in the [general list](#).

20.3.2. Connection session information

Click on the session ID in the general table to view information about the selected conferencing session, including:

- information about time and owner of the conference
- list of what time the participant was attending the conference
- general media streams quality technical data
- history of conference invitations and accepted/rejected video calls
- Sending files.

Conference Session:
Topic: Brainstorm

1

Start	End	Duration	Cause of ending	Participants	Owner	Mode	CID
17.04.2024 18:26:47	17.04.2024 18:35:32	00:08:45	Conference was ended by ...	4	flowers@video.exa	Role-based (TCP)	vc17268100313

1

Participant List

2

User	Joined ↑	Left	Duration	Disconnect c...	Bitrate in/out	CPU Load	FPS	Dimensions	Endpoint
Carla Devine	17.04.2024 18:...	17.04.2024 18:...	00:04:12	Conference en...	640 / 983	2	15	1280x720	E5238657753...
Carla Devine	17.04.2024 18:...	17.04.2024 18:...	00:00:52	Hung up	592 / 120	18	15	640x360	E5238657753...
Jane Flowers	17.04.2024 18:...	17.04.2024 18:...	00:08:43	Conference en...	670 / 992	24	15	1280x720	C2F08345BC5...
Abe Chester	17.04.2024 18:...	17.04.2024 18:...	00:08:45	Conference en...	620 / 0	0	0		E3825799E9E...
Bruce Hubbard	17.04.2024 18:...	17.04.2024 18:...	00:08:45	Conference en...	590 / 0	0	0		E3825799E9E...

Total: 6

1

Invite List

2

Date and Time ↑	User	Recipient	Accepted
17.04.2024 18:26:47	video.example.net	flowers@video.example.net	✓
17.04.2024 18:26:47	video.example.net	chester@video.example.net	✓
17.04.2024 18:26:47	video.example.net	devine@video.example.net	✓
17.04.2024 18:26:47	video.example.net	hubbard@video.example.net	✓

Total: 4

1

File List

2

Date and Time ↑	Sender	Name	Size, MB	
17.04.2024 16:46:56	Abe Chester	group.000	0.05	
17.04.2024 16:46:25	Jane Flowers	trueconf_quick_start.pdf	6.3	

Total: 2

- 1. General table interface (see the description above).
- 2. Link to user profiles of participants and invited users.
- 3. If this session has a parent server-side conference (not created ad hoc in the client application), you can find it in the general list.
- 4. Links to pages with information about connection details for each conference participant.
- 5. The list of files sent to the conference chat. When any of the files is clicked, the download page will open.
- 6. The button for deleting a file from the server.

Please note that the column **Mode** indicates in brackets whether **UDP Multicast** is used in this communication session (in the example above, it is not used).

The number in column **Participants** of the first table represents the count of distinct participants (including those from different devices). Meanwhile, the number in the second table titled **Participant List** (see row **Bcero**) and the list itself correspond to all **connection** events to the conference. These numbers may differ. In the example above, we can see that at least one user **Carla Devine** connected twice.

A guest who reconnects to a webinar from the same application or browser will not be counted again, even if a different display name is entered. For more details, refer to the [description of guest ID](#). However, the history of name changes will be displayed along with the recorded events of reconnection to the conference.

In the **Invite List** table, a server address may be listed as a user in the rows. It means that users in the **Recipient** column were called by the server at the start of the conference. If a TrueConf Server user is the inviting party, it means that he/she invited the participant after the conference

start. If participants joined the conference on their own, there will be no inviting user for them (no row in the table).

20.3.3. Connection properties

Here you can view all connection details to a given conferencing session for each user (e.g., the client application version, operating system and CPU). The example below shows some of these parts:

Endpoint properties (A244B2B1E4687DDA60F1D725980D1E07)

Logged User:

bob@server.company.com/8ec2d06d

IP:

192.168.88.181

Local Ip:

192.168.80.1:65019, 192.168.234.1:65020, 192.168.88.181:61856, fe80::79:44e6:fc89:7d6a:44308, fe80::7d67:d379:9c12:8960:44308, fe80::8dd:6787:d1e5:259c:61858

Audio Capture:

Микрофон (SplitCam Audio Mixer)

Набор микрофонов (Realtek(R) Audio)

Audio Render:

Динамики (Realtek(R) Audio)

Direct X:

Version: 12.0

Driver: aticfx64.dll AMD Radeon(TM) Vega 8 Graphics

Resolution: 1920x1080, 32 bit

Video Memory: total - 4095 MB, free - 4088 MB

20.4. Settings changes

In this section, one can view the log of the following changes:

- settings TrueConf Server;
- List of conferences stored on the server
- changes to the parameters from [section Dashboard → PRO Licenses](#), including the manual reassignment of perpetual PRO licenses by the administrator;
- Modification of external systems integration settings (LDAP, DLP, corporate email)
- History of creating and modifying [surveys and campaigns](#), including the deletion of participants' responses
- settings TrueConf AI Server, with which [integration is configured](#) in full access mode;
- Settings of user groups and separate user accounts (available only in [Registry storage mode](#)).

Every entry in the table corresponds to a certain change. If you click on an entry, the panel on the right will display the server settings before and after this change.

Configuration Changes

[Help ?](#)

02.07.2022 0:00 - 02.08.2022 23:46		All actions	All objects	Username	Search	
Date and time ↑	Action	Object type	Username	Changes in	Details	
02.08.2022 11:20:15	edit	user	anonymous	id, company, first_na...	Date and Time: 01.08.2022 16:13:59 Action: edit Object Type: conference Username: anonymous Changes: id: 0477158272 -> 0477158272 topic: webinar -> Webinar schedule: { "type": 1, "duration": 28800, "start_time": 1659268800, "time_offset": 0, "special_time_offset": 180 } -> { "type": 1, "duration": 28800, "start_time": 1659528000, "time_offset": 0, "special_time_offset": 180 } registration: { "end_at": 1659297600, "fields": { "email": { "index": 1, "is_required": true }, "display_name": { "index": 0, "is_required": true } }, "enabled": true, "start_at": null, "allow_users_access": false, "participants_limit": null, "participants_limit_enabled": true } -> { "end_at":	
01.08.2022 18:36:43	create	conference	anonymous	id, pin, url, tags, typ...		
01.08.2022 17:20:34	create	user	anonymous	id, email, groups, sta...		
01.08.2022 16:13:59	edit	conference	anonymous	id, topic, schedule, r...		
01.08.2022 16:12:23	edit	conference	anonymous	id, topic, invitations		
30.07.2022 17:50:34	edit	conference	anonymous	id, owner, invitations		
30.07.2022 17:30:29	create	conference	anonymous	id, pin, url, tags, typ...		
30.07.2022 16:22:21	edit	https_config	anonymous			
30.07.2022 16:21:35	edit	https_config	anonymous			
30.07.2022 14:27:26	create	conference	anonymous	id, pin, url, tags, typ...		
Total: 36						

1. General table interface (see the description above).
2. Name of the modified parameter.
3. Parameter values: **previous** (before change) -> **new** (after change).

For example, the picture above illustrates an event involving some changes in the conference settings. The following parameters were changed:

- Name (`topic` parameter)
- Schedule settings (`schedule` parameter)
- Conference registration settings (`registration` parameter).

20.5. Conference recordings

This section contains a list of recorded conferences. Here you can playback, download or delete their records.

The recording storage settings are specified in [another section Recordings](#).

Conference Recordings

[Help ?](#)

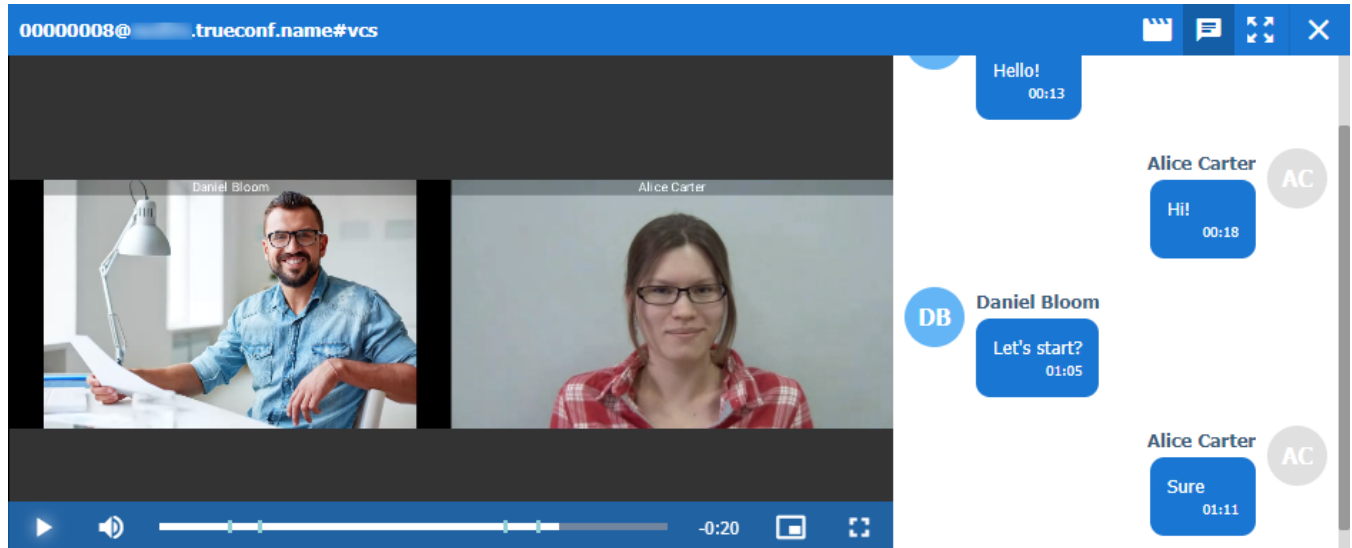
19.05.2023 0:00 - 22.05.2023 14:47		Conference name	Conference ID	Search		
Conference name	Session ID	Start	Duration	Owner	Conference ID	Size, MB
Webinar	0000002e5...	20.05.2023 09:...	00:59:51	klintz@video.e...	lcwebinar	250.5
(no title)	0000002d1...	20.05.2023 08:...	00:02:41	joe@video.exa...	lc578943531983	15.2
Meeting	0000002be...	20.05.2023 08:...	00:06:57	krowly@video...	lc9676777659...	29.4
Brainstorm	0000002ae...	20.05.2023 08:...	00:23:04	joe@video.ex...	lc785724251543	172.7
Conference	000000266...	19.05.2023 13:...	00:28:26	klintz@video.e...	lc115969749177	225.4
Total: 5						

1. General table interface (see the description above).
2. Link to the [page with detailed information](#) about the communication session.
3. Go to the conference card in the [general list](#).

4. Playback button
5. Recording download button
6. Delete button.

For point-to-point video calls, the name will be specified as **(no title)**.

You can use the ► button to playback recorded conferences with chat synchronization (for group conferences only):



Can I play a video recorded in TrueConf Server using third-party programs?

Yes, it can. In order to do it you will need to download and install a media player with VP8 video codec support, e.g. [VLC](#).

You can also upload any of your recordings to YouTube to share with your colleagues.

20.6. Connections

This section provides information about user endpoints. This information can be useful for **real time** technical support.

Endpoints

[Help](#) ?Show entriesSearch: 

Endpoint	Logged User	Application	IP
2BFA8A24F1CD0A7CA945BB2DCFD51765	smith@video.example.test/6700b600	TrueConf Android 2.2.0.198	10.160.2.47
442BEE7CC0D3B1756CE0F0E093DAE3EC	#guest:6984d2f1@video.example.test/0000	WebClient	127.0.0.1
4CBA1A1CD51F12834B60B58EC5771C7B	#guest:6d676ttt@video.example.test/0000	TrueConf Windows 8.3.0.1804	10.160.1.141
8CBEE50904C1B6B5F8149E0E2D5B60D0	#guest:54faa2f1@video.example.test/0000	WebClient	127.0.0.1
ABD6529586408CABF2A7E9C45B80EAD6		WebClient	127.0.0.1
D4163FC29C07C08BF0B1C4FE3A59774A		WebClient	127.0.0.1
D8B369622F06648EDA3A6565E923A6F8		WebClient	127.0.0.1
F021A1285D934697DD9D99B6CACCE452	kintz@video.example.test/bfc63314	TrueConf Linux 8.3.0.1804	10.160.1.141
F9349F7FBAE823E2D141FED9913223E7	#guest:b9b6feed@video.example.test/0000	WebClient	127.0.0.1

Showing 1 to 9 of 9 entries

Previous

1

Next

Use the quick search field to filter records by any of the parameters. The search is case-insensitive and can be performed for all fields (the table is filtered and you can see only those records that have at least one field with the entered string). It is possible to combine multiple searches. For example, to display only guest connections from the browser, search for **webclient guest**.

The **Application** column shows the application version, which can also be helpful for assisting users (for example, connections from mobile devices may be affected by the quality of the wireless connection or background operation settings in the OS). If a person connects from a browser, **TrueConf WebClient** will be displayed.

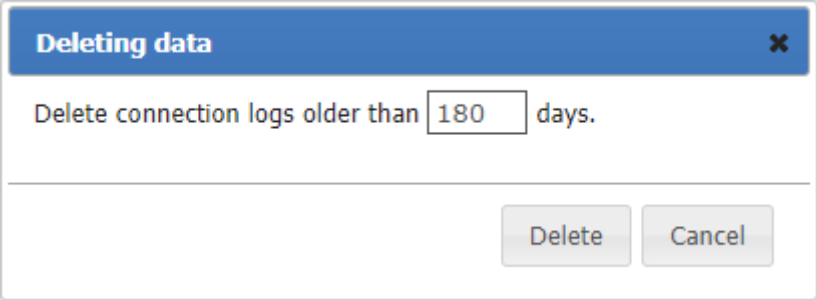
Authentication from a browser is logged only in two specific cases:

- The user, who connects from a browser, participates in a conference
- The user opens the **Chats** section in the personal area, if a person only signs in to the personal area, a new entry will not be created in the logs.

When you click on an entry in column **Endpoint**, the previously mentioned [user-specific connection details](#) page will open. Additionally, clicking on a field in column **Logged User** containing the user's TrueConf ID of this TrueConf Server will take you to the corresponding [profile page](#).

The absence of data about the authenticated user in the connection string indicates that this user has already left the meeting (e.g., if a guest participated in the conference from a browser and then closed the conference page).

It is possible to delete the entries older than a specified date. To do it, click the  button and specify the number of days beyond which data should be deleted (the default range is 180 days):



20.6.1. Events that update device information

Event	Editable fields
Connecting a device to the server or restoring the connection	• Network Info Type • Audio Capture • Audio Render • Video Capture • Direct X • Hardware Config
Ending the conference	Last Conf Name
Performing a network test (by pressing the corresponding button in the client application)	Network Test
Server Authentication	System information

21.2.1. Configuring Connection with the DLP System

Integration with DLP system

[Help](#) ?

This extension enables connection to a third-party DLP system via ICAP (RFC 3507).

☒ **Activate extension**

ICAP-server

Host

Port

Connection security

Test connection

Status: **DLP system is available (Cool DLP)**

1. Before you start using the DLP system, you need to check the box **Activate extension**. Until the box is checked and settings are saved with the **Apply** button at the bottom of the page, no checks will be active.
2. In section **ICAP-server**, configure the connection settings to the DLP system: host (IP or FQDN without the `http: / https:` prefix), port, and connection type (standard or secure via TLS).
3. Click the **Test connection** button to check the system's availability. You will see the result of the check in the status bar below.

21.2.2. Configuring Message Verification

In section **Text message checking**, set the parameters for handling regular messages:

Text message checking

☒ **Enable**

ICAP-request

REQMOD icap://%host:%port/ ICAP/1.0
Host: %host
Allow: 204
Connection: keep-alive
Encapsulated: req-hdr=0, req-body=%body_offset

POST / HTTP/1.1
Host: %server_name
X-Client-IP: %src_ip
X-Src-User: %src
X-Dst-User: %dst
X-Chat-Id: %chat_id
X-Chat-Title: %chat_title
X-Received-Date: %date
Content-Type: application/octet-stream

%body_length
%body

Set by default
Cancel

Action with an unwanted text message
☒ Replace the message with the text specified in the DLP system
☐ Replace the message with

☐ Leave unchanged
The DLP system responses will be ignored

Action with a text message if the DLP system does not respond
☐ Replace the message with

☒ Leave unchanged

DLP system response timeout (seconds):

1. Activate the checkbox **Enable**. Until the checkbox is selected and the settings are saved using the **Apply** button at the bottom of the page, the verification will not work.

2. In field **ICAP-request**, specify the fields to be transferred to the DLP system. The request format depends on the specific system, and below are listed the [variables used in the template](#), which are replaced with actual values when transferring data for analysis.
3. To reset the ICAP request settings, click the **Set by default** button.
4. The **Cancel** button allows you to undo the latest changes to the query text that were not saved using the **Apply** button.
5. In section **Action with an unwanted text message**, specify what to do if a message fails the DLP check. You can replace the message with the text selected in the DLP system, specify your own version, or leave it unchanged. In the latter case, users will receive all messages, but the DLP system logs will record the sending of unwanted messages.
6. In section **Action with a text message if the DLP system does not respond**, specify what to do if there is no connection with the DLP system. For example, you could specify the text **No connection with the security system** to prevent any messages from being delivered to recipients until the integration issue is resolved.
7. The parameter **DLP system response timeout (seconds)** is used to set the timeout for applying the settings from the previous sections. If the connection to the DLP system is disrupted, the time specified here will pass before the response selected in block **Action with a text message if the DLP system does not respond** is triggered (as attempts to restore the connection will be made). Subsequently, the connection check is performed in the background, and the transmission or blocking of messages will occur almost instantly.

21.2.3. File transfer verification in chats

In section **File checking**, set the parameters for handling the transferred files:

File checking

☐ Enable

Data format (MIME type)
 application/octet-stream
 If this parameter is changed, the template "ICAP-request" will be reset to default

ICAP-request
 REMOD icap://%host:%port/ ICAP/1.0
 Host: %host
 Allow: 204
 Connection: keep-alive
 Encapsulated: req-hdr=0, req-body=%body_offset

 POST / HTTP/1.1
 Host: %server_name
 X-Client-IP: %src_ip
 X-Src-User: %src
 X-Dst-User: %dst
 X-Chat-Id: %chat_id
 X-Chat-Title: %chat_title
 X-Received-Date: %date
 X-Filename: %filename
 Content-Type: application/octet-stream

 %body_length
 %body

Set by default
 Cancel

Action with an unwanted file
☒ Replace the file with the message specified in the DLP system
☐ Replace the file with a text message

The file was blocked

☐ Leave unchanged
The DLP system responses will be ignored

Action with a file if the DLP system does not respond
☐ Replace the file with a text message

The file was blocked

☒ Leave unchanged

DLP system response timeout (seconds): 300

The list of settings is similar to those ones for [message checking](#), but an extra parameter was added for selecting the request body type which improved compatibility with various DLP systems.

Don't forget to press the **Apply** button to save changes.

21.2.4. Trusted servers and advanced configuration for sending the list of chat participants

In the **White-listed servers** section, you can add addresses (FQDNs only, not IP addresses) of the video conferencing servers from which incoming messages and files do not need to be verified. This will speed up verification when multiple servers are integrated with the same DLP system, but be careful when using this feature. To edit an address, just click on it in the list:

White-listed servers

The messages from these TrueConf servers do not need to be checked.

Server name

video.example.net

Add

Additional

☒ Send the list of group chat participants if their number does not exceed

Apply

How whitelist verification works:

1. Let us suppose that you have the servers `example1.com` and `example2.com`; besides, [federation is configured](#) between them.
2. You want to use a single DLP system to check files in chats, including those ones sent between users of these servers, not just within a single server.
3. If the same DLP system is configured on two federated servers without a whitelist, the same message/file will be checked twice when sent in a federated chat. For instance, it will be checked as outgoing for the user registered on `example1.com` and as incoming for the user from `example2.com`, and vice versa.
4. To avoid double-checking the same message, you can whitelist the address of the other server on both servers. For instance, in the control panel of `example1.com`, add the address `example2.com`, and in the settings of `example2.com`, add the address `example1.com`.

Example of the activated **Send the list of group chat participants if their number does not exceed** parameter in action:

1. Let us suppose that the template includes the `%dst` and `%dst_user` parameters.
2. A limit of 30 participants is set for group chats.
3. For each chat with 30 users or less, the list of full TrueConf IDs and the list of logins will be sent in this format `domain\user`.

4. If the number of chat participants exceeds the limit, the list will not be generated (an empty list will be sent to the DLP system).
5. If the checkbox **Send the list of group chat participants if their number does not exceed** is unchecked, but the template contains the `%dst` parameter, the full TrueConf ID of the interlocutor will be transmitted for personal chats on DLP, while the participant list will not be transmitted for group chats.

21.2.5. Variables in ICAP request templates

- `%body` — request content (text message from the chat)
- `%body_length` — request content length (measured in bytes)
- `%body_offset` — request content offset in the encapsulated section (measured in bytes)
- `%chat_id` — unique GUID of the chat
- `%chat_id_origin` — `%chat_id` from which a message is forwarded (this field is empty if the message is not forwarded)
- `%chat_title` — chat name
- `%chat_title_base64` — `%chat_title` in base64 format
- `%content_length` — the content length of the request (decimal, in bytes)
- `%date` — date in [ISO 8601](#) format
- `%dst` is the recipient's full TrueConf ID in the format `user@server`. For a group chat, a list of all participants will be passed if the restriction from parameter **Send the list of group chat participants if their number does not exceed** does not apply. This holds true for all parameters of the form `%dst_YYY` except for `%dst_size`.
- `%dst_size` — the number of participants in the group chat. If the participant limit is triggered (see parameter **Send the list of group chat participants if their number does not exceed** at the bottom of the page) and the complete list of recipients is NOT transmitted, this number can be used to estimate the size of the data leak.
- `%dst_base64` — `%dst` in [base64 format](#)
- `%dst_user` — the recipient's login (part of TrueConf ID up to the `@` character) with the domain specified as `domain\user`
- `%dst_user_at_domain` — the recipient's login in the `user@domain` format (`@domain` may be omitted if the recipient is in the main domain)
- `%dst_user_at_domain_base64` — `%dst_user_at_domain` in base64 format
- `%dst_user_base64` — `%dst_user` in base64 format
- `%dst_user_no_domain` — recipient's login
- `%dst_user_no_domain_base64` — `%dst_user_no_domain` in base64 format
- `%host` — the value is taken from the field **Host**
- `%message_id` — unique message identifier
- `%multipart_boundary` — the value of the `boundary` parameter in the message header (intended to be used in the following way: `Content-Type: multipart/form-data; boundary=%multipart_boundary`)
- `%port` — the value is taken from the field **Port**
- `%server_name` — domain name TrueConf Server
- `%src` — complete TrueConf ID of the sender

- `%src_base64` — `%src` in base64
- `%src_user` — sender's login (part of TrueConf ID up to the `@` character) with the domain specified as `domain\user`
- `%src_user_at_domain` — the sender's login in the `user@domain` format (`@domain` may be omitted if the sender is in the main domain)
- `%src_user_at_domain_base64` — `%src_user_at_domain` in base64 format
- `%src_user_base64` — `%src_user` in base64 format
- `%src_user_no_domain` — sender's login
- `%src_user_no_domain_base64` — `%src_user_no_domain` in base64 format
- `%src_ip` — sender's IP address

Additional information is available for files:

- `%filename` — name of the file being sent
- `%filename_base64` — `%filename` in base64 format

21.3. Email Plugins

The **Email plugins** extension provides access to TrueConf's plugin settings for integration with popular email applications. Learn more about them in the [dedicated section on corporate calendars and email applications](#).

22. Integration with Calendars and Email

TrueConf offers a special module for seamless integration with corporate calendars and email plugins for popular mail and calendar applications: Microsoft Outlook, Mozilla Thunderbird.

22.1. Integration with a corporate calendar

To integrate with corporate calendars, the software [module TrueConf Calendar Connector](#) acts as a bridge between the server and the corporate calendar server software (e.g., Microsoft Exchange). It is installed on a separate server and can serve as a gateway for multiple TrueConf Server instances.

When editing conferences linked to a corporate calendar event in case of integration with TrueConf Calendar Connector, the server administrator will be able to change only a limited group of settings. For more details, refer to the [section describing how to work with conferences](#).

Before integration, ensure that the TrueConf Calendar Connector software is installed on a server that can access your TrueConf Server (see below). Additionally, TrueConf Calendar Connector requires a separate license for its operation, but no additional licenses will be needed for the video conferencing servers connected to it.

A separate settings block in section **Manage add-ons → TrueConf Calendar Connector** is used for configuring the integration.

Integration with TrueConf Calendar Connector

[Help ?](#)

TrueConf Calendar Connector is an external module for synchronizing data with the corporate calendar of your organization. The server users can view information about events and meetings from their mail calendar in TrueConf client applications.

If this extension is activated, all conferences scheduled earlier will not be displayed in the user interface.

To disable invitations to these conferences, [go to settings](#).

How to set up integration with TrueConf Calendar Connector

☒ Activate extension

Connection to TrueConf Calendar Connector

Host

outlook.com

Port

4315



Status: **Connection successful**

Apply

1. First, you need to check the box **Activate integration** to enable information exchange with TrueConf Calendar Connector.
2. Specify the domain name (FQDN) or IP address of the machine where TrueConf Calendar Connector is installed. To set up correct integration, you need to make sure that both servers can communicate with each other. The domain name (FQDN) or IP address of your

video conferencing server instance must also be configured on the side of TrueConf Calendar Connector.

3. Specify the TCP port used for communication with TrueConf Calendar Connector (default is **4315**).
4. Press the **Apply** button to activate the integration and view the connection status.

To ensure proper functioning, you need to activate TrueConf Calendar Connector and configure integration on its side [as outlined in its documentation](#).

22.2. Email Plugins

The **Email plugins** extension allows you to:

- Control the web version of Microsoft Outlook plugin that will be downloaded from your server
- obtain direct links to install the Windows version of the add-in for Outlook and plugin for Thunderbird;
- Customize a template invitation to a conference.

This extension is provided free of charge, including with version TrueConf Server Free.

Go to the **Manage add-ons → Email plugins** section. In the **Plugins** tab, you will be able to:



1. In section **Outlook (web)**, you can download the XML file to install the web version of the add-on (plugin) and update the current version on the server. You can copy the installation link using the  button and distribute it among users of the corporate network (including

those on a closed network without Internet access) so they can install it directly from your TrueConf Server.

2. Copy the download link for the desktop version of the Outlook add-on with the button  in the **Outlook (for Windows)** section and share it among users. They will be able to download the plugin from our website via the Internet. You can also distribute the application with the help of group policies since it is provided as an msi package.

For more details on installation and features of the desktop and web versions of the MS Outlook add-in, [refer to our knowledge base](#).

3. In section **Thunderbird**, use the  button to copy the link for installing the plugin for the Thunderbird application and distribute it among users.

On the **Settings** tab, you can change the default text of the description which is added when a new event is created with the help of any TrueConf mail plugins. Here, you can enable PIN code to be added in the description (providing that PIN was set previously):

Email plugins [Help ?](#)

Plugins **Settings**

Conference invitation

You are invited to the meeting %conf_name.

The conference owner: %owner_name

Click to join:
%conf_url

Reset to default

Cancel

The template supports HTML tags and variables ?

☒ Add conference PIN to invitation (when specified)

SAVE

By configuring a special `config.json` file, you can set certain fields available in the email plugin and their default values. In the knowledge base article TrueConf, we explain how to do this for different plugins:

- [Outlook](#)
- [Mozilla Thunderbird](#).

22.2.1. Configuring an invitation template

In the invitation template, one can use a group of constants similarly to the email templates available when [configuring SMTP](#):

- `%owner_name` — display name of the [conference owner](#);
- `%conf_id` — ID of the conference, e.g. `\c\df0a2adebe`
- `%conf_url` — link to the [conference page](#), for example:
`https://example.com/c/CID`
- `%conf_name` — name of the conference
- `%conf_type` — [conference access type](#) (private or public);
- `%max_speakers` — the maximum number of speakers (for a moderated role-based conference and a smart meeting, this is the left value in the pair of numbers $M \times N$)
- `%max_participants` — the maximum total number of participants (for moderated role-based conferences and smart meetings, this is the right-hand value in the pair of numbers $M \times N$)
- `%conf_mode` — [conference mode](#);
- `%conf_pin` — the PIN code for joining the conference
- `%conf_url_app_join` — a link for quick one-click connection in a client application without having to open the conference web page
- Server administrator contacts parameters:
 - `%admin_name` — display name
 - `%admin_email` — email address
 - `%admin_phone` — phone number.

22.2.2. Plugin configuration when using a self-signed certificate

If a [self-signed certificate](#) is configured on , additional settings will be required:

- If the Outlook plugin is used: no action is needed for the COM plugin, while for the web plugin, a user only needs to go to the server guest page in the browser and trust the self-signed certificate.
- If the mail plugin is used for the Thunderbird application, the certificate should be imported to each user's PC in the following way:

1. Export the TrueConf Server certificate from the control panel. To do this, go to the **Web → HTTPS** section, click on the **Download ca.crt** link, and choose where to save the **ca.crt** file. Distribute it to user PCs through any convenient method.
2. On the user's PC, open the settings in the Thunderbird application.
3. Go to the **Privacy & Security** section and click the **View Certificates** button.
4. In the window that opens, go to the **View Certificates** tab and click the **Import** button.
5. Select the **ca.crt** certificate file that you moved to this PC during Step 1.
6. Check all the boxes in the certificate trust settings window and click **OK**.

23. Integration with AI server

Let us discuss separately how to add AI capabilities for meeting transcription and summarization to your video conferencing server.

To integrate AI features into the video conferencing system, you need to use the stand-alone [solution TrueConf AI Server](#). A transcript is a text generated when the audio recording of a conference is recognized. If transcription is enabled for a conference, its audio is recorded during the video conferencing session and sent to the AI server according to the settings specified below.

To achieve integration, configure settings on both sides:

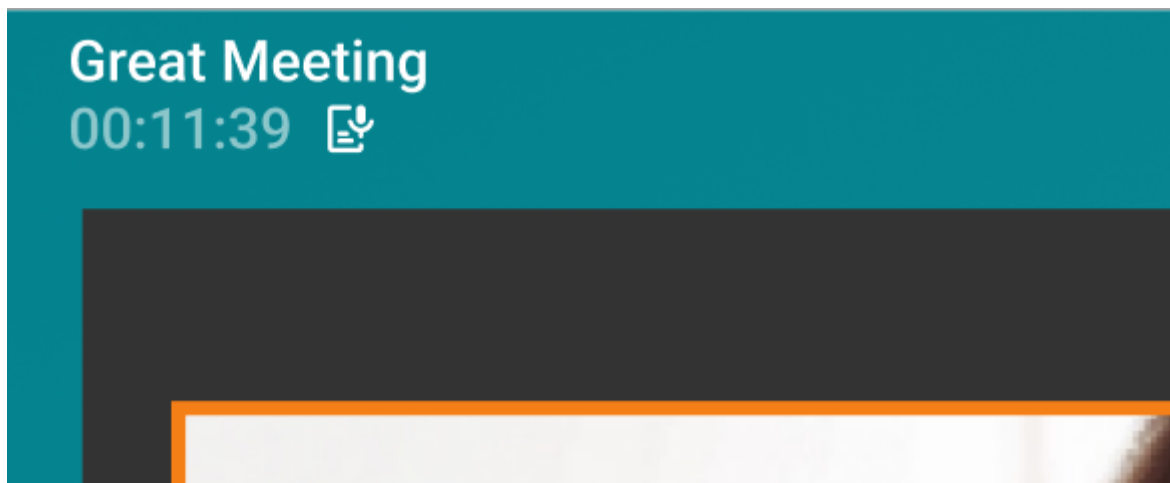
- in the TrueConf Server control panel under the **Manage add-ons → TrueConf AI Server** section (as explained later);
- in the [control panel TrueConf AI Server](#).

This integration offers the following features:

- Transcription (writing meeting minutes) of a past conference
- Access configuration for a transcript
- Send notifications when a transcript is ready and when a user is allowed access to a transcript
- Ability to start transcription automatically or manually.

To configure the integration of TrueConf Server with the installed TrueConf AI Server, go to the **Manage add-ons → TrueConf AI Server** section.

When the software begins to record the audio that will be sent to the AI server, participants will see the indicator in their TrueConf client applications (it will be displayed next to the duration timer):



This indicator is not displayed in browsers (for WebRTC participants) and for SIP/H.323 endpoints, but you can contact [our technical support](#) to activate this indicator by using a special parameter.

23.1. General data transmission and storage scheme for integration with an AI server

Data transmission occurs in the following way:

1. The user enabled conference recognition either during creation or "on the fly" through real-time meeting management.
2. On a machine with TrueConf Server installed, an .mp4 file containing audio but no video is created and starts recording in a separate folder for the conference. If the user starts and stops recording multiple times for a single session, multiple files will be generated.

Recording of the audio file that will be sent to the AI server does not depend on the video recording feature. Separate files are created for transcription purposes and stored in a separate directory on the server.

3. After the recording is completed (either by stopping the transcription or ending the conference), the file is sent to TrueConf AI Server.
4. Once the file transfer is complete (the file is fully uploaded to the AI server), recognition begins according to the settings: either [general](#) or at the conference level (see [the General tab](#)). This means that text creation may not start immediately, and the recording will wait until the user enables recognition.
5. Until the transcript is created, the user will not be able to download the original audio in the personal area or in the transcript section of the TrueConf application.
6. If the AI server has the capability to create meeting summaries, they can only be generated after the transcript is completed.
7. Если до того как запись была отправлена на ИИ сервер, она будет удалена на стороне TrueConf Server, то стенограмму создать не получится (записи же не будет у ИИ для работы с ней). Но если стенограмма была создана, то удаление записей на сервере не влияет на стенограмму. На стороне TrueConf AI Server есть свои настройки хранения аудио записей (ограничение на занимаемый объём). Стенограммы (текст) при удалении аудио не очищаются.

23.2. Access levels for conference protocols

You can connect only one instance of TrueConf AI Server to the video conferencing server with full access and an unlimited number of instances in read-only mode.

Reading is the integration mode of TrueConf Server with TrueConf AI Server, where users of the video conferencing server can have maximum access to viewing and downloading transcripts.

Full access — in this mode, all users of the video conferencing server can get all permissions for working with transcripts. In addition to viewing and downloading these files, they can grant other users access to them, start transcription, and delete the recording.

Access to each transcript can be configured individually and can override the default settings (see below).

23.3. AI server connection settings

The connection parameters with the AI server are set in tab **Connection**.

TrueConf AI Server

Help ?

Connection

Transcripts

Settings

How to configure integration with TrueConf AI Server

TrueConf AI Server

Enter a domain name

Read-only

Generate key

SSL certificate

☒

Verify the SSL certificate

This option allows you to disable the verification of TrueConf AI Server certificate

Generated keys

Domain name	Key	Access	Actions
10.110.0.38	eyJpZCI6InVhN2NtIiwibm...	Full	
10.110.0.39	eyJpZCI6InVhN2NtIiwibm...	Read-only	

1. Enter the domain name of the AI server in the corresponding field (without the `http://` or `https://` prefix).
2. In the drop-down list, select the maximum access level for your users when they will be connecting to the AI server.
3. Click the **Generate key** button to obtain the integration key, which you will need to specify later on the AI server side.
4. If you do not need to verify the authenticity of the SSL certificate (for testing purposes or due to issues with using a self-signed certificate on the TrueConf AI Server side), then uncheck the **Verify the SSL certificate** box.
5. Below you will see the list of added AI servers, their keys, and buttons for deleting unnecessary configurations. It is impossible to edit the settings of the servers which were added previously. They can only be deleted and added once again.

After generating the key, you (or another administrator) will need to [configure the integration on the TrueConf AI Server](#) side.

23.4. Viewing the list of completed and pending transcripts

On the **Transcripts** tab, you can see the list of transcripts for all conferences held on your server, where transcription was enabled:

TrueConf AI Server

Help ?

Connection

Transcripts

Settings

🔍 Name or ID

📅 All time

Status ▾

☐	Conference name	Session ID	CID	Date and time ↑	Duration	Status	Language	Actions
☐	Conference	00000532d9a677b5@vide...	/c/0061431750	17.03.2026 22:44	00:00:40	Not transcribed	En	
☐	Testing AI	000005225f6f54ce@video...	/c/7210535310	12.03.2026 12:35	00:10:02	Transcribed	Fr	

For the sake of confidentiality, the server administrator cannot download transcripts or configure access permissions for them. The [security admin](#), however, can view the content of transcripts and is allowed to configure access for them.

In each entry, there is a link that leads to the respective conference and even to the [page of a specific session \(call session\)](#). Please note that a single conference may have multiple sessions if it was launched more than once.

Column **Status** shows the current status of each transcript and can have the following values:

- **Added to queue** — The audio recording has been sent to TrueConf AI Server and is awaiting decryption.
- **Not transcribed** — the recording was not sent to the AI server and, accordingly, was not decrypted (for example, [manual recognition On request](#) is activated and has not yet started);
- **Transcribed** - The audio recording was successfully sent to the AI server and transcribed;
- **Transcribing** - Audio recording in progress (an approximate completion percentage will be displayed).

To quickly find required transcripts, filter the list by name or [conference ID](#), as well as by event time and the status of the transcript.

To start recording recognition, press the  button (available if it has not yet been started).

You can delete the transcript by clicking . This will remove both the transcription and the original corresponding audio track of the conference.

You can select multiple transcripts with checkboxes and delete them all at once.

23.5. Conference transcription settings

In the **Settings** tab, you can specify the general rules for audio transmission for recognition and sending notifications.

TrueConf AI Server [Help](#)

Connection Transcripts **Settings**

TRANSCRIPT RECORDING

Activation rule: On request Determined when scheduling a conference

RECORDING RECOGNITION

☒ Automatically
Transcription will start automatically when recording ends

☐ On request
It will be necessary to select a recording and activate transcription

Default transcription language: Russian

Default access to transcripts: Full access is given only to moderators. Other participants will be allowed to view and download records [Change](#)

Storage period for untranscribed recordings: 1 month

NOTIFICATIONS

Select the sender of notifications: AI Bot
ai-bot@video.example.net

☒ Recording is saved to the database

☒ Transcript is ready

☒ User is given access to a transcript/recording

SYSTEM NOTIFICATIONS

☒ Notify the administrator of system problems

[Apply](#)

1. Select the audio recording activation logic from the dropdown list **Activation rule**: record all conferences, only those specified on the [tab Advanced](#), or disable recording altogether.
2. After the conference ends, the recorded audio is sent to TrueConf AI Server, but the recognition process must be started separately. If the switch **Automatically** is activated in block **Recording recognition**, transcription will automatically start for all conferences (in queue order on the AI server side). If option **On request** is selected, the recognition process will need to be manually started for the required recording from either the [personal area of the video conferencing server](#) or the AI server.
3. Choose the default language that will be used when transcribing all conferences. Please note that the AI server can detect when conference participants switch to a different language. Moreover, it will correctly recognize different languages spoken by event participants. However, by selecting the main language spoken by participants, you can make transcription more accurate.
4. In parameter **Default access to transcripts**, specify which event participants will have access to the transcript. These are not final settings, and for each conference, those with full access can override permissions for other users from the [personal area of the VCS server](#) or AI server. The following default access options are available: full access for moderators and read-only for other participants; full access open to all participants; recordings available only to moderators and the server administrator, and not accessible to others; recordings available only to the server administrator, who can configure access for participants if necessary. In all cases except option **Records are available only to TrueConf Server administrators**, the conference owner always has access to the transcript.
5. The parameter **Storage period for untranscribed recordings** specifies the time period each audio recording will wait for recognition before being automatically deleted to reduce

the space occupied on the video conferencing server. Deletion occurs only on the TrueConf Server side and only for those recordings that have not been sent to the AI server.

6. In the **Notifications** section, you can select the account on whose behalf notifications about transcription events will be sent to users. This step is optional but it will help users to work with transcripts because all involved participants will receive relevant notifications. You can send notifications about the following events: an audio recording is added to the database of the AI server, a transcript is ready, and a user is given access to a recording or transcript.
7. Additionally, you can check the **Notify the administrator of system problems** box to send emails to the administrator (specified in the main server settings) regarding integration issues. For example, if the storage space allocated for audio files of this video conferencing server instance is running low on TrueConf AI Server.

There is no need for a continuously running chatbot to send notifications; so, no additional online licenses are used. You just need to [create a separate account](#) for notifications.

24. Security Admin Role Capabilities

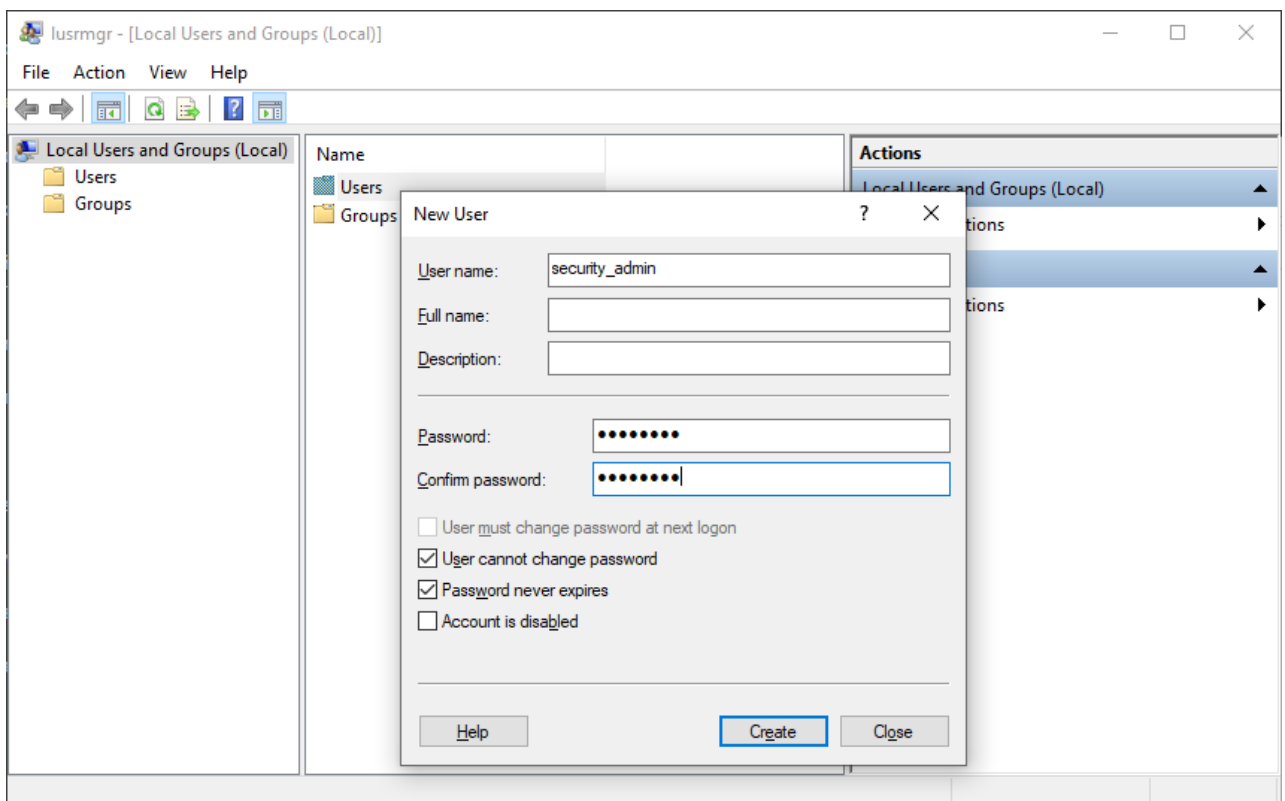
To enable limited access to the TrueConf Server control panel, a local **TrueConf Server Security Admin** user group on Windows and **tcsecadmins** on Linux is automatically added to your operating system during the server installation process. TrueConf Server administrators can add to this group the accounts of admins with view-only rights that should not be allowed to access TrueConf Server settings. Security admins only have the permissions to view:

- [event reports of the server](#);
- [history of video calls and conferences](#);
- [connection data to the server](#);
- [control panel access parameters](#);
- [chat messages](#);
- [conference recordings](#);
- in the case of integration with TrueConf AI Server — [access to transcript management](#);
- [server settings change history](#).

24.1. How to add a Windows account to the Security Admin group

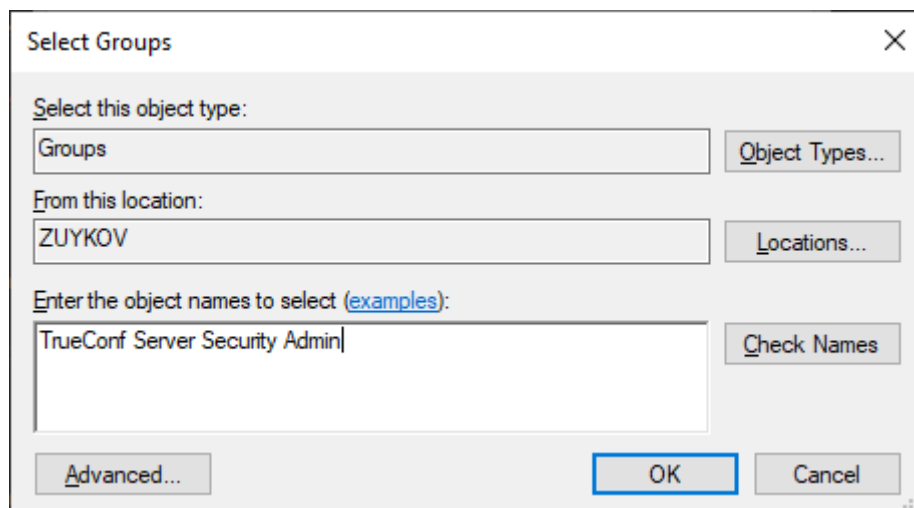
To create a new local Windows account with necessary rights:

1. Go to the **Local Users and Groups** snap-in. To do this, press **Win+R** and run the `lusrmgr.msc` command in the window that appears.
2. Right-click on the **Users** list and select **New User...**
3. Fill in the required fields and configure the password change settings.



4. Go to the **Users** list.
5. Right-click on the created account and navigate to **Properties**.
6. On the **Member Of** tab, click **Add...**

7. Specify **TrueConf Server Security Admin** as the name of the object to be selected and click **OK**.



Accounts imported from Active Directory/LDAP can also be added to the local group TrueConf Server Security Admin.

24.2. How to add an account to a group with the Security Admin role on Linux OS

The commands listed below need to be executed with superuser privileges or using `sudo` (e.g., `sudo command`). Please note that **sudo** may be unavailable by default in your operating system. You can check its availability using the `sudo -V` command.

For Debian

1. Run the following command:

```
sudo adduser --ingroup tcsecadmins [new_admin]
```

sh

where `[new_admin]` is the username of the admin.

2. Enter your password in the corresponding field and confirm it.
3. Optionally, provide additional information for the admin (full name, phone number, etc.).

For Debian

1. Run the following command:

```
sudo adduser --ingroup tcadmins [new_admin]
```

sh

where `[new_admin]` is the username of the admin.

2. Enter your password in the corresponding field and confirm it.
3. Optionally, provide additional information for the admin (full name, phone number, etc.).

For CentOS

1. Run the following command:

```
sudo adduser -G tcadmins [new_admin]
```

sh

where `[new_admin]` is the username of the admin.

2. Set the password for the new user `[new_admin]` with the following command:

```
sudo passwd [new_admin]
```

sh

In a similar way, you can [add a user](#) to the administrators group TrueConf Server with full access to the control panel.

24.3. How to configure rights for an existing user

You can also assign the appropriate access level to a user already existing in the OS.

For Windows OS

Simply go to the **Local Users and Groups** snap-in and complete steps 4-7 from the [section on adding an account](#).

For Linux OS

To configure system accounts, use the `usermod` command. For example, to add the user `[user]` to the **tcsecadmins** group, run the following command (as a superuser or using the `sudo` utility):

```
usermod -aG tcsecadmins [user]
```

sh

On Linux, one can view the list of user's groups or check if the user is actually available by running a single command:

```
groups [user]
```

sh

If the account `[user]` is included in the system, you will see the list of its groups; otherwise there will be a notification indicating that such a user has not been found.

The following instructions are intended for server administrators whose accounts are added to the user group **TrueConf Server Security Admin** on Windows and **tcsecadmins** on Linux operating systems.

24.4. How to access the control panel (admin panel)

1. Go to the [guest page TrueConf Server](#). You can get the address from the server administrator.
2. Click the **Administrator login** button at the bottom of the page.
3. Enter your username and password, then click **Enter**.

24.5. Server Status

Current status of your TrueConf Server performance is displayed in the upper right corner of the control panel. It shows server status and registration information.

When the server is functioning normally, you will see the text in green: **operational, registered**. If there are issues with the startup or registration, a red message will be displayed. Contact the server administrator to resolve the issue or to [submit a request to technical support](#).

24.6. Configuring Preferences

By navigating to the [section System → Preferences...](#) in the top right corner, you can configure the following settings for your account:

1. Language displayed in the TrueConf Server control panel.
2. Time zone. This setting affects the event time specified in all reports.
3. Settings for exporting logged data to a **csv** file: encoding and field delimiter.

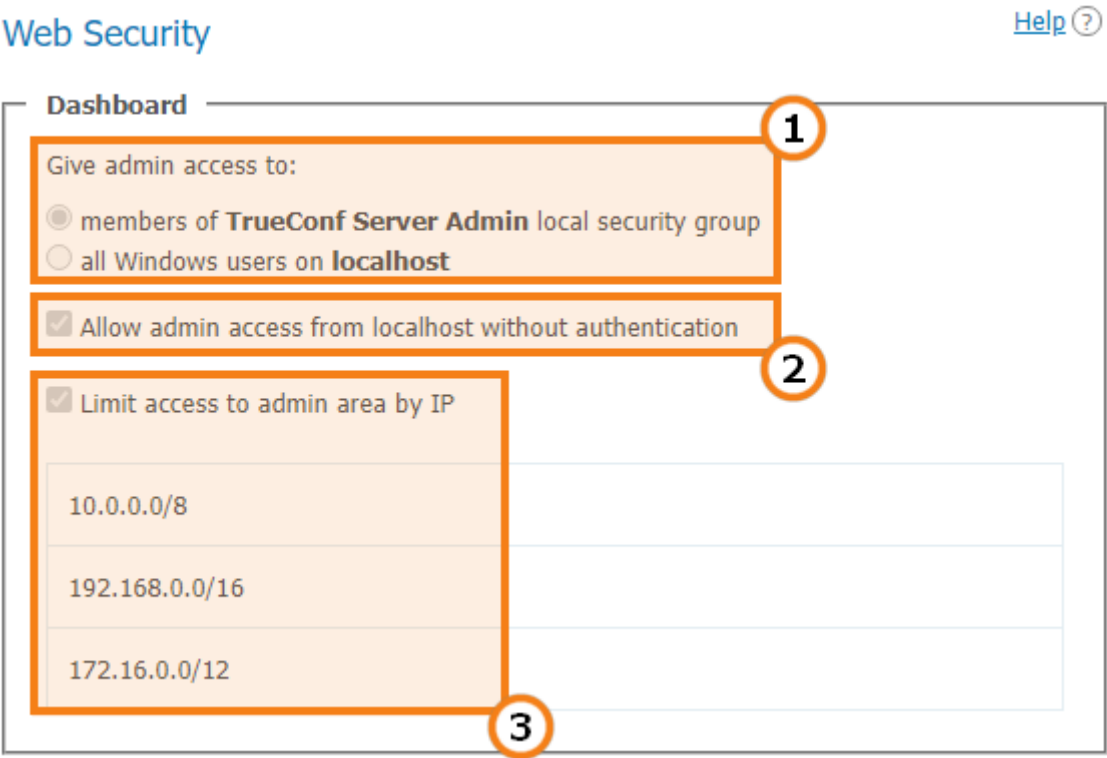
24.7. Server Log

To access detailed logs about the operation of TrueConf Server, go to the [section System → Server log](#). It stores events and errors related to the server services startup, connection to the [registration server](#), [license activation](#), and more.

You can save the log in a **txt** file using the  button. This will be useful for subsequent data analysis or for sending it to technical support.

24.8. Access Parameters

To view information about access settings for the server control panel, go to section **Web → Security**:



- 1. Operating system users that have full access to the control panel.
- 2. If this option is enabled, the user does not need to be authorized to perform administration when accessing the server from the following IP addresses.
- 3. This option means that administrative access to TrueConf Server control panel is limited only to the IP addresses specified in the list.

Security Admins are not allowed to change the settings described above; only TrueConf Server admins with full access rights can manage these settings.

24.9. Transcripts

The **Manage add-ons → TrueConf AI Server** section displays a list of conference transcripts (requires integration with the separate TrueConf AI Server solution):

TrueConf

video.example.net#vcs

System

Web

Security

Reports

Events

Call history

Chat messages

Configuration changes

Conference recordings

Endpoints

Manage add-ons

TrueConf AI Server

Logout

TrueConf AI Server

Help

Transcripts

Search Name or ID

All time

Status

	Conference name	Session ID	CID	Date and time ↑	Duration	Status	Language	Actions
☐	Conference	0000004fa0c968b0@video...	/c/1376217292	17.03.2026 22:40	00:00:17	Not transcribed	Fr	
☐	Brainstorm	0000004c579748ea@vide...	/c/5895612481	17.03.2026 21:30	00:02:15	Transcribed	Auto	
☐	Test AI	0000004baee17dc8@vide...	/c/3091438996	17.03.2026 16:36	00:33:10	Transcribed	Auto	

In each entry, there is a link that leads to the respective conference and even to the [page of a specific session \(call session\)](#). Please note that a single conference may have multiple sessions if it was launched more than once.

Column **Status** shows the current status of each transcript and can have the following values:

- **Added to queue** — The audio recording has been sent to TrueConf AI Server and is awaiting decryption.
- **Not transcribed** — the recording was not sent to the AI server and, accordingly, was not decrypted;
- **Transcribed** - The audio recording was successfully sent to the AI server and transcribed;
- **Transcribing** - Audio recording in progress (an approximate completion percentage will be displayed).

To quickly find required transcripts, filter the list by name or [conference ID](#), as well as by event time and the status of the transcript.

To start recording recognition, press the  button (available if it has not yet been started).

To configure access to a transcript, click the  button. In the pop-up window, you can add or remove users and specify the access level for each of them:

Record access management

 Add users by name or ID

Participants

 Allow to everyone
 Deny to everyone



Joe Smith
smith@video.example.net

Read-only





Ann Rose
admin@video.example.net

Full access



CANCEL SAVE

A user with full access will be able to download a transcript, configure access to it for other users, and delete it. In read mode, a user will only be able to download the recording and transcript. You can specify the TrueConf ID (login) of a user from another video conferencing server if your TrueConf AI Server is integrated with this server.

You can select multiple items with checkboxes and either download them or start recognition for all of them at once.

24.10. Reports

The **Reports** section contains all event logs related to server configuration changes, connections and video calls or conferences held on the server.

All reports are tabular data where the time of each event is displayed according to the [time zone selected in preferences](#).

Fields for data filtering are displayed above all tables except for information about connections to the server. You can also [save any report in csv format](#) except for the conference recording and endpoint lists by pressing the  button.

Clicking on any column in the table will sort the rows by that column in descending or ascending order. The current sorting direction will be marked with an arrow next to the column name.

Below you will find a brief description of the reports. You can learn more about logs in the [administrator guide](#).

24.10.1. Event Log

In the [section Events](#), you can view the history of user status changes TrueConf Server and the status of the VCS server. When you select a specific event in the table, detailed information about it will be displayed on the right side of the page.

Events [Help ?](#)

18.06.2023 0:00 - 19.06.2023 16:36 
All sources 
All severity levels 



Date ... 	Source	Object n...	Event	Severity	Description
19.06.202...	user	flowers@v...	status	Low	
19.06.202...	user	flowers@v...	login	Low	
19.06.202...	server	video.exa...	start	Medium	
19.06.202...	server	video.exa...	stop	High	
19.06.202...	admin	admin	restart	High	
19.06.202...	user	campbell...	status	Low	
19.06.202...	user	hayes@vi...	status	Low	
19.06.202...	user	white@vid...	status	Low	

Total: 115750

Host: 10.100.2.241
 Login: flowers
 appId: E7323A7A7FF655A2F74148F2124D9DE1
 Result: 0
 Rights: 000101110011111011111111111110001
 AppName: TrueConf Linux
 ExecTimeMs: 32
 DisplayName: Jane Flowers

1. General interface for interacting with the table: sorting, filtering, searching, and exporting. In the **Event** drop-down list, you can select one or multiple event types for more flexible information search or analysis.
2. TrueConf ID The username of the user who performed the action.
3. Event details. They include detailed information necessary for troubleshooting potential issues; the administrator may have to provide this information when contacting [technical support](#).

24.10.2. Call History

To view the list of past and active sessions, go to section **Call History**.

Call History Help ?

02.07.2022 0:00 - 02.08.2022 23:24

Conference ID

Owner

All modes

Search

Session ID	Start ↑	End	Duration	Participants	Owner	Mode	CID
0000009855057d39...	02.08.2022 16:57:21	02.08.2022 17:08:43	00:11:22	2	bronson@video.comp...	All on screen...	\c\19156941...
00000097b7c62da8@...	02.08.2022 16:21:01	02.08.2022 16:26:48	00:05:47	3	bronson@video.comp...	All on screen...	\c\brainstorm
00000096e9003773...	02.08.2022 16:18:39	02.08.2022 16:21:21	00:02:42	2	dawson@video.comp...	Video call	\c\04232061...
000000920367bc92@...	01.08.2022 18:33:28	01.08.2022 18:34:39	01:01:11	10	peters@video.comp...	All on screen...	\c\03860136...
000000902daa3a1e@...	01.08.2022 16:21:25	01.08.2022 16:59:38	00:38:13	5	smith@video.compan...	All on screen...	\c\10372891...
0000008ef5be8bc9@...	30.07.2022 17:50:53	30.07.2022 18:44:59	00:54:06	7	bush@video.compan...	All on screen...	\c\10372891...
0000008d2e1f0d28@...	30.07.2022 17:40:11	30.07.2022 17:41:51	00:01:40	3	bob@video.company...	All on screen...	\c\10372891...

Total: 23

Here you can view data for each videoconferencing session: session ID, start and end time, duration, number of participants, TrueConf ID of the owner, mode, and conference ID.

Clicking on the session ID will open a new tab with the detailed list of invited users and participants, as well as a  button to access the chat history.

24.10.3. Connection session information

Click on the session ID in the general table to view information about the selected conferencing session, including:

- information about time and owner of the conference
- list of what time the participant was attending the conference
- general media streams quality technical data
- history of conference invitations and accepted/rejected video calls
- buttons for exporting the lists of participants and invitees to a file
- button for opening the conference chat
- Sending files.

Conference Session:

Topic: Brainstorm

Start	End	Duration	Cause of ending	Participants	Owner	Mode	CID
17.04.2024 18:26:47	17.04.2024 18:35:32	00:08:45	Conference was ended by ...	4	flowers@video.exa...	Role-based (TCP)	vc17268100313

Participant List

User	Joined	Left	Duration	Disconnect c...	Bitrate in/out	CPU Load	FPS	Dimensions	Endpoint
Carla Devine	17.04.2024 18:...	17.04.2024 18:...	00:04:12	Conference en...	640 / 983	2	15	1280x720	E5238657753...
Carla Devine	17.04.2024 18:...	17.04.2024 18:...	00:00:52	Hung up	592 / 120	18	15	640x360	E5238657753...
Jane Flowers	17.04.2024 18:...	17.04.2024 18:...	00:08:43	Conference en...	670 / 992	24	15	1280x720	C2F08345BC5...
Abe Chester	17.04.2024 18:...	17.04.2024 18:...	00:08:45	Conference en...	620 / 0	0	0		E3825799E9E...
Bruce Hubbard	17.04.2024 18:...	17.04.2024 18:...	00:08:45	Conference en...	590 / 0	0	0		E3825799E9E...

Invite List

Date and Time	User	Recipient	Accepted
17.04.2024 18:26:47	video.example.net	flowers@video.example.net	✓
17.04.2024 18:26:47	video.example.net	chester@video.example.net	✓
17.04.2024 18:26:47	video.example.net	devine@video.example.net	✓
17.04.2024 18:26:47	video.example.net	hubbard@video.example.net	✓

File List

Date and Time	Sender	Name	Size, MB
17.04.2024 16:46:56	Abe Chester	group.jpg	0.05
17.04.2024 16:46:25	Jane Flowers	trueconf_quick_start.pdf	6.3

24.10.4. Chat messages

In the [section Chat Messages](#), you can view the history of all conversations between users of your TrueConf Server, including in group conference chats.

Chat Messages

02.07.2022 0:00 - 02.08.2022 23:42

Date and time	Sender	Recipient	Message	Details
02.08.2022 23:42:02	Ann Smith	bill@video.company...	So we can move on to the next step	Date and Time: 02.08.2022 23:39:39 Sender: Bill Browning [bill@video.company.com] Recipient: 0000009978eb6be8@video.company.com#vcs Message: I think we'll begin now. First I'd like to welcome you all and thank everyone for coming, especially at such short notice 🙏
02.08.2022 23:39:39	Bill Browning	0000009978eb6be8...	I think we'll begin now.	
02.08.2022 23:36:55	Bill Browning	ann@video.compan...	Hello. It's really great news 🙏	
02.08.2022 23:36:10	Ann Smith	bill@video.company...	Hi. Our presentation is ready! 🙏	
02.08.2022 23:35:20	Bill Browning	Group chat "New co...	Hi to all.	

Total: 10

- 1. General interface for interacting with the table: filter entries, export them to a CSV file, delete the entries selected in filter settings, sort by columns.
- 2. TrueConf ID (sender's and recipient's) usernames for personal messages.
- 3. Link to a [page with detailed information](#) about the session to the common chat of which a message was sent.

24.10.5. Changes to settings

To view the edit history of TrueConf Server settings, go to the [section Configuration Changes](#). This section also shows the creation/deletion of group conferences and their parameter changes by the server administrator.

Every entry in the table corresponds to a certain change. If you click on an entry, the panel on the right will display the server settings before and after this change.

Configuration Changes

[Help](#)

02.07.2022 0:00 - 02.08.2022 23:46		All actions	All objects	Username	Search
Date and time ↑	Action	Object type	Username	Changes in	Details
02.08.2022 11:20:15	edit	user	anonymous	id, company, first_na...	
01.08.2022 18:36:43	create	conference	anonymous	id, pin, url, tags, typ...	
01.08.2022 17:20:34	create	user	anonymous	id, email, groups, sta...	
01.08.2022 16:13:59	edit	conference	anonymous	id, topic, schedule, r...	Date and Time: 01.08.2022 16:13:59 Action: edit Object Type: conference Username: anonymous Changes: id: 0477158272 -> 0477158272 topic: webinar -> Webinar schedule: { "type": 1, "duration": 28800, "start_time": 1659268800, "time_offset": 0, "special_time_offset": 180 } -> { "type": 1, "duration": 28800, "start_time": 1659528000, "time_offset": 0, "special_time_offset": 180 } registration: { "end_at": 1659297600, "fields": { "email": { "index": 1, "is_required": true }, "display_name": { "index": 0, "is_required": true } }, "enabled": true, "start_at": null, "allow_users_access": false, "participants_limit": null, "participants_limit_enabled": true } -> { "end_at":
01.08.2022 16:12:23	edit	conference	anonymous	id, topic, invitations	
30.07.2022 17:50:34	edit	conference	anonymous	id, owner, invitations	
30.07.2022 17:30:29	create	conference	anonymous	id, pin, url, tags, typ...	
30.07.2022 16:22:21	edit	https_config	anonymous		
30.07.2022 16:21:35	edit	https_config	anonymous		
30.07.2022 14:27:26	create	conference	anonymous	id, pin, url, tags, typ...	
Total: 36					

1. General interface for interacting with the table: filter by events and objects, date, user. Additionally, it is possible to export filtered values to a CSV file.
2. Name of the modified parameter.
3. Parameter values: **previous** (before change) -> **new** (after change).

24.10.6. Conference recordings

In the [section Conference Recordings](#), you can view a list of all video call and conference recordings saved on the server, including detailed information about each.

To download or view the recording file, use the  and  buttons respectively.

24.10.7. Connections

To view connection statistics for your TrueConf Server, go to the [section Endpoints](#). It displays information about all [connections to the server](#) made using client applications or through a browser via [WebRTC technology](#).

Authentication from a browser is logged only in two specific cases:

- The user, who connects from a browser, participates in a conference
- The user opens the **Chats** section in the personal area, if a person only signs in to the personal area, a new entry will not be created in the logs.

Click on a row to display detailed information about the selected connection:

Endpoint properties (A244B2B1E4687DDA60F1D725980D1E07)

Logged User:

bob@server.company.com/8ec2d06d

IP:

192.168.88.181

Local Ip:

192.168.80.1:65019, 192.168.234.1:65020, 192.168.88.181:61856, fe80::79:44e6:fc89:7d6a:44308, fe80::7d67:d379:9c12:8960:44308, fe80::8dd:6787:d1e5:259c:61858

Audio Capture:

Микрофон (SplitCam Audio Mixer)

Набор микрофонов (Realtek(R) Audio)

Audio Render:

Динамики (Realtek(R) Audio)

Direct X:

Version: 12.0

Driver: aticfx64.dll AMD Radeon(TM) Vega 8 Graphics

Resolution: 1920x1080, 32 bit

Video Memory: total - 4095 MB, free - 4088 MB

25. Security in TrueConf Server: How we protect user data

When holding corporate video conferencing, privacy is an essential factor. Intruders should be prevented from accessing data even in case they manage to invade a company's internal network.

We take the privacy of our customers' conferences seriously.

TrueConf Server offers multiple levels of security, ranging from basic to cryptographically secure. It uses encryption technologies, modern authentication methods, and server-level access settings for each conference or for general communication features.

25.1. Level 1. Administrative settings

An outsider cannot connect to the corporate VCS system TrueConf without your knowledge. Authorization data is either [set by the network administrator](#) for each user individually or [imported via LDAP from a directory service](#) (such as Active Directory, OpenLDAP, FreeIPA, ALD Pro, etc.).

TrueConf does not store users' passwords in an unencrypted form in any of its solutions. Cryptographic hash functions are used for authorization.

The administrator can configure additional settings to increase access security:

- [activate two-factor authentication \(2FA\)](#);
- Use [single sign-on \(SSO\) technology](#) when integrating with directory services via LDAP
- [Select authentication methods](#) depending on the network from which users are trying to log in: external network or trusted (corporate) network
- [Configure various options \(for example, restrict file transfer\) for users depending on the network](#) they are authenticated from: external network or trusted (corporate) network
- At any time, you can both [log out a user](#) from TrueConf on all authenticated devices and completely deactivate the account.
- [Restrict the lifetime of authorization session keys](#) to make sure that users have to sign in with their password if they want to continue working with the system (this precaution may be helpful in some cases when users forget to lock their PCs)
- [set password complexity](#) (when manually creating accounts in Registry mode);
- [Configure account lockout policy](#) if a user enters an incorrect password multiple times (also available when running the server in integration with an LDAP directory)
- Restrict permissions for certain [user groups](#), for example, prohibit accountants from sharing content, while granting operator privileges to the IT department so they can assist colleagues during conferences.
- [Select the content](#) that will be sent in push notifications to mobile devices
- Restrict permissions specifically for external users, i.e., the users, who have an account on a federated server (more details on how to [use federation for external chats are provided below](#))
- Restrict permissions specifically for external users, i.e., the users, who have an account on a federated server
- [Prohibit the use of specific application versions](#) on certain operating systems.

To hold [public conferences](#) (e.g., [webinars](#)), you can provide unauthorized users with guest access (participation parameters can be finetuned). You will be able to:

- [restrict the list of features for guests](#) at the conference level;
- [enable mandatory registration](#) for the webinar;
- [Restrict the features available to guest users](#) (restrictions will apply to all conferences).

25.2. Level 2. Unique chats for different sessions

If you escalate a group chat into a conference multiple times, each conference will be a new event with its own ID. This means that the participant list may vary, and not all users from the chat need to be included. To confidentially discuss certain matters with a limited group, you can create a unique chat for each conference. In this way, you can make sure that the conversation remains private and is not visible to other group chat members. By default, the chat remains shared for the sake of convenience (i.e., the original chat), and to create a new confidential chat for a conference, you need to unlink it [as shown in the application documentation](#).

25.3. Level 3. Proprietary video codec

To encode video streams, we use our own implementation of VP8 video codec with advanced [SVC support](#). Eventually, even if a video stream is seized (which is also almost impossible – see the following sections), intruders cannot decode video by standard means.

25.4. Level 4. Single port operation

For transmitting media streams and signaling data over the TrueConf protocol between the TrueConf applications and the TrueConf Server [server, only one TCP port](#) is used, which is 4307. The traffic is encrypted using AES and, if necessary, additionally according to GOST standards.

If you are not planning to use third-party protocols (WebRTC, SIP, H.323, RTSP or RTMP), you can close all ports except for 4307 and 443 (used for secure HTTPS connection) on your networking equipment. This will guarantee total safety of your video conferencing system on a hardware level.

We urge you to [configure HTTPS](#) immediately after installation, as it affects users' ability to access their personal area and use several application features, such as conference scheduling, working with surveys, transcripts, etc.

25.5. Level 5. Administration access control in the video conferencing server

You can grant [access to the server control panel](#) at different levels:

- Only from the computers in the local network
- specify the [range of IP addresses](#) from which the control panel is accessible;
- [select the OS user accounts](#) where TrueConf Server is installed;
- Specify the access level for each administrator: full access or view-only access for reports and video conference recordings.

This prevents unauthorized access to the [control panel](#).

25.6. Level 6. Control data encryption

Our protocol for transmitting signals regulating data exchange is encapsulated within a well-established transport layer security protocol (TLS 1.3), a more modern version of SSL protocol. This protocol is also used for connection security via SIP and WebRTC third-party protocols. They are used for connection with browsers and video conferencing endpoints via TrueConf Server multiprotocol gateway.

When setting up integration with directory services, one can use the [secure LDAPS protocol](#) with a TLS certificate.

25.7. Level 7. Media data encryption

TrueConf Server employs the AES-256 algorithm, which uses the maximum key length available, to encrypt media data. Hardware-accelerated AES support is built into all modern Intel, AMD, and ARMv8 processors, significantly enhancing videoconferencing security without compromising performance.

Media data (video, audio, content) transmitted via TrueConf Server gateway are also encrypted, depending on the technology used:

- WebRTC – with DTLS and SRTP protocols and algorithms.
- SIP – with SRTP protocol.
- H.323 – with H.235 protocol.

25.8. Level 8. End-to-end encryption using VPN gateways

To make sure that the privacy of communications in your enterprise network segments is protected, you can install software or hardware VPN gateways that provide end-to-end encryption of all corporate traffic over the ports used by TrueConf services. As we've mentioned earlier in this post, only two ports are required.

Our [support team](#) will be happy to help you configure integration of our software with these systems.

25.9. Level 9. Offline operation in your corporate network

Most importantly, when using TrueConf Server, you can fully eliminate the risks related to cloud providers:

- Only your employees have physical access to servers that provide the functionality of video conferencing system services.
- TrueConf Server is stand-alone and doesn't require an Internet connection so it can be isolated in the local network. So, only your users can access its services.
- You are not dependent on the stability of Internet connection and power supply in the data processing center (you can also order a stand-alone generator to ensure power supply in case of an emergency)
- You take full control over the allocation of hardware resources for the components of TrueConf Server. One can rest assured that these resources are not taken by third-party software solutions.

When using cloud-based and hybrid video conferencing systems, you cannot ensure that:

- The developers of cloud-based services do not have remote access to their servers, reports, parameters of conference participants' devices, and other sensitive information.
- System administrators who operate data centers of such video conferencing services do not have access to the runtime environment and its file system.
- The employees of these services do not compromise information about your negotiations in order to comply with foreign legislation on the disclosure of user data or to obtain certain certifications.
- Recordings of your negotiations cannot be accessed by any hacker in the Internet who intercepted the login and password to your account.

When using TrueConf Server, you completely eliminate these risks. Only your employees have physical access to the servers that ensure the operation of the video conferencing service. Moreover, TrueConf Server is entirely autonomous and does not require an Internet connection to work, which means that it can be isolated within the corporate (private) network and only your users will have access to its services.

25.10. Level 10. Flexible settings of file storage period

To improve data security, a TrueConf Server administrator can configure separate storage period settings for:

- [conference and call recordings](#);
- [files transferred in personal and group chats](#).

In addition, it is possible to limit the amount of disk space available for storing chat files.

25.11. Level 11. Access to API via OAuth 2.0 protocol

TrueConf Server provides a [rich set of API tools](#) for a complete integration of your video conferencing system and third-party software. OAuth 2.0 mechanism that is used for this purpose provides a number of advantages:

- Working over the secure HTTPS Protocol.
- Delimiting application access to the API according to the role and configured permissions.
- Application authorization process using a complex short-lived access token without the need to visibly enter a username and password.

25.12. Level 12. Regular security updates

For TrueConf Server, maximum protection against potential attacks is supported because:

- In addition to internal audit, our software is regularly tested for potential vulnerabilities by domestic and foreign customers.
- All discovered vulnerabilities are recorded in the [FSTEC National Vulnerability Database](#) and in the U.S. National Institute of Standards and Technology databases ([NIST](#)).
- As a vendor, we promptly release security updates for all detected vulnerabilities.

25.13. Level 13. Encryption support for all stored data

Feel free to use third-party encryption methods because they will not affect the performance of TrueConf Server:

- Hardware encryption of the entire disk
- [Software encryption](#) at the level of logical disk partition (e.g., eCryptis for Linux or BitLocker for Windows).

25.14. Level 14. Integration with DLP

[TrueConf Enterprise](#) is a communications platform for large customers. It supports integration with **DLP systems (Data Leak Prevention)**, specialized software designed to prevent data leaks and comply with security policies adopted in organizations. Thanks to the support for the ICAP protocol, you can configure the verification of messages and files in chats through any DLP system. This will provide an additional layer of security for corporate discussions.

Integration settings with DLP are detailed in [this section of the documentation](#).

25.15. Level 15. Connection of external users via a separate server

If users in your organization often need to communicate with external users in private or group chats, you can deploy a separate server in the DMZ zone of the corporate network. It is possible to set up federation between this server and the main video conferencing server. This approach not only enables communication with users outside your organization but also allows you to flexibly set permissions for external users. For instance, you can restrict file sharing for security purposes. Moreover, placing the server in the DMZ ensures that the main network perimeter of the company is not at risk.

For more information on using a guest server, refer to the [relevant article](#).

25.16. Level 16. Traffic protection with the border controller

The comprehensive solution [TrueConf Enterprise](#) offers a dedicated module for securing external connections (outside the network) called TrueConf Border Controller. It allows for efficient filtering of traffic from TrueConf client applications, permitting only secure protocols TrueConf and HTTPS towards the video conferencing servers. Additionally, traffic encryption is available using a variety of symmetric algorithms, including the use of PSK (Pre-Shared Key).

More information and the workflow schema can be found in the [solution documentation](#).

25.17. Level 17. Custom push notification service

In the standard scheme of push notifications delivery, an external TrueConf service at the address `reg.trueconf.com` is used. All notifications are proxied through this service and then sent to a client application on the mobile device, depending on where the application was installed from (more details can be found [here](#)).

Such a setup may not be suitable for large clients requiring integration with MDM systems or needing the highest priority for sending push notifications (without going through the general queue at `reg.trueconf.com`). In this case, TrueConf can provide an on-premises notification server, which will be installed within the customer's infrastructure. It will independently proxy

push notifications through notification providers. For more details, your IT security managers can contact TrueConf team in [any convenient way](#). We will answer each of your questions.