

TrueConf Server

Administrator guide



Version 5.4.3

Table of Contents

1. Description of the video conferencing server and its features	8
1.1. Why do I need a video conferencing server?	8
1.2. Features	8
1.2.1. Supported protocols and codecs	8
1.2.2. Modules of the video conferencing server and their functionality	9
1.3. Choose your license	11
1.4. Advantages	11
1.4.1. Relatively low system requirements	11
1.4.2. Working in a closed network	11
1.4.3. Convenient administration	11
1.4.4. Advanced data transmission technologies	11
1.4.5. 4K video conferencing	12
1.4.6. Collaboration tools	12
1.4.7. Streaming conferences to popular services	12
1.4.8. Managing video layouts and participants' devices	12
1.5. Useful guides	12
2. User types	13
2.1. User roles	13
2.2. User identifier	13
2.3. Roles of conference participants	13
2.4. Admin roles	14
3. Types of video conferencing	15
3.1. What is a video call?	15
3.2. What is a video conference? Types of video conferences	15
3.3. Video conferencing modes	16
3.4. Conference ID	17
3.5. What is a waiting room	17
4. Extensions	18
4.1. SIP / H.323 / RTSP gateway	18
4.2. Integration with LDAP and Active Directory	18
4.3. Public Web Conferences	18
4.4. Live streaming	18
4.5. Simultaneous interpretation	18
4.6. Federation	19
4.7. Integration with DLP	19
4.8. Support for SDK applications	19
4.9. UDP Multicast	19
4.10. TrueConf Directory	21
4.11. TrueConf License Manager	21
4.12. TrueConf Border Controller	21
4.13. TrueConf Enterprise	21

5. Licensing of the video conferencing server	23
5.1. Online users	24
5.2. PRO licenses and conference participation	24
5.2.1. Key aspects of using PRO licenses	25
5.2.2. Use of PRO licenses during federation	26
5.2.3. Examples of how PRO licenses are counted	26
5.3. SIP/H.323/RTSP connections	27
5.4. Guest connections	27
6. Installation and upgrade. System Requirements	28
6.1. System requirements for the video conferencing server	28
6.2. Registration key validation	29
6.3. Installation	29
6.3.1. Which services will be added to the OS after installation	29
6.3.2. For Windows	30
6.3.3. For Linux	31
6.3.4. How to change the port to access the control panel without reinstalling TrueConf Server	33
6.4. Upgrading the video conferencing server	34
7. Registration	35
7.1. What is the registration key and server ID?	35
7.2. TrueConf Server Name	36
7.3. Registration process	37
7.4. Offline registration	37
7.4.1. Re-registering the server in a private network	38
7.4.2. Registration of a re-installed server	39
7.5. Changing the registration key	40
7.6. Registration: Frequently Asked Questions	40
8. Initial setup	41
8.1. Control panel access settings	41
8.2. Server status	41
8.3. Server log	41
8.4. Configuring preferences	42
8.5. Adding users	42
8.5.1. Where can I find client applications	42
8.5.2. How to connect client application to the video conferencing server	43
8.6. PDF file import settings	44
8.6.1. For Windows	44
8.6.2. For Linux	45
9. Information about the server and PRO licenses. Storage settings	46
9.1. Control panel	46
9.1.1. Summary	46
9.1.2. PRO licenses	48
9.1.3. Main settings	49
9.1.4. Configuration back-up and restore	51

9.1.5. Settings for client application connection	51
9.2. How to use other folders on Linux with symlink	52
9.3. Mounting a network storage on Linux	54
9.4. Access settings for network storage on Windows	55
9.5. File Storage	55
9.6. Recordings	56
10. Settings for network, notifications and federation	59
10.1. Network Settings	59
10.2. SMTP	60
10.2.1. Email template settings	61
10.2.2. Notifications about missed calls	61
10.2.3. Conference invitations	61
10.2.4. Reminders about the upcoming conference	61
10.2.5. Confirmations of registration for a public conference	61
10.2.6. Notifications about removal from a conference	61
10.2.7. Parameters used in email templates	62
10.3. Federation	62
11. SIP/H.323/RTSP gateway and transcoding	65
11.1. Sip gateway	65
11.1.1. Network settings	65
11.1.2. Rules for SIP connections	66
11.1.3. New rule form	66
11.1.4. Skype for Business integration configuration	69
11.1.5. Global SIP settings section	69
11.1.6. Invitation of the SIP endpoint to the conference on TrueConf Server	70
11.1.7. How to join a conference with its CID (conference ID) from an SIP endpoint	70
11.2. H.323 gateway	71
11.2.1. Network settings	71
11.2.2. Rules for H.323 connections	71
11.2.3. New rule form	71
11.2.4. Global H.323 settings	73
11.2.5. How to call TrueConf users and conferences from H.323 devices	73
11.2.6. How to register H.323 devices on the video conferencing server	73
11.3. Chat during calls on TrueConf MCU	74
11.4. RTP	74
11.5. WebRTC	74
11.6. Transcoding	75
11.6.1. Quality settings	75
11.6.2. Adding background and watermark	76
12. Web and HTTPS settings	78
12.1. Web Settings	78
12.1.1. Guest page settings	78
12.1.2. Additional documents	79

12.2. Security	80
12.3. HTTPS	82
12.3.1. HTTPS configuration	82
12.3.2. Self-signed and custom certificates	83
12.3.3. Self-signed certificate	83
12.3.4. Custom certificate	83
13. Server users. Integration with LDAP/Active Directory	85
13.1. User Accounts	85
13.2. User profile	86
13.2.1. User deactivation	87
13.2.2. Calls and conferences	87
13.2.3. Application settings	88
13.2.4. User address book	89
13.3. Groups	90
13.3.1. Editing groups in Registry mode	91
13.3.2. Editing Groups in LDAP Mode	92
13.3.3. How the restrictions of rights work	92
13.3.4. Editing group's name and its members	92
13.3.5. Setting up address book for users of the group	94
13.3.6. Setting application settings for group users	94
13.4. Aliases	95
13.4.1. Description	95
13.4.2. Use for federation	95
13.5. Authentication	96
13.5.1. Access zones settings	97
13.5.2. SSO and AD FS settings	97
13.6. LDAP / Active Directory	99
13.7. Registry mode	100
13.8. LDAP mode	100
13.8.1. How to upload user accounts from different domains	102
13.8.2. Certificate installation for LDAPS connection	103
13.9. How to address typical issues when using LDAP	103
13.10. Password and account lockout settings	104
13.10.1. Password requirements	104
13.10.2. Automatic lockout	105
14. Group conferences and streams	107
14.1. Conference list	107
14.2. Conference page	108
14.3. How to configure an ongoing meeting	109
14.3.1. "Information" tab	109
14.3.2. "Participants" tab	111
14.4. Creating a new conference	111
14.4.1. "General" tab	112

14.4.2. "Participants" tab	114
14.4.3. "Interpretation" Tab	116
14.4.4. "Layout" tab	117
14.4.5. "Media" Tab	118
14.4.6. "Advanced" tab	119
14.4.7. Restrictions for webinars	123
14.4.8. "Registration" tab	124
14.5. Templates	126
14.6. Streaming	127
14.6.1. Streaming through CDNvideo cloud service	128
14.6.2. Streaming via third-party services and products	129
14.6.3. Wowza Streaming Engine	130
14.6.4. Wowza Streaming Cloud	130
14.6.5. YouTube	131
14.6.6. Manual settings	132
14.7. Conference settings	134
14.7.1. Automatic conference deletion	134
14.7.2. Limit on incoming video quality	135
14.7.3. Ways of joining conferences	135
15. Working with the server API	136
15.1. How API and OAuth 2.0 work	136
15.2. Permissions	137
15.3. Creating new OAuth 2.0 application	137
15.4. Editing application	137
16. Server logs (reports)	138
16.1. Events	138
16.1.1. Description of event types	140
16.2. Call History	141
16.2.1. Call list	141
16.2.2. Session information	141
16.2.3. Connection properties	143
16.3. Chat Messages	143
16.4. Configuration Changes	143
16.5. Conference Recordings	144
16.6. Endpoints	145
16.6.1. Events that update device information	146
17. Configuration of extensions	147
17.1. TrueConf Directory	147
17.2. Integration with DLP	147
17.2.1. Variables in the templates of ICAP requests	149
17.3. Mail plugins	150
18. Permissions of the administrator with the Security Admin role	153
18.1. How to add a Windows account to the Security Admin group	153

18.2. How to add an account to the Security Admin group on Linux	154
18.3. How to configure rights for an existing user	154
18.4. How to access TrueConf Server control panel	155
18.5. Server status	155
18.6. Configuring preferences	155
18.7. Server log	155
18.8. Access settings	155
18.9. Reports	156
18.9.1. Events	156
18.9.2. Call History	156
18.9.3. Chat Messages	157
18.9.4. Configuration Changes	157
18.9.5. Conference Recordings	157
18.9.6. Endpoints	157

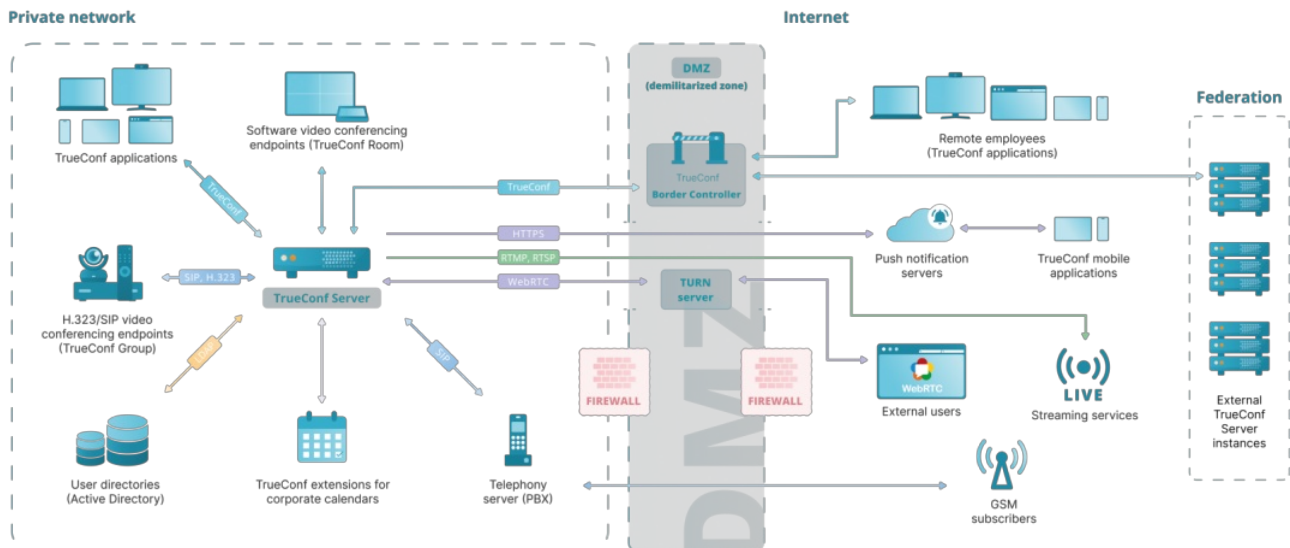
1. Description of the video conferencing server and its features

1.1. Why do I need a video conferencing server?

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

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

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. Features

TrueConf Server core features can be extended by the following TrueConf 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 set: BFCP for content sharing; FECC for camera control; SRTP for media stream encryption; TLS for signaling protocol protection.
- WebRTC: SRTP and DTLS for media stream encryption.
- RTSP video calls.
- QoS support: DSCP, DiffServ.
- Work with TrueConf API using OAuth 2.0 protocol.

1.2.1.2. Supported video codecs

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

1.2.1.3. Supported audio codecs

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

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 server. It is installed as multiple operating system services and provides:

- user authentication and authorization: multilogin is also supported which means that it is possible to work in several client applications under the same account
- support for [multi-point video conferences](#) and [point-to-point video calls](#)
- events logging (call history, usage stats, chat messages, etc)
- NAT traversal and proxy servers to connect users
- media stream processing with [scalable video coding \(SVC\)](#)
- Compatibility of conferences with third-party protocols and systems ([SIP/H.323](#), [RTSP](#), [WebRTC](#), [LDAP](#), DLP systems)
- [federation](#) with other TrueConf Server instances
- connecting multiple TrueConf Server instances in a unified communications platform with [TrueConf Enterprise](#).

1.2.2.2. Administrator control panel

This component is used to [control and modify TrueConf 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 (by login/password, via SSO, with the help of two-factor authentication providers, for example, 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 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.
- Stream conferences via CDNvideo, Wowza Streaming Engine, Wowza Streaming Cloud, YouTube, etc. (**Streaming** extension required).
- Send email invitations and newsletters to users via external SMTP server.
- Set up media transmission between conference participants bypassing the server (**UDP Multicast Conferences** extension 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 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. Control panel of the administrator with the Security Admin role

You can add individual administrators to the [TrueConf Server Security Admin](#) group. They will be able to view information about the server operation in the control panel but will not have access to TrueConf Server settings.

TrueConf Server Security Admin Role gives 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. User's personal area

[Personal area](#) is a web page accessible to every user who is registered on your TrueConf Server instance. In the personal area, users can:

- 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

TrueConf Server guest page is a web page which your users can access to download client applications and [connect to your TrueConf Server instance](#). You can share your guest page link with your employees and [guests](#) who are going to attend meetings hosted on your server.

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

- read [user manual](#)
- view contact details of your TrueConf Server administrator.

1.3. Choose your license

You can choose one of the available licensing options: TrueConf Server Free, TrueConf Server, and a free 3-week trial version. You can find a detailed license comparison [here](#) or [calculate your license price](#) on our website.



If you would like to request a 3-week trial version of TrueConf Server, please [contact us](#), we will be happy to help.

TrueConf Server Free provides basic features for video conferencing; however, it also has certain limitations. [TrueConf Server Free](#) is a great solution for small and medium-sized businesses to get acquainted with TrueConf benefits and deploy a self-hosted video conferencing system.

1.4. Advantages

TrueConf Server video conferencing system provides a number of advantages and unique technologies.

1.4.1. Relatively low system requirements

You do not need a powerful server to deploy TrueConf Server. Instead, you can use a PC based on a modern Intel or AMD CPU and choose between Microsoft Windows Server or Linux operating systems. You can find system requirements for common configurations [in our article](#).

1.4.2. Working in a closed network

TrueConf Server is a secure solution that allows you to conduct video conferences within a corporate (closed) network without an Internet connection.

Advantages of working in a closed local network:

- complete independence from external providers and guaranteed protection from the unavailability of external services due to reasons beyond your control;
- Super fast operating speed thanks to local infrastructure
- Your server is fully managed by your system administrator
- Independence from Internet connection quality
- Fast troubleshooting
- Additional [levels of data protection](#).

1.4.3. Convenient administration

TrueConf Server has a number of features that can simplify its administration:

- [TrueConf's proprietary protocol](#) that works with TrueConf client applications using a single [TCP port](#).
- Operation in LAN/VPN of any configurations, including satellite communication channels.
- Synchronization with user and group directories via LDAP protocol.
- Endpoints (PC, browsers and mobile devices) do not need to have a direct IP address for communication.
- Works through NAT, Firewall and Proxy.

1.4.4. Advanced data transmission technologies

TrueConf Server uses the following [technologies to improve the quality and reliability of video communication](#) :

- dynamic adjustment of data transmission rate
- scalable video coding (SVC)
- direct connection priority using Hole punching technology
- automatic connection restoring if the connection fails

- adaptive buffer for incoming audio and video data streams.

1.4.5. 4K video conferencing

With TrueConf Server and TrueConf Server Free, you can organize UltraHD (3840x2160, 4K) video meetings. In group conferences, total image resolution can be up to 7680×4320 (Ultra HD 8K).

Read more about [UltraHD video calls](#) and [system requirements](#) for user devices [in our articles](#).

1.4.6. Collaboration tools

TrueConf Server provides a number of collaboration tools:

- [team messaging and file sharing](#)
- [display of slides](#), photos, diagrams, drawings and tables
- [sharing your desktop or separate application windows](#) to all conference participants
- [remote desktop control](#) of other conference participants
- [reactions and voting](#)
- [conference recording](#).

1.4.7. Streaming conferences to popular services

Do you want to organize a video conference and [stream it for a broad audience in real time](#) ? With TrueConf, you can stream your meetings using the built-in RTSP gateway. TrueConf Server supports the following popular services:

- [YouTube](#)
- [CDNVideo](#)
- [Wowza](#)

You can also manually [set up conference streaming to other third-party services](#), for example, [Facebook](#).

1.4.8. Managing video layouts and participants' devices

TrueConf Server users can configure video layouts, manage devices of conference participants, and use other options for streamlining meetings:

- choose from a number of [predefined video layouts](#) (including the layouts with one or two larger windows)
- set individual layout for SIP/H323 devices and WebRTC users
- set individual layout for each participant
- [change your view](#) during the conference
- [change video layout in an ongoing meeting](#) for all meeting participants (available for conference owner and operators)
- [control participants' devices](#), including [PTZ cameras](#).

1.5. Useful guides

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

- [Knowledge base with useful guides](#)
- [Educational portal](#)
- [Getting started with TrueConf client applications](#) – a short guide that gives new users a general idea about our video conferencing system.
- [Official Telegram channel providing news about our solutions](#)
- [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 reviews and webinars](#)
- [Facebook community](#)

2. User types

With TrueConf Server you can set different roles and privileges for users and administrators. Below you can find an overview of user and admin roles in TrueConf.

2.1. User roles

TrueConf Server users can be 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 client application ([for Windows/macOS/Linux](#), [for Android](#), [for iOS/iPadOS](#), or even [for Android TV](#))
 - in [Personal area](#)
 - in [TrueConf Group](#) or [TrueConf Videobar](#) endpoints
 - in the software-based [TrueConf Room](#) endpoint
 - with SIP/H.323 devices that can be registered on Gatekeeper or PBX, e.g. [Phoenix Spider](#) speakerphone or [Polycom HDX](#) endpoint.

If a user is registered on the server, but is not authorized, he/she will not be included in the list of **online users** whose maximum number is [set in 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, the conference owner can [restrict guest privileges](#) by forbidding guests to send messages, audio and video.

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

To learn how each type of users' connection to TrueConf Server is licensed, check the [section "TrueConf Server licensing"](#).

2.2. User identifier

Every user of TrueConf Server and TrueConf Online cloud service has TrueConf ID.

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

As a rule TrueConf ID looks like that: `<user_id>@<server>`. Where: `<user_id>` is user's name entered during registration; `<server>` is TrueConf server name.

Examples:

User `george` on TrueConf Online cloud service:

`george@trueconf.com`

User `maria` on corporate TrueConf Server `server.company.com`:

`maria@server.company.com`



Although the `@` character is used in TrueConf ID, it is not an email. If you send an email to a user's TrueConf ID, he/she will not receive it.

2.3. Roles of conference participants

During the conference, participants may be assigned with one of the following roles:

- **Conference owner** is the user who created the conference and who has full control over the flow of this meeting.

- **Moderator** is assigned by the owner or another moderator and has all the rights of the owner, except the right to download video recordings and view analytics.
- **Operator** is a member of a special operator group created by the administrator on TrueConf Server, this person receives moderator privileges in any conference he/she joins.
- **Speaker** is any conference participant who can be seen and heard by other users (this person is on the podium)
- **interpreter** — a special participant role in a conference with enabled simultaneous interpretation mode. He/She does not appear in the video window layout; his/her sole role in the conference is to translate the speakers' presentations into the selected languages. For more details, refer to: [creating a conference with simultaneous interpretation](#), [working with simultaneous interpretation in the client application](#).

To learn more about the roles of conference participants, read the [guide to the client application TrueConf for Windows, Linux, macOS](#).

2.4. Admin roles

TrueConf Server features two types of administrators that correspond to the user groups automatically added to your OS during the [TrueConf Server installation process](#):

- **TrueConf Server Admin** has full access to the TrueConf Server control panel and can manage all server settings.
- **TrueConf Server Security Admin** has read-only access to the reports and recording. TrueConf Server Security Admin cannot change any settings in the TrueConf Server control panel.

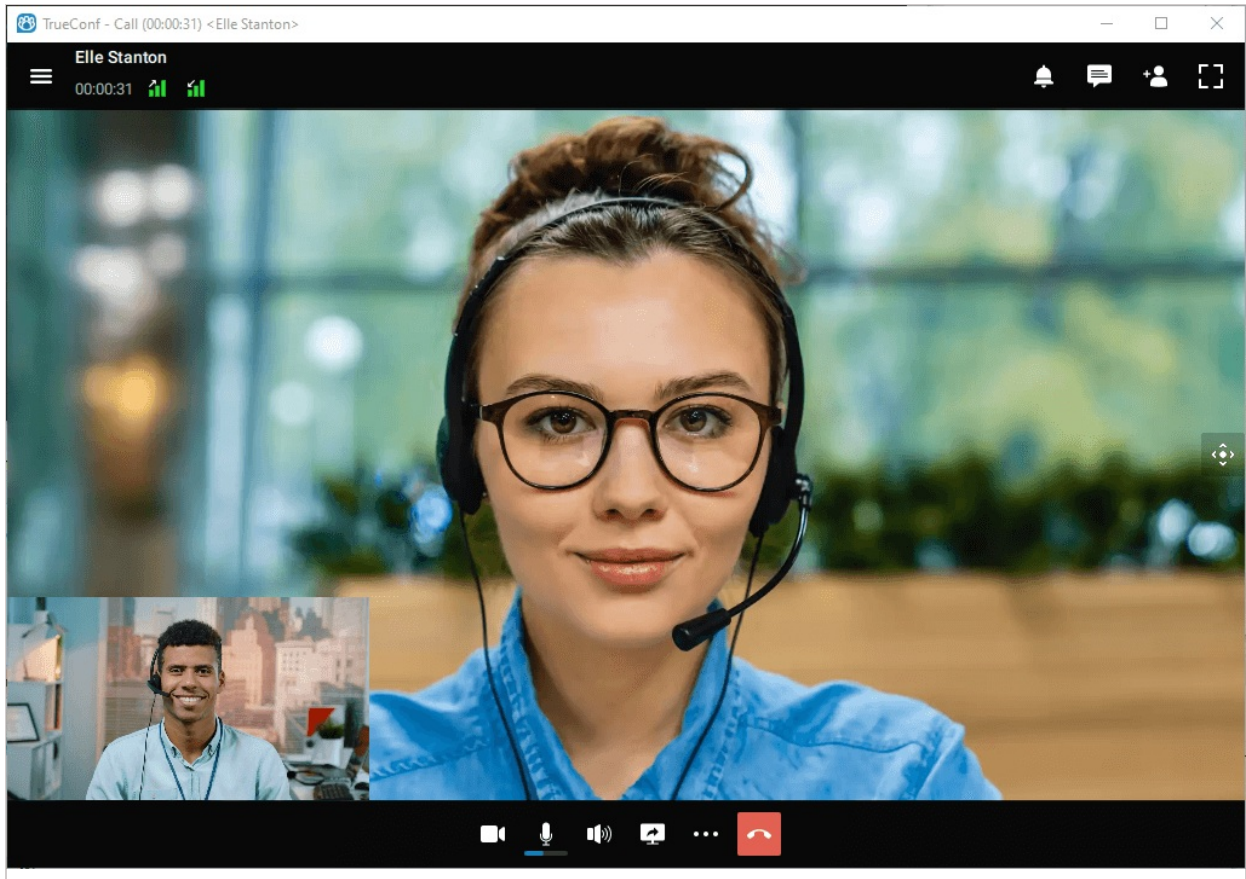
To learn more about the access to the TrueConf Server control panel, read the [section about the initial configuration](#).

3. Types of video conferencing

Depending on your business tasks, you can choose from a number of conferencing modes available with TrueConf Server.

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.

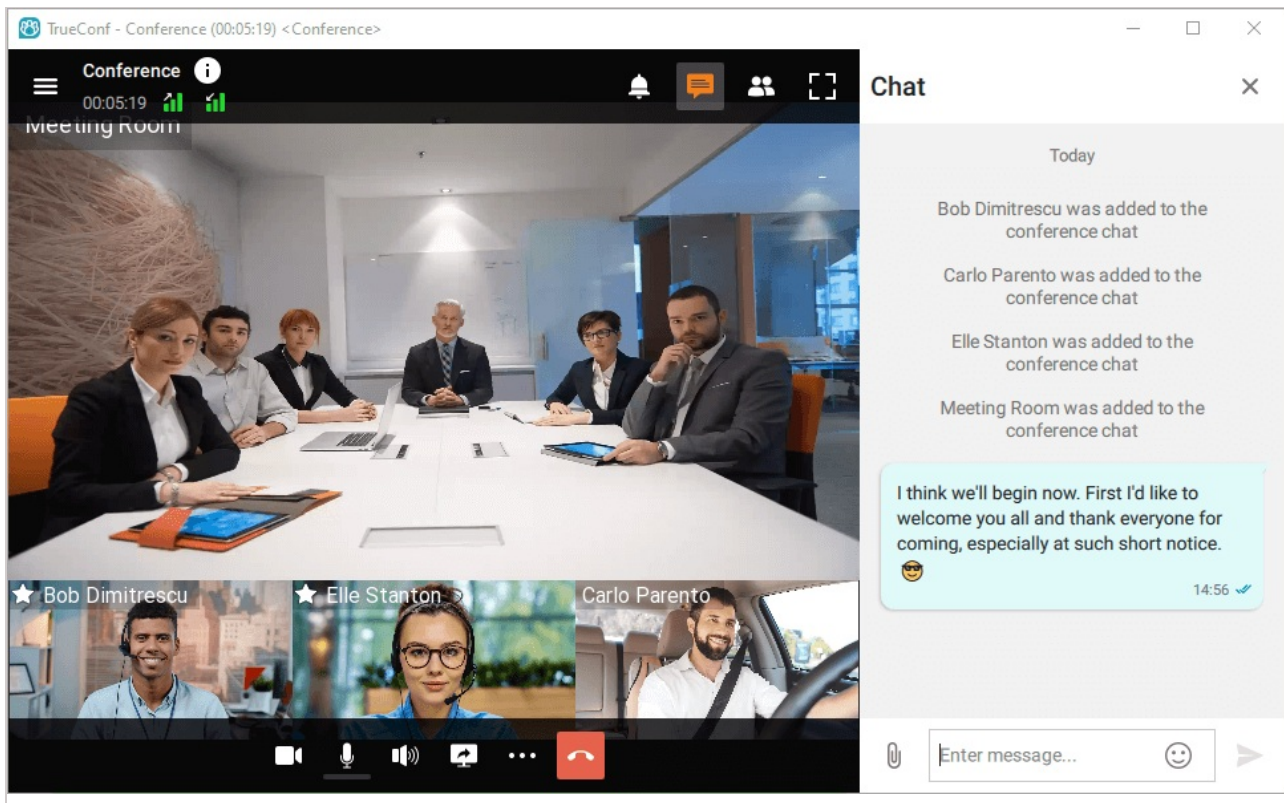


TrueConf provides a number of additional options during video calls: chat, file sharing, content sharing (e.g. sharing screen or separate application windows) and other collaboration tools.

You can learn more about video calls [on our website](#), check out our [system requirements](#) and read 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.



With TrueConf Server you can organize video conferences of the following types:

- **Private.** Secure conference available to users authorized on your TrueConf Server instance or on a federated TrueConf Server 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 TrueConf 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.

TrueConf group conferences may also have different launch types:

- **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.

Read [our step-by-step guide](#) to learn how to join a meeting.

TrueConf Server administrator can create any group video conference and view information about ongoing or scheduled conferences in the [control panel](#). TrueConf Server users can perform similar actions [in their personal area](#) or [in the scheduler](#) available from their client applications.

You can check system requirements for different video conferencing modes [here](#).

3.3. Video conferencing modes

TrueConf Server offers 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.

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

3.4. Conference ID

Conference ID (CID) is the unique identifier of a video conference on TrueConf Server (each meeting has such an identifier).

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.

Before the conference is started, one can set its ID:

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

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

To join a conference, a user only has to know its ID. In particular, the link to the [conference page](#) is generated on the basis of this ID.

3.5. What is a waiting room

Waiting room is a preliminary queue for joining an event. When this feature is activated, participants will be automatically directed to this room as soon as they join the meeting, if they belong to the category selected when the conference was created (for more details, check the [section "Creating a new conference"](#)). The use of the waiting room is available in conferences of any launch type (both private and public) and in 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. Extensions

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

You can use this extension to connect third-party devices to your TrueConf meetings, for example:

- Third-party video conferencing endpoints and [PBXes](#), as well as users of popular [cloud-based services](#) such as Zoom, BlueJeans, Cisco Webex, LifeSize Cloud and Skype for Business via SIP/H.323 protocols.
- [IP cameras and video surveillance systems](#) via 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.

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 TrueConf Server Free.

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 Free, 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.

4.4. Live streaming

With this extension you can [stream video conferences](#) via third-party platforms or content delivery services such as CDNvideo, YouTube, Facebook or Wowza. You will be able to reach more than 1 million viewers; the maximum number is limited only by the capacity of your preferred streaming platform.



This extension is available when purchasing 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 across multiple TrueConf Server instances in different branches of your network, use the **Federation** extension. You can also connect with other companies that use self-hosted or cloud-based TrueConf solutions. Federation allows your server users to call other TrueConf users or invite them 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.

* Federation is a basic feature included in every TrueConf Server standard license. To enable federation, you need to [purchase any TrueConf Server paid license](#).

4.7. Integration with DLP

This extension is a part of [TrueConf Enterprise](#); it allows TrueConf Server to be connected to a third-party DLP system via [ICAP \(RFC 3507\)](#) [↗](#) protocol.

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.

4.8. Support for SDK applications

With [TrueConf SDK](#) you can develop your own video conferencing applications based on TrueConf technologies or integrate video conferencing to an existing application or website.

TrueConf provides libraries for all popular desktop (Windows, Linux, macOS) and mobile (iOS, Android) platforms.

An example of an application created using TrueConf SDK is [TrueConf Kiosk](#), a video-enabled customer care solution.

In addition to SDKs available for various platforms, we [offer TrueConf VideoSDK](#) as the framework allowing you to develop custom solutions for meeting rooms of any size and self-service kiosks. This solution provides an interface for participating in video calls (display of video windows, notifications, and so forth) and the web-based control panel for changing settings. To moderate the flow of a meeting, one can use a [wide range of API commands](#) that can be run in any program code.

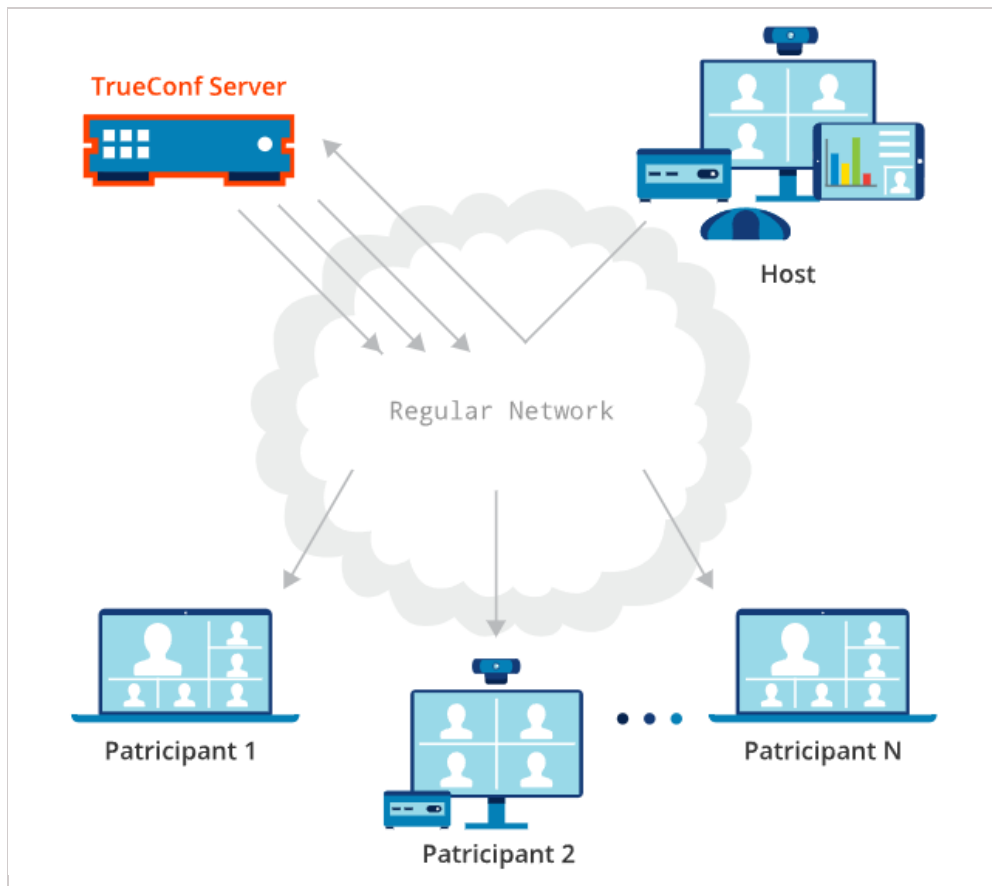
4.9. UDP Multicast

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 when purchasing the [full technical support package](#).

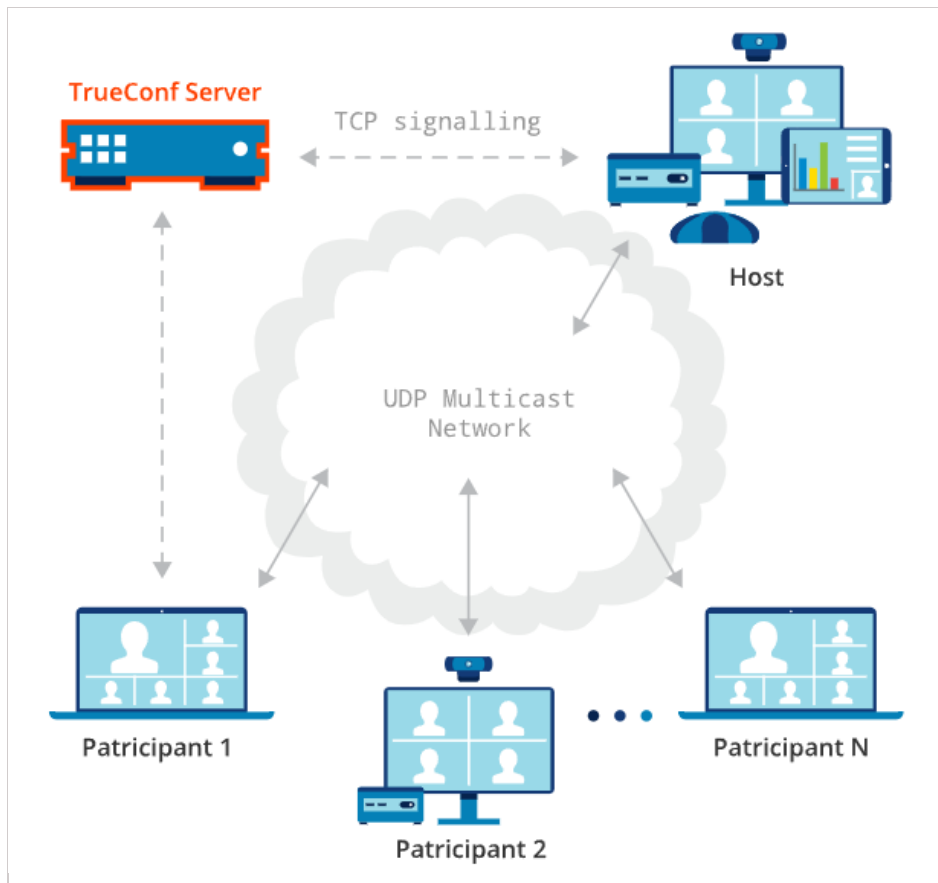
During a standard group video conference (without UDP Multicast mode) data are transmitted through a TrueConf Server instance to each participant. Data traffic during such a conference can substantially load the

server channel.



The implementation of [UDP Multicast mode](#) during a group conference allows its participants to exchange data directly with each other without the server, thus decreasing its network load. 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 under UDP Multicast protocol is available only inside a closed corporate network.

If UDP Multicast technology is used, there can be up to 1600 participants in a conference (e.g., in a [moderated role-based conference](#) with only one speaker).



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.

4.10. TrueConf Directory

This extension allows users of your TrueConf Server instance to search for users/groups on all TrueConf servers synchronized with it and add them to the address book. TrueConf Directory offers a global address space available in [all client applications](#).

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

4.11. TrueConf License Manager

This extension is a part of [TrueConf Enterprise](#). It is needed for distributing the pool of licenses used by a group of TrueConf Server instances.

4.12. TrueConf Border Controller

TrueConf Border Controller is an extension included in [TrueConf Enterprise](#). This extension is supposed to be installed in the DMZ (demilitarized zone) of the corporate network and used to protect video conferencing servers from unwanted outside traffic.

To learn more about the work of this extension and its configuration, check the [documentation](#).

4.13. 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.

To meet the needs of such clients, TrueConf offers **TrueConf Enterprise**, a turnkey solution with a unique configuration tailored to the requirements of a particular customer.

Main benefits:

- The complete replication of key nodes ensures 99.99 % availability of all system components across the entire enterprise.
- TrueConf Enterprise users have exclusive access to a premium tech 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 about this solution and request it on [our website](#).

5. Licensing of the video conferencing server

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

1. Availability of [extensions](#).

Name	Terms of provision
LDAP/Active Directory	Free
SIP/H.323/RTSP gateway	Free, one has to purchase licenses for a certain number of connections
Public conferences (webinars)	Free, one has to purchase licenses for a certain number of connections
Federation	Purchase of any paid license
Live streaming	Purchase of the extended or full technical support package
Conference UDP Multicast	Purchase of the full technical support package
Integration with DLP	Included in TrueConf Enterprise
TrueConf Directory	Included in TrueConf Enterprise
TrueConf License Manager	Included in TrueConf Enterprise
TrueConf Border Controller	Included in TrueConf Enterprise
Simultaneous interpretation	Purchase of any paid license
SDK applications support	Provided on request



To learn more about different levels of TrueConf technical support, follow this [link](#).

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

License type	Who can use it	Features
Online users	Users authorized on TrueConf Server	All features provided by the video conferencing server, except participation in group conferences
PRO users	Users authorized on TrueConf Server	Participation in group conferences
Guest users	Users without a permanent account on TrueConf Server	Participation in public conferences (webinars)
SIP/H.323/RTSP connections	Connections via SIP, H.323, and RTSP protocols (endpoints, PBX users, IP cameras)	Participation in conferences via SIP, H.323, and RTSP protocols

On the **Summary → License info** tab, one can check the number of available licenses for each type.




In TrueConf Server Free there are restrictions on the number of licenses for each type of connection. To learn more, go to the [web page of this solution](#).

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

5.1. Online users

Online users are the users who are authorized 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 authorized 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 in idle mode), TrueConf Server will not count such connections as online users. For example, if a user is authorized on a mobile device and has the status  (recent activity), no online license 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.

So, the main competitive advantage of licensing online users on TrueConf Server separately is that it enables employees to be constantly online in a messenger and make [video calls](#) from time to time. In other words, authorized users have access to all the features of the TrueConf collaboration platform except participation in [group conferences](#).

5.2. PRO licenses and conference participation

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

- TrueConf client applications for desktops (Windows, macOS, Linux)
- TrueConf client applications for mobile devices (Android and iOS/iPadOS)
- TrueConf client applications for Android TV
- TrueConf Room software-based endpoint
- TrueConf Videobar hardware-based endpoint
- TrueConf Kiosk, a software solution for information and self-service kiosks
- 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 are the users authorized on your TrueConf Server who are allowed to participate in group conferences. The user, who is authorized 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 slots for participation in conferences is regulated by the parameter **PRO users** that you can check in the TrueConf Server control panel on the **License info** tab of the **Summary** section.


The screenshot displays the TrueConf Server administrator interface. The top navigation bar shows the TrueConf logo, the server address 'video.example.net#vcs', and a 'System' dropdown menu. The left sidebar contains a list of navigation links: 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, API, and OAuth2. The main content area is titled 'Summary' and includes a 'Help' link. Below this, there are three tabs: 'Dashboard', 'License info', and 'Registration details'. The 'License info' tab is active, showing a table of license details. The table has columns for the license type, the number of licenses, and an 'Add' button. The 'PRO users' row is highlighted with an orange border. To the right of the table, there is a 'Registration details' section showing the server ID, organization name, and contact person. Below this, there is a 'License details' section showing the license type, connection to the registration server, user accounts, active conferences, and the license expiration date. To the right of the license details, there is an 'Extensions' section showing a list of enabled extensions and their status.

5.2.1. Key aspects of using PRO licenses

The administrator of TrueConf Server can distribute the common pool of PRO licenses into two groups: **permanent** and **temporary**.

Permanent licenses are given without any time restrictions to the users from the groups selected by the administrators. They can join conferences at any moment without waiting for licenses to be released into the common pool. Distribution of licenses is not available on 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 that will be described below.

1. If a user, who was not given a permanent PRO license, tries to join a group conference when PRO licenses are available, this person will automatically receive a **temporary PRO license**. It 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 license is automatically renewed.
2. The TrueConf Server administrator can instantly revoke a temporary PRO license from any user by clicking on the  button next to this user's name (check the description of the [PRO licenses section](#) in the control panel).
3. The server administrator can allow users to request a PRO license manually before participating in a conference (it will also be active for 24 hours after reception).
4. The number of devices used by a person for participating in conferences does not affect the number of available PRO licenses since such a license is linked to a specific user account (TrueConf ID). It is not tied to the device on which the user is authorized. 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.
5. When the number of available PRO licenses becomes equal to 0 and a user tries to join a group conference, the following checks will be made:
 - If this person has a permanent PRO license, he/she will be allowed to participate in the conference.
 - If this user previously received a temporary PRO license, and it is still valid (check part 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.
5. 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):

5.1 If the pool of available licenses is not sufficient for the users with permanent licenses, they will be taken away from the users with temporary licenses (starting from the users whose temporary PRO license has the shortest expiry period).

5.2. If a user is removed in the group with permanent licenses after the redistribution, this person will be given a temporary PRO license (if such licenses are available). This step will be performed after part 5.1.

5.3. If there are ongoing conferences, only the participants, whose licenses were taken away after the automatic redistribution (part 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 TrueConf Server administrator can check the validity period of temporary PRO licenses and distribute permanent licenses in the [PRO Licenses section](#) of the control panel.

5.2.2. Use of PRO licenses during federation

If a conference hosted on your TrueConf Server is joined by external users from a [federated server](#), no PRO license will be taken.

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

5.2.3. Examples of how PRO licenses are counted

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 temporary 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 [TrueConf Server control panel](#), you will see that 1 PRO license and 4 licenses for online users are taken (the PRO license is taken by the person with the login **user**).
6. The PRO license will be released by the person with the **user** login in 24 hours after he/she leaves the conference.

Case 2

1. There are 10 PRO licenses on the server.
2. Permanent licenses are given to the **IT** group that 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 the [TrueConf Server control panel](#), the administrator will see that 4 PRO licenses and two licenses for online users are taken. This result can be explained by the fact that permanent licenses are reserved (always available to three users from the **IT** group) and one temporary license is given to the user who is currently participating in the conference (check part 3).
6. At the same time, 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. No permanent licenses were given to users which means that 10 temporary 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. One of the users (this person's login will be **user**) is authorized on 2 different devices and is participating in two

group conferences from these devices.

5. In the [TrueConf Server control panel](#), you will see that 1 PRO license is taken by the person with the * **user** login due to the rule according to which a PRO license is bound to TrueConf ID instead of a user's devices. In addition to that, 5 licenses for online users will be taken (two of them are taken by the **user** person and 3 by other authorized users from part 3).
6. The PRO license will be released in 24 hours by the **user** person 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 authorized 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. 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 (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 taken.

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 users who are not registered on your server. The number of such participants is determined by a separate license for guest connections. TrueConf Server Free offers 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 point-to-point call.

Example

1. There are 150 online licenses, 100 PRO licenses and 5 guest licenses.
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 guest licenses are taken.

6. Installation and upgrade. System Requirements

6.1. System requirements for the video conferencing server

	Basic configuration	Recommended configuration
CPU	Intel Core i3-8100 @ 3.6GHz Intel Core i5-7400 @ 3.0GHz Intel Xeon E-2234 @ 3.6GHz Intel Xeon W-2223 @ 3.6GHz or any other CPU with at least 4 logical cores and PassMark® CPU mark 7000+	Intel Core i7-10700 @ 2.9GHz AMD Ryzen 7 2700 @ 3.2GHz Intel Xeon E-2288G @ 3.7GHz Intel Xeon W-2245 @ 3.9GHz or any other CPU with at least 16 logical cores and PassMark® CPU mark 14000+
Typical configurations capabilities	<ul style="list-style-type: none"> Up to 200 online users connected via TrueConf client apps. Recording or streaming of one video conference of any type. 	<ul style="list-style-type: none"> Up to 1,000 online users connected via TrueConf client apps. Recording or streaming of one video conference of any type.
	<i>Plus</i>	
	<ul style="list-style-type: none"> 1 all-on-screen conference for up to 36 participants connected via TrueConf client apps. or <ul style="list-style-type: none"> Up to 6 smart meetings or moderated role-based conferences for up to 20 participants connected via TrueConf client apps, including 4 speakers on the podium. or <ul style="list-style-type: none"> 1 smart meeting or moderated role-based conference for up to 240 participants (60 WebRTC connections and 180 client app users) with 5 speakers on the podium (2 WebRTC participants and 3 client app users). or <ul style="list-style-type: none"> Up to 25 WebRTC participants on screen in conferences of any type. or <ul style="list-style-type: none"> Up to 10 SIP/H.323 endpoints on screen in a conference of any type. 	<ul style="list-style-type: none"> Up to 3 all-on-screen conferences for up to 36 participants connected via TrueConf client apps. or <ul style="list-style-type: none"> Up to 15 smart meetings or moderated role-based conferences for up to 20 participants connected via TrueConf client apps, including 4 speakers on the podium. or <ul style="list-style-type: none"> Up to 2 smart meetings or moderated role-based conferences for up to 240 participants (60 WebRTC connections + 180 client app users) with 5 speakers on the podium (2 WebRTC participants and 3 client app users). or <ul style="list-style-type: none"> Up to 36 WebRTC participants on screen in conferences of any type. or <ul style="list-style-type: none"> Up to 20 SIP/H.323 endpoints on screen in a conference of any type.
	Other examples of typical configurations →	
GPU-based hardware acceleration	With NVIDIA Quadro P2000 (or a comparable graphics card), you can add 20 individual layouts for SIP/H.323 participants without changing other hardware.	
Operating system	Dedicated or virtual 64-bit operating system: <ul style="list-style-type: none"> Microsoft Windows Server 2012/2016/2019/2022 (including Core editions) with the latest updates installed Debian 11 / 12 CentOS Stream 9 	
RAM	16 GB	32 GB+
Hard drive	20 GB of free space	

Network	Ethernet 1 Gbit/s
Ports	<ul style="list-style-type: none"> • Port 443 (can be changed in the control panel) is the default HTTPS port for transmitting service information between the server, client applications and browsers. <i>If this port is closed, the following TrueConf client application features won't be available: meeting scheduler and real-time meeting manager.</i> • Port 4307 (may be changed in TrueConf Web Manager) is used to exchange media data with client applications. Learn more →
IP	A static IP address is required for the server to work properly
Supported hypervisors	Microsoft® Hyper-V, Xen, KVM, Oracle VM VirtualBox, VMware Workstation and ESXi.

6.2. Registration key validation

Before installing TrueConf Server, please make sure you have the [registration key](#). You have probably received a registration key when downloading the installation file from our official website or when purchasing it from one of [our partners](#). In this case, skip this step and start [TrueConf Server installation](#). Otherwise, you will need to receive the key as it is described in the ["Registration"](#) section.

6.3. Installation

TrueConf Server is distributed as a software installation package that contains the server side components and client applications for Windows PC. TrueConf client applications for other popular platforms are available on TrueConf website (alternatively, you can find the download links on the [guest page](#)).



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 have purchased a paid license, it is not necessary to open the port and you will be able to [use offline registration](#).

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

6.3.1.1. 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** is a PostgreSQL database server service. The database stores chats and logs. The TrueConf Database service will not start if the TrueConf Server Manager service is not enabled.
- **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** is a manager for working with the Windows Registry and configuration 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.

6.3.1.2. 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 PostgreSQL database service. This database stores all the TrueConf Server data: 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** is a manager for working with databases and configuration files. It is required to display certain data in the TrueConf Server control panel.
- **trueconf-php** — this service is responsible for processing certain scripts. It 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.

6.3.2. For Windows

After [filling out the form](#), open the **Windows** tab and press **Download TrueConf Server**.

Thank you! What's Next?

Choose your operating system:

Windows

Linux

✓

1

Fill in this form and get a registration key

2

2

Download and install TrueConf Server for Windows

[Download TrueConf Server 5.0.0.10357](#)

3

3

Register TrueConf Server with your key

Your registration key has been sent to your email address `stalker.shoc@gmail.com`.

4

4

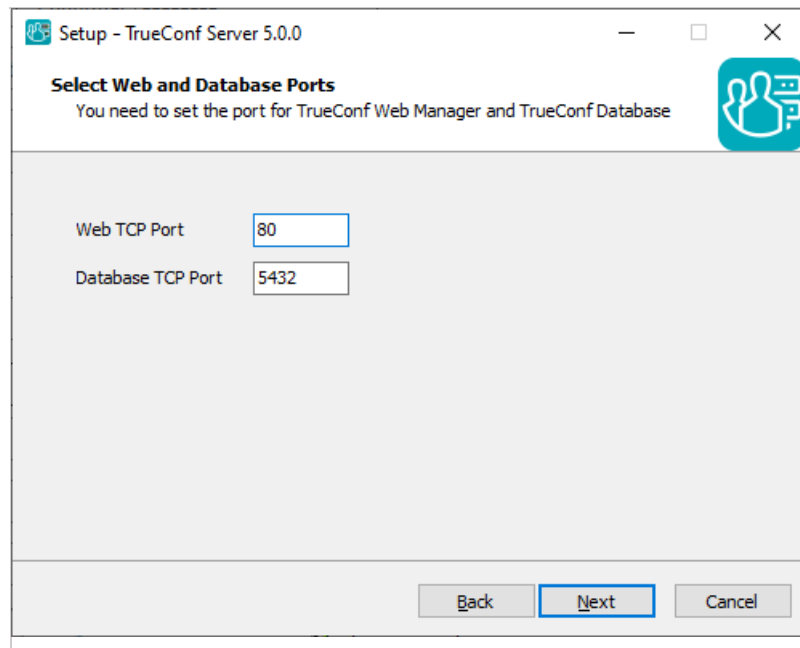
Follow our installation guide

Deployment will take only 15 minutes, simply [follow our short guide](#).

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](#).

i 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.

6.3.3. For Linux

i TrueConf Server contains its own web server. To prevent any possible conflicts or clashes, please deploy TrueConf Server 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.

***** Check the [full installation guide in our blog](#) to learn how to create a user in Linux (see Step 2).

Step 2.

After [filling out the form](#), open the **Linux** tab and proceed to our step-by-step guide on how to install TrueConf Server for Linux.

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 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](#).

Read our step-by-step guide to learn how to download and [install TrueConf Server for Linux](#).

Step 3.

Download your preferred [Linux distribution](#).



For each operating system, there is also an option to install TrueConf Server from the repository. You can find a detailed description on how to do that in the [corresponding section of our article](#).

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:

```
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:

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

sh

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

```
dnf install epel-release
```

sh

3. Right after that, you can install TrueConf Server:

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

sh

Step 5.

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

Step 6.

TrueConf services [described earlier](#page5-services-linux) will be added to the OS. 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`).



Check [Step 6 in our knowledge base article](#) to learn how one can access the control panel from outside the local network (e.g., when installing the software on a cloud server).

Since TrueConf 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 [TrueConf Server registration](#).

6.3.4. How to change the port to access the control panel without reinstalling TrueConf 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. Please reboot the computer on which 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. Go to the `/opt/trueconf/server/etc/webmanager/` directory with superuser rights
2. Open the `httpd.conf` file with any text editor.
3. Change the port number in the `Listen <port number>` parameter (e.g. `Listen 8888`) and save changes.
4. Open the `/opt/trueconf/server/etc/manager/manager.toml` file with any text editor 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. Please restart the web server service using the following command:

```
systemctl restart trueconf-web sh
```

6.4. Upgrading the video conferencing server

Updating TrueConf Server is also done via installation files or (on Linux) via repositories. Please note that when updating **major version** (the first two digits change, for example, 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 required if the configuration of the following hardware on a physical or virtual machine with TrueConf Server is changed:

- processor model (note that the number of virtual cores (vCPU) does not affect the license)
- storage size (SSD or HDD)
- the operating system used.

To learn more about connection options, check [our article](#).

7. Registration

7.1. What is the registration key and server ID?

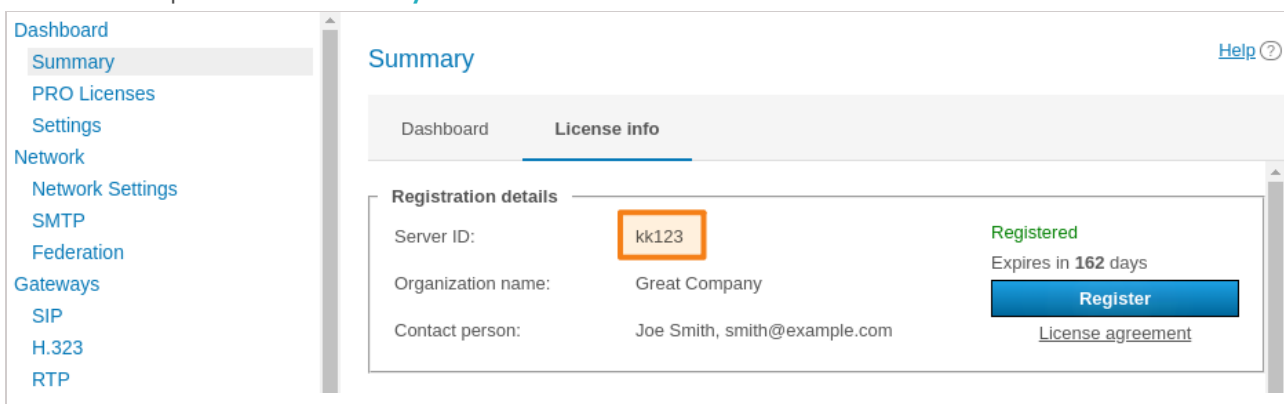
Registration key is the unique secret combination of characters that identifies the licenses for your TrueConf Server instance. It is needed for activation of the video conferencing server after [its installation](#). You probably received the registration key when downloading the server on the TrueConf website or when purchasing it from [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 the unique identifier of a TrueConf Server instance. The server identifier includes several characters that match the registration key (up to the first hyphen), for example, **EB2MM**. It will be displayed in the TrueConf Server control panel in the [Summary](#) section:



If you do not have a key, you can receive a free license by clicking the **Download free version** button on the [TrueConf Server Free webpage](#).



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

Here you will find a TrueConf Server Free download form:

Download TrueConf Server Free

TrueConf Server Free download will start automatically once you submit the form. This data is required to release a free license for your organization.

Company

Industry

-- Choose your business category --

Contact name

E-mail

Contact phone

Format: +1(123)4567890 #123

Country

United Kingdom

Valid format

☐ Please notify me about new releases, best practices and other TrueConf news.

☐ 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

Language: English

Free for up to 12 users

Self-deployed

Easy setup 15 min

SVC infrastructure

Need help?

- [What is TrueConf Server Free?](#)
- [How to setup and configure TrueConf Server in 15 minutes?](#)
- [What are the terms of use of the TrueConf Server Free?](#)
- [Can I install TrueConf Server on a regular PC?](#)
- [Are you ready to buy? Then click here!](#)
- [Contact Us](#)

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.

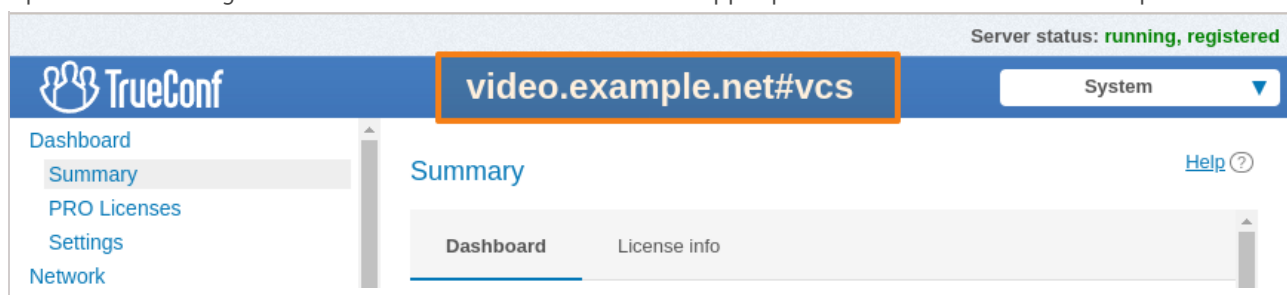
After filling out the form, select your operating system to get access to the corresponding installation guide. When TrueConf Server is deployed, you can register it.

7.2. TrueConf Server Name

TrueConf Name is a symbolic name designed to identify TrueConf Server in a network. The server name can be used to run video conferences with users of [federated TrueConf Server instances](#) or for SIP/H.323 endpoint integration (e.g. Polycom or TrueConf Group endpoints).

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.

Upon successful registration the server name is shown in the upper part of TrueConf Server control panel:





Server name can be changed only during TrueConf Server re-registration. To re-register your TrueConf Server, it is advised to contact our [technical support](#).

7.3. Registration process

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

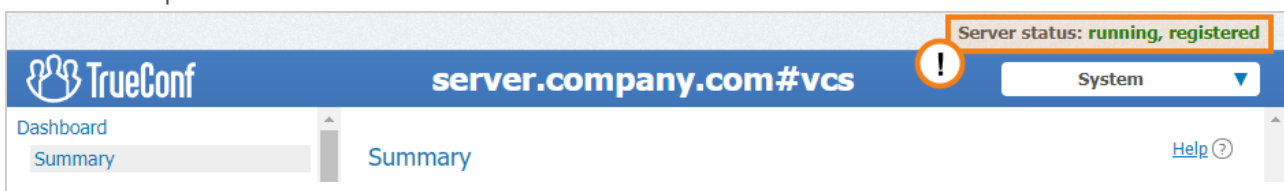
1. Open your browser and go to the TrueConf Server settings page. By default, its address is identical to the address of the machine where the video conferencing server is deployed. If you do not know how to learn the address and port, check the [installation guide](#).
2. Enter your key in the corresponding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

The screenshot shows the 'TrueConf Server Registration' form. It includes a text input field for a registration key (placeholder: 'XXXXX-XXXXX-XXXXX-XXXXX') with a 'Where do I get the key?' link below it. Below this is a 'Server Name *' field with the text 'ruwu1.trueconf.name' and a '#vcs' suffix. A blue 'Registration' button is highlighted with a red box and a red circle with the number '2'. At the bottom, there is a link to the help section and contact information for TrueConf support.



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

3. Once TrueConf Server has been successfully registered, you will see **running, registered** at the top right corner of the control panel window:



If connection with the registration server (`reg.trueconf.com` via TCP port `4310`) is lost, your TrueConf Server Free will be shut down in 12 hours. The expected shutdown time will be displayed in the **Summary** tab. The full version of TrueConf Server does not impose such limitations, regardless of the registration method (online or offline).

7.4. Offline registration

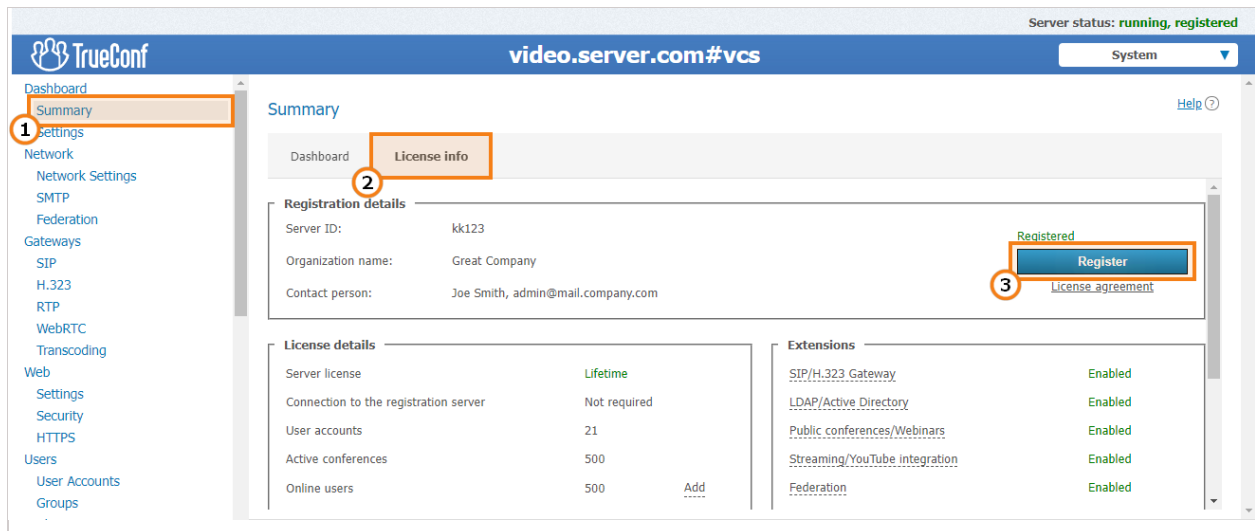


Offline registration is not included in a free license. It is available only in premium licenses or for the servers with a temporary trial license provided by managers.

7.4.1. Re-registering the server in a private network

If the server was previously operating in a closed network, and you want to change the license structure, or the server was stopped due to the error **CHECK CERT: HW key is failed!**, then **you will not be required** to go through the full offline registration procedure again. Since you already have the registration key, there is no need to obtain a new key by filling out the form required for downloading the installer file.

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



2. Enter **your current registration key** into 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?](#)

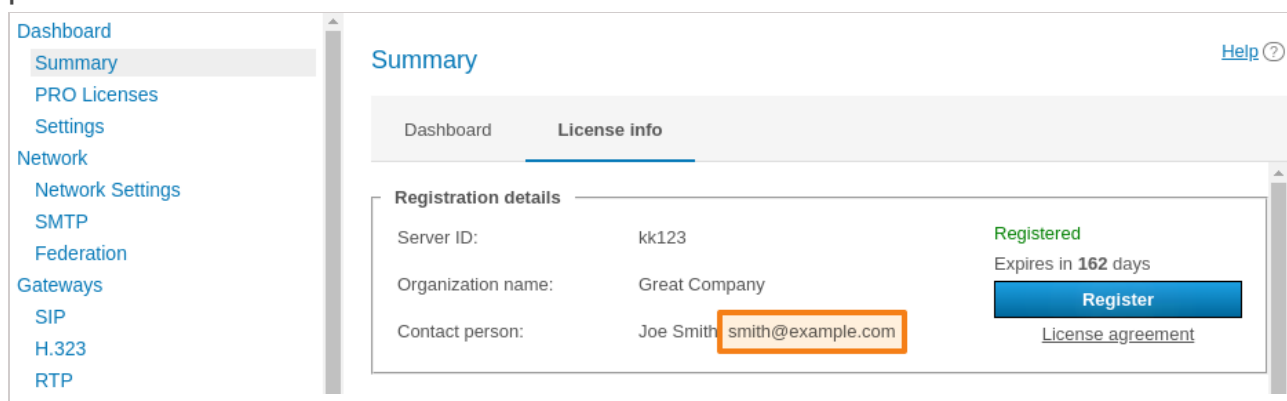
Server Name *

ruwu1.trueconf.name #vcs

2 **Registration**

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 mailbox you specified when filling out the registration form required for downloading the server. The email address is also displayed in the TrueConf Server control panel in the **Contact person** field:



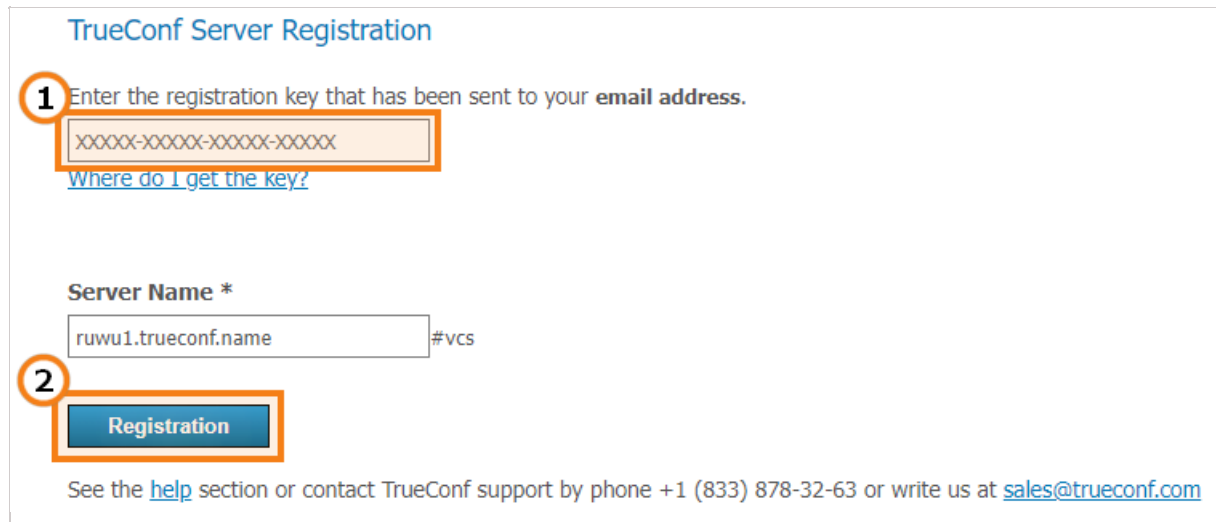
If the email was accidentally deleted, you can request the key from your manager. If you don't have your manager's contact details, just [contact us](#), provide your [server ID](#), and we will help you.

However, this method will not work, if you had changed the hardware configuration. In this case, you will need to contact us, reset the hardware binding and complete offline registration described below once again.

7.4.2. Registration of a re-installed server

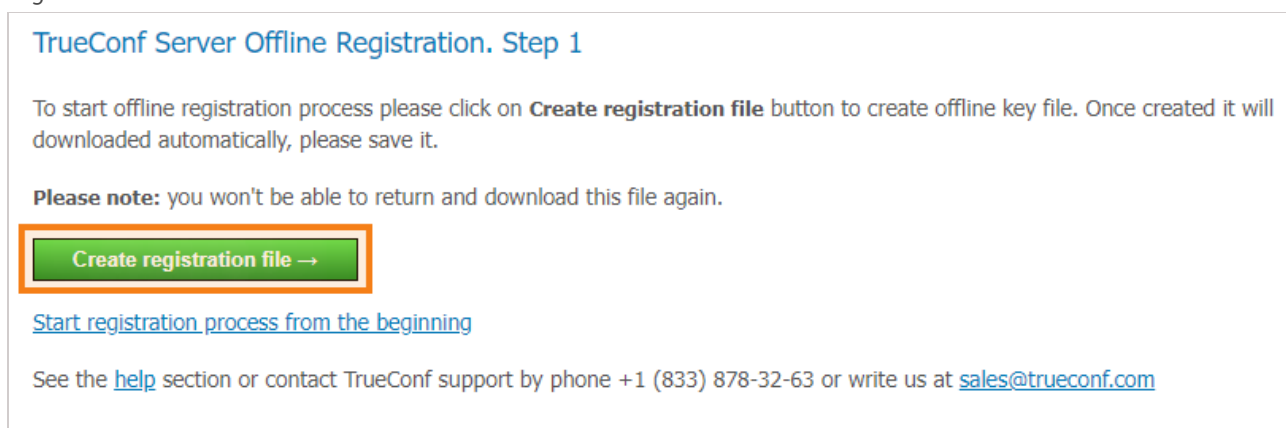
To register offline on a computer without an Internet connection, you will need a device connected to the Internet to obtain a registration key. On that device, go to [trial registration page on our website](#) and follow the instruction from the [Registration section](#).

Once you have received an email containing your registration key, open the control panel on a PC without Internet connection, enter the key into the **Registration Key** field and press **Registration**:



The image shows a web form titled "TrueConf Server Registration". It contains two main sections. The first section, labeled with a circled "1", asks the user to "Enter the registration key that has been sent to your email address." Below this is a text input field containing a placeholder "XXXXX-XXXXX-XXXXX-XXXXX" and a link "Where do I get the key?". The second section, labeled with a circled "2", has a "Server Name *" label, a text input field with "ruwu1.trueconf.name" and a "#vcs" suffix, and a blue "Registration" button. At the bottom, there is a line of text: "See the [help](#) section or contact TrueConf support by phone +1 (833) 878-32-63 or write us at sales@trueconf.com".

Create registration file button will appear in the registration window. Click on it to generate a file with your registration information:



The image shows a web page titled "TrueConf Server Offline Registration. Step 1". It contains a paragraph: "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." Below this is a "Please note:" section stating "you won't be able to return and download this file again." Underneath is a green button with the text "Create registration file →". Below the button is a link "Start registration process from the beginning". At the bottom, there is a line of text: "See the [help](#) section or contact TrueConf support by phone +1 (833) 878-32-63 or write us at sales@trueconf.com".

The generated file **offlinereg.vrg** will be saved in your browser's **Download** folder. Please send the file to sales@trueconf.com. You will receive a file that needs to be installed on the PC with the offline-registered server.



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

Click on **Select file** and select file **offline2.vrg**. Then click **Continue**:

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**.

1 **Choose a file** No file chosen

2 **Continue**

2 [Start registration process from the beginning](#)

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.

7.5. Changing the registration key

To change the registration key:

1. Open **Dashboard** → **Summary**.
2. Process the **License info** tab.
3. Press **Register** and specify a new key, as [shown above](#):

The screenshot shows the TrueConf Server control panel interface. The top bar indicates the server status as 'running, registered' and the URL as 'video.server.com#vcs'. The left sidebar contains a navigation menu with 'Dashboard' and 'Summary' highlighted. The main content area shows the 'Summary' page with the 'License info' tab selected. The 'Registration details' section shows the Server ID as 'kk123', Organization name as 'Great Company', and Contact person as 'Joe Smith, admin@mail.company.com'. The 'License details' section shows the Server license as 'Lifetime', Connection to the registration server as 'Not required', User accounts as '21', Active conferences as '500', and Online users as '500'. The 'Extensions' section shows various features like SIP/H.323 Gateway, LDAP/Active Directory, Public conferences/Webinars, Streaming/YouTube integration, and Federation, all of which are 'Enabled'. A 'Register' button is highlighted in the top right corner of the 'License info' tab.

7.6. Registration: Frequently Asked Questions

1. **Can I register TrueConf Server Free without an Internet connection?**

No, this feature is only available to those users who purchased annual or lifetime TrueConf Server license. If you need a trial version of TrueConf Server that operates without Internet connection, feel free to [contact us](#).

2. **What should I do if I get the message Computer change is not available for this server code**

It means that your key is "bound" to the computer where the server was installed. To disable this binding, please [contact us](#) in any convenient way.

3. **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. Initial setup

8.1. Control panel access settings

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.*`.

* Access settings are discussed more closely in the description of the [Web → Security section](#).

To get remote access to the TrueConf Server control panel, you need to sign in with an admin account. The admin is a member of one of the following groups:

- **TrueConf Server Admin** for Windows (**tcadmins** for Linux) to manage TrueConf Server
- **TrueConf Server Security Admin** for Windows (**tcsecadmins** for Linux) to view logs and conference recordings.

When the server is installed on Windows, the current user account is added to the first group. On Linux, users who are [manually specified during the installation process](#) are added to the **tcadmins** group. To grant another user access to the control panel, the administrator has to add this user's account to one of the groups.

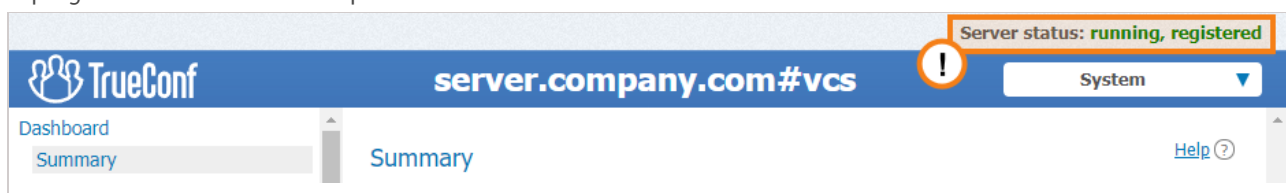
* You can learn how to create a new user account on different operating systems and add it to the desired group on the [example of TrueConf Server Security Admin in our documentation](#).
TrueConf Server does not impose any restrictions on the number of administrators of each type.

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 TrueConf Server control panel](#).

* Learn how to administer TrueConf Server outside your local network [in our article](#).

8.2. Server status

Server status is shown in the **Server status** field in **green** (if the server is working) or in **red** (if it has stopped) in top right corner of the control panel:



* What to do if server is not running?

Stopped status is displayed in the **Server status** string.

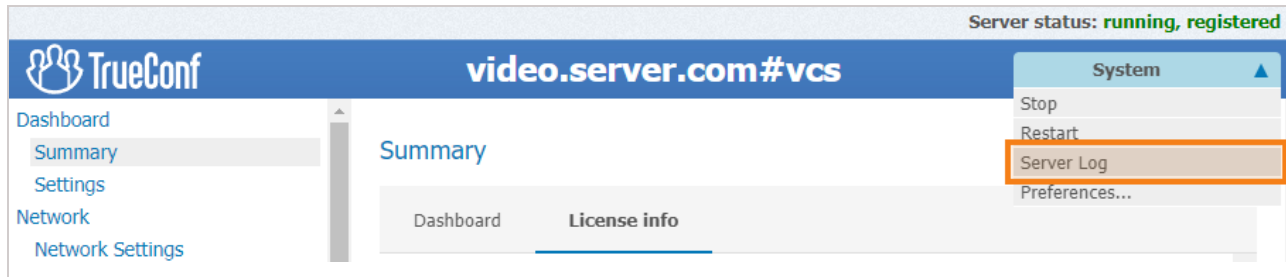
There are three possible reasons for this:

- **Invalid license:** contact your system supplier to get a license.
- **Some server files are missing or have been damaged:** reinstall TrueConf Server (see [Installation](#))
- **Server hardware key is broken:** please refer to the [instructions for resolving the problem with the key](#).

8.3. Server log

If you encounter any issues with TrueConf Server, TrueConf support team will be able to help you troubleshoot

them more efficiently if you provide your server log files. To access the main log, go to **System → Server log** located in the top right corner of the control panel.

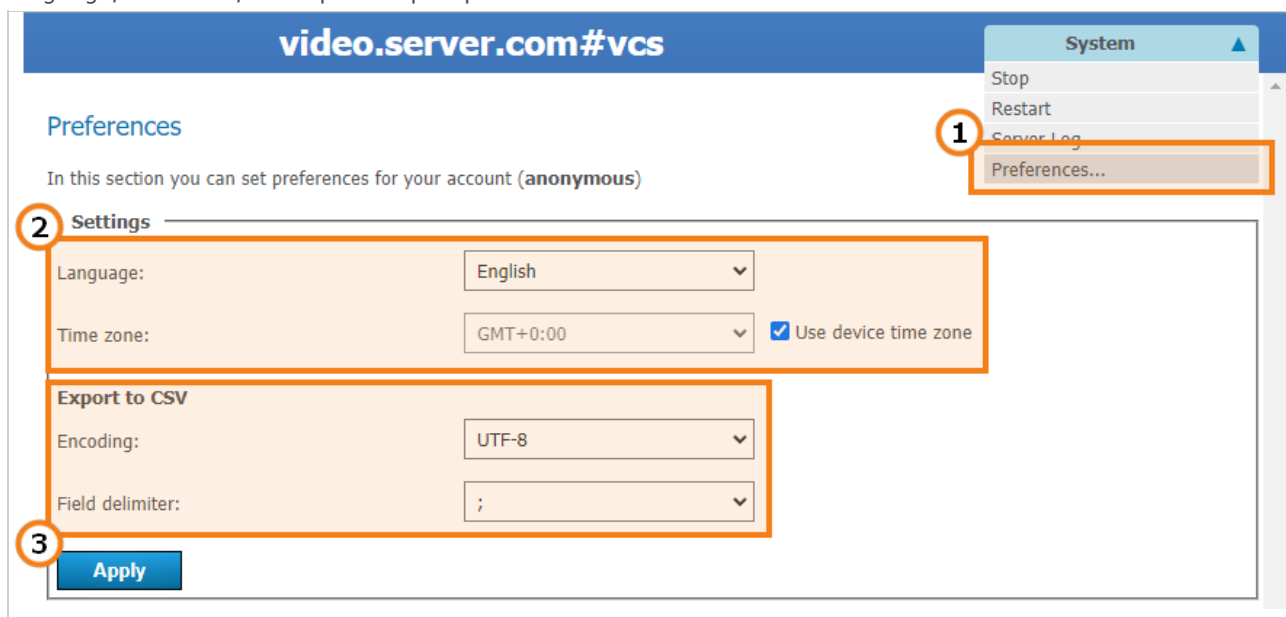


Check **Enable detailed logging** in **Dashboard → Settings** section of the control panel to collect more detailed information in your server logs. Our technical support managers may ask you to do it to ease the troubleshooting process.

A range of additional log files is saved in the TrueConf Server working directory. Learn more about additional log files [in our article](#).

8.4. 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.



1. Proceed to **System → Preferences...** 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 TrueConf Server is installed by checking the corresponding box.
3. You can set [report export](#) parameters (encoding and field delimiter to convert the table string to text format) in the **Export to CSV** section.

After making any changes make sure to click **Apply** button.

8.5. Adding users

8.5.1. Where can I find client applications

Send out the link to the [guest page](#) to your users to allow them to connect to your video conferencing system. They will be able to download client applications for any supported platform on the guest page.

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

- `<server>` - address of the PC with TrueConf Server installed
- `<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.compan.y.com`
- `http://100.120.12.12:7777`



You can configure the guest page URL in the [Web → Settings](#) section of the control panel.

8.5.2. How to connect client application to the video conferencing server

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.

Once connected to the server user will be prompted to authenticate on this TrueConf Server instance with [username and password](#).

8.5.2.1. Client application manual setting

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.

8.5.2.2. Client application automatic settings

Desktop client applications can automatically search for local TrueConf Server instance. To make this possible administrator needs to specify the address of the server in **primary DNS suffix** by creating a new SRV record for vcs2 service.

The following example shows how to do this using DNS utility in Microsoft Windows 2012 Server:

- Choose **Other New Records...** in a right-click menu
- Choose type «Service Location (SRV)»
- Set the following parameters.

New Resource Record

Service Location (SRV)

Domain:

Service:

Protocol:

Priority:

Weight:

Port number:

Host offering this service:

☐ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

OK Cancel Help

In this example the TrueConf Server instance has **videosever.your.domain.com** address and port 4307. Please make sure that protocol name (tcp) does not contain underscores.

8.6. PDF file import settings

With TrueConf Server (both free and paid license), users can enjoy a number of [collaboration tools](#): share screen or separate application windows, show slides, control desktops remotely, etc. However, you need to set up additional third-party software to [display slides created from PDF files](#) in TrueConf for Windows client applications.

To create a slideshow from a PDF file and to view PDF documents directly in TrueConf for Windows, the open-source **Ghostscript** library is used. It will be automatically downloaded from TrueConf Server and installed on a user's PC when the first PDF file is imported. However, since this library is not integrated into the TrueConf software, it must be manually pre-configured on the server side.

* TrueConf client applications for Linux and macOS use system libraries for working with PDF files. The import of these files will be available when connecting to TrueConf Server for Linux and TrueConf Server for Windows. Please [contact our technical support](#) if you have any problems or additional questions about this feature.

8.6.1. For Windows

1. Please contact [TrueConf technical support](#) to request the archive with compiled Ghostscript libraries. The archive will include four files: **gsdll86.lib**, **gsdll64.lib**, **gsdll86.dll**, **gsdll64.dll**.
2. Create a `third_party_extensions` directory in the [TrueConf Server working folder](#) (`C:\TrueConf\` by default).
3. Unpack the archive from step 1.
4. Open the registry (for example, by running the **regedit** command from your console).
5. Go to the registry branch

`HKEY_LOCAL_MACHINE\SOFTWARE\TrueConf\Server\AppProperties`

and create a string parameter `pdflibrary_url` with the value `https://[server_address]/third-party_extensions/gsdll.dll`, where `[server_address]` is the FQDN (domain name) or IP address of your TrueConf Server instance. This address will be used for connecting to the server from client applications.

6. Open the file `[installation_path]\httpconf\opt\redirects.conf`, where `[installation_path]` is the server installation path and add the following text starting from a new line (all other line should be commented out):

```
RewriteEngine On

Include opt/work_dir.conf
<IfDefine work_dir>
    RewriteCond %{REQUEST_URI} ^\./third-party_extensions/gsdll.dll$
    RewriteCond %{QUERY_STRING} ^(.+&)?(arch=x(64|86))(.)?
    RewriteRule ^(.*)$ "${work_dir}/third_party_extensions/gsdll%3.dll" [L,QSA]
</IfDefine>

<IfDefine work_dir>
    AliasMatch ^/third-party_extensions/(.+)$(.)$
    "${work_dir}/third_party_extensions/$1.$2"
</IfDefine>
```

7. Restart TrueConf Server and TrueConf Web Manager services from your Task Manager. TrueConf Web Manager service will not be affected if you restart TrueConf Server from the control panel.

8.6.2. For Linux

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.

1. Please contact [TrueConf technical support](#) to request the archive with compiled Ghostscript libraries. The archive will include four files: `gsdll86.lib`, `gsdll64.lib`, `gsdll86.dll`, `gsdll64.dll`.
2. Create the redirect configuration file, e.g., with `nano` editor in the terminal:

```
nano /opt/trueconf/server/etc/webmanager/opt/redirects.conf
```

3. Write the following lines to the configuration file and save it:

```
RewriteEngine On
Include /opt/trueconf/server/etc/webmanager/opt/work_dir.conf
<IfDefine work_dir>
RewriteCond %{REQUEST_URI} ^\./third-party-extensions\./gsdll.dll$
RewriteCond %{QUERY_STRING} ^(.+&)?(arch=x(64|86))(.+)?
RewriteRule ^(.*)$ "${work_dir}/third_party_extensions/gsdll%3.dll" [L,QSA]
</IfDefine>
<IfDefine work_dir>
AliasMatch ^/third-party-extensions/(.+)\.(.+) "${work_dir}/third_party_extensions/$1.$2"
</IfDefine>
```

4. Add a parameter with a link for loading the necessary libraries in the application by running this command:

```
/opt/trueconf/server/bin/vcs/tc_regkey set "AppProperties" "pdflibrary_url" str
"https://[server_address]/third-party-extensions/gsdll.dll"
```

where `[server_address]` is the FQDN (domain name) or IP address of TrueConf Server that will be used for connecting to the server from client applications.

5. Create a directory for libraries:

```
mkdir /opt/trueconf/server/var/lib/third_party_extensions
```

6. Unpack all files from the archive (received at Step 1) to the `third_party_extensions` directory.
7. Restart the web server services and the main TrueConf Server service:

```
systemctl restart trueconf-web
systemctl restart trueconf
```

9. Information about the server and PRO licenses. Storage settings

TrueConf Server control panel (web manager, TrueConf Web Manager) is a web interface that allows administrating 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`.

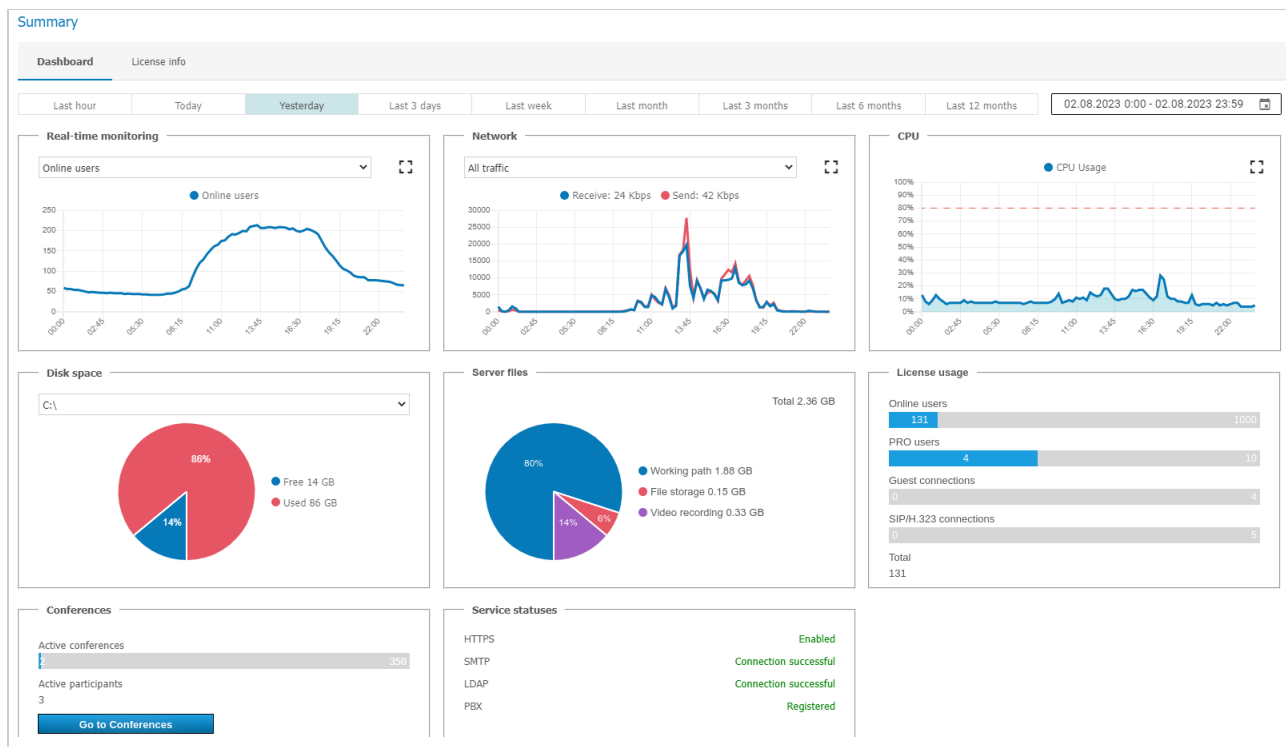
9.1. Control panel

9.1.1. Summary

The **Summary** section opens automatically every time you access your TrueConf Server control panel.

In the **Dashboard** tab, you can view the following information:

- 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
- Storage space taken by the [working directory](#), [chat files](#) and [conference or call recordings](#)
- 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.



You can press the button to enlarge any of the graphs and click the button to select any date range for your data display.

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

- Renew the server license or change the [server name](#) by clicking on the **Register** button
- Purchase additional features from the **Extensions** section.

Summary [Help ?](#)

Dashboard **License info**

Registration details

Server ID: kk123 **Registered**

Organization name: Great Company Expires in 162 days

Contact person: Joe Smith, smith@example.com [Register](#)

[License agreement](#)

License details

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	

Extensions

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
Improved Security	Enabled

In case of any problems with TrueConf Server registration, the administrator may reach out to [TrueConf technical](#)

support team via the contacts that will be displayed in case of an error.

! If connection with the registration server (`reg.trueconf.com` via TCP port `4310`) is lost, your TrueConf Server Free will be shut down in 12 hours. The expected shutdown time will be displayed in the **Summary** tab. The full version of TrueConf Server does not impose such limitations, regardless of the registration method (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.

9.1.2. PRO licenses

In the **Dashboard** → **PRO licenses** section, the TrueConf Server administrator can [distribute PRO licenses](#) needed for participation in group conferences. The administrator can also view information about the use of these licenses.

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 1
- ☒ Allow users to request temporary PRO licenses 2

Client license management

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

Permanent (10) 3 **Temporary (0)** 5

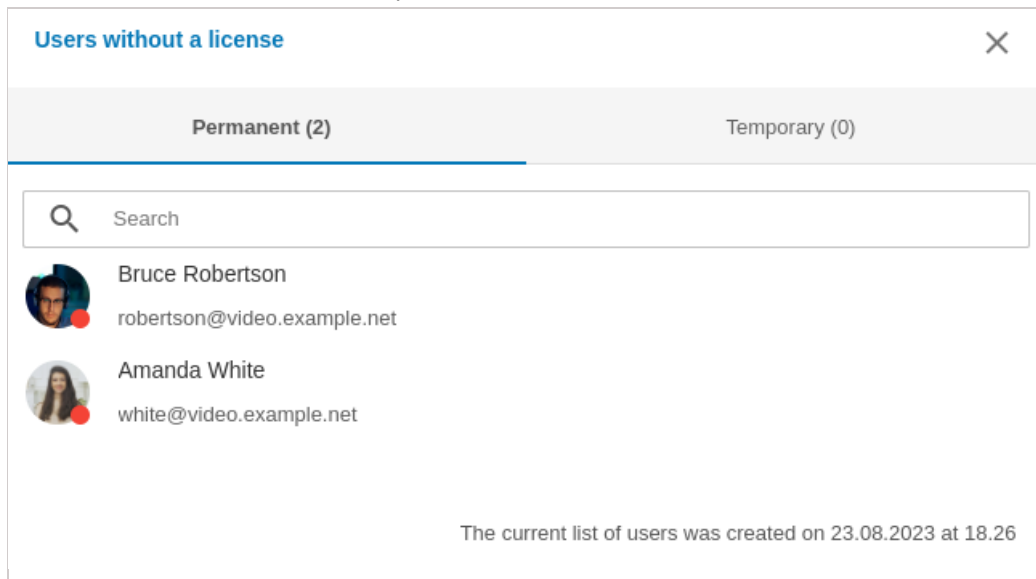
EDIT 4

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 have received temporary PRO licenses, with the validity period for each license indicated. You can also revoke a temporary license from any user by clicking the button **X** next to a user's name. The

license will then instantly return to the pool of available temporary PRO licenses. Please note that if a user is participating in a conference at the moment when the license is revoked, this person will be automatically removed from the conference.

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.



Two separate lists will be generated there:

- **Permanent** — here, one can find the list of users who did not receive permanent PRO licenses when these licenses were distributed (below the list one can check the date when TrueConf Server was last restarted)
- **Temporary** — users who tried to get a temporary PRO license but none were available on TrueConf Server. This list is not cleared when the TrueConf Server service or the computer is restarted. Each user is removed from the list 24 hours after being added to it.



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.

9.1.3. Main settings

In the **Dashboard → Settings** section, one can specify the path where TrueConf Server data will be saved, view server performance information, and configure client applications.

The screenshot shows the 'Settings' page of the TrueConf Server. It is divided into several sections: 'Work path', 'Reports', 'Configuration', 'Application', and 'Application settings'. Numbered callouts (1-9) highlight specific elements: 1 points to the 'Path' field in 'Work path'; 2 points to the 'Enable detailed logging' checkbox in 'Reports'; 3 points to the 'Backup settings' and 'Restore settings' buttons in 'Configuration'; 4 points to the 'Application' table; 5 points to the 'Generate a new key' button for 'User connections authentication key'; 6 points to the 'Generate a new key' button for 'Guest connections authentication key'; 7 points to the 'Authorization token lifetime on a device' dropdown; 8 points to the 'Display the Reactions panel in multipoint conferences' checkbox; and 9 points to the 'Save application settings' button.

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

1. Server working directory. 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. Enable detailed [logging](#) of your TrueConf Server activities. Might be required by our technical support team for troubleshooting.



You can read more about [TrueConf Server log files](#) and learn [which logs are required](#) for troubleshooting and reporting tickets to the technical support department in our knowledge base.

3. Backup and restore TrueConf Server settings ([learn more below](#)).
4. Go to [customize client applications TrueConf](#) from which users will connect to your conferences.
5. A field for generating a secret key. It is used for creating session keys to authenticate users in a video conference. To replace your key with a new one, press **Generate a new key** button. By replacing the key you can make your conference more secure (e.g. inhibit third-party connections).
6. A key similar to the previous one. It controls authorizing using guest accounts in public conferences.
7. Specify the validity period of the authorization token; it determines the time interval during which the session will be maintained after a user connects to TrueConf Server from a client application or signs in to the personal area. When the validity period 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](#).

8. **Enable statuses** (icons used as reactions) during a conference.
9. Save application settings.



We strongly advise you not to use settings 5-7, unless being told so by our technical support team, as they might significantly decrease the quality of your video conferences or put TrueConf Server security at risk. The ability of TrueConf Server to automatically and dynamically manage video streams encoding parameters is crucial for effective collaboration.

9.1.4. Configuration back-up and restore

Backup copy of TrueConf Server settings will enable you to save the main server settings, including users, groups, scheduled conferences, network settings and then restore the server settings from the file where the settings were saved. This feature may be helpful when the operating system is re-installed or when the server is migrated to a different physical machine. You will not have to configure the server once again. Check full guides in our knowledge base to learn more about saving and restoring settings:

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

When TrueConf Server settings are saved to a file, the reserve copy of this file will be automatically created in the `[working_path]\registry_backups` folder where `[working_path]` is the working directory of a server. This applies both for Windows and Linux versions of TrueConf Server.

9.1.5. Settings for client application connection

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.

To choose the allowed application versions, click on the selected name in the first table column:

Application

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

Here, you can edit the following parameters:

1. Minimal version of the client application supported by TrueConf Server. If the current version of client application is lower than the one specified here, client application will be stopped and mandatory updated.
2. Preferred version of the client application. If the version of the app is older than the version specified in this field, the user will be prompted to update. It's possible to cancel the update and continue to use the application unless it's version is higher than the Minimal one.
3. The version of client application which will be offered for 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](#).

9.2. 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 for 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:
2. 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 -RT /opt/trueconf/server/var/lib/recordings /var/server/recordings
```

sh

- file copying

```
cp -RT /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 web service:

```
systemctl restart trueconf-web
```

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

9.3. 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 instance, to mount an external network storage accessible via the [SMB protocol](#), take 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

9.4. Access settings for network storage on Windows

TrueConf Server for Windows can gain access to network drives, if two of its services are allowed to read and write to network paths. However, by default these services are run under the system account (Local System) which does not have access to network resources. So, they should be configured to run on behalf of a user 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. Find the **TrueConf Server** service (the main service of the video conferencing server) in the list.
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:** switcher.
5. Enter the username and password for the required account, for example, a Windows administrator, and click **Undefined**.
6. Repeat steps 2-5 for the **TrueConf Web Manager** service.

9.5. 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 setup storage settings for files your users are exchanging:

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. Maximum storage capacity allocated for files from chats.
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.

9.6. Recordings

In this section, 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.

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:
 - users participating in a meeting from TrueConf client applications
 - 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 the recording files will be saved.
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).

**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.

What will happen to an ongoing conference, if I run out of storage space while this conference is being recorded?

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

10. Settings for network, notifications and federation

In this section you can adjust some network settings for your TrueConf Server instance:

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

10.1. Network Settings

In this section you can specify IP addresses and ports which will be used by TrueConf client applications to connect to TrueConf Server. IP address of the computer where TrueConf Server is installed is used by default.



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.

In the **Internal addresses** list, one will find the addresses and ports that the server will listen to for connections from client applications. These should be the addresses of the network interfaces on the machine where TrueConf Server is installed, or its internal DNS name, which resolves to one of the network interfaces by IP. When the box **Listen on all IP addresses** is checked (the default option), the list will be automatically created and will contain all such addresses, including virtual ones.

To edit the **Internal addresses** list, you will need to:

1. Uncheck the **Listen on all IP addresses** box.
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 installer name of TrueConf for Windows client application and will be used during the first launch of the application. If the list does not include addresses accessible to all TrueConf for Windows users (both external and internal), they will not be able to connect to the server until they specify a correct address in the application settings. So, we suggest that in this section, 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 new address). If the server will be used only within a local network, this list will not be needed.

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

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.

When the external address is adopted, go to the [Web → Settings](#) section in the control panel and change the external address of the web page to a public IP (indicated in the **External addresses** list). Then restart the server so that external users can connect to it 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.

10.2. SMTP

Although TrueConf Server doesn't have a built-in mail server, it can use an external SMTP server or service to deliver email notifications, invitations and other important messages to your users. You can change the templates used for these messages in this section as well.



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:

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 authentication mode (**simple password** or **no authorization**). If you have chosen password-protected authentication mode, please enter login and password to connect your TrueConf Server instance 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. Check your settings using the **Check connection** button. The current status of your connection to the mail server is displayed in the **Status** field: **successfully connected** in case of successful connection to the SMTP server and **invalid server** if the connection can not be established.

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 changes.

10.2.1. Email template settings

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

To restore default templates for all emails, click the **Set default** button in the **User mails** section. In this case, the language of the templates will match the language [selected in the preferences](#) by the current administrator.

10.2.2. Notifications about missed calls

To receive missed call notifications, enable the **Notify users about missed calls** checkbox. If any of the users is offline during the call or conference invitation, TrueConf Server will send an email notification at the email address specified in the **E-mail** field in the [user account settings](#) or in the corresponding field [imported via LDAP synchronization](#).

Notifications about missed calls are sent to those unregistered users who were called by a user from your video conferencing server: he/she did not know their TrueConf ID and tried to call them by email. Such calls must be made with the `#mailto:` prefix, for example, `#mailto:user123@example.com`. This issue occurs because TrueConf ID format coincides with an email address; so, a special prefix in the call string is required to distinguish between them.

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

10.2.3. Conference invitations

To enable email invitations for all new scheduled conferences, enable the **Send invitations to participants of the group conference** checkbox. In this case, when scheduling a meeting, all invited users will receive email invitations where date and time of the meeting (if any) is specified.



You can enable or disable email invitations for each meeting individually in [the Advanced tab](#) when creating or editing the conference.

10.2.4. Reminders about the upcoming conference

You can send automatic reminders about upcoming events. In this case all participants added to a scheduled conference will receive an email reminder before the start of this meeting. The reminder template can be set below in the **Reminder about upcoming conference** section.

In the **Reminders** list one can select when email reminders should be sent to participants. If the box is checked, but no option is selected in the list, the administrator or owner can manually select the period when [scheduling a meeting](#). If a period has already been selected, for example, 1 day and 5 minutes before the meeting, email reminders will be sent according to the existing settings if a conference is created.



If the administrator checks the box **Send users reminders about upcoming conference** and selects a period in the **Reminders** section, automatic reminders with the specified time periods will be added for the scheduled conferences that were initially created without reminders.

10.2.5. Confirmations of registration for a public conference

To send confirmations of a successful webinar registration (available if corresponding settings have been adjusted), use the **Conference registration notification** template.

10.2.6. Notifications about removal from a conference

To notify users when they are removed from the list of invited participants, mark the **Notify users if they are**

removed from the participant list checkbox. These settings will be applied to all conference modes. If registration settings have been configured for the webinar, the notification will be received by the participants who signed up for the webinar and those users who were invited to the list of participants when the conference was created.

10.2.7. 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` is the [guest page URL 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](#)
 - `%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` — conference description [specified](#) in the **Advanced → Description** section when the conference is being created.
 - `%conf_url` — the link to the [conference page](#), e.g.,:

`https://example.com/c/CID`
- 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.

10.3. Federation

The [federation mode](#) allows TrueConf Server users to make calls and join conferences with users from other TrueConf Server instances. Federation is only available in the full version of TrueConf Server (for example, when purchasing additional [licenses of any type](#)). There is no limit on the number of servers that can be joined through federation. The restrictions on holding group conferences will correspond to the limits set in the TrueConf Server instance that initiated connection.

The federation has to be configured for both servers so that they could be accessible to each other according to the rules specified below. To configure federation, you will need to:

- In the drop-down list, select the federation mode:
 - Disabled**
 - Allowed for whitelisted servers.** In this mode, only TrueConf Server instances specified in the whitelist can be federated
 - Allowed for all but blacklisted servers.** In this mode, all TrueConf Server instances can be federated except for those specified in the blacklist.
- 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**.

i 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.*`.

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

i To be able to operate in federation, your TrueConf Server instance should be available to other servers and client applications by its DNS (FQDN) name indicated [during the registration process](#). The server should be registered either under an existing DNS name or a server address using SRV DNS records. If you would like to learn more, proceed to the [client application automatic settings](#) section.

Let us take a look at some examples.

Case 1

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

- Add `videoserver.company.com` to the white list
- Activate federation on the side of `videoserver.company.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).
- Make sure that both servers and TrueConf client applications connected to these servers are accessible to each

other via their domain names.

Case 2

If the `videosever.company.com` server was added to the black list, the users from your server and all the users with `id@videosever.company.com` ID will not be able to make calls to each other.

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. SIP/H.323/RTSP gateway and transcoding

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

With the gateway you can:

- [Configure integration of TrueConf Server and Asterisk](#)
- [Configure integration of TrueConf Server and Cisco UCM via SIP](#)
- [Register TrueConf Server on an external H.323 gatekeeper](#) by adding the required configuration.



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.

TrueConf Server can process tone dialing signals; so, you will be able to send the following DTMF commands from your SIP/H.323 endpoint in "smart meeting" mode:

- **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 discussed the use of [Polycom HDX series endpoints](#) together with TrueConf Server, including sending DTMF commands from them.

11.1. 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.

Calling up devices via SIP gateway requires specific [call string formats](#).

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

11.1.1. Network settings

This list contains the addresses that are used by the gateway to listen for incoming SIP 2.0 connections. By default

the list is prefilled with IP addresses provided by your operating system. You can edit this list by unchecking **Listen on all IP addresses** checkbox.

11.1.2. 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 **Add a configuration** and select one of the two possible templates: [manual configuration](#) or [Skype for business connection](#). Skype for business template has some preselected features required for Skype for business interoperability, e.g. port, protocol, used video codec and registration mode.

11.1.3. New rule form

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 IP address which will be specified in SDP for receiving and sending media streams when calling users behind NAT.

The **Outgoing SIP domain for callback to TrueConf Server** field is used to generate an SIP URI for outgoing calls to SIP devices. It is generated in the format `user@server`, where `server` is the IP address or FQDN value and `user` is the ID of the user who made the call. It is usually displayed as a caller address on SIP devices. Possible values are as follows:

- **Do not specify** — in this case, the address will include only TrueConf ID.
- **Use server public name** — the server external address will be used (this address is specified in the [Web → Settings](#) section).
- **Use other domain** — the required domain has to be specified in the input field.

The following block of fields is designed to authorize on an SIP device for which the rule is created. If the **Authorization name** is the same as login, you may leave this field blank. You can use **International call prefix** to replace the '+' symbol used in phone numbers with another value, e.g. '810'. If you leave this field blank, '+' symbol will not be replaced in the phone numbers your users are calling to.

Registration mode defines registration method for the rule:

- **off** — REGISTER request is not sent, registration or authorization on the external SIP device is not performed.
- **permanent** — registration is performed automatically when TrueConf Server starts.
- **before call** — registration is performed before every call and is kept 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.

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 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)

Available codecs

<input checked="" type="checkbox"/> H.265	<input checked="" type="checkbox"/> G.722.1C 32 kbit/s	<input checked="" type="checkbox"/> G.711 ulaw
<input checked="" type="checkbox"/> H.264 High Profile	<input checked="" type="checkbox"/> G.722.1C 48 kbit/s	<input checked="" type="checkbox"/> G.711 alaw
<input checked="" type="checkbox"/> H.264 Main Profile	<input checked="" type="checkbox"/> G.722.1C 24 kbit/s	<input checked="" type="checkbox"/> OPUS
<input checked="" type="checkbox"/> H.264 Baseline Profile	<input checked="" type="checkbox"/> G.722.1 32 kbit/s	<input checked="" type="checkbox"/> Speex
<input checked="" type="checkbox"/> X-H264UC	<input checked="" type="checkbox"/> G.722.1 24 kbit/s	
<input checked="" type="checkbox"/> H.263++	<input checked="" type="checkbox"/> G.722	
<input checked="" type="checkbox"/> H.263+	<input checked="" type="checkbox"/> G.723	
<input checked="" type="checkbox"/> H.263	<input checked="" type="checkbox"/> G.728	
<input checked="" type="checkbox"/> H.261	<input checked="" type="checkbox"/> G.729A	
<input checked="" type="checkbox"/> VP8		

Role

☐ Default SIP trunk

☐ Default VoIP server

If you want to reduce SIP packets and headers and prevent potential issues that can be caused by exceeding maximum allowed packet size (MTU), you can use options in the **Reduce SIP messages size** block.

Enable ICE support (Interactive Connectivity Establishment) checkbox makes TrueConf Server gateway available behind NAT.

Enable SRTP support checkbox is used to encrypt media data sent in this direction. For some SIP devices encryption is mandatory (e.g. for Skype for business servers).

Enable content sharing via BFCP checkbox will allow you to [send and receive content from SIP devices](#) as a second video stream. For example, it can be used to share desktop from the PC connected to SIP endpoint, or send slides back from TrueConf applications to SIP endpoints.



When you share content as a second stream from your SIP or H.323 device, the content is transmitted with a reduced frame rate to save traffic. If you need to transmit the second stream content at a higher frame rate, please contact [our technical support](#) to switch to the appropriate mode.

Enable far end camera control via Q.922/H.224/H.281 checkbox enables support for far end camera control of SIP endpoints from TrueConf client applications.



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 an SIP endpoint from a conference in case of a connection loss. This box is disabled by default.

You can manually specify **Max session refresh interval (seconds)** (1800 seconds by default).

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 SIP devices. For more details please contact our [technical support](#) team.

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.

11.1.4. Skype for Business integration configuration

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 on Skype for business server for TrueConf Server gateway.
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. Enter Skype for business server IP address or domain name in the **Host** field.
4. Check **Default SIP proxy** checkbox.
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 users from TrueConf client applications, use the following format: `#sip:User`, where `User` is TrueConf username. This user will receive an incoming call from the TrueConf Server account. The same method is used to invite Skype for business users into the conference or add them to 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 <TrueConf_ID>`, where `<TrueConf_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 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.

11.1.5. Global SIP settings section

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 will allow you to choose the behavior in case of such a SIP call to any of the addresses from [the Network settings](#) block via 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 the [TrueConf ID of the user](#) or [conference ID](#). Then you should specify this ID in the field below.

Other settings are similar to those used to [create connection rules](#).

11.1.6. Invitation of the SIP endpoint to the conference on TrueConf Server

There are multiple ways of inviting a SIP endpoint into a conference: the conference owner can call a SIP endpoint using a [specifically formatted call strings](#) from TrueConf client application. Alternatively, administrator can do it from TrueConf Server control panel.

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

- Select a conference in [Group conferences list](#).
- Add SIP endpoint as a participant of the conference if it's not started yet, or invite in case it's already running. Use a [call string](#) to address the SIP endpoint.

11.1.7. 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>` is an IP address of TrueConf Server gateway e.g., `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.

11.2. 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.

H.323 connections are generally used to call third-party video conferencing endpoints. With TrueConf Server you can also set up H.323 integration with MCU, H.323 gatekeeper and PBX, which can be useful for addressing endpoints and users registered on these devices via H323-ID or E.164 without specifying IP address of the endpoint in the call string. To call an endpoint via H.323 gateway, there is a [special call string format](#).

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.			

Add a configuration

11.2.1. Network settings

This section includes the list of addresses listened by the gateway for incoming H.323 connections. By default the list is prefilled with IP addresses provided by your operating system. You can edit this list by unchecking **Listen on all IP addresses** checkbox. The list of ports used for H.323 connections [is available in our blog](#).

11.2.2. 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.

11.2.3. New rule form

Name field value is used only to distinguish one rule from another. **Host** and **Port** fields are also mandatory. They are required to determine call direction to which this rule will be applied. Please note that it isn't possible to create different rules for one host but for different ports on it.

In the **External NAT IP address** field, you can specify the server IP address which will be specified in SDP for receiving and sending media streams when calling users behind NAT.

H323-ID and **Password** fields can be provided to authorize on H.323 device for which the rule is created. To maintain permanent connection with this device, you'll need to select necessary item in the **Registration** drop-down list.

Once successfully registered on the H.323 device, TrueConf Server can be reached via phone number in the E.164 format provided it has been specified in the **DialedDigit** field. This setting can be useful if bundled with **Default call destination** option in the [global H.323 settings](#) section. In this case all calls to the specified **DialedDigit** number outgoing from the connected H.323 device will be redirected to a specific user ID or conference ID on TrueConf Server side.



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

Enable H.235 encryption checkbox enables encryption of the media streams sent to H.323 devices according to ITU-T H.235 version 3 recommendations. It is required for proper interoperability with some endpoints.

Enable content sharing via H.239 checkbox allows to [send and receive content from H.323 devices](#) as an additional video stream. For example, it can be used to share desktop from the PC connected to H.323 endpoint or to send content from TrueConf applications in the opposite direction.



When you share content as a second stream from your SIP or H.323 device, the content is transmitted with a reduced frame rate to save traffic. If you need to transmit the second stream content at a higher frame rate, please contact [our technical support](#) to switch to the appropriate mode.

Enable far end camera control via Q.922/H.224/H.281 checkbox enables support for far end camera control of H.323 endpoints via ****Q.922, H.224 and H.281**** protocols from TrueConf client applications.



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.** This role allows users to avoid entering full address of the [H.323 device](#) using `#h323:` prefix. For example, all calls in any direction in the `#h323:Endpoint` format will be automatically replaced with `#h323: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 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.

11.2.4. 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.

Use **Default call destination** field to enter TrueConf ID or conference ID (CID) which will receive all incoming calls over H.323 protocol in cases where destination user ID wasn't specified.

11.2.5. How to call TrueConf users and conferences from 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 TrueConf Server IP address and `User` is ID of the user or device registered on TrueConf Server
- `Server##00CID`, where `Server` is the IP address of TrueConf Server while `CID` is the ID of a conference hosted 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 ID of the conference on TrueConf Server and `Server` is TrueConf Server IP address
- `00CID@Server`, where first two characters are zeroes, `CID` is ID of the conference on TrueConf Server and `Server` is TrueConf Server IP address.

[Call formats for H.323](#) and their examples are fully described in the user guide.

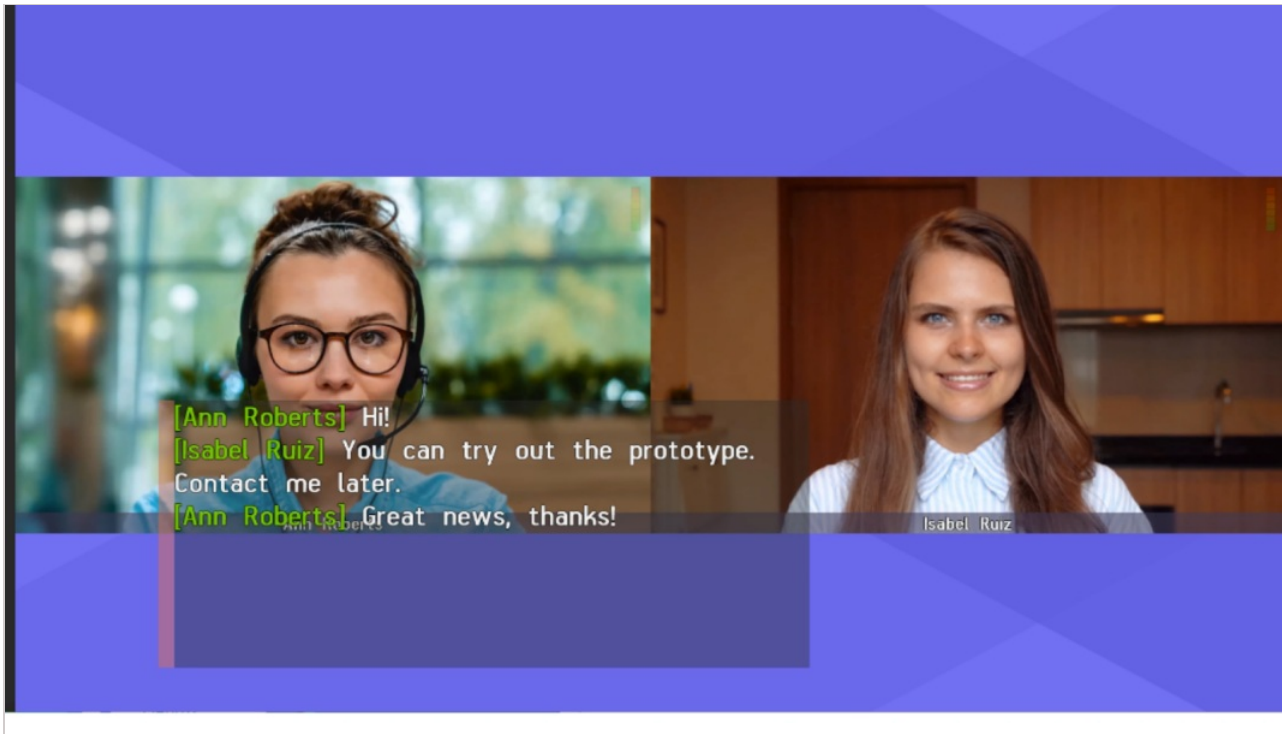
11.2.6. How to register H.323 devices on the video conferencing server

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.

11.3. Chat during calls on TrueConf 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:



11.4. RTP

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

RTP [Help ?](#)

UDP port range

From

50000

—

To

51999

Apply

11.5. WebRTC

In this section you can configure the [UDP or TCP port range for a WebRTC connection](#) (53000-55000 by default).

You can also specify the IP address used for NAT traversal if automatic detection fails for some reason in the **Public IP address is added to SDP as an extra ICE candidate** field in the TrueConf Server control panel.

WebRTC

[Help ?](#)

UDP/TCP port range

-

Apply

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

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

Apply

11.6. Transcoding

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

11.6.1. Quality settings

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.



Quality settings for the video streams sent from conference participants to TrueConf Server are selected in [conference settings](#).

Transcoding [Help ?](#)

Restrictions for modules

FPS: 60 ▼

Recording: 1080p ▼

SIP/H.323: 1080p ▼

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

☐ Use GPU to reduce CPU load

☐ Automatically spotlight active speaker window

Checking the box **Do not display self-view in video layout for H.323 and SIP endpoints** allows displaying the conference layout for SIP and H.323 devices without the self-view window. In other words, an individual layout will be created for an SIP/H.323 participant with no video from the camera connected to the endpoint.

If you enable the box **Do not display self-view in video layout for WebRTC participants**, it will be possible to create a layout for each browser connection without including the video window of the participant. In other words, the individual layout is created for the WebRTC connection, and the video feed from the camera used in the browser will be excluded.



When an individual video layout is created for each SIP/H.323 and WebRTC connection, CPU load may significantly increase on the physical machine where TrueConf Server is installed.

When the box **Use GPU to reduce CPU load** is checked, video conferences will be processed by the GPU of the physical machine with TrueConf Server installed.



GPU transcoding is available only in TrueConf Server for Windows.

The parameter **Automatically spotlight active speaker window** enables automatic enlargement of the speaker's window based on voice activity. The settings for hiding the self-view and automatic enlargement of a speaker's video window will take effect only if the layout is not explicitly set for SIP/H.323/WebRTC participants when [the conference is scheduled](#) or in the [real-time meeting management](#) section.

11.6.2. Adding background and watermark

In the **Gateways → Transcoding → Visual settings** section, one can specify the global settings for background and watermark displayed in the video layout of all conferences. After selecting a watermark image, you can choose 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

12. Web and HTTPS settings

In this section, you can find settings for your guest page and control panel access.

12.1. Web Settings

12.1.1. Guest page settings

To change the guest page URL and its appearance, you can use the following options:

The screenshot shows the 'Web Settings' configuration page. It is divided into three main sections: 'External address of TrueConf Server web', 'Guest page', and 'Company logo'.
 1. 'External address of TrueConf Server web': A text field containing 'https://10.140.2.195' with an 'Apply' button next to it.
 2. 'Guest page': A section containing a 'Link to the guest page' field with the same URL, a 'Display name of your company' field with 'True Company', and 'Contact details of the server administrator' fields for 'Contact name' (Joe Smith), 'Email' (admin@example.com), and 'Phone' (+8080899999).
 3. 'Company logo': A section with a 'Logo to be displayed on the guest page' area showing a TrueConf logo, and a file upload interface with 'Choose a file', 'No file chosen', 'Upload', and 'Set by default' buttons.
 Numbered callouts (1-6) highlight these specific elements in the interface.

1. The TrueConf Server address which is used to generate links to the server guest page and conference pages. Make sure that it is available to all users of your TrueConf Server instance. In case of an unstandardized port (different from HTTP 80 or HTTPS 443), type it with a colon in the address field, e.g., `https://video.server.com:4433`. When using an external service to proxy traffic, the external address of TrueConf Server will be its address. Such a service can be, for example, NAT or [TrueConf Border Controller](#). Through the specified `address:port` the following will also be passed to client application users: advanced conference management widget, conference scheduler, second stream content display and slideshow (presentation).
2. The link to the [guest page](#) which provides instructions on how to connect new users to TrueConf Server. Matches the external address of the server.
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.

12.1.2. Additional documents

You can add your custom documents in the **Personal data processing** block:

- 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	<input checked="" type="checkbox"/>	Edit
Privacy Policy	<input checked="" type="checkbox"/>	Edit
Terms of Use	<input checked="" type="checkbox"/>	Edit
Agreement	<input checked="" type="checkbox"/>	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 **Display link** box.
3. Check the **Display cookie notification** box if you want to display a pop-up notification with a link to the cookie policy for each new visitor of your TrueConf Server guest page or public conference webpages.
4. If you want to display an additional document or agreement (up to 2 additional documents and up to 5 documents in total), click **Add document**. Do not forget to check the **Display link** box to display your document on the TrueConf Server public webpages.
5. Click **Delete document** to remove documents from the list. Please note that you cannot remove default documents, but you can hide them on your TrueConf Server public webpages 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 ~~S~~

- -
- -

Normal

It is additional information for VCS users.

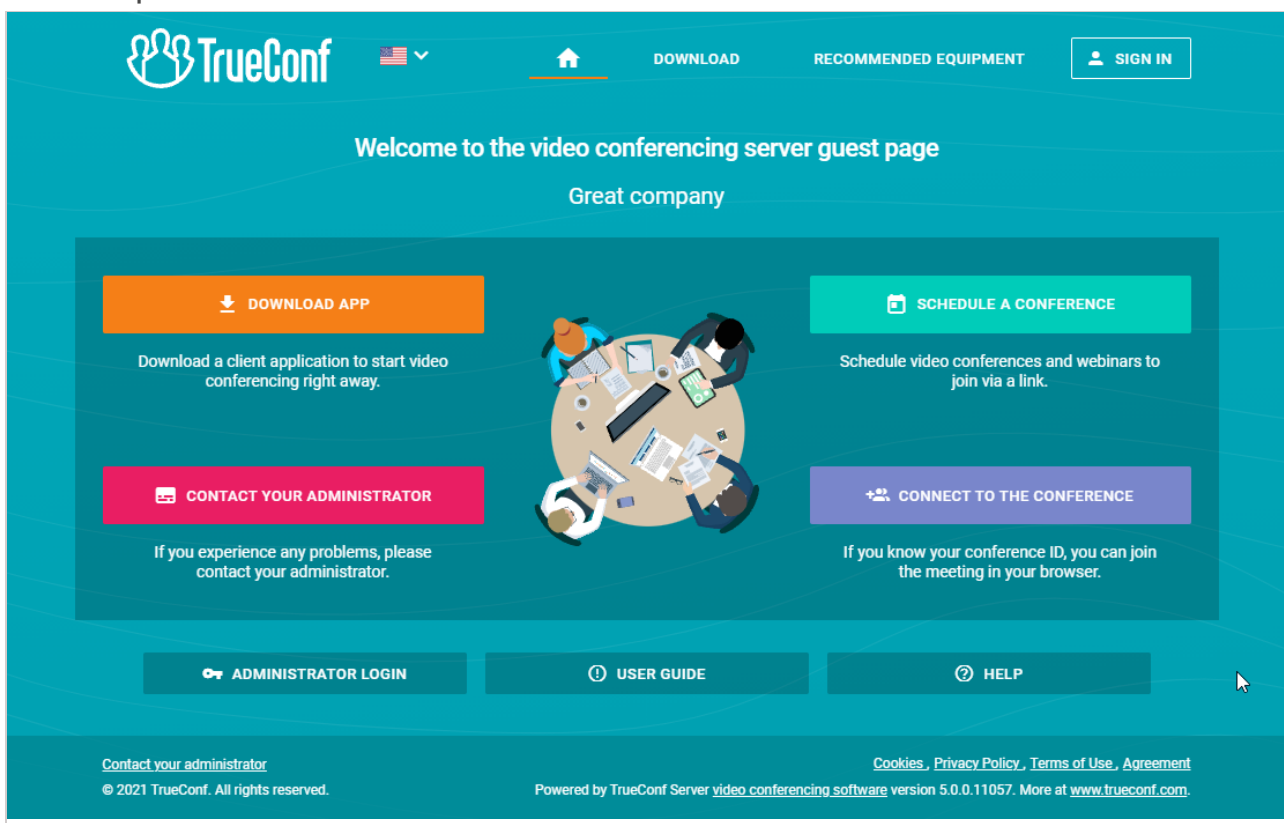
This text is available on the guest page.

Apply

To display additional information:

1. Check the **Display the Help button** box.
2. Enter your information in the field below.
3. Press **Apply**.

Below you can see an example of a guest page with three default documents, one additional document and a custom **Help** button:



12.2. Security

In this section you can set up access to your TrueConf Server control panel and TrueConf Server API.



Read more about [TrueConf Server admin roles](#) on different operating systems in the TrueConf Server installation and initial setup section.

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. If this option is enabled (it is enabled by default), the control panel can be accessed without authorization from the computer on which your TrueConf Server instance is installed (browser's host is `localhost` or `127.0.0.1`). Uncheck the box if you require all admins to authorize.



Please make sure that you have a user account that is a member of **TrueConf Server Admin** group (for Windows) and **tcadmins** (for Linux) on the computer where your TrueConf Server instance is installed. Otherwise, you will not be able to authorize and access the TrueConf Server control panel after you've saved the changes. If you've still faced this issue, please reinstall TrueConf Server or contact our [technical support department](#).

3. 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.
4. Press this button to add a subnetwork with access to the control panel. Add the address in the **Network address** field (admissible symbols are numbers and dots, admissible format is 4 octets in decimal representation without initial noughts 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. `32 - 255.255.255.255` mask is set by default.
5. Secret security key for accessing API of your TrueConf Server.



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](#).

6. Click to generate a new secret key. Reverting to the previous key or using your own is not possible.

7. Click to apply the changes.

12.3. HTTPS

In this control panel section you can configure the safety data transfer parameters between your 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.

HTTPS is also required for users connected to your TrueConf Server instance from their client applications. Without it, they won't be able to access and use [conference scheduler](#), [show slides](#) and [manage meetings in real time](#).



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, you need to update the external address of your server in the [Web → Settings section](#) and make sure that it starts with `https`. For example: `https://video.company.com`. Or if an external service is used to proxy traffic, specify its address there.

12.3.1. 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.

The screenshot shows the 'HTTPS Settings' window. It includes a 'Help ?' link in the top right. The main section is 'HTTPS configuration'. It features a dropdown menu for 'HTTPS mode' currently showing 'Use self-signed certificate', a text box for 'HTTPS port' with the value '443', and two checked checkboxes for 'Usable TLS protocol versions': 'TLSv1.2' and 'TLSv1.3'. There are two buttons at the bottom: 'Test configuration' and 'Apply'. A link titled 'Why HTTPS is important and how to properly configure it' is located to the right of the 'HTTPS mode' dropdown.

1. Select one of the three operating modes in the **HTTPS mode** dropdown list:
 - **Disable HTTPS**. HTTPS protocol will not be used.
 - **Use self-signed certificate**. This mode uses a certificate automatically obtained from the server (this certificate is not suitable for connecting external users via WebRTC).
 - **Use custom certificate**. This mode uses a certificate uploaded by the TrueConf Server administrator.
2. Specify the TCP port that the web server will use for HTTPS connections (use numbers) in the **HTTPS port:** port

field. Port **443** is set by default.

Set the versions of the **TLS protocol** that your TrueConf Server instance will use for HTTPS operation.

4. Click the **Test configuration** button to verify the HTTPS configuration data without restarting the web server. This action does not change the configuration file of the web server.

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 TrueConf Server instance restart.

12.3.2. Self-signed and custom 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




Learn how to create a free Let's Encrypt certificate for [Windows](#) or [Linux](#) in our knowledge base.

12.3.3. Self-signed certificate

If you have previously created a self-signed certificate, here you can find the basic parameters of the root certificate, **Create a new SSL certificate** button, as well as the certificate to be used by the web server and TrueConf Server:

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

To create a new self-signed certificate, press **Create a new SSL certificate**. You may use this option to renew your certificate for 365 days or to update information about your company in the certificate (if your company's name has changed). Administrator can download a root certificate file for sharing among client devices via the link **Download ca.crt**.

12.3.4. Custom 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** button 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 not saved.



Read how to [convert an existing commercial certificate](#) to a format supported by the TrueConf Server in our knowledge base.

13. Server users. Integration with LDAP/Active Directory

13.1. User Accounts

In the **User Accounts** section you can add new user accounts, as well as edit and remote existing user accounts.



You cannot edit user details in [LDAP mode](#). User data entry form is available only in [Registry mode](#).



In TrueConf Server Free the number of user accounts is restricted. To learn more, go to the [web page of this solution](#).

The screenshot shows the 'User Accounts' management interface. It includes a title bar with a 'Help' link, an 'Add a user' button (1), a search bar (2), a 'Groups' toggle switch (3), and an export button (4). Below these is a table of users with columns for 'User', 'TrueConf ID', and 'Email'. Each user row includes an avatar with a status indicator (5) and a trash icon for deletion. The table lists six users: Leila Olson, Mary Humphrey, Sara Baros, Terry Reed, Wayne Moore, and William Hubbard.

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. Add a new user.
2. Search users by TrueConf ID, first name, last name, display name, or email.
3. View user groups available on your TrueConf Server instance.
4. Export the list of users to a CSV file for later import to the address book of TrueConf Group (can be done in the [Maintenance section of the endpoint control panel](#)). This button is available only in the [Registry mode](#). The CSV file will be saved in the UTF-8 encoding and ";" will be used as a separator which means that the [preference settings](#) will be ignored.
5. The list of the users registered on your TrueConf Server instance. At the bottom of each user's avatar, user status is displayed:
 - the user is online
 - the user is offline
 - the user is in a conference or in a call
 - the user is [the owner in the conference](#)
 - the user account is deactivated by the administrator (check the [Status section](#) in the profile).



Read how to connect users from outside your network to your TrueConf Server instance [in our knowledge base](#).

In order to change user information, click on the username. To remove a user, click on the button.

13.2. User profile

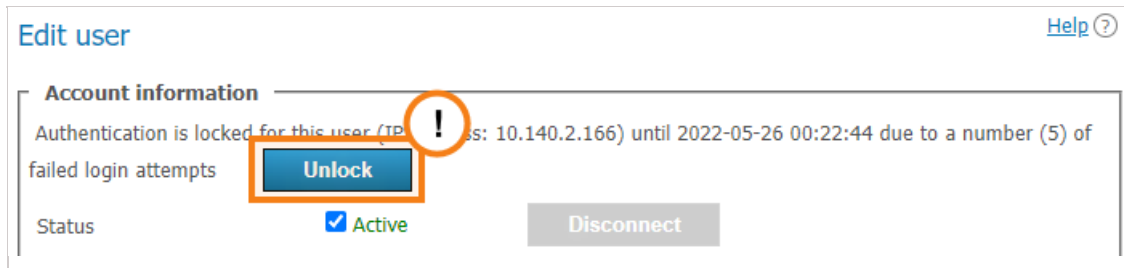
Click on any user account in any control panel section to proceed to edit mode:

The screenshot shows the 'Account information' form for a user named Sara Baros. The form includes fields for Status, TrueConf ID, Password, E-mail, Display name, First name, Last name, Company, Groups, Mobile, Work, Home, and SIP number. Numbered callouts indicate specific features: 1. Status toggle (Active/Inactive); 2. Disconnect button; 3. TrueConf ID field; 4. Password field with a help icon; 5. E-mail field; 6. Display name field; 7. First name field; 8. Last name field; 9. Company field; 10. Groups dropdown; 11. Save, Delete, and Back buttons at the bottom.

1. Change a user's status to "active" or "inactive" ([see below](#)). Such users will be displayed semi-transparent with a gray status in the [general list](#).
2. Forcefully disconnect all user's client applications from your TrueConf Server instance. You may use this option to allow another user to connect to your server when the maximum number of connections in your license has been reached.
3. **TrueConf ID** is a unique user identifier. It can be used for authorizing in client applications and making calls and conferences. Username is a part of your TrueConf ID displayed before the "@" symbol. It may consist of Latin characters, numbers, underscores, hyphens and dots. The server name displayed after the username (`@server` next to the input field) is required for calling a user of another TrueConf Server instance. The username is set when creating a user account and cannot be changed afterwards.
4. Enter the user's password. After creating or editing an account, you cannot see the password you've set. However, you can always change the password. To check [password requirements](#), click on the button which is next to the password confirmation field.
5. User's email address. You can set automatic email notifications to this address [via SMTP server](#) connected to your TrueConf Server instance.
6. The name you have entered will be displayed in the address book of other users. This field, as well as the username indicated at step 3, is prefilled. However, the field value can be changed.
7. User's personal details. These fields are not required.

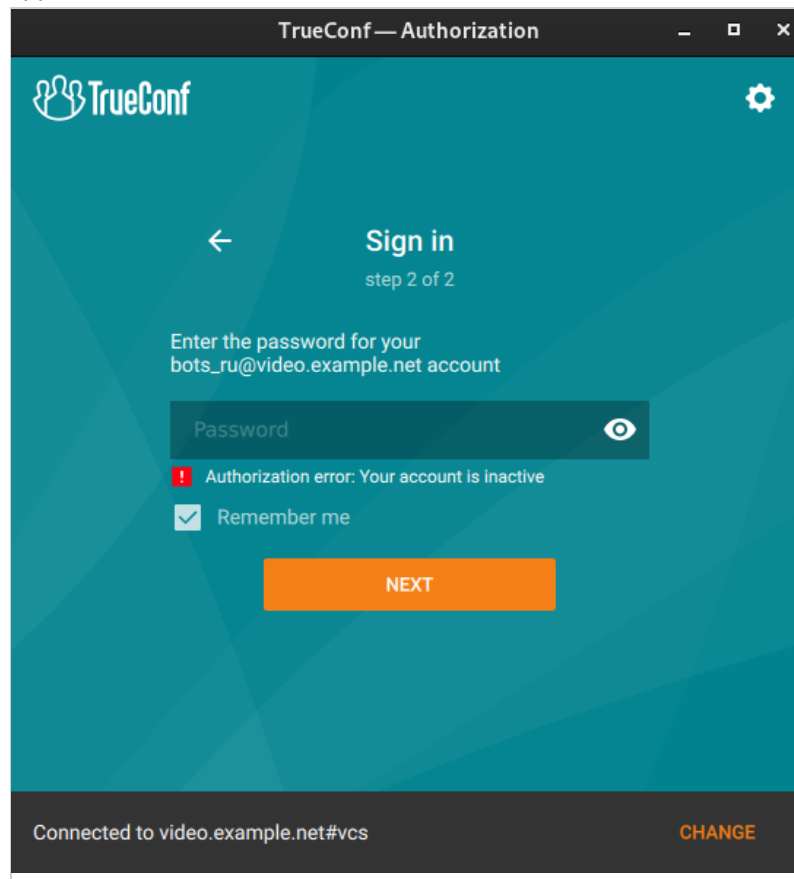
8. User groups. Click the arrow icon to view existing groups on your TrueConf Server instance. To add a user to one or more groups, check the box on the left of each group name.
9. If necessary, you can enter the user's phone numbers. One can call any of these numbers by clicking on it in the [user profile](#) section of TrueConf client application.
10. If SIP telephony is used, you can enter a number for making SIP calls in this field. Then, the corresponding field will be displayed in the [user profile](#) in TrueConf client application. When a user clicks on this number, the call will be started in the format `#sip:<number>` and the number can be specified as `<number>`, `sip:<number>`, or `#sip:<number>`.
11. Save changes, delete account, or return to the list of users.

If a user has entered an incorrect password multiple times in a row (the exact number will be specified in the **Users → Settings** section), the authorization via the web application will be locked for 24 hours. You can enable the access to the application manually by clicking the **Unlock** button on the user profile page:



13.2.1. 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:



13.2.2. Calls and conferences

If you are editing the user account created previously, you will see the **Calls and conferences** section where you

can find the links for accessing:

- 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

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** (selected by default)
 - **Incoming call**
 - **Outgoing call**
 - **Missed call**
 - **Conference.**
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. 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
 - Link to the detailed information about the session in the **Call history** section
 - 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.

13.2.3. 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)	<input checked="" type="checkbox"/> <input type="text" value="1024"/>	<input type="text" value="2048"/>
Outbound bandwidth limit (kbit/s)	<input type="checkbox"/> <input type="text"/>	<input type="text" value="4096"/>

Apply

If bitrate limits are set at the user or group level, the user will not be able to change them in the client application TrueConf, but will see what settings have been set.



User application settings have higher priority than group settings: if you put user restrictions lower than group restrictions, user restrictions will be applied.

13.2.4. User 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.

The screenshot shows the 'Address book' interface. It includes a form to add a user (1) with fields for 'Enter user ID' and 'Display name', and an 'Add' button. Below this, it shows the groups a user belongs to (2), with 'Developers, IT' listed. A search bar (3) is also present. At the bottom, a table (4) lists users with their TrueConf ID and Email.

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.

13.3. 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 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** — this group automatically includes the users who were not explicitly added to any group when [their account was set](#) or in this section as it will be [described below](#).
- **Federated users** — the users who make calls to the users or conferences on your TrueConf Server instance from a [federated server](#).
- **Guest users** — the guests who joined your public conferences (webinars).



It is impossible to rename or delete the default groups.

13.3.1. Editing groups in Registry mode

The screenshot displays the 'Groups' management interface. At the top, there's a 'Group list' section with a 'Group Name' input field and a 'Create' button. Below this is a table with columns for 'Group Name', 'Address Book', and 'Application'. A 'User rights' section on the right contains a grid of icons for various permissions. Numbered callouts 1 through 6 highlight specific UI elements: 1 points to the 'Group list' header, 2 points to the 'User rights' grid, 3 points to the 'Group Name' input field, 4 points to the 'Customize' link in the 'Address Book' column, 5 points to the 'Customize' link in the 'Application' column, 6 points to the 'Delete selected' button, and 7 points to the 'Operators' group row.

1. To add a new group, enter its name and press **Create**.
2. At the group level you can allow or forbid the following features:
 - 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 video calls. However, users can still receive incoming calls.
 - Creating group conferences.
 - Sharing the screen and application windows
 - Ability to permit the remote control of one's desktop
 - Slideshows
 - Sending files in both private and group chats
 - Downloading files in chats. If a user does not have this right, instead of a file, he/she will see the notification indicating that this feature is unavailable.
 - Conference recording in the client application. This feature does not affect the ability to activate video recording when creating a conference in the application scheduler or personal area.
 - Operator rights. Operator right enables a group participant to become a moderator and have access to the [real-time meeting management tool](#) of any conference he or she joins.

These settings allow you to distinguish between different server users.

3. [Edit the name of the group and its members](#) .

4. [Set up address book](#) for group members.



5. [Adjust bandwidth settings](#) for group members.

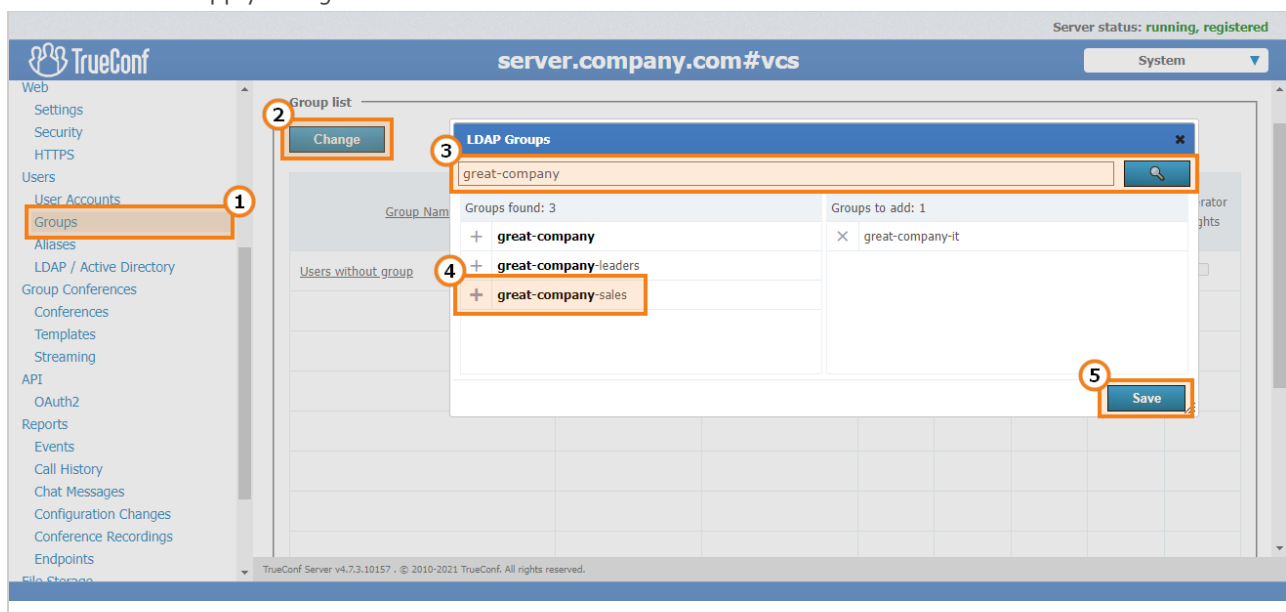
6. To delete one or more groups, check corresponding boxes and click **Delete selected**. Accounts of the group members will not be deleted from your TrueConf Server instance.

13.3.2. Editing Groups in LDAP Mode

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. Open the TrueConf Server control panel and go to **Users → Groups**.
2. Click **Change** above the group list.
3. Enter your search and press . You can type both full group name or a keyword.
4. Click  to add required groups to the list.
5. Press **Save** to apply changes.



For groups imported from LDAP, settings for [user permissions](#) and the [address book](#) are available, just like in Registry mode.

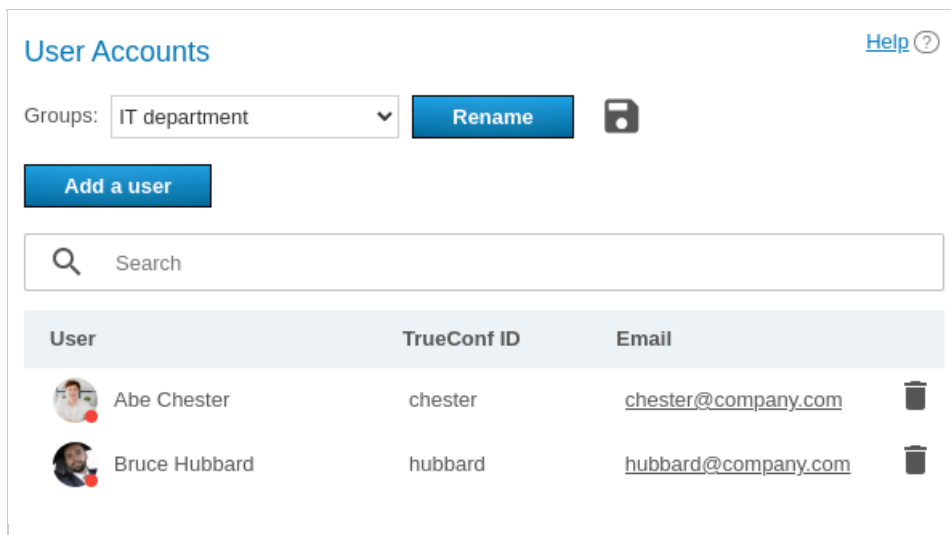
13.3.3. How the restrictions of rights work

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.


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 group **Federated users**) 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.

13.3.4. Editing group's name and its members

Click on the group name from the list to access the **User Accounts** page. Here you can rename the group and edit the list of members using the corresponding buttons:







User Accounts [Help ?](#)

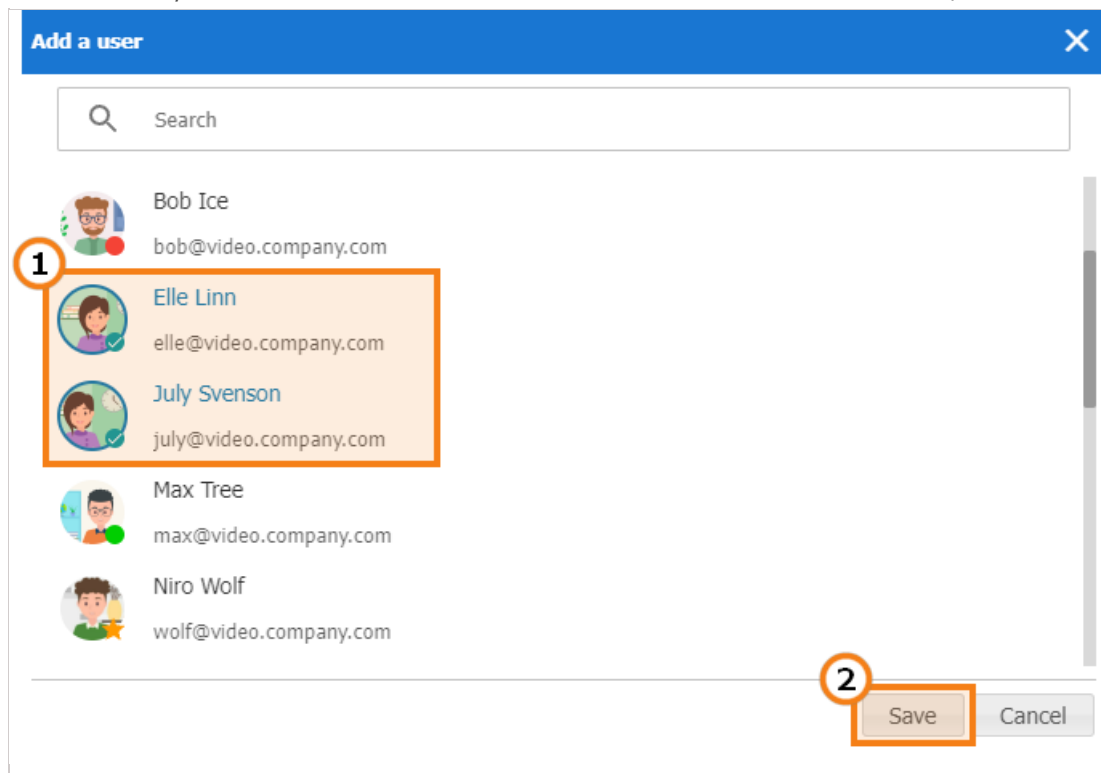
Groups: IT department **Rename** 

Add a user

Search

User	TrueConf ID	Email	
 Abe Chester	chester	chester@company.com	
 Bruce Hubbard	hubbard	hubbard@company.com	






Click the **Add a user** button to complete the list. Select the users you want to add to the chosen group in the window. After that they will be marked with a checkmark. After all users have been selected, click **Save**:



Add a user ×

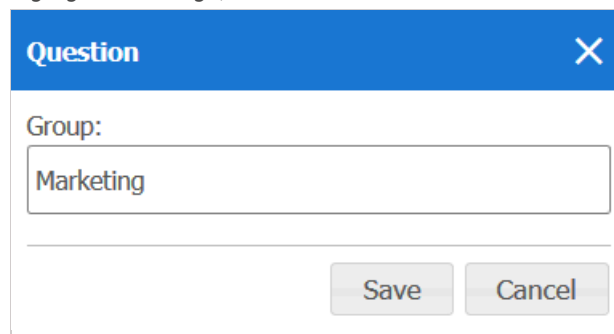
Search

1

-  Bob Ice
bob@video.company.com
-  Elle Linn
elle@video.company.com
-  July Svenson
july@video.company.com
-  Max Tree
max@video.company.com
-  Niro Wolf
wolf@video.company.com

2 **Save** **Cancel**

Click **Rename** to change the group name. Enter the new name and press **Save** (or press **Cancel** if you want to close the window without changing the settings):




Question ×

Group:

Marketing

Save **Cancel**

You can also click the  button to export the user list of a specific group to a CSV file for subsequent [import into the TrueConf Group address book](#).

13.3.5. Setting up address book for users of the group

In the **Address Book** column of each group, click **Customize**. Click on it to edit the address book of this group. Group members can also add new contacts to the address book if they have a corresponding right (to enable it, please check **Address Book Editing** box).

You can add all users belonging to another group at once to the group's address book (i. e. to the address book of each of its members). To that end, use **Define, which users will be shown in the address book of the users in the group**. Please note that automatic addition of users to the address book and manual addition are applied independently of each other.

Address Book for "Developers" [Help ?](#)

Define, which users will be shown in the address book of the users in the group

☐ All users
 ☒ User Groups

Developers ▼

☐ No One

Apply

Address Book of the Group





Add user:

Enter user ID

Display name

Add

Search

User	TrueConf ID	Email	
 Bill Bush	bill	bill@mail.company.com	
 Ann Branson	ann	ann@mail.company.com	
 Alonso Lopez	alonso	alonso@mail.company.com	

You can also manually add users of different types (this process is similar to [adding users to the address book in the user's profile](#)). However, group members cannot delete users themselves, because these contacts are added to the entire group and not to their personal address book.

Group members can search for other TrueConf Server users and add them to their list of contacts on their own (if you have enabled address book editing).

13.3.6. Setting application settings for group users

Click **Customize** in **Application** column to set bandwidth limits for the group users.

Applications settings for "Developers"
[Help ?](#)

Group:
Developers

Application settings

Inbound bandwidth limit (kbit/s)	<input type="checkbox"/>	
Outbound bandwidth limit (kbit/s)	<input checked="" type="checkbox"/>	4096

Apply

13.4. Aliases

13.4.1. Description

Thanks to aliases, you can call TrueConf Server user or any other user who can be called via the server (e.g. SIP, H.323, RTSP or other server users) using a short alias without entering full call string. By adding an alias, you create an extra name for existing user. When calling an alias, your call is redirected to the existing user corresponding to this alias.

This option is very useful for those users who are [making calls to TrueConf Server users from mobile devices](#) using a dialer. You can create digital aliases for server users so that they can be called from mobile devices.

Aliases
[Help ?](#)

Aliases

<input type="checkbox"/>	Alias	User
<input type="checkbox"/>	123	bill@server.company.com
<input checked="" type="checkbox"/>	124	bob@server.company.com
<input type="checkbox"/>		
<input type="checkbox"/>		

Create an alias:

Alias

User

Add

Delete selected

1. An alias may contain numbers and letters. The maximum number of characters is 32. You can update aliases only after restart you have restarted the server.
2. Call string (including username of the server user). The calls to the alias will be forwarded to this user.
3. Press the button to add a new alias to the list.
4. To delete one or more aliases, mark them and click **Delete selected**.



After adding or removing aliases, please restart your server to update the list of aliases.

13.4.2. Use for 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.

13.5. Authentication

In this section you can configure authentication options for the users of your TrueConf Server.

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 methods	State
Trusted Network	Login and password, NTLM SSO	<input checked="" type="checkbox"/>
Internet	Login and password	<input checked="" type="checkbox"/>

Authentication methods

Name	Status	State
Login and password	Enabled	<input checked="" type="checkbox"/>
NTLM SSO	Enabled	<input checked="" type="checkbox"/>
Kerberos SSO	Not configured	<input type="checkbox"/>
AD FS	Not configured	<input type="checkbox"/>

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. Configurable verification methods. If you click on **Kerberos SSO** and **AD FS**, a [configuration pop-up](#) will be displayed. There are no settings for **Login and password** and **NTLM (Single Sign-On)** options; they can be simply activated with switchers on the right.
5. The configuration and work status of each method.
6. Activation of authentication options.



To enable **Kerberos SSO**, **NTLM SSO**, and **AD FS** methods, you have to select and configure [LDAP account storage mode](#).

13.5.1. Access zones settings

Click on the name of a **trusted zone** to open its settings:

The screenshot shows the 'Zone editing' window. It has a title bar with 'Zone editing' and a 'Help' icon. The main content area is divided into sections. The first section is 'Name' with a text input field containing 'Trusted Network', highlighted by a red box and a circled '1'. The second section is 'SUBNET MASKS' with a table of four subnets: '10.0.0.0/8', '192.168.0.0/16', '172.16.0.0/12', and '169.254.0.0/16'. The first row is highlighted by a red box and a circled '2'. Below the table is an 'ADD' button, highlighted by a red box and a circled '3'. The third section is 'AUTHENTICATION METHODS' with four options: 'Login and password' (checked), 'NTLM SSO' (checked), 'Kerberos SSO' (unchecked), and 'AD FS' (unchecked). The 'NTLM SSO' option has a note: 'This authentication method is used for client applications by default'. The 'Kerberos SSO' and 'AD FS' options have a note: 'Not configured. Go to settings'. The entire 'AUTHENTICATION METHODS' section is highlighted by a red box and a circled '4'. At the bottom right are 'CANCEL' and 'SAVE' buttons, with the 'SAVE' button highlighted by a red box and a circled '5'.

1. Changing the zone name, e.g., to "Corporate network".
2. The subnets of this zone. If you click on any entry, you will see a window when one can edit the address or masks of the subnet. Here, you can also delete the subnet.
3. Adding a new subnet.
4. Selection of authentication methods.
5. Don't forget to save changes.

You can specify the name of the **external zone** and configure authentication methods for it.

13.5.2. SSO and AD FS settings

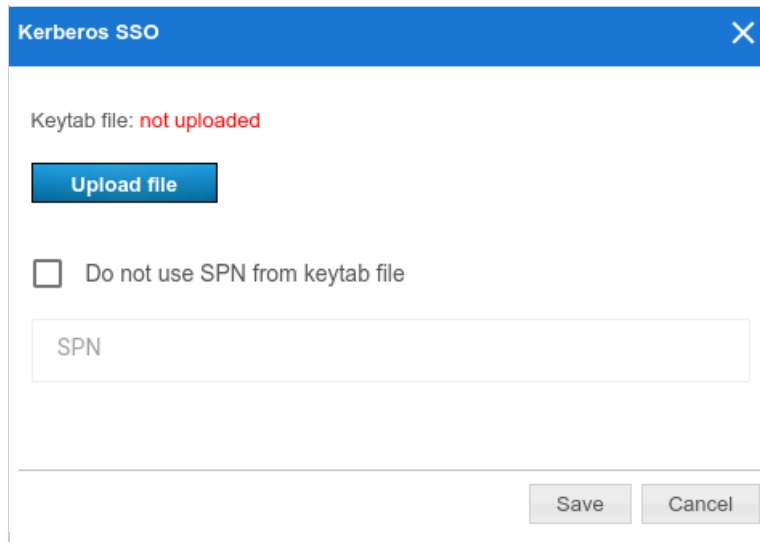
When integrated with an LDAP server, **SSO (Single sign-on)** technology will enable the users of your TrueConf

Server to authorize automatically after logging into the operating system and starting TrueConf client application. For this purpose, one can use one of the two protocols: [Kerberos](#) or [NTLM](#).

i 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** you only need to enable this option in the **State** section; there are no additional settings.

To configure connection via **Kerberos**, click on the **Kerberos SSO** link in the **Authentication methods** section (on the **Authentication** page with the list of security zones):



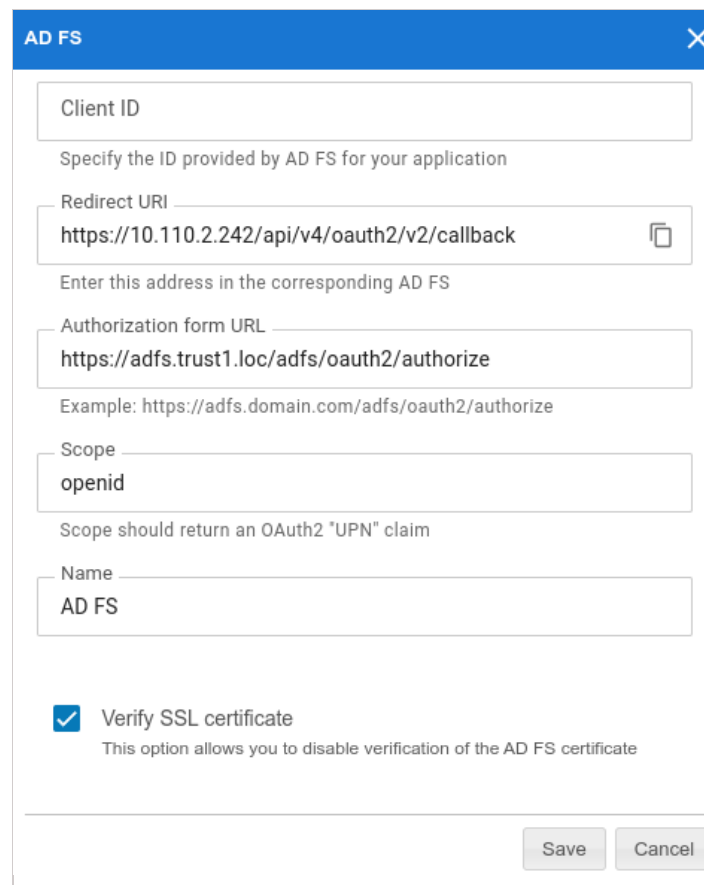
In the pop-up window, select:

- The keytab file that will be used for authentication
- If necessary, click on **More** and specify your own value for **ServicePrincipalName (SPN)** instead of the value saved in the file.

[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.

***** In addition to AD FS, one can use other solutions to implement two-factor authentication, for example, Keycloak.

To configure integration with federation services, click on the **AD FS** link in the **Authentication methods** section and specify the required parameters:



AD FS

Client ID

Specify the ID provided by AD FS for your application

Redirect URI

https://10.110.2.242/api/v4/oauth2/v2/callback

Enter this address in the corresponding AD FS

Authorization form URL

https://adfs.trust1.loc/adfs/oauth2/authorize

Example: https://adfs.domain.com/adfs/oauth2/authorize

Scope

openid

Scope should return an OAuth2 "UPN" claim

Name

AD FS

☒ Verify SSL certificate

This option allows you to disable verification of the AD FS certificate

Save Cancel

1. The identifier (Client ID) of the OAuth application which is configured on the side of AD FS for receiving the access token
2. URL on the side of used for receiving the response from AD FS; it also needs to be specified on the federation service.
3. If you click on **More**, you will be able to change the following parameters (if necessary):
 - **Authorization form URL** which has to be specified on the side of AD FS and used for receiving the access token for a TrueConf Server user during connection
 - Scope
 - The authorization provider name displayed in the list of authorization options on the [page where access zones are configured](#) and in TrueConf client applications when two-factor authorization is used
 - On the side of TrueConf Server, you can also disable the verification of the SSL certificate received from AD FS.

13.6. LDAP / Active Directory

Switching between user data storage modes. TrueConf Server supports two types of data storage: Registry and LDAP. You can switch to any type by pressing **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

13.7. 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.

13.8. 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 user list and user group settings via control panel. By default, configuration settings for LDAP match Microsoft Active Directory. User information is edited using Active Directory management tools.



To learn more about the LDAP protocol and the Microsoft Active Directory service, [read our website](#).

In LDAP mode, user rights correspond to the Active Directory group where users belong. To activate this mode, check **LDAP → Enable** and press **LDAP settings** button at the bottom. LDAP settings window will open:

The screenshot shows the LDAP configuration page with the following elements highlighted by numbered callouts:

- 1**: Server Type dropdown menu (set to Active Directory).
- 2**: Secure connection checkbox.
- 3**: Auto detect / Manual configuration radio buttons.
- 4**: Domain text input field (trust1.loc).
- 5**: Server text input field.
- 6**: Port text input field (389).
- 7**: Authentication dropdown menu (set to NTLM).
- 8**: Name and Password text input fields for authentication.
- 9**: Path (distinguishedName) text input field and Browse button.
- 10**: Apply button and the ++Advanced section toggle.

1. Server type, the following types are supported: **Active Directory**, **OpenLDAP**, **389 Directory Server**. This will determine the default names of attributes that will be parsed by the server from the LDAP directory. It is also possible to select the **Custom** option if you want to specify the attribute name manually. When the server type is selected, open the **Advanced** section and click the **Default** button to switch to the attribute name that corresponds to this type of server. You will see that the attribute name in the **Value** column has changed. If necessary, you can specify the required values and then click the **Apply** button which is also in the **Advanced** section.
2. Connecting to the LDAP server in protected mode (via LDAPS protocol) to ensure secure transfer of user data over the network.
3. LDAP server settings configuration (automatic and manual).
4. 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. The address and port of the LDAP server when manual configuration is used. It is possible to use the global directory for connecting to the directory service. To do it, specify **3268** or ***3269** as the connection port when working via LDAP and LDAPS respectively.
6. Base Distinguished Name is a directory object designed for searching users, e.g. `ou=People,dc=example,dc=com`.
7. TrueConf Server authorization modes on the LDAP server.
8. Authorization parameters on the LDAP server.
9. In this section, you can specify an LDAP group of users who will be allowed to authorize on TrueConf Server, for example, `cn=TC_Users,ou=People,dc=example,dc=com`. It is possible to select a group by clicking on the **Browse** button. To enable this button, you need to fill out the fields required for connection to the LDAP server (in the **Server settings** and **Authentication** blocks) which will enable the **Base DN** field.
10. Additional LDAP parameters. Allow to adjust the parameters to other types of LDAP servers.

Please note that if the server type is changed (for example, from Active Directory to OpenLDAP), the additional LDAP parameters are not automatically reset. To switch to the default parameter values for the new server, open the **Advanced** section and click the **Default** button.

When changing from LDAP mode to Registry mode it is possible to import user data. To do this, choose the Registry mode in the **User storage** tab, tick on **Import User Information** and click on **Switch**.

i User passwords are not imported. After being imported the user accounts are inactive (see [User accounts section](#)).

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, open **Users → Groups**. Click the **Change** button and select corresponding groups in the drop-down list. Read more in our [article on how to set up user groups](#).

***** When groups of users are imported from LDAP, the list will include only the groups that are included in it by default.

i If you have several TrueConf Server 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 Server instance connected to a common LDAP directory using an auto-generated login.

13.8.1. How to upload user accounts from different domains

1. Create a group with the area of application (range) **Domain Local** on the main domain to which TrueConf Server will be connected.
2. 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.
3. Complete the steps 1 and 2 for all domains that will be used for uploading accounts.
4. Specify this group in the field **Path (distinguishedName)** in LDAP settings.
5. Make sure that the parameter **Trust Enabled** in LDAP settings is equal to **1** (default value) in the **Advanced** section.

13.8.2. 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. Click on the **Install Certificate** button in the certificate installation window.
3. Select **Local Machine** in the pop-up where the storage location has to be specified.
4. Select **Place all certificates in the following storage** and click **Browse** in the storage settings window that will be displayed next.
5. In the list of storages, select **Trusted Root Certification Authorities** and click **OK**.
6. To complete configuration, click the **Next** and **Finish** buttons.

Ha Debian:

1. Run the following command in the terminal as the administrator:

```
cp /home/$USER/cert.crt /usr/local/share/ca-certificates && update-ca-certificates
```

sh

where `/home/$USER/cert.crt` is the absolute path to the **.crt** certificate copied to the machine with TrueConf Server.

2. Please reboot the computer on which TrueConf Server is installed.

Ha 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. Please reboot the computer on which TrueConf Server is installed.

13.9. 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:

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.

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).

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. The **Trust Enabled** parameter equals **1** in the **Advanced** section, LDAP settings.
2. The account used for connecting to the domain controller server has the right to read the attribute **member of** from the container **ForeignSecurityPrincipals**.

13.10. Password and account lockout settings

13.10.1. Password requirements

When using the Registry mode, you can specify the minimum password length (from 2 to 64 characters) and specify other requirements (upper and lowercase characters, digits, special characters) for a TrueConf Server user. These parameters will be checked when adding a new user account or changing the password. These requirements will also be applied when a user will be editing the password in the 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

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

E-mail

Display name

First name

Last name

Company

Groups

Password requirements **x**

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

13.10.2. Automatic logout

In this 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** (6 hours);
- **Maximum number of failed login attempts** = **5**;
- **Reset account lockout counter after** = **00:10** (10 minutes).

Then, if a user makes 5 unsuccessful authorization attempts with the login (TrueConf ID) existing on the server and the time difference between these attempts will be less than 10 minutes, the account will be locked for 6 hours. And if after any of the attempts (for example, the 4th) there will be 10 minutes, then the counter will count again starting from one.

14. Group conferences and streams

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.

* In TrueConf Server Free the number of group conferences that can be held at the same time is restricted. To learn more, go to the [web page of this solution](#).

14.1. Conference list

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
- 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. It includes a table of conferences and a detailed view on the right. Numbered callouts indicate the following elements:

- 1**: 'Create' button
- 2**: Filter dropdowns (Topic / CID, Owner, Participant, All modes, All types, All sources)
- 3**: 'CID' column header
- 4**: 'Information' tab
- 5**: 'Participants(0/7)' link
- 6**: 'Available options' link
- 7**: 'Launch' button
- 8**: 'Go to the conference page' button
- 9**: 'Edit' button
- 10**: 'View history' button
- 11**: 'Delete' button

Topic ↑	Start time	Owner	Mode	Type	CID
Brainstorm	Without sch...	Amanda W...	All on screen	🔒	lc13662477...
Meeting	25.08.2023 ...	Jane Flowers	Role-based	🔒	lc1meeting
Webinar	29.08.2023 ...	Abe Chester	Role-based	🌐	lc10699653...

Meeting Details:

- Conference ID: lc1meeting
- 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
- Show more
- Type and Mode: Private, Role-based 6x290
- Recording: Scheduled
- Meeting location: Main office
- Source: TrueConf
- Integration: Available options
- Hide conference details

Conference Manager:

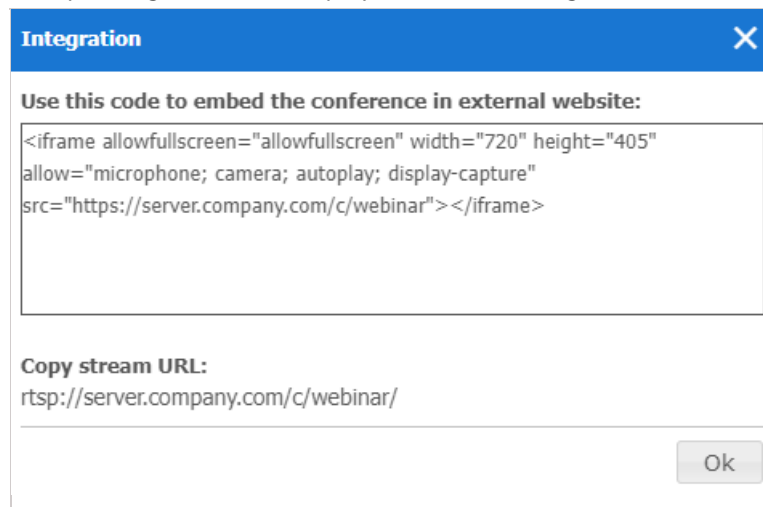
- Launch
- Go to the conference page
- Edit
- View history
- Delete

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 video conference](#).
2. Filter the list by the name (or ID) of the required conference, by the owner of this meeting, one of its participants, access type, and source.
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 page, email reminders (if added), location (if specified), mode, type of launch, tool used to create this event (TrueConf or email plugin), and if this conference will be video recorded.
5. Open the list of invited participants.

- 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:

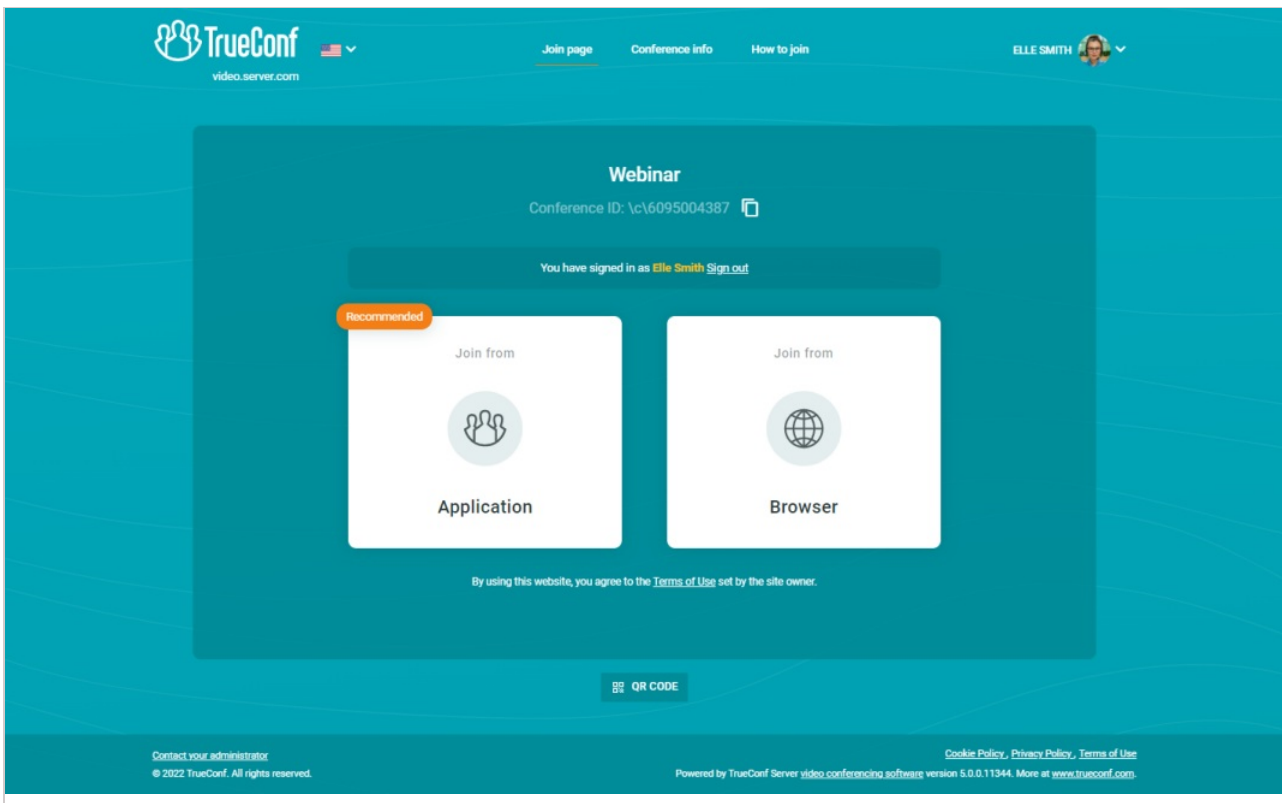


- Start the conference manually. Before the start you will be offered to invite all the participants to the conference or select particular users. At conference forced start, only online users will be invited to the conference. Email invitations will not be sent out.
- Go to the [conference page](#).
- 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](#).
- View the previous sessions (history) of the selected conference in the [Call History section](#).
- Remove selected conference.

14.2. 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](#).



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.

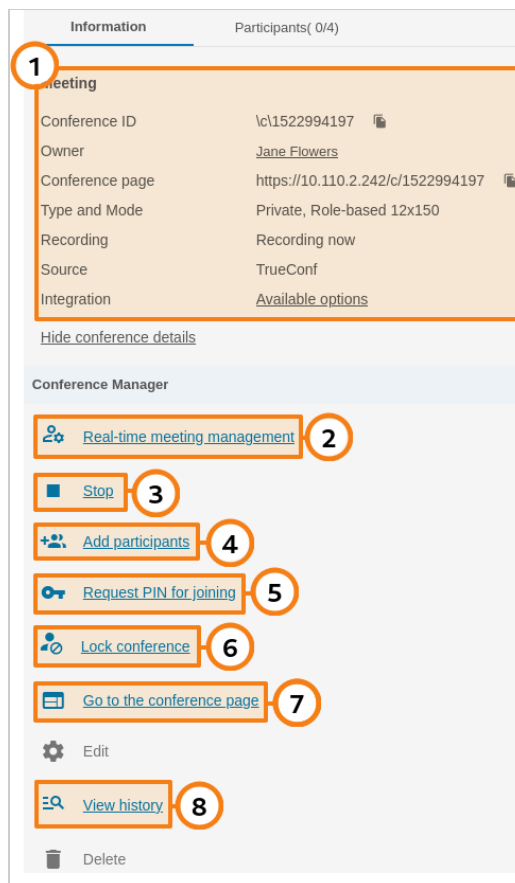
To learn more about connection options, check [our article](#).

14.3. How to configure an ongoing meeting

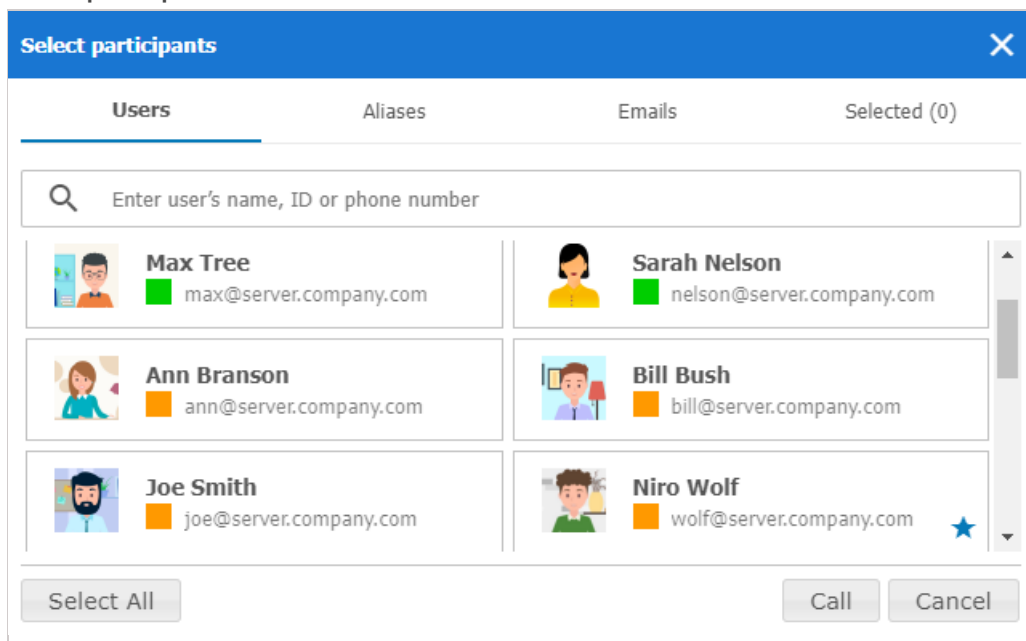
When selecting an ongoing conference, the administrator can view information about it or change some of its parameters (e.g., the layout or PIN code). Standard editing and deletion options will be unavailable.

14.3.1. "Information" tab

Display conference information and the control buttons:



1. Basic meeting information and options for [integration with third-party websites](#).
2. Proceed to [real-time meeting manager](#).
3. Stop the meeting for all participants.
4. Click on the **Add participants** to select new users:



To add participants to a conference, select the users in the **Users** tab. You can select all server users at once by clicking on the **Select All** button. In the **Aliases** and **Emails** tabs, you can add a participant by his or her [alias](#) and [send](#) the invitation, specifying the email and the name displayed in the meeting. The resulting list is displayed in the **Selected()** tab. After the list is formed, click the **Call** button at the bottom of the window.

5. Changing or disabling PIN needed for joining a conference. If secure access is disabled, you can activate it 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.

i Each time when a conference ends, its access status is switched to **unlocked** which is the default value.

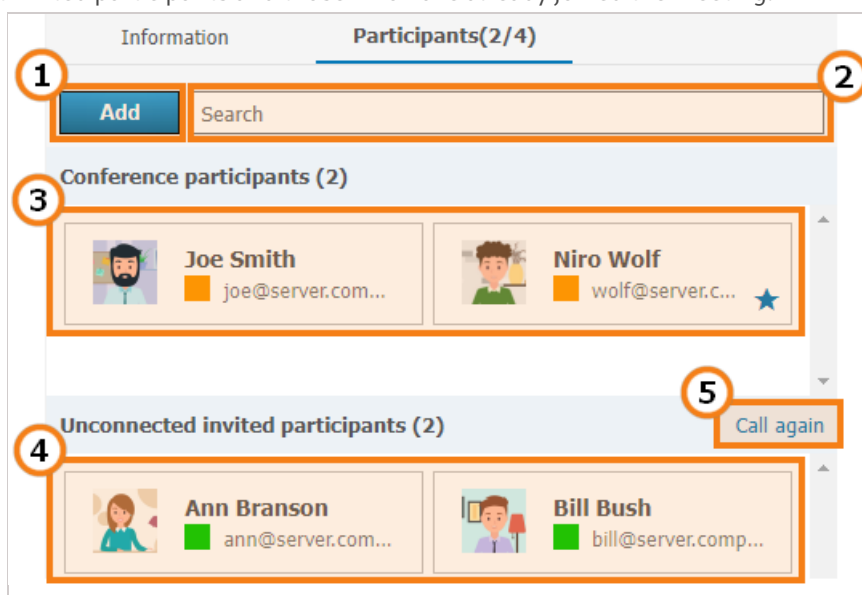
7. Go to the [conference page](#).

***** It is also possible to set a PIN for a conference or lock it in the real-time meeting management tool.

8. View the previous sessions (history) of the selected conference in the [Call History section](#).

14.3.2. "Participants" tab

Information about invited participants and those who have already joined the meeting:



1. Adding [new participants](#) to a conference.
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 non-connected participants to a meeting, click the **Call again** link. Then, click the **Invite** button in the opened window.

14.4. Creating a new conference

Click on the **Create** button in the **Conference List** menu to select a conferencing type:

You can quickly create a meeting by selecting one of the [previously saved templates](#).

Otherwise, specify the access type for a new conference. You will not be able to change the type after the conference has been created (for example, a private event cannot be transformed into a webinar):

- **Private** conference (selected by default) is a conference that can be joined only by the users registered on TrueConf Server and third-party SIP/H.323 or RTSP devices (if you are making a call directly by the conference ID or if the device is invited as a conference participant). Unauthorized users cannot join a private conference.
- **Public** meetings can be [joined by external users \(guests\)](#) who do not have a user account on TrueConf Server.

* The maximum number of guests in a webinar is determined by your license (and by overall restrictions depending on a specific conference mode). TrueConf Server Free has its own [restrictions on the number of guests](#).

Check the **Language interpretation mode** box if you want to hold a multi-language meeting supported by simultaneous interpreters. The interpretation mode must be activated in advance; it cannot be configured when the conference has already been created. The feature is **available only in moderated role-based conferences** so, this conference mode will be automatically selected. When a conference with language interpretation is recorded, several audio tracks will be created: the main track and separate tracks, one for each language into which the presentation was translated. For more details on how to configure simultaneous interpretation, read the [description of the corresponding tab](#).

Click **Continue** to proceed to the meeting settings.

* **Learn more about webinars in our articles and videos:**

- [What is a webinar?](#)
- [Tips for secure webinars](#)
- [How to organize webinars](#)

Apart from the conference settings listed below, it is possible to add a background and/or watermark to the conference layout. They can be selected for all events in the **Gateways → Transcoding → Visual settings** section.

14.4.1. "General" tab

This tab contains the settings required for creating a meeting:

The screenshot shows the 'Conference' configuration window with the 'General' tab selected. The interface includes a 'Conference name' input field, an 'OWNER' section with a 'SELECT' button, and a 'MODE' section with four radio button options: 'Smart meeting', 'Moderated role-based', 'All on screen', and 'Video lecture'. Each mode option includes a brief description and a resolution dropdown menu. The 'Smart meeting' option is currently selected and highlighted with a blue border and a circled '3'.

1. Conference Name Field, e.g. "Marketing Department Meeting".
2. Select the [conference owner](#).

* When scheduling a conference, the administrator assigns the conference owner (who automatically becomes moderator) and other moderators. Other [roles](#) will be given by users in a conference.

3. Select the [conference mode](#): all on screen, smart meeting, moderated role-based conference, and video lecture.

The mechanism determining how the layout will be filled in [smart meeting](#) mode with different types of connection is fully described in the [documentation for TrueConf client application](#).

Specify the number of [presenters](#) if a moderated role-based conference or smart meeting is selected.

* The maximum number of participants in a [moderated role-based conference](#) and smart meeting depends on the type of your license. The number of participants can reach up to **1500** (or **1600** if you are using [UDP Multicast](#)). The maximum number of speakers in a smart meeting or moderated role-based conference is **49**.

4. Indicate the [conference type](#): scheduled meeting or a virtual room.

5. Setting time and regular schedule for the scheduled meeting.

6. Configure the display of notifications that the conference is about to end (enabled by default). Available only for a scheduled conference. All moderators will see the notifications, not just the owner.

7. Allow moderators to extend the duration of the event. This action will be available in the personal area and the real-time meeting management of client applications. Besides, one can also click the button in the pop-up notification about the impending conference ending (if this option was activated).

8. Set up email reminders that will be sent to event participants. This option requires the corresponding feature to be enabled in [SMTP settings](#) beforehand. You can add up to 4 reminders for a single conference by clicking the **Settings** button. To align your notification settings with global ones, click the button **Use administrator specified settings**.



Sometimes when editing a conference created previously, you will see the reminders that were not added by you or the conference owner. This issue may occur due to the activation of the global notifications settings in the [SMTP section](#) at the moment when the conference had already been created.

9. If necessary, you can save the conference settings as a template to create future conferences with the same parameters in just one click.

14.4.2. "Participants" tab

This 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 an SIP/H.323 or RTSP device in the search field on the **Contacts** tab and click **Select ID** to make it a meeting participant.

Adding email notification recipients

i 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 the **Name** and **Email** fields with the participant's personal details.
3. Click **Select** to add the user to the guest list.

After selecting all users, click **Add** to include users to the list of meeting participants.

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)**

How to Make a Participant a Moderator

1. Select a user from the list of added conference participants and click three dot button.
2. Press **Assign as a moderator**.

Conference [Help ?](#)


General **Participants(4)** Layout Media Advanced

Number: 4 / 160

Search

- Abe Chester**
chester@video.example.com
- Alice Campbell**
campbell@video.example.com
- Albert Moore**
moore@video.ex...
- Ana Bai**
baros@video.example.com

Assign as a moderator

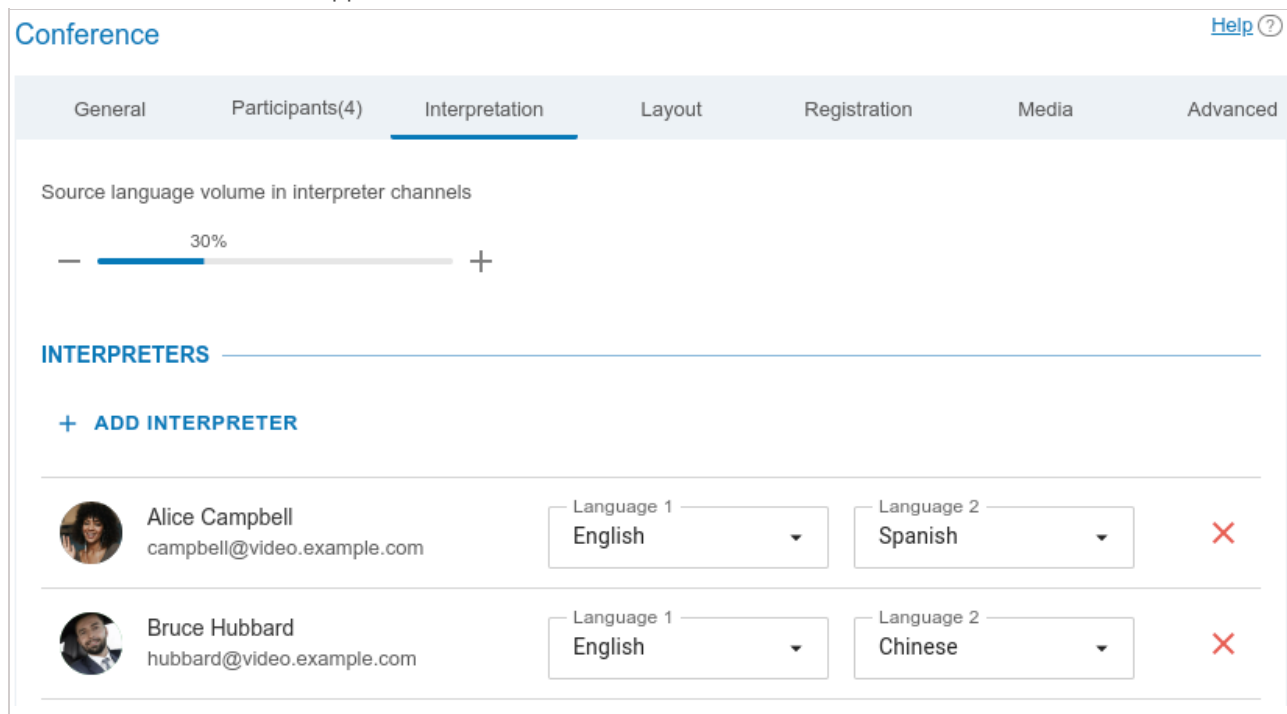
The participant appointed as a moderator is marked with a star icon: .

14.4.3. "Interpretation" Tab

i This tab will be available only if simultaneous interpretation mode was enabled when [the conference was created](#).

TrueConf Server allows hosting conferences with simultaneous interpreters. This enables full participation in the event for users from different language groups, ensuring they don't miss any important information from the speakers. Each participant can select the language in which to listen to the speaker's presentation [in the client application](#) or in the browser (depending on their connection method). The number of interpreters is limited only by the number of participants, excluding webinar guests (see below).

Simultaneous interpreters are selected among the invited participants of a conference. Just click the **Add interpreter** button and choose which language they will be translating from and to. In the example below, the pair **English - Spanish** is selected. During the event, the interpreter will be able to change the direction of translation in the TrueConf application:



Conference [Help ?](#)



General Participants(4) **Interpretation** Layout Registration Media Advanced

Source language volume in interpreter channels

— 30% — +

INTERPRETERS

+ **ADD INTERPRETER**

	Alice Campbell campbell@video.example.com	Language 1 English	Language 2 Spanish	×
	Bruce Hubbard hubbard@video.example.com	Language 1 English	Language 2 Chinese	×

As a simultaneous interpreter, you can add a user from your TrueConf Server as well as from a [federated video conferencing server](#). Guests of a public conference cannot be assigned the role of interpreter, whether they were manually added during planning or self-registered when registration is enabled.

An interpreter cannot be added to the video layout either in the conference settings or in the real-time meeting management when the event has already started. In this way, you can select multiple translators, including the cases when two translators work with the same language pair (for example, so that one can rest while the other works with the same languages).

At any given time, only one person can translate from one language to another. For instance, only one participant will be able to translate from English to Hindi; however, the second interpreter will be able to 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](#).

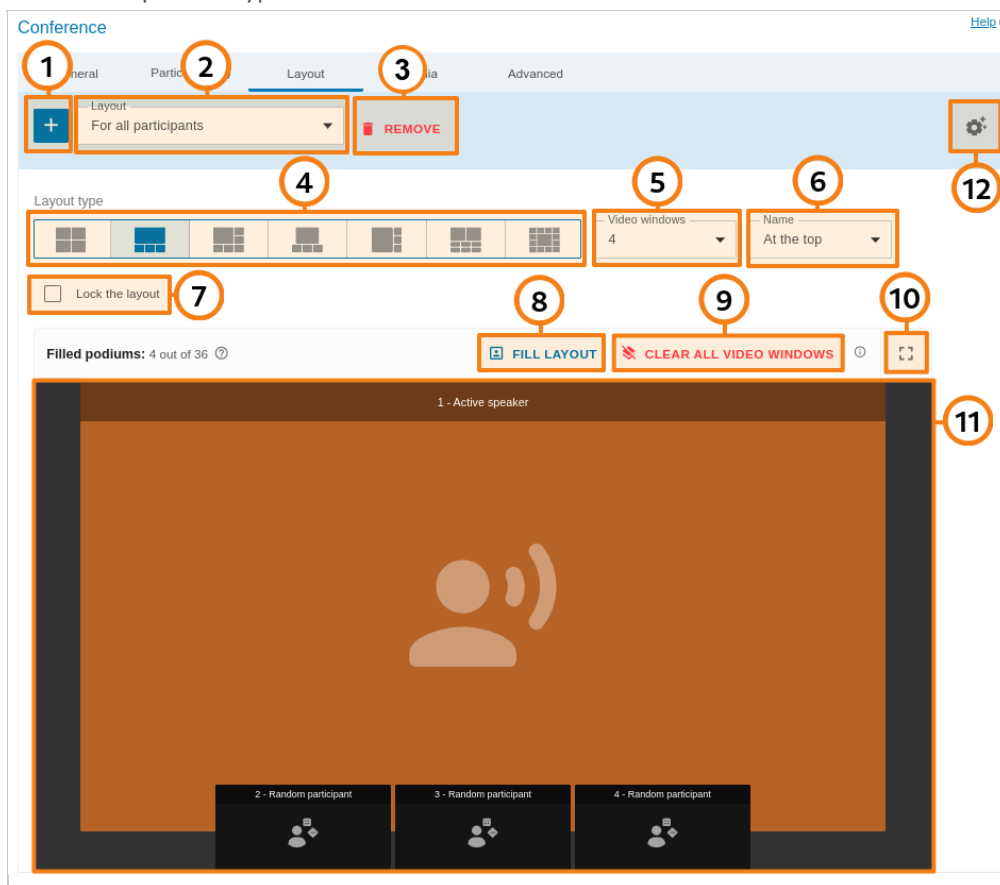
14.4.4. "Layout" tab

i Apart from the settings specified in the **Layout** tab, it is possible to add a background and/or watermark. They can be selected for all events in the **Gateways → Transcoding → Visual settings** section.

Apart from the conference settings listed below, a background and/or watermark can be added to the conference layout as a result of the general settings specified for all events in the **Gateways → Transcoding → Visual settings** section.

On this tab, you can set the **video layout** (arrangement of participants' video windows). Learn more about the types of video windows and their features in the [user documentation for TrueConf Server](#).

Layout customization is not available in **video lecture** mode. In **smart meeting** mode, there must be at least 2 windows of the "active speaker" type.



1. Add a new layout.
2. Select the conference layout that you want to edit (it must be added in advance): a common layout (for all participants), an individual layout for a specific participant (including a separate SIP/H.323 endpoint), or a common layout for [SIP/H.323 devices](#) and browsers (WebRTC).
3. Remove unnecessary layout.
4. Select the position of video windows in the layout.
5. Select the number of participants' video windows in a layout.
6. Select the location of a user display name in a video window.
7. Forbid conference participants from changing layouts.
8. You can auto-fill the participants in video windows.
9. Clear layout.
10. Go to the layout preview in full screen mode.
11. Edit the conference layout. You can move a participant's video window and prioritize it (enlarge) by double-clicking. When clicking on any video window, you can choose its type: **Fixed**, **Random**, **Time-based shuffling**,

Active speaker, Content.

- Go to the menu where the time-based alteration (rotation) of participants can be configured. These settings apply to all video windows of the **Time-based shuffling** type in all layouts created for this conference. You can select the order of displaying participants who were not added to the layout, type of rotation, and the frequency at which participants will be rotated:

Shuffling settings

Shuffling order

From 1 to 36

From 36 to 1

Participants get shuffled from smaller to larger slot numbers

Shuffling type

Replace

Move

1

2

3

4

5

6

Shuffling interval (sec)

30

CANCEL

APPLY

14.4.5. "Media" Tab

On this tab you can set limits on the quality of video streams for different destinations:

- in the **Limits for participants** section — for streams coming to the server from participants of all connection types
- In the **Transcoding** section — for streams coming from the server via third-party protocols.

You can to set media quality parameters of the current conference for **incoming** to the server video streams from all participants in all conferences: client applications, participants joining from browsers via WebRTC, and connections via SIP/H.323/RTSP protocols. To do this,, enable the checkbox **Limits for participants → Use custom settings** and select the required values in the dropdown lists. The framerate limit on content sharing applies if a participant is sharing content in his/her video window, but not in the secondary stream. So, there is one video quality limit set for a participant's window. However, you can specify different frame rates depending on whether the speaker or content is being displayed at the moment.



The resolution limitation for SIP/H.323/RTSP will be applied only when 720p and below is specified. To get 1080p stream from terminals and RTSP you can use experimental settings, if you need it [contact support](#).

Settings in the **Transcoding** section are almost identical to the settings in the [Gateways → Transcoding](#) section, except for the GPU acceleration option (which is configured once for the entire video conferencing server). Enable the checkbox **Use custom settings** to override resolution settings at the conference level independently for each direction: SIP/H.323 endpoints, WebRTC connections, recording, and streaming. The frame rate is set globally. Additional layout settings are specified below. They are activated if layouts for SIP/H.323/WebRTC participants are not defined during [conference scheduling](#) or in the [real-time meeting management](#) section.

14.4.6. "Advanced" tab

If necessary, you can set up additional conference settings.

14.4.6.1. Access settings and participant management


Set the ID and security parameters for the conference:

1. Enter a custom conference join URL to make it easier for participants to join.
2. Enable the use of PIN to join the conference. PIN boosts your meeting security and protects your conference from third-party access (even if a third party has a conference join URL in case you organize a webinar). PIN will be generated automatically upon checking the box. However, you can always change the PIN in the field below. PIN protection will be unavailable if you allow users to sign up for a public conference (webinar).



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@<trueconf_server>:<port>
```

3. Manually set your PIN or refresh it using the  button.
4. Allow users to join the conference without invitation (for internal conferences only).
5. Activate the [waiting room](#) for the event. You will be able to select which participants should be directed to this room. This list will be slightly different 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)** – all participants *except the owner and moderators* will be moved to the waiting room (this includes the participants who signed up for the event)
- **Uninvited participants and guests** (selected by default) – the following participants will be *moved* to 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 (if they did not sign up for the event) and users from a federated server, who were **not invited in advance**, will be directed to the waiting room.
- **Guests only** – only guests, if they did not sign up for the event, will be directed to the waiting room.

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.**

6. Select if it is necessary to automatically turn off participants' microphone and camera when they join the conference. If necessary, you can disable audio remarks (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.

14.4.6.2. Recording and streaming

Recording and streaming of the event can be activated below:

RECORDING

☒ Enable conference recording

STREAMING

☒ Enable streaming

YT

1. You can activate conference recording (check the description of the **Recordings** section). If this feature is enabled, the corresponding text hint will be displayed on the **event web page**, and the owner will be able to manage the recording (pause and resume) on the fly during the conference. All participants (including those, who join from SIP/H.323 endpoints and from a browser) will see that the event is being recorded, but you need to activate the indicator in the **Recordings** section.
2. Below you can enable conference streaming. To do it, select a streaming template in the dropdown list (read the description in the **Streaming** section).



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.

14.4.6.3. 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. If the conference will be joined only by SIP/H.323/WebRTC/RTSP participants, you can activate MCU mode. In this case, the server will optimize stream processing for gateway connections, and the selection of connection methods will be unavailable. The conference can be joined **only** from an SIP/H.323 endpoint or from a browser. It will also be possible to connect an RTSP camera. Please note that if you activate MCU mode and then uncheck this checkbox, the list of available connection methods will not return to the old state. That is, the checkboxes for client applications and QR code will have to be checked manually.
3. If necessary, you can enable UDP Multicast mode. To learn more about this mode, check the [description of extensions](#). This will enable you to increase the number of participants (up to 1600 in role-based conference modes). In this case, there will be no dependence on the number of podiums. For example, you can create a moderated role-based conference or smart meeting with up to 1600 attendees and 36 podiums for speakers. However, there will be multiple restrictions described 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**.

14.4.6.4. Sending invitations and conference description

Configure settings for sending email invitations and specify the additional event description:

INVITATIONS

☒ Send email invitations to conference participants

MEETING LOCATION

DESCRIPTION

B **I** **U** Normal

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 option is disabled regardless of the conference settings configured earlier. This is specifically designed to prevent the invitations from being mistakenly resent when editing an event. If you need to reactivate conference invitations (e.g., when adding participants), please manually activate the **Send email invitations to conference participants** checkbox.

2. Specify the conference location. The location will be displayed in the **Information** tab on the [conference page](#) and in the [list of conferences](#)).
3. Add guide text to the scheduled event (e.g. presentation description or event program). This text will be displayed on the conference page.

14.4.7. Restrictions for webinars

If you check the **Public conference (webinar)** box when [creating the conference](#), this tab will also contain permission settings for guest users:

1. Permission settings for guest users
2. This parameter is used to restrict the number of guests in the selected webinar (by default they can join the event up until the moment when the licence limit for guest connections is reached). This 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):

Conference [Help ?](#)

General Participants(1) Layout Registration **Advanced**

GUEST PERMISSIONS

- ☒ Allow to send messages
- ☒ Allow to send audio
- ☒ Allow to send video
- ☒ Limit the number of guests

Number (from 1 to 50)
30



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.

14.4.8. "Registration" tab

The **Registration** tab will be displayed if a public conference (webinar) is created. Here, you can configure registration settings for conference participants who want to sign up for your online event (this option will be available only for a scheduled conference):

Conference [Help](#)

General Participants(1) Layout **Registration** Advanced

☒ Enable conference registration
All users, except invited participants, will be able to join the conference only after registration

CLOSE REGISTRATION

- ☐ Without limitation
- ☐ At conference start
- ☐ At conference end
- ☒ Custom date and time

Select start date and time: 26.05.2022 13:00
 Select end date and time: 26.05.2022 21:00

☒ Close registration when the maximum number of participants is reached (depends on the selected webinar mode)

☐ Allow authorized users to join without registration

REGISTRATION FORM SETTINGS

Select, add, and arrange input fields.
You will not be able to edit the form once the conference is created

Field title	Required field
Email	<input checked="" type="checkbox"/>
Name	<input checked="" type="checkbox"/>
Job position	<input checked="" type="checkbox"/>
Phone number	<input type="checkbox"/>

SETTINGS

1. Enable registration (disabled by default)
2. Specify the time when the registration will be closed:
 - **Without limitation** — available only for a recurring conference (registration for such an event will be constantly open)

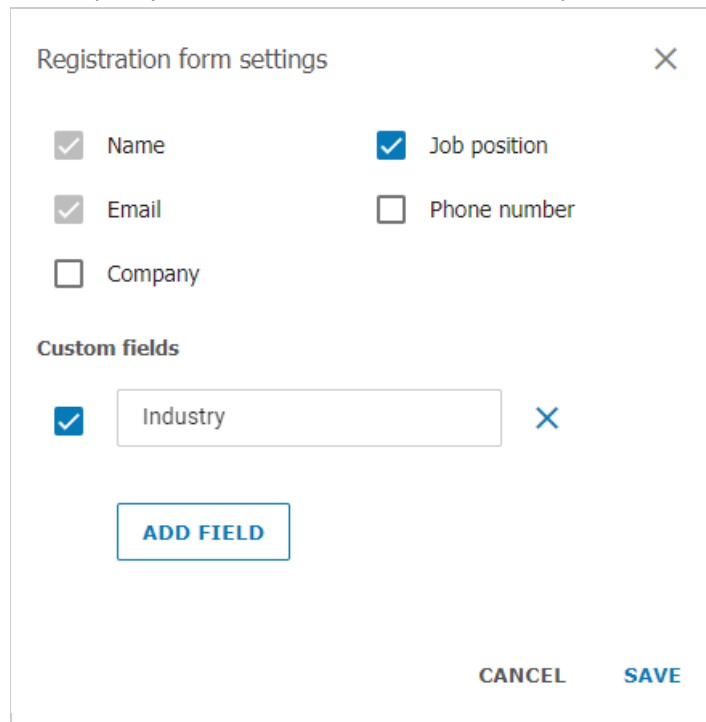
- **At conference start** — the registration will be closed right after the webinar start
- **At conference end** — the registration will be available up until the conference end
- **Custom date and time** — set a custom period during which the registration will be open.

3. Automatically close the webinar registration when the maximum number of participants (depends on the conference mode) is reached.

4. Allow any authorized user to join the conference after its start. In this case, any user registered on your server can sign in on the conference page and add oneself to the list of invited participants by clicking on 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.

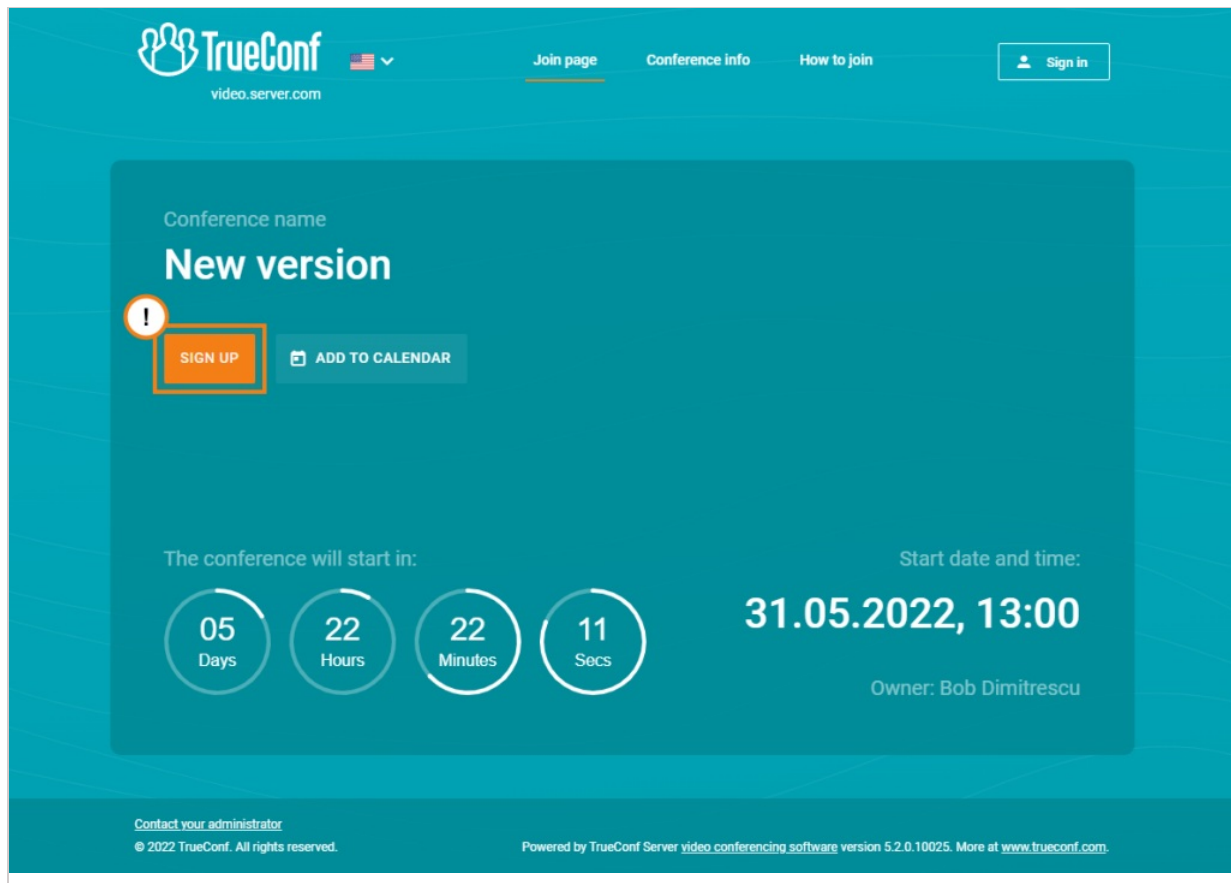
6. You can select the input fields that should be displayed during registration only when creating a conference. Click on the **Add field** button to specify both standard and custom fields (up to 10):



The image shows a 'Registration form settings' dialog box. It has a title bar with a close button (X). Inside, there are two sections: 'Standard fields' and 'Custom fields'. Under 'Standard fields', there are checkboxes for 'Name', 'Email', 'Company', 'Job position', and 'Phone number'. 'Name', 'Email', and 'Job position' are checked. Under 'Custom fields', there is a list of fields, each with a checkbox and a text input field. The first field is 'Industry', which is checked. There is an 'ADD FIELD' button below the custom fields list. At the bottom right, there are 'CANCEL' and 'SAVE' buttons.

Registration form settings	
<input checked="" type="checkbox"/> Name	<input checked="" type="checkbox"/> Job position
<input checked="" type="checkbox"/> Email	<input type="checkbox"/> Phone number
<input type="checkbox"/> Company	
Custom fields	
<input checked="" type="checkbox"/>	Industry
<input type="button" value="ADD FIELD"/>	
<input type="button" value="CANCEL"/> <input type="button" value="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...

14.5. 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
- Parameters from the **Additional** tab (except conference ID)
- 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](#).

The screenshot shows the 'Template list' interface. At the top, there is a 'Create a template' button (callout 1) and a search bar. Below is a table with columns: Topic, Owner, Mode, and Type. The table lists three templates: 'Meeting Template' (Administrator, Role-based, Lock icon), 'Sales' (Ann Branson, All on screen, Lock icon), and 'Webinar' (Administrator, Video lecture, Globe icon). To the right of the table, there is a sidebar with 'Information' and 'Participants(1)' tabs. Under 'Information', details for the 'Sales' template are shown, including Owner (Ann Branson), Type and Mode (Private, All on screen 49x49), Creation time (17.11.2021 14:07:47), and Edition time (17.11.2021 14:07:47). Below this is the 'Template Manager' section with three buttons: '+ Create a conference' (callout 2), 'Edit' (callout 3), and 'Delete' (callout 4).


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.

14.6. Streaming

In this section, you can create and set streaming configurations used [for setting up a conference](#).


Click the **Add a configuration** button to create the configuration. In the window that appears, select your streaming type:

Streaming

CDNvideo Cloud Streaming


The service for content delivery and streaming management. We will automatically create an account and set up everything for you. Please note that streaming service is provided according to the terms of use and plans of CDNvideo service.

Automatic Setup
[Or sign in if you already have an account](#)

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 preset

Manual Configuration

If you are not afraid of RTSP Push or RTSP Pull abbreviations, then follow this way. The whole streaming configuration process is in your hands.

Configure

14.6.1. Streaming through CDNvideo cloud service

Click on **Automatic Setup** to create a new account at CDN video service. To continue please make sure that a PC with installed TrueConf Server on it is connected to the Internet:

Create a new configuration

Streaming server:

CDNvideo



1
[Or sign in if you already have an account](#)

2
This email is used to create CDNvideo service account.

admin@mail.company.com

3
☒ By clicking on the "Create" button, you agree to [Pricing and Terms of Service](#)

4

← Back

Create

1. If you already have a CDNvideo account, click on this link to enter your username and password.
2. Email address that will be used to create a new CDNvideo account. TrueConf Server administrator email is used by default.
3. By creating a CDNvideo account you agree with CDNvideo terms of use.
4. Save current streaming configuration.

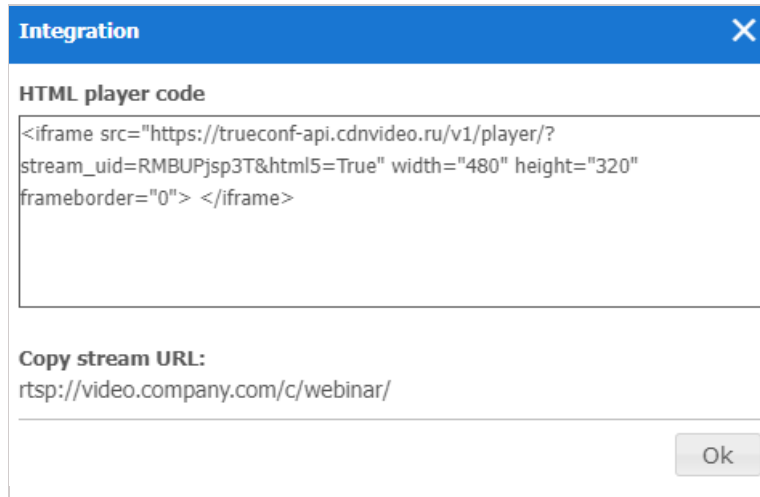
How to connect to CDNvideo streaming

Conference streaming is available on any intranet or Internet HTML page with the CDNvideo video player widget embedded on it. The streaming will start automatically when participants join the conference or, in case it is a

moderated role-based conference, when the first participant takes the podium. Widget code is unique and is set up to stream only the current conference.

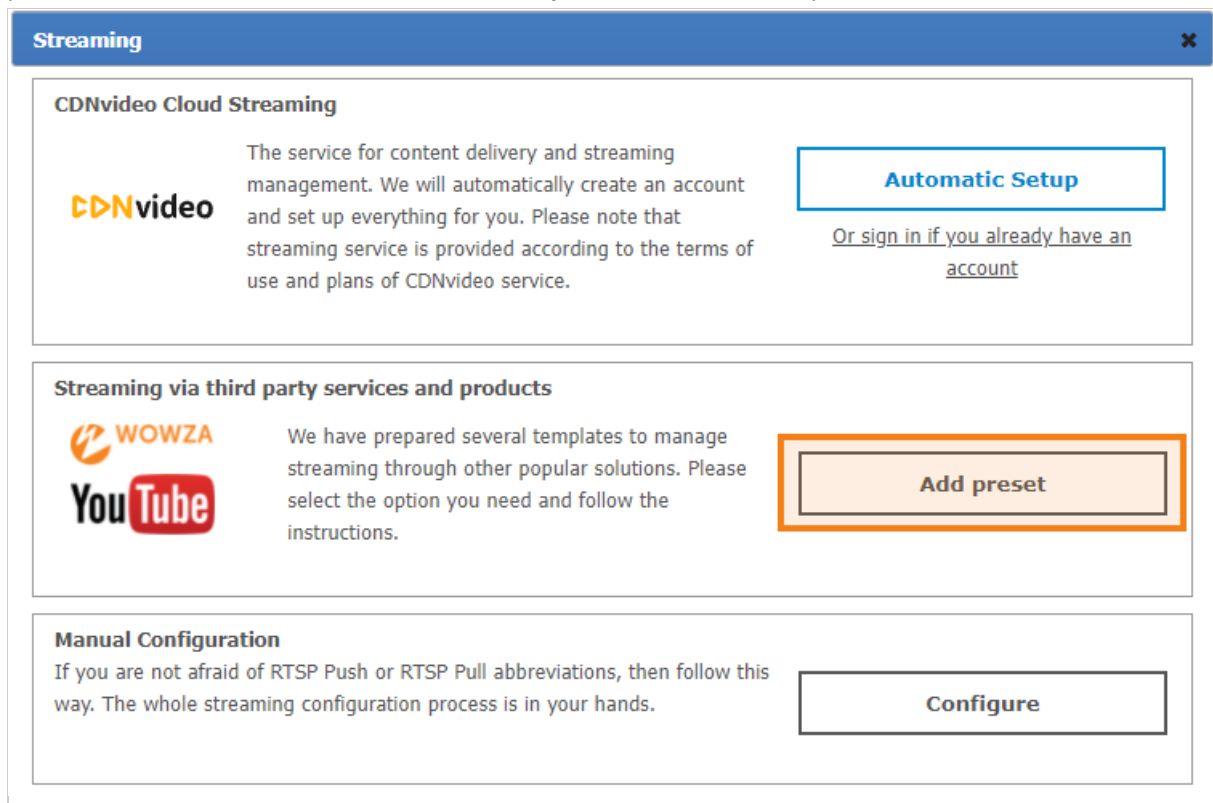
To get the CDNvideo video player code:

1. Go to the [conference list page](#).
2. Select a conference pre-configured for streaming.
3. Click the link **Display conference details** in the side menu of the page.
4. Follow the link next to **Integration**.
5. Copy the HTML code of the video player widget.



14.6.2. Streaming via third-party services and products

This section includes ready-to-use templates for popular streaming services and products, designed to work in corporate networks and via the Internet. Press **Add preset** to choose a template to start with:



In the configuration window select a required streaming service. Streaming service settings are listed below.

14.6.3. Wowza Streaming Engine

To stream video to [Wowza Streaming Engine](#), specify the following parameters:


1. Configuration name displayed in streaming configuration list on the conference edit page.
2. Address of the Wowza Streaming Engine.
3. Wowza Streaming Engine accepts connections on this port (e.g. 1935 or 1940).
4. Read the description of this field in [Wowza Streaming Engine documentation](#).
5. Check **Authentication** to enter username and password to access Wowza Streaming Engine if required.
6. This section includes additional settings for current streaming configuration (see [Advanced streaming settings](#) in present user's guide).
7. Save current streaming configuration.

14.6.4. Wowza Streaming Cloud

The following settings will be helpful when streaming a conference to Wowza Streaming Cloud:

Create a new configuration [X]

Streaming server:

Wowza Streaming Cloud [v]  [Follow our guide](#)

This streaming template can be applied only for one of the conferences running simultaneously.

2 Template Name: []

3 Primary Server:

[]

Host Port: [] Stream Name: []

☐ Authentication

4 [Show advanced settings](#)

← Back **5** Create

1. Click to read our detailed manual on [how to configure conference streaming via Wowza Streaming Cloud](#) .
2. Configuration name displayed in streaming configuration list on the conference edit page.
3. Streaming settings that you received on the Wowza Streaming Cloud service when you created the streaming.
4. This section includes additional settings for current streaming configuration (see [Advanced streaming settings](#) in present user's guide).
5. Save current streaming configuration.

14.6.5. YouTube

Specify the following parameters for YouTube streaming:

1. Proceed to our manual on [how to stream TrueConf conferences on YouTube](#).
2. Configuration name displayed in streaming configuration list on the conference edit page.
3. Server URL from the webpage where YouTube stream is created.
4. Stream name/key from the webpage where YouTube stream is created.
5. This section includes additional settings for current streaming configuration (see [Advanced streaming settings](#) in present user's guide).
6. Save current streaming configuration.

14.6.6. Manual settings

This section allows you to manually setup streaming for the majority of existing streaming services and products, including those listed above. TrueConf Server supports two ways of content transmission: RTSP Publish (aka RTSP Push) and RTSP Pull. When using RTSP Publish, your server notifies streaming platform about content available to be picked up. When using RTSP Pull, the platform itself collects the content from your server.

RTSP Publish manual settings

The screenshot shows a 'Create a new configuration' dialog with a blue header bar containing the title and a close button. The main content area has a white background. At the top, there's a 'Streaming server:' label followed by a dropdown menu showing 'Manual setting - Publish'. Below this, there are four numbered callouts: 1. A text input field for 'Template Name:'. 2. A long text input field for 'URL Publish:'. 3. A checkbox labeled 'Authentication'. 4. A blue link labeled 'Show advanced settings'. At the bottom left is a '← Back' button, and at the bottom right is a blue 'Create' button.

1. Configuration name displayed in streaming configuration list on the conference edit page.
2. The address which will be used to notify about available stream via RTSP ANNOUNCE protocol.
3. Check **Authentication** to enter username and password and gain access to the service.
4. This section includes [additional settings](#) for the current streaming configuration.

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](#).

The screenshot shows a 'Create a new configuration' dialog with a blue header bar containing the title and a close button. The main content area has a white background. At the top, there's a 'Streaming server:' label followed by a dropdown menu showing 'Manual setting - Pull'. To the right of the dropdown, there's a text block: 'RTSP Pull streaming should be configured manually for every conference. You can set advanced settings here.' Below this, there are two numbered callouts: 1. A text input field for 'Template Name:'. 2. A blue link labeled 'Show advanced settings'. At the bottom left is a '← Back' button, and at the bottom right is a blue 'Create' button.

1. Configuration name displayed in streaming configuration list on the conference edit page.
2. This section includes [additional settings](#) for the current streaming configuration.

Additional streaming configuration settings

[Hide advanced settings](#)

Video codec: H264 Audio codec: AAC **1**

☒ Send outgoing RTP streams over TCP **2**

Server response time: 0 **3**

Retries: 0 **4**

Retry delay: 10 **5**

1. You can change video and audio codecs used for the stream encryption.
2. Check if you need to send outbound RTP streams via TCP protocol. UDP is used by default.
3. Response waiting time (in seconds) for the information about published conference stream being successfully received by streaming platform.
4. In case connection with streaming platform is terminated, TrueConf Server will attempt to publish the stream again. This parameter sets the number of such attempts.
5. Delay (in seconds) between stream publication attempts.

14.7. Conference settings

In the **Group Conferences** → **Settings** section, you can configure automatic deletion of conferences and select how participants will be able to join events:

Settings [Help ?](#)

Deleting conferences automatically

☐ Delete scheduled one-time conferences in 30 days after their ending

☐ Delete virtual rooms that have not been started for more than 365 days

Apply

Limits for participants

Limits for video streams outgoing from conference participants

Video 720p

FPS (Video) 30

FPS (Content sharing) 30

Apply

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

Apply

14.7.1. Automatic conference deletion

It may be sometimes helpful to delete a conference from the general list if it was held a long time ago, and

information about this event is no longer needed. TrueConf Server allows you to set up automatic deletion of such conferences.

The launch history of the conferences deleted in this way will still be stored in the [Reports → Call History](#) section. Additionally, chats of automatically deleted conferences and chat files will remain available in the server control panel and on the side of participants.

The following features are available:

1. Delete one-time scheduled conferences. It is possible to specify for how long such conferences should be stored after their ending. The storage period ranges from 1 to 10 000 days.
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 will be checked every 60 minutes and certain meetings that match the specified criteria will be deleted.

14.7.2. Limit on incoming video quality

You can specify general quality settings for **incoming** video streams from all participants in all conferences: client applications, participants joining from browsers via WebRTC, and connections via SIP/H.323/RTSP protocols. This will be the upper limit for incoming video quality. Additionally, you can separately set the frame rate limit for two scenarios: when the speaker is displayed in the video window or when this person is also sharing content in this stream. This does not affect the settings for content sharing via a secondary stream which always uses FullHD 1080p quality with low FPS, prioritizing resolution.

The server administrator can [set individual quality settings](#) for a conference when creating or editing this event.

14.7.3. Ways of joining 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:

- Web pages of [quick conferences](#) created in client applications
- Pages of scheduled conferences.

The parameters for private and public conferences have to be specified separately. You can choose the following connection options: from client applications, browsers (via WebRTC), by QR code from a conference page, and from hardware or software SIP/H.323 endpoints.

15. 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.

15.1. How API and OAuth 2.0 work

The **API → OAuth2** section is used to manage applications or services which utilize TrueConf Server API. Permissions are controlled based on OAuth 2.0. protocol. You can learn more information about OAuth 2.0. protocol in [RFC 6749 official documentation](#) or in the note 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 [\[TrueConf Server API documentation\]](#). TrueConf Server administrator can manage third-party application permissions and access tokens obtained via this section.

- * Learn more about [TrueConf API use cases](#) in 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.

OAuth 2.0 authorization method	Access token scope	Authorization result
Client Credentials The client gets access token, the scope of which is server wide. User authorization is not performed. This method is recommended for trusted applications only.	Server wide	<i>Access token</i> valid for 1 hour is issued.
User Credentials (a.k.a. <i>Resource Owner Password Credentials Grant</i>) To obtain access token, it is required to provide username and password received on the application side.	User's scope	Access token valid for 1 hour and (<i>refresh token</i>) valid for 7 days are issued.
Authorization Code <i>Access token</i> is issued after user has successfully authorized on TrueConf Server special web page. The application cannot access username and password of the user.	User's scope	Access token valid for 1 hour and refresh token valid for 7 days are issued.
Refresh Token This method is used to obtain a new <i>access token</i> based on your existing <i>refresh token</i> .	Equal to scope of the user who has received refresh token initially	Access token valid for 24 hours is issued. This method cannot be used to obtain new refresh token.

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.

15.2. Permissions

API capabilities of a third-party application depend on the permissions it obtained.

The list of permissions increases with each API version as the capabilities of the videoconferencing server increase. See the [API documentation](#) for a list of API and server version compliance.

Each method is assigned with a set of permissions required for successful method call. All sets of permissions are specified in [TrueConf Server API](#) documentation.

* 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.

15.3. Creating new OAuth 2.0 application

To add an OAuth 2.0 application:

1. Click the **Create a new application** button.
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. Check the [rights](#) required for your application in the **Permissions** list.
5. Save your changes by clicking the **Create** button.

15.4. Editing application

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.

16. Server logs (reports)

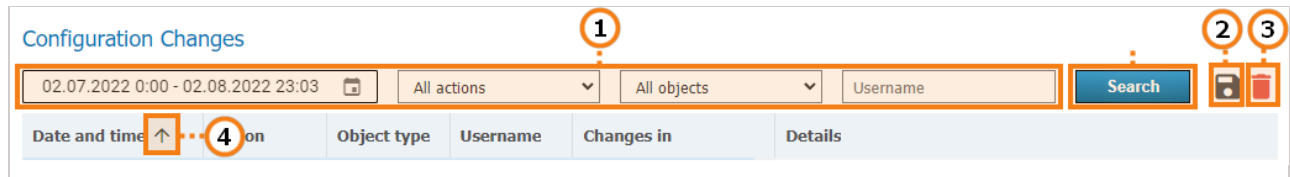
The **Reports** section stores all information about user connections, calls, messages, and video conference recordings. Data can be filtered according to various parameters and downloaded in [CSV format](#). In the tables, time is displayed according to the time zone selected in the [preferences menu](#).



Please note that the main log of TrueConf Server can be [viewed](#) in the **System → Server log** menu in the top right corner of the control panel.

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. Save a table in the CSV format (the export format can be selected in the [preferences section](#)). Please note that in this case, you will save the selection obtained after applying filters and clicking on the **Search** button.
3. Deleting the user accounts selected through filtering. Please note that you will only delete the accounts 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).

16.1. Events

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)
- 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](#).
 - A user's temporary PRO license was revoked by the administrator (in the [Dashboard → PRO Licenses section](#)).
- [Deletion of video recordings](#) by clicking on the  button in the control panel
- Deletion of entries from the logs in the **Reports** section; in this case the event type in the **Event** column will point to the corresponding subsection (check the [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	
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

- 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.
- Link to an active [user profile](#).
- Event details. Contains detailed information required for the [technical support department](#) to solve possible issues you may face. The most common event details:
 - Users:** the list of users' [TrueConf IDs](#) (displayed in multiple cases, e.g., if some users could not get a PRO license after these licenses were redistributed)
 - IP address:** the IP address of the connected user
 - Entered login:** specified during an authorization attempt of a [TrueConf ID](#) user (if authorization fails, this information helps to determine that the user made a mistake in the login)
 - Real user ID:** an existing [TrueConf ID](#) involved in user authorization or another event
 - Endpoint ID:** the unique identifier of a connection, for more information follow the link which leads to the [Endpoints](#) section
 - Application name:** the name of the application that was used to log in to TrueConf Server
 - Authentication method:** authentication method, such as username and password in [Registry mode](#), or the corresponding method for [SSO login](#) (NTLM, Kerberos) will be displayed
 - User rights:** a binary sequence for user's rights encryption
 - Display name:** displayed username
 - 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 to which the user transitioned as a result of the event (has the same values as **Previous status**).
 - Description:** a detailed description of the event
 - Administrator type:** the administrator's access level when an action is performed on his/her behalf, it may be either **sysadmin** (full access to the control panel) or **security** (limited access, check the [description of 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:** 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.

16.1.1. Description of event types

Below you can find the list of all event types logged by TrueConf Server (some events can be either successful or unsuccessful, for example, authorization **login**):

Event Type	Description
authorize	User authorization on TrueConf Server via SSO provider
login	Authorization of: <ul style="list-style-type: none"> • a user by login and password in the client application or personal area in the browser • a TrueConf Server administrator in the control panel
logout	De-authorization (logout) of a user or server administrator
lock	Locking a user account when an incorrect password is entered (see account blocking settings)
unlock	Unlocking a user account by an administrator or after the timeout specified in locking settings
activation	Activation of a user account (see the Active checkbox in the profile description)
deactivation	Deactivation of a user account (see the Active checkbox in the profile description)
status	User status change (online/offline, busy, owner, check the numeric values in the details description above in the events history tab)
connect	Connection of your TrueConf Server to an LDAP server
disconnect	Loss of connection between your TrueConf Server with an LDAP server
delete_chat_messages	Deletion of records from the Chat Messages table
delete_chat_messages_cascade	Deletion of records from the Chat Messages table in case when the conference is deleted from call history
delete_conferences	Deletion of records from the Call History table
delete_connections	Deletion of records from the Endpoints table
delete_events	Deletion of records from the Events table
delete_logs	Deletion of records from the Configuration Changes table
delete_video_recording	Deletion of records from the Conference Recordings table
delete_video_recordings	Automated deletion of recordings from the Conference Recordings table after a timeout, set in the Group Conferences → Settings section
start	TrueConf Server start
stop	TrueConf Server stop
restart	TrueConf Server restart

pro_license_limit	Revocation of a PRO license from a user due to one of these reasons: <ul style="list-style-type: none"> there was not enough PRO licenses when a user tried to join a group conference user lost a PRO license (permanent or temporary) as a result of license redistribution after server restart or automatic revocation after a timeout
pro_license_revocation	Revocation of a temporary PRO license from a user by an administrator (in the Dashboard → PRO Licenses section)

16.2. 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.

16.2.1. Call 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;
- sessions that have [server-side recordings](#).

Other rows will be successfully deleted from the table. In addition, messages for each conference in the [Chat Messages](#) section will also be deleted.

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...

- General table interface ([see the description above](#)).
- Link to the [page with detailed information](#) about a session.
- Link to a [profile](#) of the conference or call owner.
- 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](#).

16.2.2. 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)	va7268100313

2

Participant List

1

User Search

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		E3825799E9F...
Bruce Hubbard	17.04.2024 18:...	17.04.2024 18:...	00:08:45	Conference en...	590 / 0	0	0		E3825799E9F...

Total: 6

3

5

Invite List

1

User Recipient Search

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

3

File List

1

Sender Name Search

Date and Time ↑	Sender	Name	Size, MB
17.04.2024 16:46:56	Abe Chester	group.png	0.05
17.04.2024 16:46:25	Jane Flowers	trueconf_quick_start.pdf	6.3

Total: 2

3

6

7

1. General table interface (see the description above).
2. Conference [chat](#) button.
3. Link to [user profiles](#) of participants and invited users.
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](#).
5. Link to the pages with each conference participant [connection details](#).
6. The list of files sent to the conference chat. When any of the files is clicked, the download page will open.
7. The button for deleting a file from the server.

The number in the **Participants** column of the first table indicates the number of different participants (including those ones connected from different devices). In its turn, the number in the **Participant List** table (check the line **Total**) and the list itself correspond to all **connection** events during the conference. Moreover, these numbers may differ. In the example above, we see that at least one user **Carla Devine** joined twice.



Please note that the use of [UDP Multicast](#) in this session can be specified in brackets in the **Mode** column (not used in the example above).

A server address can be specified as a user in the rows of the **Invite List** table. This means that in these rows, the call to the users from the **Participants** column was initiated by the server at the conference start. If a user is indicated as the inviting party, it means that this person invited the participant when the conference had already started. If any of the participants joined the conference on their own, there will be no inviting user (the corresponding table row will not be included).

16.2.3. 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

16.3. Chat Messages

Chat Messages section features all messages sent by TrueConf Server users both in personal chats and group conference chats. Please note that the table contains time sorted messages from all users at once (you can change sorting features in the table header). To view messages in personal or group chat, you can filter them by **Sender**, **Recipient**, **Session ID**, and message date.

Date and time ↑	Sender	Recipient	Message	Details
02.07.2022 0:00 - 02.08.2022 23:42	Sender	Recipient	Message	Session ID
02.08.2022 23:42:02	Ann Smith	bill@video.company...	So we can move on to the next step	
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				

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 🎉

1. General table interface (see the description above).
2. Links to [user profiles](#) of the sender and recipient of a private message.
3. Link to a [page with detailed information](#) about the session to the common chat of which a message was sent.

16.4. Configuration Changes

In this section, one can view the log of the following changes:

- TrueConf Server settings
- List of conferences stored on the server
- Changes in the parameters from the [Dashboard → PRO Licenses](#) section, including the cases when PRO licenses were manually redistributed by the administrator
- 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

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).

16.5. Conference Recordings

This section contains a list of recorded conferences. Here you can playback, download or delete their records.

The parameters for storing conference recordings are set in a [different section, Recordings](#).

Conference Recordings

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...	lc\webinar	250.5	▶ ⬇ 🗑
(no title)	0000002d1...	20.05.2023 08:...	00:02:41	joe@video.exa...	lc\578943531983	15.2	▶ ⬇ 🗑
Meeting	0000002be...	20.05.2023 08:...	00:06:57	krowly@video...	lc\9676777659...	29.4	▶ ⬇ 🗑
Brainstorm	0000002ae...	20.05.2023 08:...	00:23:04	joe@video.ex...	lc\785724251543	172.7	▶ ⬇ 🗑
Conference	000000266...	19.05.2023 13:...	00:28:26	klintz@video.e...	lc\115969749177	225.4	▶ ⬇ 🗑

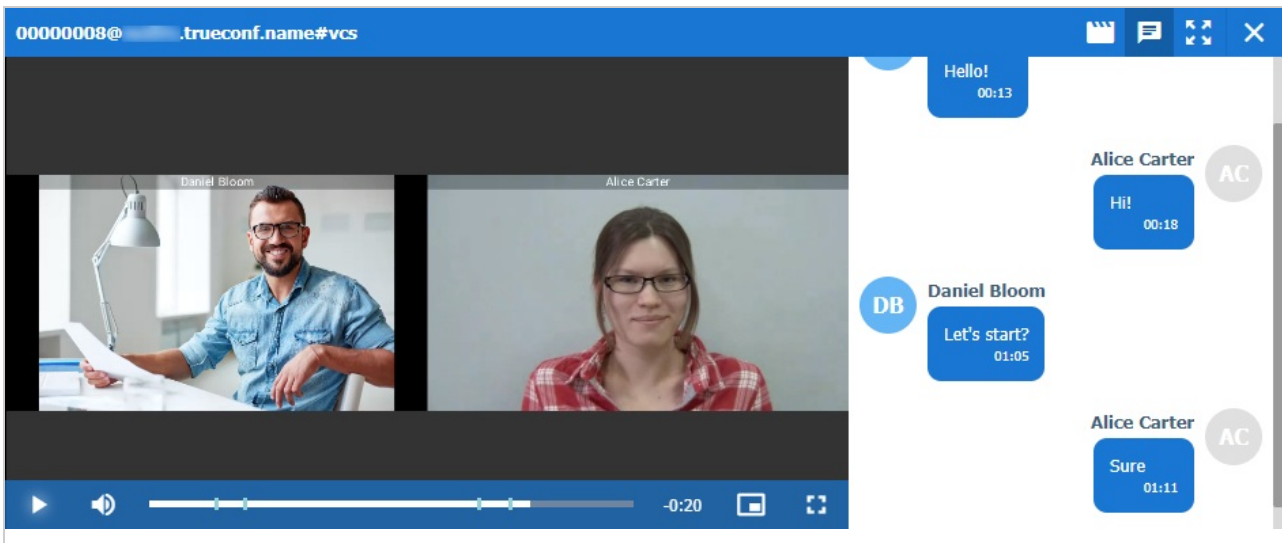
Total: 5

1. General table interface (see the description above).
2. Link to the [page with detailed information](#) about a session.
3. Go to the conference card in the [general list](#)
4. Playback button
5. Recording download button

6. Delete button.

Point-to-point video calls will be named **(no title)**.

You can use the  button to playback recorded conferences with chat synchronization (for group conferences only):



Can the video recorded with TrueConf Server be played 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.

16.6. Endpoints


This section provides information about user endpoints. This information can be useful for **real time** technical support.

Endpoints Help ?			
Show <input type="text" value="10"/> entries	Search: <input type="text"/>		
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**.

If you click on an entry in the **Endpoint** column, you will see the page [providing detailed information about the connection of the selected user](#) (we have discussed this page previously). In turn, by clicking on the field in the **Logged User** column that contains TrueConf ID of the selected TrueConf Server user, you will open 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 recordings made earlier than the selected date. To do it, click on the  button and specify the number of days for storing information (180 days by default):

Deleting data

Delete connection logs older than days.

Delete

Cancel

16.6.1. Events that update device information

Event	Variable Fields
Connecting or reconnecting device to the server	<div><div></div><div>• Network Info Type</div><div>• Audio Capture</div><div>• Audio Render</div><div>• Video Capture</div><div>• Direct X</div><div>• Hardware Config</div></div>
Conference end	Last Conf Name
Taking network test (by clicking a corresponding button in the client application)	Network Test
Authorization on the server	System information

17. Configuration of extensions

17.1. TrueConf Directory

In the **Extensions → TrueConf Directory** section, you can configure integration of your TrueConf Server instance (a part of **TrueConf Enterprise**) with solution TrueConf Directory.

To do it, click on the **Activate** button. To disable integration, click on the **Deactivate** button.

TrueConf Directory

[Help ?](#)

TrueConf Directory is a solution that combines multiple servers into a single address space. This product allows users from one server to search among users of other independent servers within TrueConf Enterprise solution, as well as view information about them, add them to address books, make point-to-point and group video calls and exchange instant messages in chat.

Activate

In the large box below the table, the secret key will be generated.

TrueConf Directory

[Help ?](#)

TrueConf Directory is a solution that combines multiple servers into a single address space. This product allows users from one server to search among users of other independent servers within TrueConf Enterprise solution, as well as view information about them, add them to address books, make point-to-point and group video calls and exchange instant messages in chat.

Deactivate

Directory	Requirements
Version	3.0.0 or above
SSL (HTTPS)	enabled

eyJpZCI6InViMm1tIiwibmFtZSI6InViMm1tLnRydWVjb25mLm5hbWUuIjI2ZXJzaW9uIjojNC40LjQuMTAxMzMlLCJ1cmwiOm51bGwsInNlY3V5ZV91cmwiOiJodHRwcpcL1wvMTAuMTIwLjEuMTE5IiwiaWY2xpZW50X2lkIjoiaHJ1ZWVbmZfZGlyZWNoY3J5IiwiaWY2xpZW50X3NlY3JldCI6IjRkYzIxZmI4NzhhMTI2OGJiOWYyNGRlbnJkdM2ZlMTJjNDQ2MTY5NTIifQ==

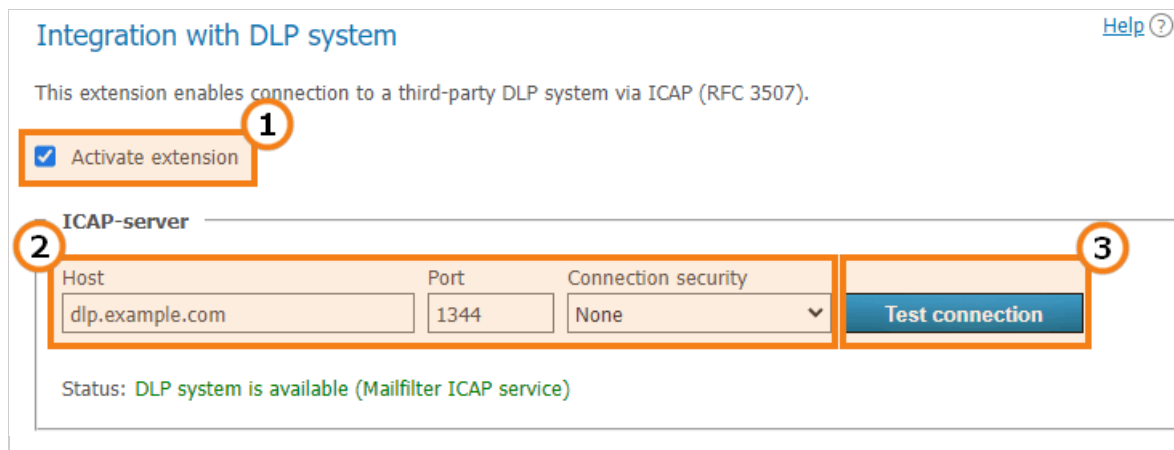
Copy

If you want to learn more about TrueConf Directory extension, as well as how to purchase and set it up, please [contact us](#) in any convenient way.

We demonstrated TrueConf Directory features [at ISE 2019](#) .

17.2. Integration with DLP

If the **Integration with DLP extension** is activated in your TrueConf Server license, you will be able to configure connection to such a system and select the actions that should be performed when violations of information security rules are detected.



Integration with DLP system [Help ?](#)

This extension enables connection to a third-party DLP system via ICAP (RFC 3507).

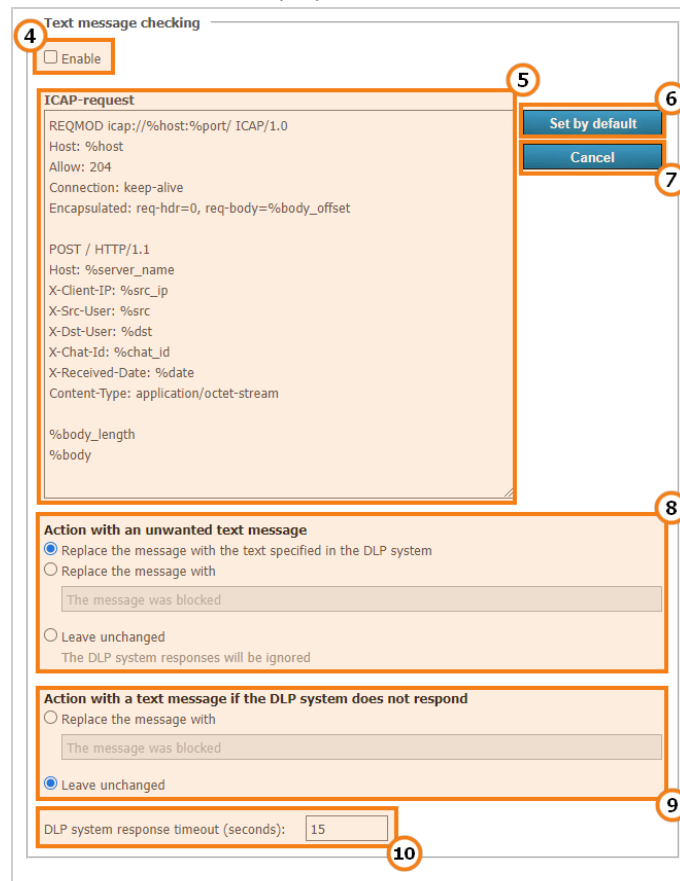
1 ☒ **Activate extension**

2 **ICAP-server**

Host dlp.example.com	Port 1344	Connection security None	3 Test connection

Status: DLP system is available (Mailfilter ICAP service)

1. Extension activation. If the box is not marked and settings have not been saved with the **Apply** button, no checks will be performed.
2. DLP connection parameters: host (IP or FQDN without the `http: / https:` prefix), port and connection type (cloud or secure TLS connection).
3. System availability test. The test result will be displayed in the status line below.



4 **Text message checking**

☐ **Enable**

5 **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-Received-Date: %date
Content-Type: application/octet-stream

%body_length
%body
  
```

6 **Set by default**

7 **Cancel**

8 **Action with an unwanted text message**

☒ Replace the message with the text specified in the DLP system

☐ Replace the message with

The message was blocked

☐ Leave unchanged

The DLP system responses will be ignored

9 **Action with a text message if the DLP system does not respond**

☐ Replace the message with

The message was blocked

☒ Leave unchanged

10 DLP system response timeout (seconds): 15

4. Activation of text message verification. If the box is not checked, and no settings have been saved with the **Apply** button, no verification will be available.
5. ICAP request containing the fields that should be sent to a DLP system. The request format will depend on the specific system. Here, we have listed the [variables used in the template](#), These variables will be replaced with specific values when data is sent for analysis.
6. Reset the ICAP request to the default template.
7. Discard the last changes that were not saved with the **Apply** button.
8. Actions with a message marked as unwanted by the DLP system. It is possible to replace the message with a text selected on the side of the DLP system. One can also specify a custom text for the message or leave the initial message unchanged. In the last case, users will receive all messages, but the logs of the DLP system will include records of unwanted messages.

9. Actions with an unwanted message if there is no connection with the DLP system. For example, it is possible to enter the text “No connection with the security system” so that no messages can be sent to recipients until the problem is solved.
10. DLP response waiting time. If connection with the system is disrupted, the time period specified here will have to expire until TrueConf Server responds when the first message is sent. It will follow the settings from step 9 (attempts will be made to restore the connection). Then, connection availability will be tested in background mode, In this case messages will be sent or blocked almost instantaneously.

11. Activation of file verification. If the box is not checked, and no settings have been saved with the **Apply** button, verification will be unavailable. Please note that file analysis and response may take some time depending on the file size since the file will be first uploaded on TrueConf Server and then sent to the DLP system.
12. ICAP request containing the **fields that should be sent to the DLP system**.
13. Reset the ICAP request to the default template.
14. Discard the last changes that were not saved with the **Apply** button.
15. Actions with a file marked as unwanted by the DLP system. It is possible to replace this file with the text specified on the DLP system. One can also specify a custom text message or make no changes. In the last case users will receive all files, but the logs of the DLP system will include records of unwanted files.
16. Actions with an unwanted file in case there is no connection with the DLP system. For example, it is possible to enter this text “No connection with the security system” so that no files could be sent to recipients until the problem is solved.
17. DLP system response waiting time. The logic similar to the one used for messages is applied here (check step 10).
18. Limitation on the number of participants in the group chat for sending their list to DLP.
19. Don’t forget to click the **Apply** button to save changes.

17.2.1. Variables in the templates of ICAP requests

- `%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 the [ISO 8601](#) format
- `%dst` — the recipient's full TrueConf ID presented as `user@server`
- `%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 taken from the **Host** field
- `%port` — the value taken from the **Port** field
- `%server_name` — the domain name of TrueConf Server
- `%src` — sender's full TrueConf ID
- `%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

17.3. Mail plugins



This extension enables you to:

- Control the web version of Microsoft Outlook plugin that will be downloaded from your server
- Receive direct links for installing the Windows version of the Outlook add-on and Thunderbird plugin
- Customize a template invitation to a conference.

This extension is offered for free (including TrueConf Server Free as well).


On the **Plugins** tab, you can:



1. Download the xml file for installing the web version of the add-on (plugin) and update the current version on the server in the **Outlook (web)** section. The plugin installation link can be copied with the button  and then distributed among the users of the corporate network (including the private network that does not have access to the Internet) so that these users could install the plugin 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.



To learn more about installation and features of desktop and web versions of the MS Outlook add-on, [check out our knowledge base](#).

3. Copy the installation link for the Thunderbird plugin with the button  in the **Thunderbird** section and share this link 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

In the invitation template, one can use a group of constants similarly to the email templates available when [configuring SMTP](#):

- `%conf_name` — name of the conference
- `%conf_id` — ID of the conference, e.g. `\c\df0a2adebe`
- `%owner_name` — display name of the [conference owner](#)
- `%conf_url` — the link to the [conference page](#), e.g.,:
`https://example.com/c/CID`
- Server administrator contacts parameters:
 - `%admin_name` — display name
 - `%admin_email` — email address
 - `%admin_phone` — phone number.

18. Permissions of the administrator with the Security Admin role

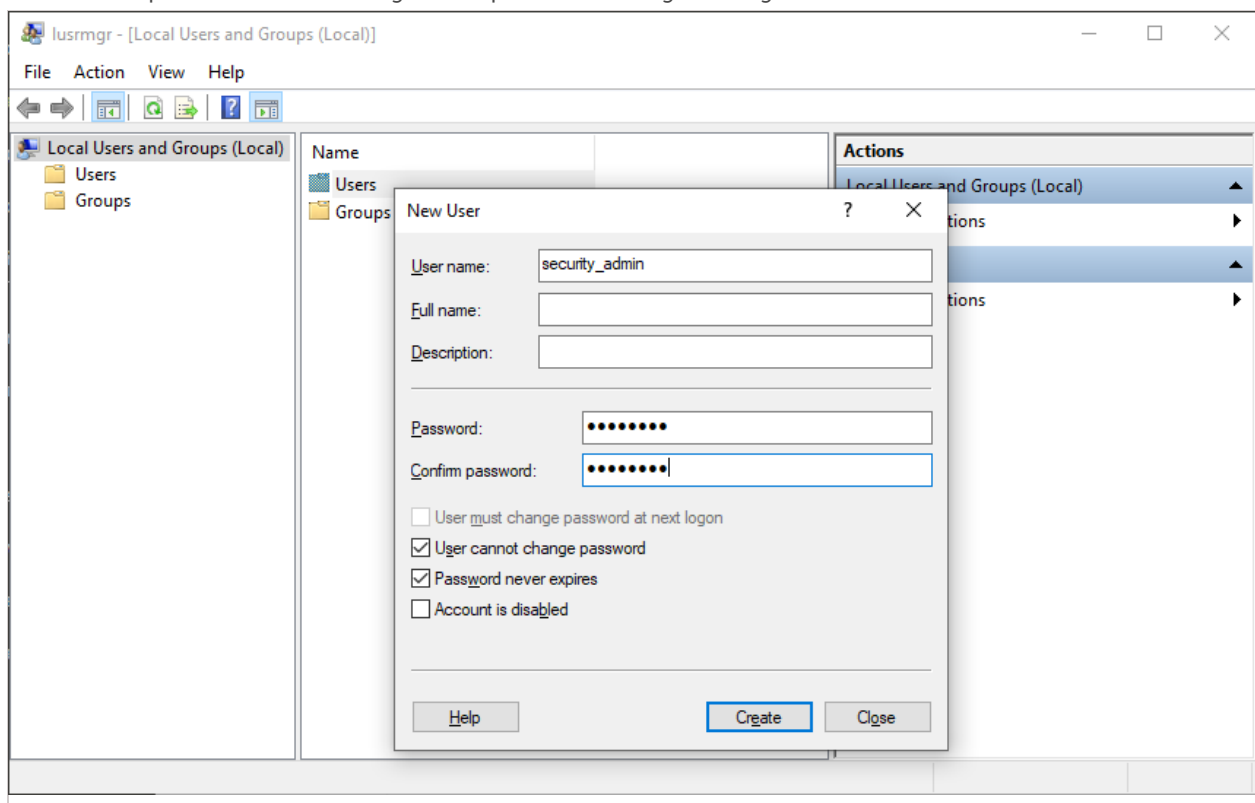
To enable limited access to the TrueConf Server control panel, a local **TrueConf Server Security Admin** user group on Windows and **tcsecadmins** on Linux is automatically added to your operating system during the server installation process. TrueConf Server administrators can add to this group the 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 logs](#)
- [call history](#)
- [active connections](#)
- [chat messages](#)
- [conference recordings](#)
- [configuration logs](#).

18.1. 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** section. To do this, press the **Win+R** key combination and execute the `lusrmgr.msc` command in the appeared window.
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 select **Properties**.
6. Click **Add...** on the **Member Of** tab.
7. Enter **TrueConf Server Security Admin** as the name of the selected object and click **OK**.



The user accounts imported from Active Directory/LDAP can also be added to the local TrueConf Server Security Admin group.

18.2. How to add an account to the Security Admin group on Linux



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:

```
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.).



You can add a user to the TrueConf Server administrator group and provide them with full access to the control panel in the same way. To do this, replace `tcsecadmins` with `tcadmins` in the commands listed above.

18.3. 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

You just need to go to the **Local Users and Groups** tool and complete the steps 4-7 from the [section describing how to add an account](#).

For Linux OS

The `usermod` [command](#) is used to configure account settings. For example, to add `[user]` to the group `tcsecadmins`, run this command as a superuser or with the help of the `sudo` program.

```
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.

Further instructions are intended for the administrators, whose accounts are added to the **TrueConf Server Security Admin** user group on Windows and **tcsecadmins** on Linux.

18.4. How to access TrueConf Server control panel

1. Open the [TrueConf Server guest page](#). Please contact your server administrator to obtain your guest page URL.
2. Click the **Administrator login** button at the bottom of the page.
3. Enter your username and password and click **Enter**.

18.5. 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 TrueConf Server operates in the standard mode, **running, registered** status is displayed. If there are any issues when running or registering TrueConf Server, you will see the corresponding red message. In this case you should contact your server administrator or submit a ticket to [our technical support](#).


18.6. Configuring preferences

By clicking on [System → Preferences...](#) section in the upper 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.

18.7. Server log

To open detailed logs about TrueConf Server operation, go to the [System → Server log](#) section. It stores events and errors related to the launch of server services, [connection to the registration server](#), [license activation](#), etc.

You can save the log to a **txt** file using the  button. TrueConf Server logs are the best resource for determining the root cause of the problem, which is why we recommend sending the **txt** file to our technical support when submitting tickets.

18.8. Access settings

To view information about TrueConf Server control panel access settings, proceed to **Web → Security** section:

Web Security [Help ?](#)

Dashboard

Give admin access to:

- ☒ members of **TrueConf Server Admin** local security group
- ☐ all Windows users on **localhost**

☒ Allow admin access from localhost without authentication

☒ Limit access to admin area by IP

10.0.0.0/8
192.168.0.0/16
172.16.0.0/12

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.

18.9. Reports

The [Reports](#) section contains all the event logs related to changing server settings, connecting to it, as well as holding video calls and meetings on it.

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 TrueConf Server logs in the [administrator guide](#).

18.9.1. Events

In the [Events](#) section you can view the history of changes of the TrueConf Server users user status, as well as the server status. If you select an event in the table, detailed information will be displayed on the right side of the page.

18.9.2. Call History

To display the list of previous and ongoing conferencing sessions, go to the [Call History](#) section.

Here you can view information about each video conferencing session: ID, start and end time, duration, number of

participants, TrueConf ID of the owner, conferencing mode, as well as meeting ID.

Click on the session ID to open the [list of invited participants](#) in a new tab. Press the  button to open [chat history](#).

18.9.3. Chat Messages



The [Chat Messages section](#) displays the history of all messages between TrueConf Server users, including group chat history.

18.9.4. Configuration Changes

To open TrueConf Server configuration history, go to the [Configuration Changes section](#). When the server administrator creates/deletes/edits group conferences, all changes are also displayed in this section.

18.9.5. Conference Recordings

In the [Conference Recordings section](#), you can view the list of video recordings stored on the server with detailed information about each of them.

To download or playback a recording file, use  and  buttons respectively.

18.9.6. Endpoints

To view the details of connections to your TrueConf Server instance, go to the [Endpoints section](#). There you can see information about all [connections to the server](#) using client applications or via a browser using [WebRTC technology](#).

To learn more about the connection selected, click on the corresponding line.