TrueConf

TrueConf Server

Administrator guide

Version 5.5.1

Table of Contents

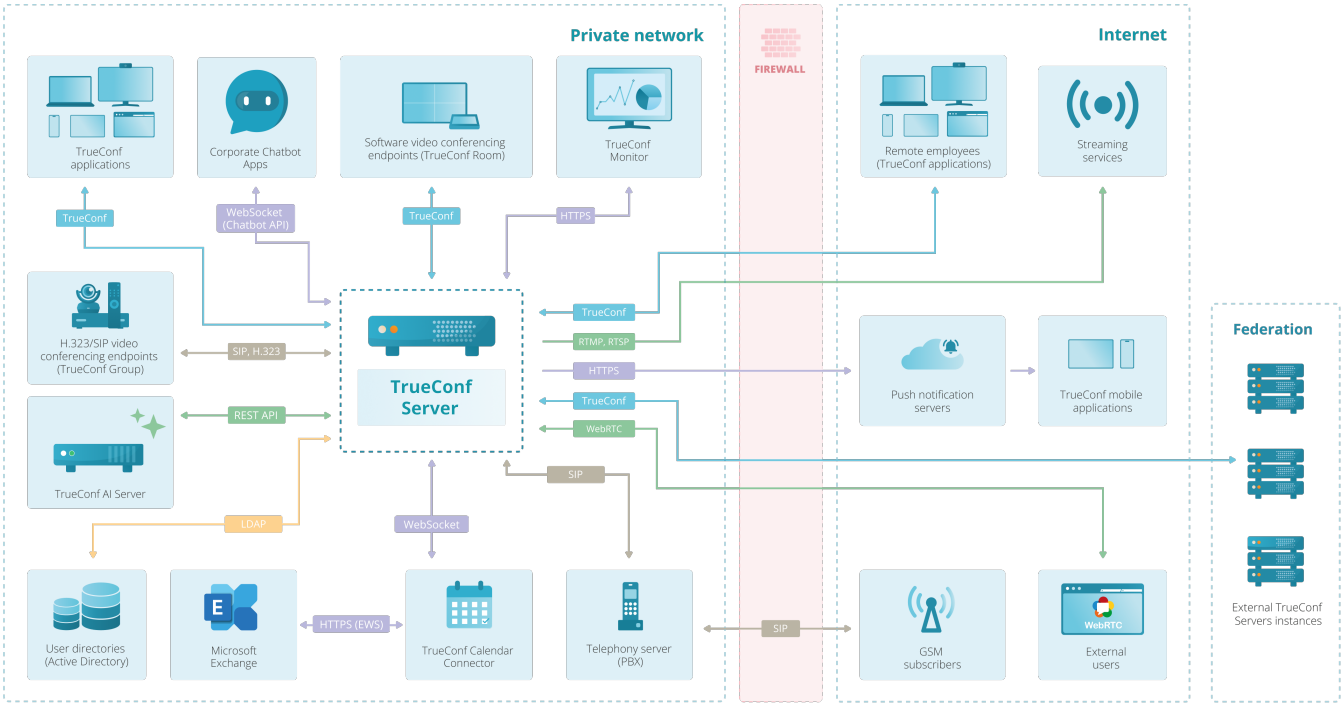
1. Description of the video conferencing server and its features

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 suite: BFCP for content sharing; FECC for camera control; SRTP for media stream encryption; TLS for the secure signaling protocol (SIPS).
- WebRTC: SRTP and DTLS for media stream encryption.
- Connection of IP cameras and external streams (e.g., conferences) via the RTSP protocol.
- Stream your conferences to third-party services via RTSP and RTMP protocols.
- Integration with mail servers via the SMTP protocol.
- QoS support: DSCP, DiffServ.
- Integration with directory services via LDAP and LDAPS protocols.
- 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++, H.261

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, PCM

1.2.2. Modules of the video conferencing server and their functionality

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

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

You can find the main features of each component below.

1.2.2.1. System services

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

- user authentication and authorization: multilogin is also supported which means that it is possible to work in several client applications under the same account
- holding group video conferences and one-on-one video calls
- server events logging (calls, user authentications, chat messages, etc.)
- NAT traversal and proxy servers to connect users
- 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)
- synchronization with supporting TrueConf solutions: TrueConf Monitor, TrueConf Calendar Connector, TrueConf AI Server
- 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 conferences supporting simultaneous interpretation for international online events
- Create a general layout for all participants, for SIP/H.323/WebRTC participants or individual layout for each user.
- Manage cameras and microphones of active conference participants, change their devices remotely.
- Add and remove participants from ongoing conferences.
- 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 and start surveys, both internal and public (for external participants)
- Create backups and restore server settings.
- Customize your guest page and indicate administrator's contact info.
- Limit access to the TrueConf Server control panel for certain admin roles or using IP filters.
- Monitor server performance both in real time and for a certain time range.
- View server reports (log files) and all user actions (call history, message history, connection history, etc.).
- Check information about the mail plugins that can be used to create conferences when adding new events to the calendar (MS Outlook and Thunderbird are supported)
- Configure access to the TrueConf Server API.

1.2.2.3. 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:

- Relatively low system requirements. You can find system requirements for common configurations in our article.
- Work in a corporate (closed) network without connecting to the Internet and transferring data to third-party servers.
- Additional levels of data protection.
- Convenient administration.
- Advanced technologies to improve the quality and reliability of video communication.
- 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).
- Collaboration tools.
- Streaming conferences to popular services.
- Managing video layouts and participants' devices.

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 applications (for Windows/macOS/Linux, for Android, for iOS/iPadOS, or even for Android TV)
  - in the personal area
  - in TrueConf Group or TrueConf Videobar endpoints
  - in the software-based TrueConf Room endpoint
  - with SIP/H.323 devices that can 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 currently authenticated, he/she will not be counted as one of **online users** whose number is limited by the license.

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

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

When creating a public conference, you can restrict permissions for guests by forbidding them to send messages, audio, and video.

Unlike authorized users, guests can only see TrueConf ID (login) and the displayed name in the cards of other event participants. This is done for security reasons and cannot be changed by the server administrator.

- **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).

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

2.2. User identificator

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`

> *i* 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

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

2.3.1. Moderator

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

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

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

The moderator role can also be given to a guest or a participant from a federated TrueConf Server.

2.3.2. Owner

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

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

A moderator cannot remove the owner from the conference.

2.3.3. Operator

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

In addition to moderator rights, an operator can:

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

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

2.3.4. Speaker

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

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

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

2.3.5. Interpreter

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

2.4. Admin roles

In TrueConf Server, there are two types of administrators depending on the user groups that are automatically created in the OS during server installation:

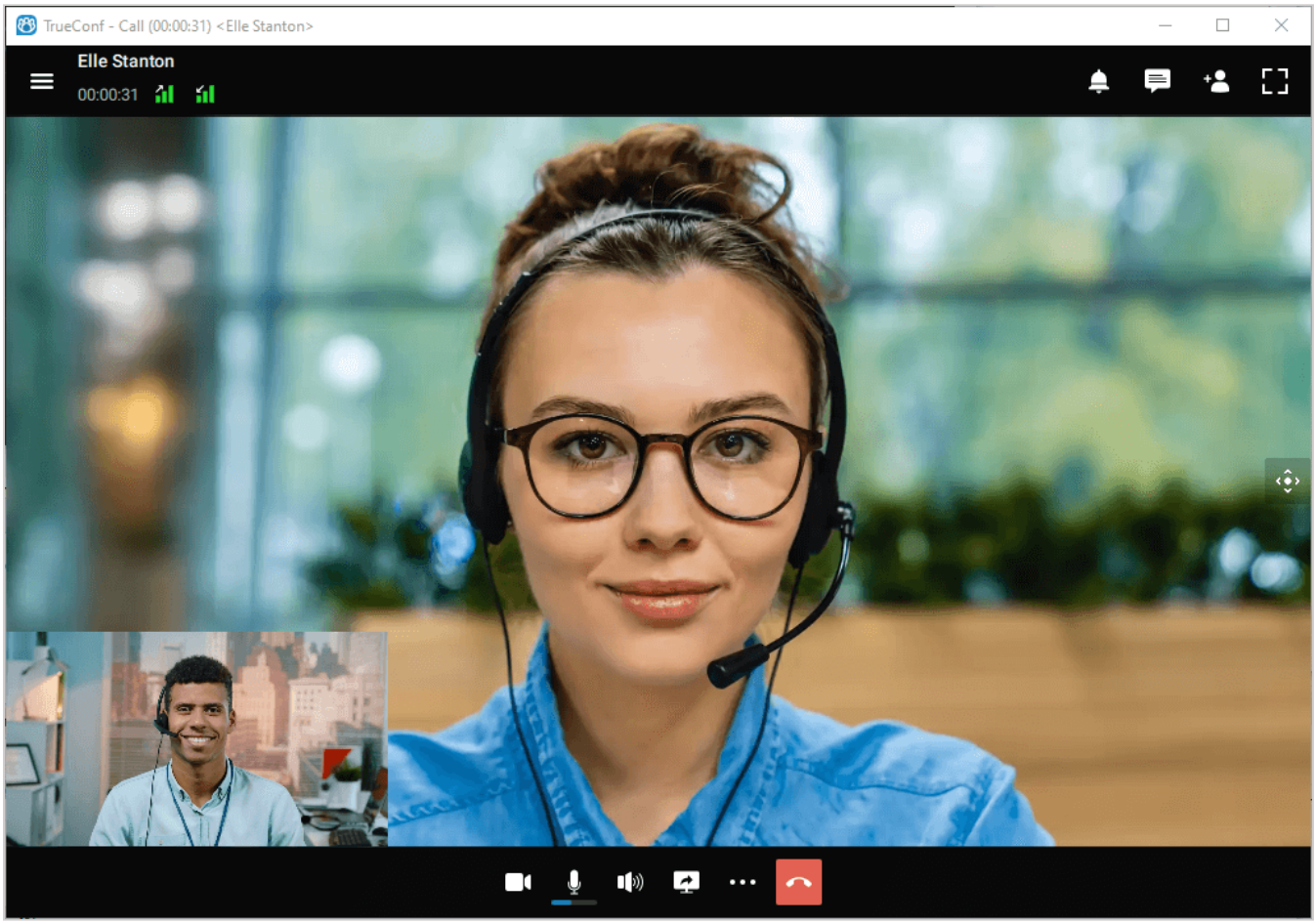
- **TrueConf Server Admin** has full access to the TrueConf Server control panel and can manage all server settings.
- **TrueConf Server Security Admin** has read-only access to the reports and recording. TrueConf Server Security Admin cannot change any settings in the TrueConf Server control panel.

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.

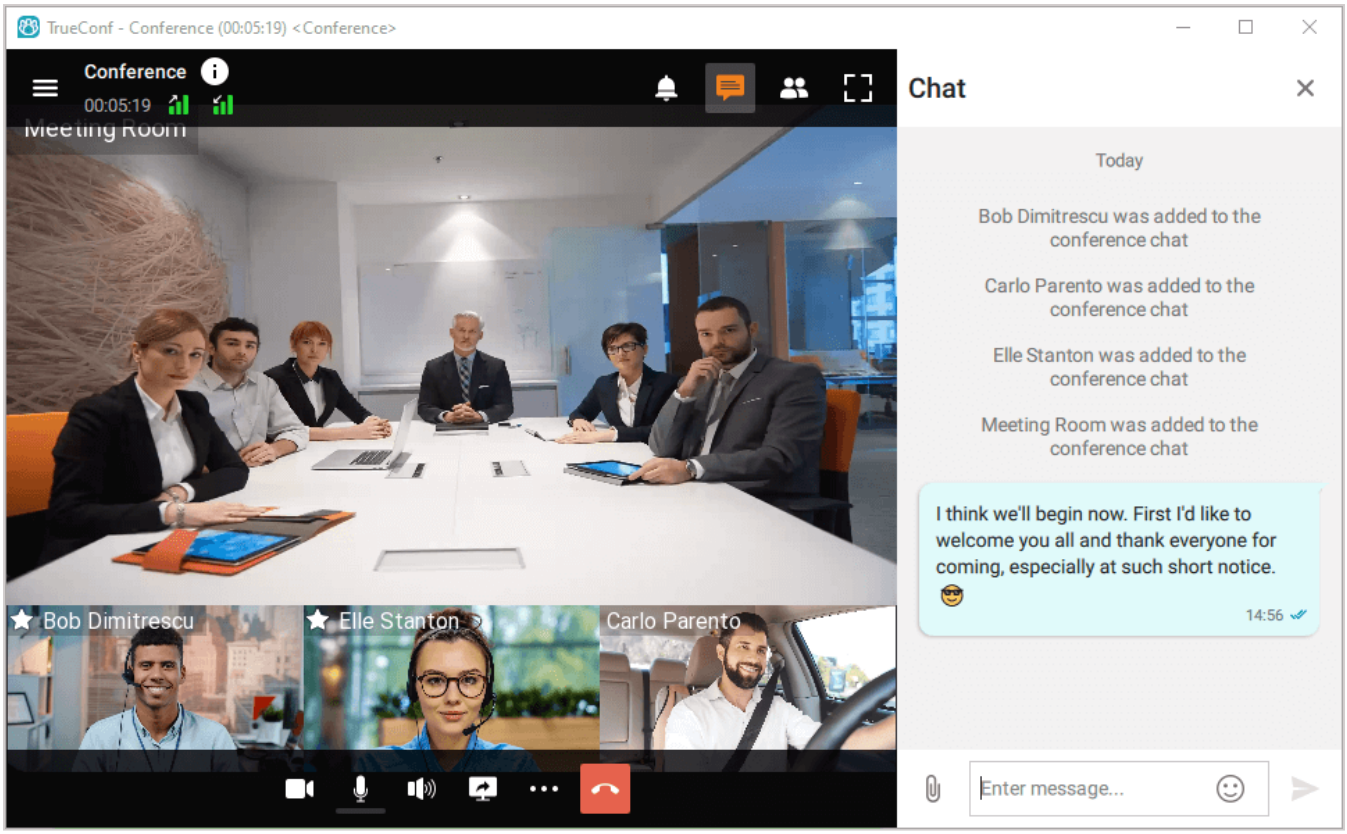


TrueConf provides a number of additional options during video calls: chat, file sharing, content sharing (e.g. sharing screen or separate application windows) and other collaboration tools.

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.

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

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.

To learn more about the advantages of each mode, refer to our website.

3.4. Conference ID

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

Examples:

`\c\interview`

`\c\12345`

`\c\interview@video.example.com` — the full CID, including the server address.

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

> *i* Manual assignment and editing of conference IDs can be disabled for all events by server administrator.

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

- in the server control panel
- in the client application scheduler
- in the personal area.

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

If a person knows the ID of a conference, he/she will be able to join this event. The ID is used for generating the link to the conference page.

3.5. What is a waiting room

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

There is a participant in the waiting room:

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

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

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

4. 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, Cisco Webex, LifeSize Cloud and Skype for Business via SIP/H.323 protocols.
- IP cameras and video surveillance systems as well as streams (e.g., streams of other conferences) — via the RTSP protocol.

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

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

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. Integration with AI server

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

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

4.10. Integration with a corporate calendar

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

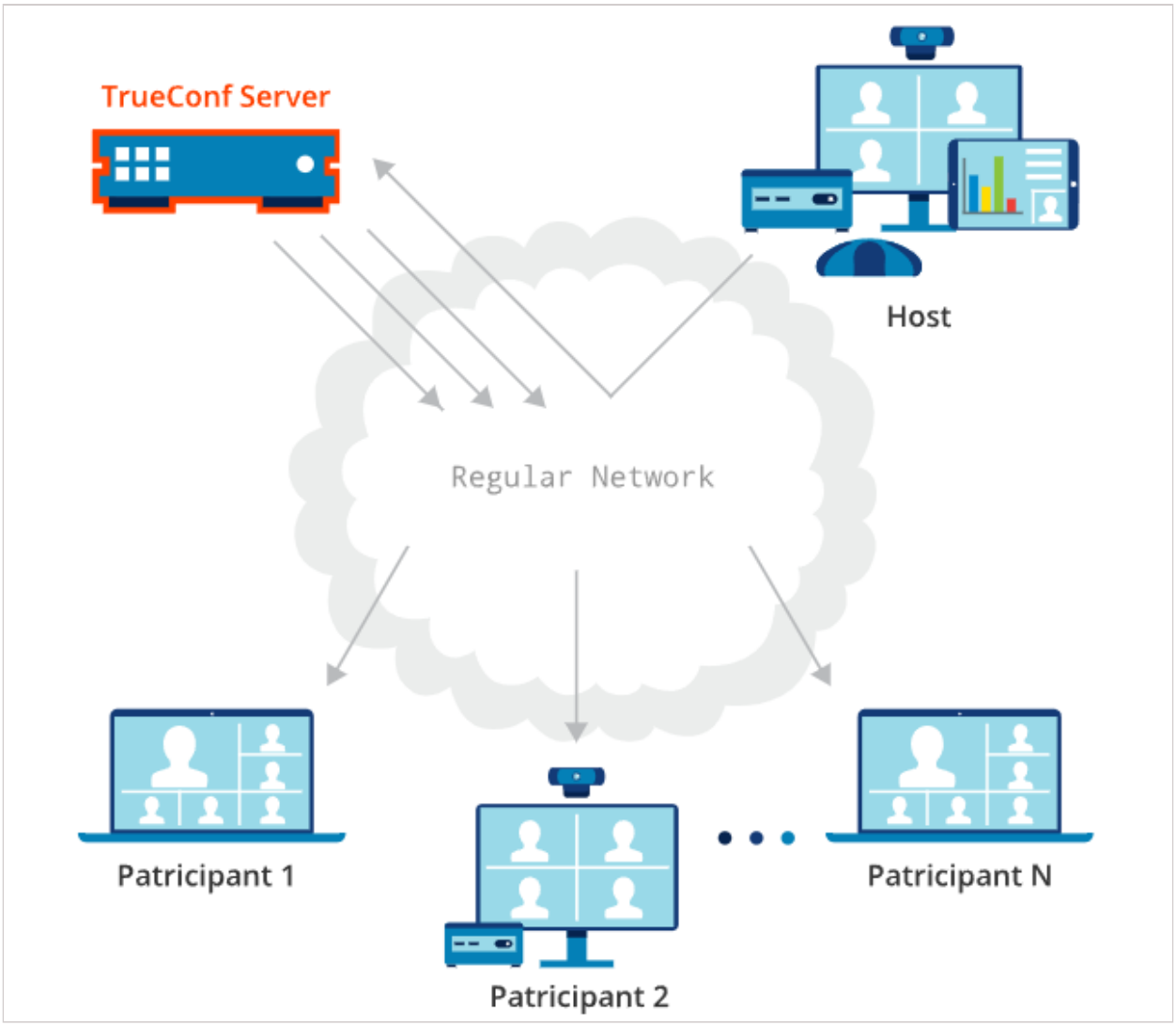
To integrate the corporate calendar with the video conferencing system, you only need to purchase a license for TrueConf Calendar Connector. Additionally, some features are available even in the free version. For more details on how to set up integration with TrueConf Calendar Connector, refer to the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

4.11. UDP Multicast

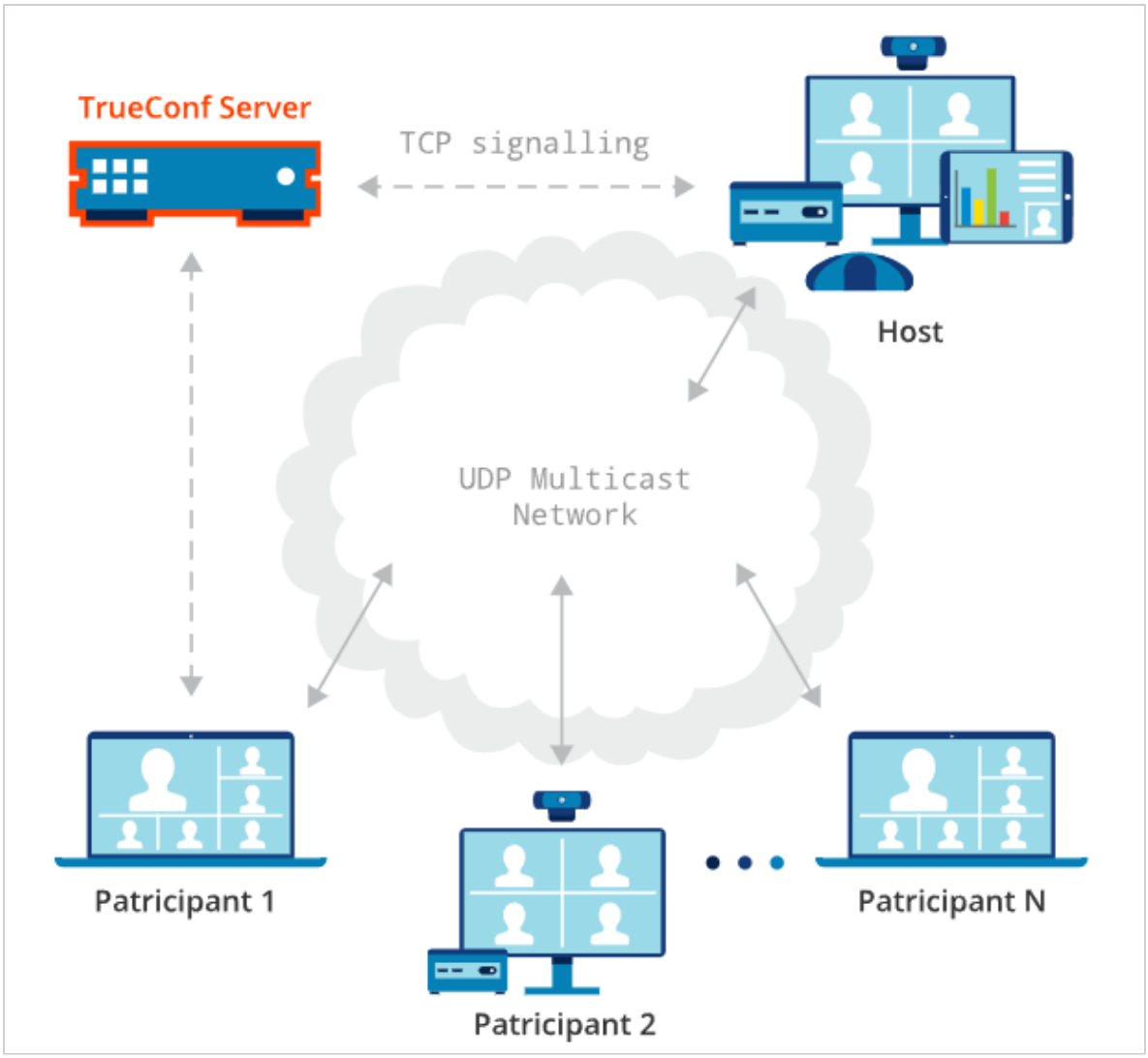
UDP (User Datagram Protocol) Multicast is a data transmission protocol under which a signal is transmitted through the Multicast switch, bypassing the server.

* 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.



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

4.12. TrueConf Directory

This extension 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.

4.13. 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.

4.14. 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.

4.15. TrueConf Enterprise

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

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.

4.16. Advanced monitoring of video conferencing servers

The TrueConf Server control panel includes the monitoring page with basic information about the server operation. Additionally, TrueConf offers a separate solution named **TrueConf Monitor** intended for advanced monitoring of performance metrics and data collection. It enables the administrator to track information across multiple servers and provides other advantages:

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

5. Licensing of the video conferencing server

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

1. Availability of extensions.

Name	Provision condition
LDAP/Active Directory	Free
SIP/H.323/RTSP gateway	One has to purchase the required number of gateway connections (1 connection is available in TrueConf Server Free)
Public conferences (webinars)	It is necessary to purchase the required number of connections (1 guest connection is available in TrueConf Server Free)
Simultaneous interpretation	Free
Integration with a corporate calendar	TrueConf Calendar Connector solution is licensed separately (free version is available)
Integration with the AI Server	Licenses for the integration module and TrueConf AI Server are needed (check the integration description for more details)
Federation	Purchase of any paid license
Ability to add a watermark for the conference layout	Purchase of any paid license
Live streaming	Purchase of an extended or full technical support package
UDP Multicast conferences	Purchase of a full technical support package
Integration with a DLP system	Included in TrueConf Enterprise
TrueConf Directory	Included in TrueConf Enterprise
TrueConf License Manager	Included in TrueConf Enterprise
TrueConf Border Controller	Included in TrueConf Enterprise
SDK applications support	Provided upon 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

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

The server administrator can track the number of available connections of each type on the **Summary →License info** tab.

* In TrueConf Server Free there are restrictions on the number of each type of connection. To learn more, go to the web page of this solution.

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

	PRO user	Online user	Guest
One-on-one video calls	V	V	X
Use of collaboration tools (screen sharing, local video recording etc.) during one-on-one video calls	V	V	X
Messenger features: personal and group chats, file transfer, etc.	V	V	X
Access to the chat of a conference which has already ended	V	V	X
Address book and the personal area	V	V	X
Ability to schedule conferences and create virtual rooms	V	V	X

	PRO user	Online user	Guest
Ability to create slideshows before a conference or call	V	V	X
Participation in a public group conference (webinar)	V	X	V
Using the chat of an ongoing public conference (webinar)	V	X	V
Collaboration tools in a public conference (webinar): content sharing, local video recording, etc.	V	X	V
Ability to be a moderator in a public conference	V	X	V
Using the chat of an ongoing private group conference	V	X	X
Participation in a private group conference	V	X	X
Ability to be a moderator in a private conference	V	X	X
Collaboration tools in a private conference: content sharing, local video recording, etc.	V	X	X
Ability to start a quick conference in the application menu, chat or address book	V	X	X

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

5.1. Online users

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

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

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

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.

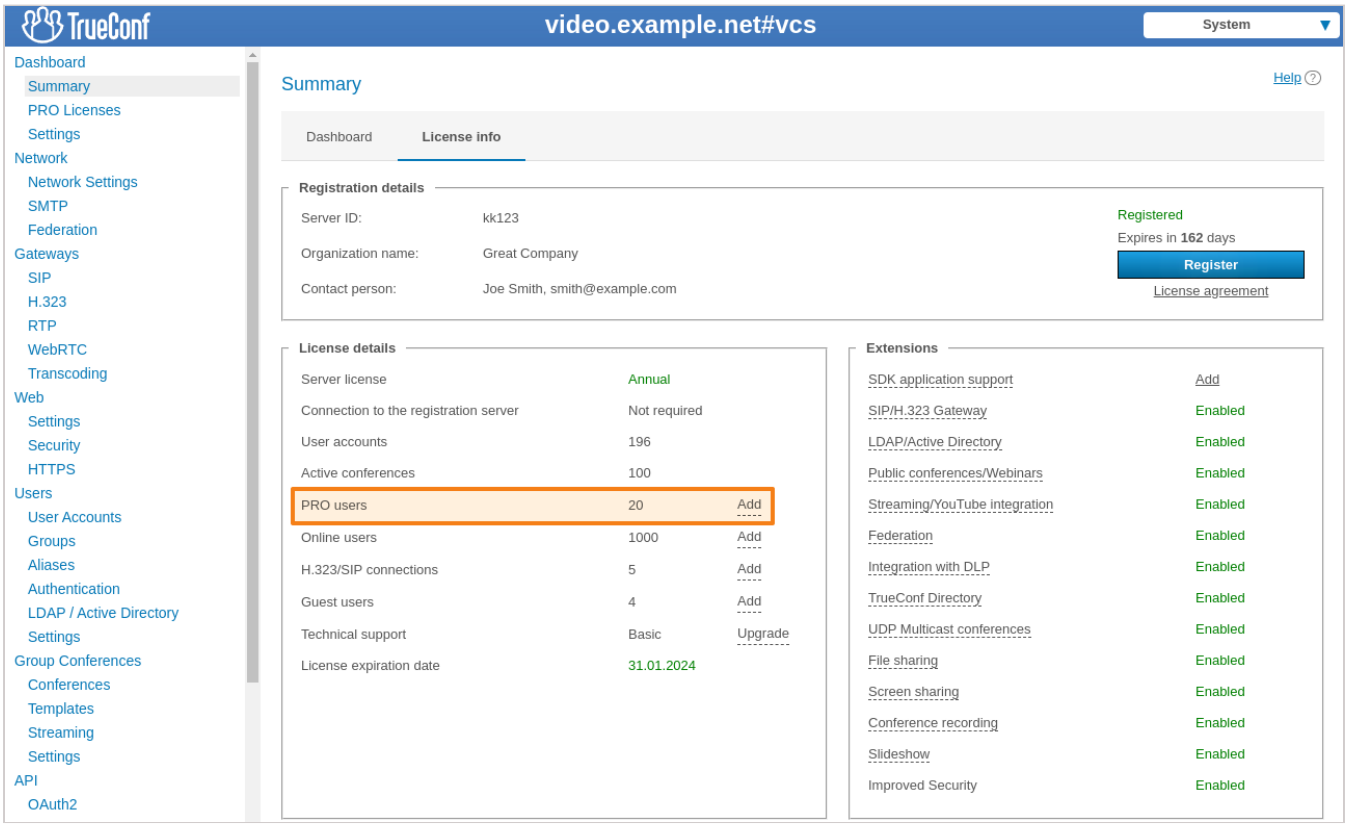
5.2. PRO users and conference participation

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

The number of available PRO licenses for 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.



5.2.1. Key aspects of using PRO connections

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

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

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

1. If a user, who is not included in the group with permanent PRO licenses, tries to join a group conference, the application will check if PRO licenses are available. If there are available licenses, the user will automatically receive a **temporary** PRO status. This status will be reserved for this user for 24 hours. If the user joins the same group conference or any other during this period, the countdown will be reset to zero. While a user is staying in a conference, the PRO status is automatically renewed.
2. The TrueConf Server administrator can instantly revoke a user's temporary PRO status by clicking on the ✕ button next to the user's name (check the description of the **PRO licenses** section of the control panel).
3. The server administrator can allow users to request a PRO license manually before participating in a conference (this status will also be active for 24 hours after reception).
4. The number of devices used by a person for participating in conferences does not affect the number of PRO licenses available on the server since the PRO status is linked to a specific user account (TrueConf ID). It is not tied to the device on which the user is authenticated. So, if the user, who is simultaneously signed in on two devices, joins two conferences from these devices, two online licenses and one PRO license will be taken.
5. When the number of PRO licenses available on the server becomes equal to 0 and a user tries to join a group conference, his/her status will be checked:
   - If this person has a permanent PRO status, he/she will be allowed to participate in the conference.
   - If this user previously received a temporary PRO status, and this status is still valid (check Step 1), he/she will be able to participate in the conference.
   - In other cases, the user will be unable to participate in a conference. At the same time, this person will still be able to participate in one-on-one calls and chats or make use of other features.

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 PRO licenses is not sufficient for the users with permanent licenses, the licenses will be taken away from the users with temporary licenses (starting from the users whose temporary PRO status has the shortest expiry period).

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

5.3. If there are ongoing conferences, only the participants, whose PRO licenses were taken away after the automatic redistribution (Steps 5.1 and 5.2) will be removed from meetings.

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

The administrator of TrueConf Server can check, when temporary PRO licenses will expire, and allocate 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 licenses available on your server will be taken.

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

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 PRO licenses are available.
3. In total, four users are authorized on the server (each one is authorized on a single device).
4. A user (this person`s login will be ***user***) takes part in a single group conference.
5. In the **PRO Licenses** section of the TrueConf Server control panel, the administrator will see that 1 PRO license (assigned to the ***user**) and 4 licenses for online users are taken.
6. The PRO license will be released by the ***user*** in 24 hours after he/she leaves the conference.

Case 2

1. There are 10 PRO licenses on the server.
2. Permanent PRO statuses are given to the ***IT*** group which includes 3 users.
3. In total, there are 2 users authorized on the server and they do not belong to the ***IT*** group.
4. One of the users from part 3 is taking part in a conference.
5. In the **PRO Licenses** section of the TrueConf Server control panel, the administrator will see that 4 PRO licenses and 2 online user licenses were taken. This result can be explained by the fact that permanent licenses are always reserved (given to three users from the ***IT*** group), and one temporary license is given to the conference participant mentioned in Step 3.

6. In this case, 6 PRO licenses will be available to other users. These licenses will be given automatically as it was described above.

Case 3

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

5.3. SIP/H.323/RTSP connections

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

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

Case 1

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

Case 2

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

5.4. Guest connections

Public conferences (webinars) can be joined by guests or the users who are not registered on your server. The number of such participants is determined by the number of guest

connections supported by your license. TrueConf Server Free supports 1 guest connection.

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

Example

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

6. Installation and update. 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	• Up to 200 online users connected via TrueConf client apps. • Recording or streaming of one video conference of any type.	• Up to 1,000 online users connected via TrueConf client apps. • Recording or streaming of one video conference of any type.
	Plus	
	• 1 all-on-screen conference for up to 36 participants connected via TrueConf client apps. or • 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 • 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 • Up to 25 WebRTC participants on screen in conferences of any type.	• Up to 3 all-on-screen conferences for up to 36 participants connected via TrueConf client apps. or • 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 • 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 • Up to 36 WebRTC participants on screen in conferences of any type. or • Up to 20 SIP/H.323 endpoints on screen in a conference of any type.

<table>
<tr><td rowspan="2"></td><td>or
• Up to 10 SIP/H.323 endpoints on screen in a conference of any type.</td><td></td></tr>
<tr><td colspan="2">Other examples of typical configurations →</td></tr>
<tr><td>GPU-based hardware acceleration</td><td colspan="2">With NVIDIA Quadro P2000 (or a comparable graphics card), you can add 20 individual layouts for SIP/H.323 participants without changing other hardware.</td></tr>
<tr><td>Operating system</td><td colspan="2">Dedicated or virtual 64-bit operating system:
• Microsoft Windows Server 2012/2016/2019/2022 (including Core editions) with the latest updates installed
• Debian 11 / 12
• CentOS Stream 9

We do not recommend using vCPU overcommitment when deploying TrueConf Server on a VM (i.e., the number of vCPUs should not exceed the number of CPU threads on the host machine). To learn more about the recommendations for a VM, read this article.

i As part of configuration and setup services, we can deploy TrueConf Server on enterprise OS distributions that are not officially supported, such as Oracle Linux, Red Hat Enterprise Linux, Rocky Linux, etc. For more details, contact us in any convenient way.</td></tr>
<tr><td rowspan="2">RAM</td><td>16 GB</td><td>32 GB+</td></tr>
<tr><td colspan="2">When installing memory modules, follow the motherboard manufacturer's guidelines on how to maximize performance (such recommendations are usually provided for server hardware). Otherwise, as a general rule, we recommend using all memory channels available on the motherboard, in other words, you need to install at least one RAM stick for each channel.</td></tr>
<tr><td>Hard drive</td><td colspan="2">20 GB of free space</td></tr>
<tr><td>Network</td><td colspan="2">Ethernet 1 Gbit/s</td></tr>
<tr><td>Ports</td><td colspan="2">• 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.
If this port is closed, the following TrueConf client application features won't be available: meeting scheduler and real-time meeting manager.</td></tr>
</table>

	• **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. Optimizing swap file usage

General recommendations for swap size on Windows and Linux:

Amount of installed RAM	Minimum swap amount	Recommended swap amount without hibernation	Recommended swap amount with hibernation
2-8 Gb	1-2 Gb	1 x RAM	1.5 x RAM
8-64 Gb	4-8 Gb	0.5 x RAM	1 x RAM
64-256 Gb	4-16 Gb	4-16 Gb	1 x RAM
>256 Гб	4-32 Gb	4-16 Gb	1 x RAM

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

- There is no single parameter for using swap depending on the percentage of RAM which is being used.
- One should not rely on the mistaken belief that having a lot of RAM (e.g., 128 GB) means that you can do without swap: this file is an important part of memory management logic in the OS.
- The use of swap is determined by the `vm.swappiness` parameter in the system file `/etc/sysctl.conf`. This parameter essentially represents the ratio between anonymous and physical memory pages. Physical pages correspond to files and their parts in the file system (typically, the code of running programs). Anonymous pages are dynamically created data (for example, variable values).
- Reduction of `vm.swappiness` prioritizes anonymous memory over physical memory which decreases the use of swap.
- By default, the value `vm.swappiness = 60` works well on standard machines (with 8-16 GB of memory). However, machines, where TrueConf Server is installed, have more RAM, so it makes sense to choose a different value.

* To learn more about swap in Linux, refer to the Red Hat website.

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

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

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

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

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

6.3. 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.

6.4. 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 purchased a paid license, there is no need to open the port, and you will be able to register the software in offline mode.

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

6.4.1.1. 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.

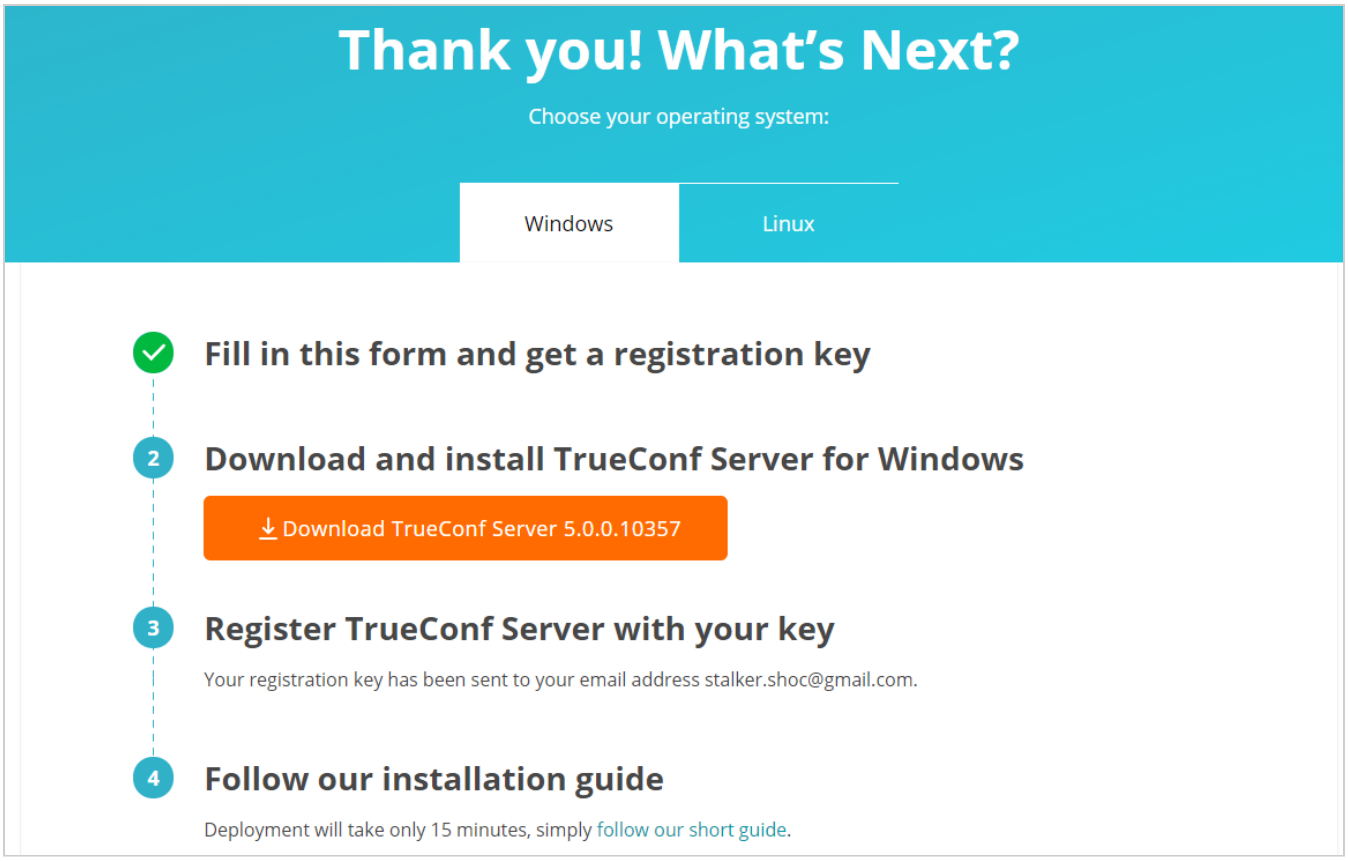
- **TrueConf Database** is a PostgreSQL database server service. The database stores chats and logs. The TrueConf Database service will not start if the TrueConf Server Manager service is not enabled.
- **TrueConf Web Manager** is responsible for the operation of the TrueConf Server control panel, guest 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.

6.4.1.2. 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.

6.4.2. For Windows

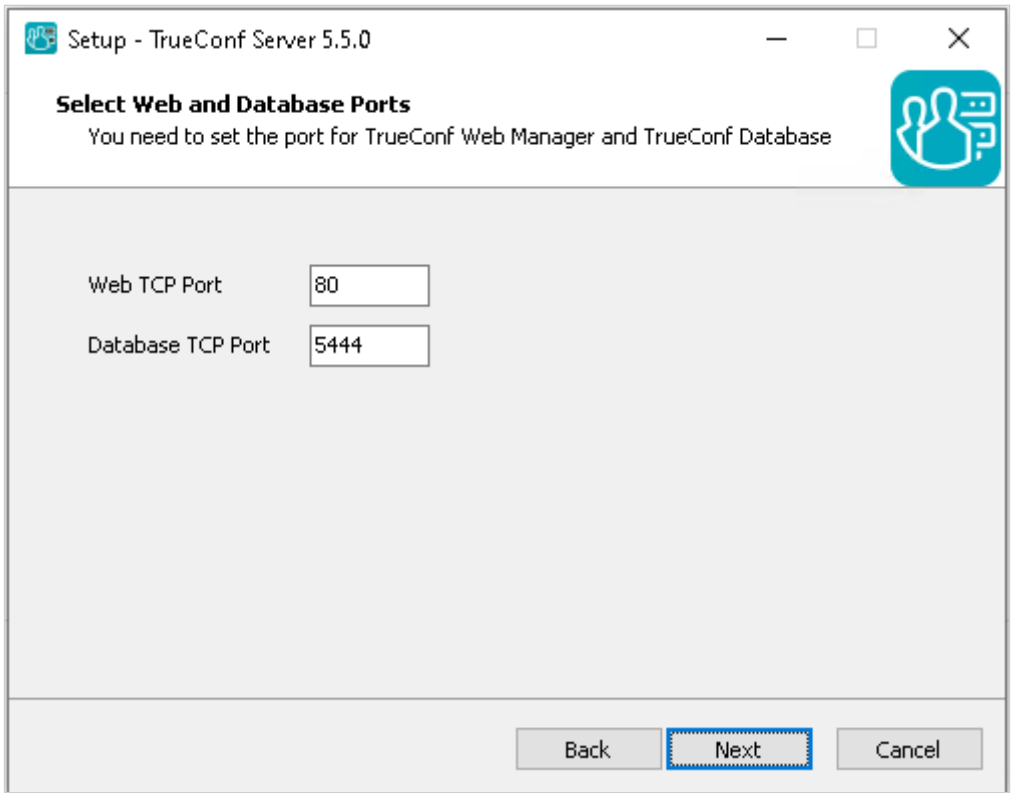
After filling out the form, open the **Windows** tab and press **Download TrueConf Server**.



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

During the installation you can specify:

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



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

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

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.

6.4.3. For Linux

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

- Debian
- CentOS Stream

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.

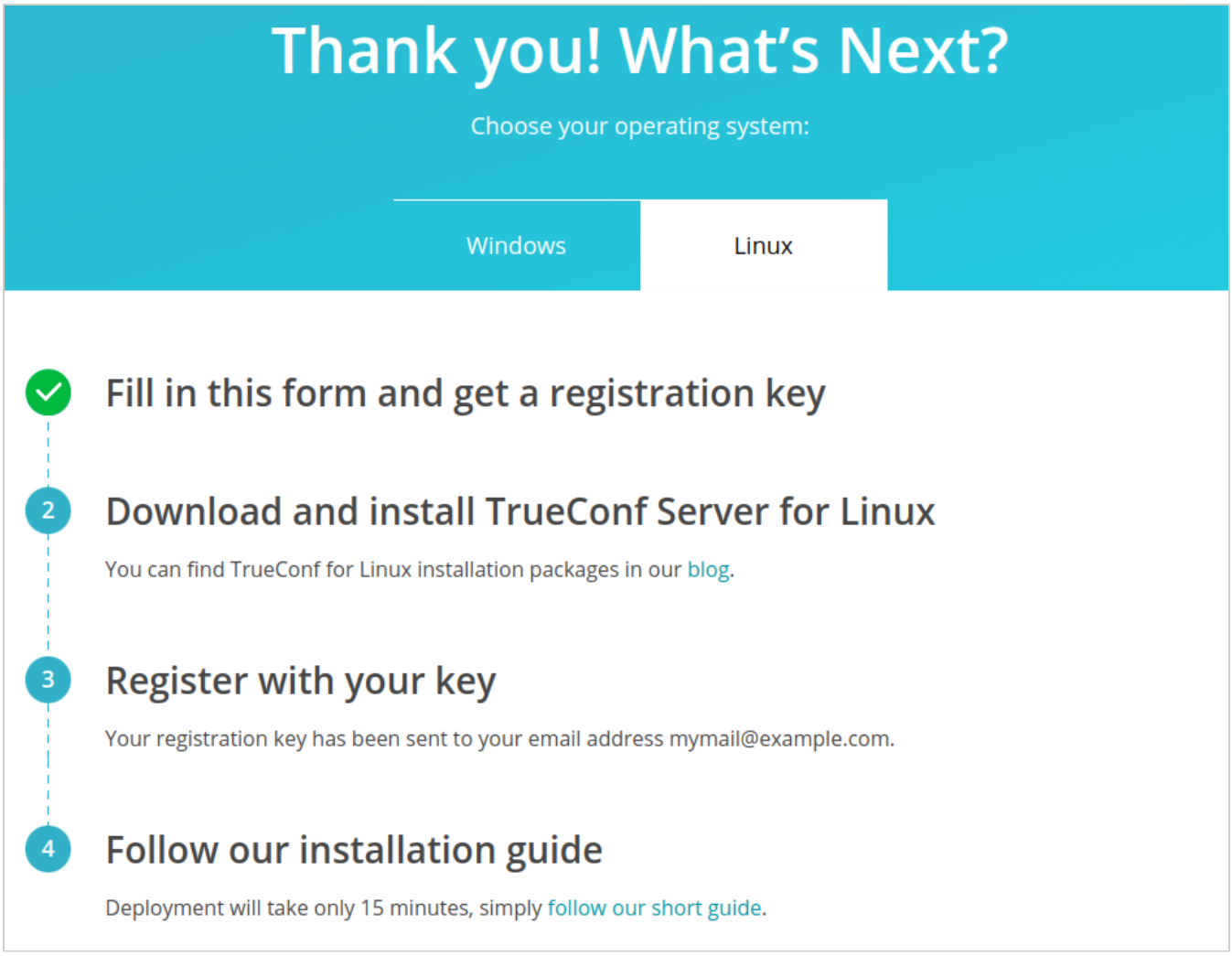
Add the user who will install TrueConf Server and get access to the TrueConf Server control panel to your OS. You can use the account that was created when installing your OS.

! 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.

***** Refer to the detailed installation guide in our blog to learn how a user can be created in Linux.

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.



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

Step 3.

Download the distribution for your operating system.

Step 4.

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

For Debian:

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

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:

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

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

```sh
dnf install epel-release
```

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

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

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

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

Or

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

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.

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`).

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

Since 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.

6.4.4. 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:

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

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

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

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

For Linux OS

> *i* 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:

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

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

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

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

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

6.5. Video conferencing server update

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

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

For more details about updating TrueConf Server, refer to this article.

6.6. 🆘 How to solve typical installation issues

6.6.1. `gnupg` error when installing from the repository on Debian

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

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

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

In this case install the missing package with this command:

```sh
sudo apt install gnupg2
```

6.6.2. Administrator login input error during installation

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

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

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

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

Since you will clear the data about socket settings saved in the OS, refer to the official documentation for more details.

Next, restart installation from the first step.

6.6.3. Unable to access the control panel

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

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

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


Refer to our knowledge base to learn how one can solve the problem with access to the control panel.

6.6.4. What are the default login and password of the administrator?

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

7. Registration

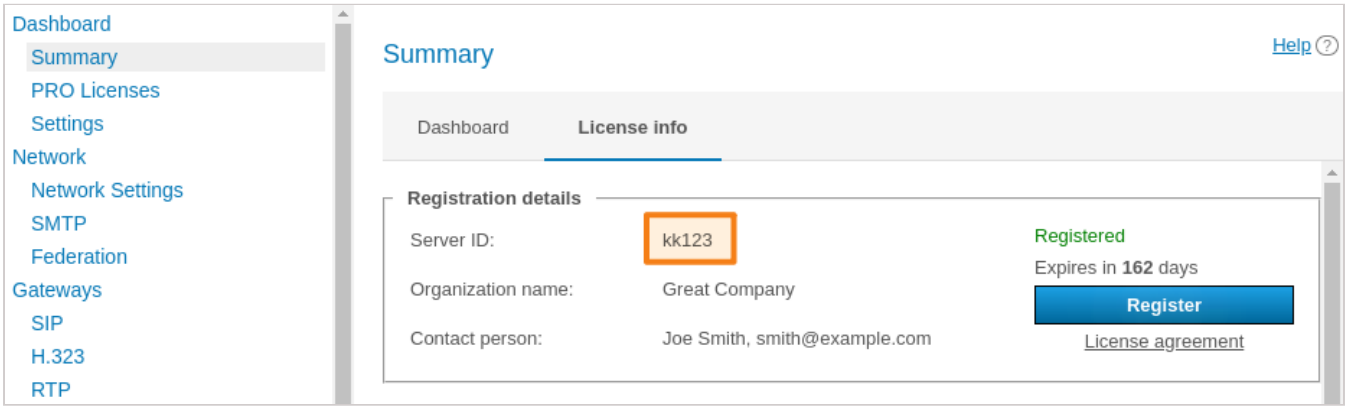
7.1. What is the registration key and server ID?

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.

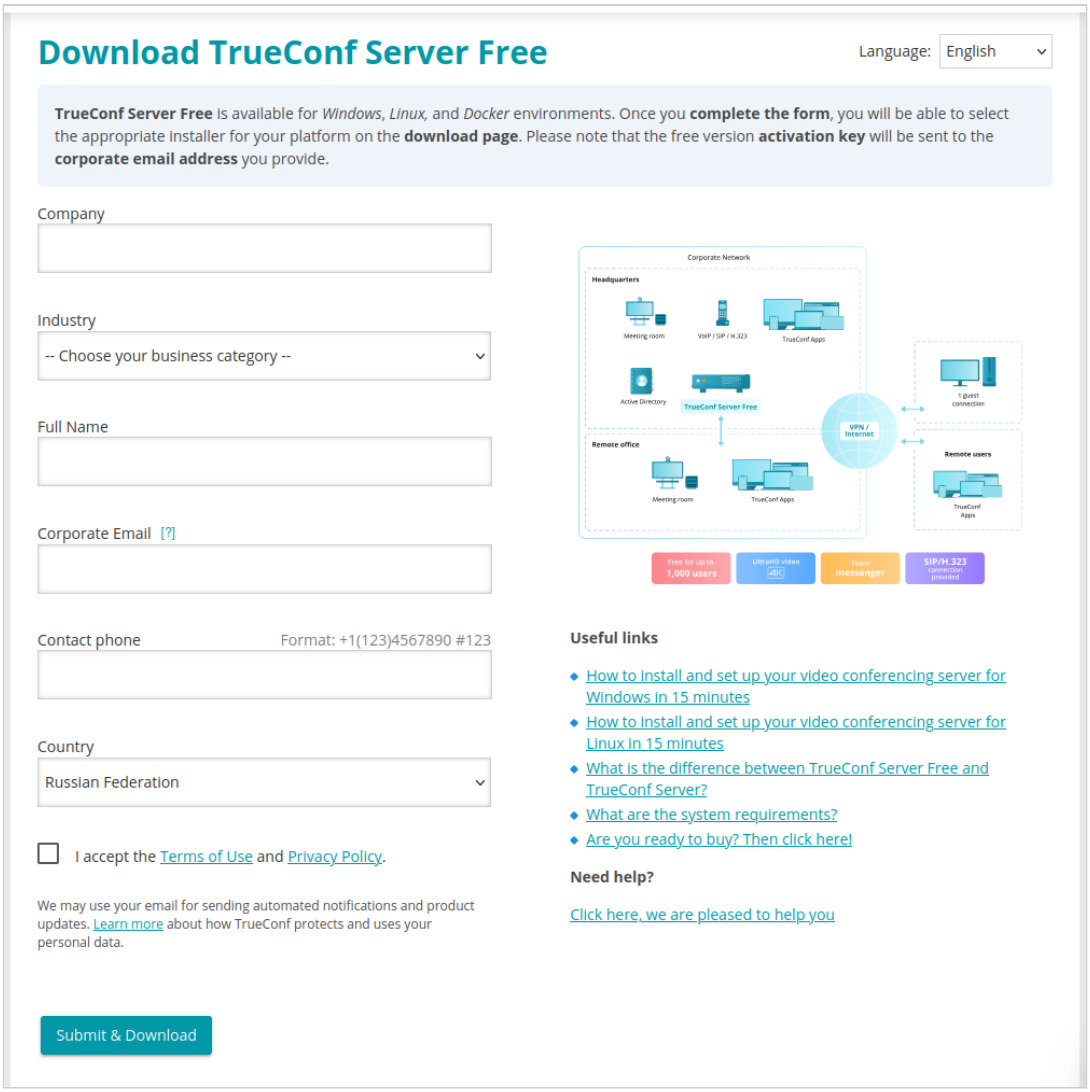
Server ID is the unique identifier of a TrueConf Server instance. The server identifier includes several characters that match the registration key (up to the first hyphen), for example, **EB2MM**. It will be displayed in the TrueConf Server control panel in the **Summary** section:



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:



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.

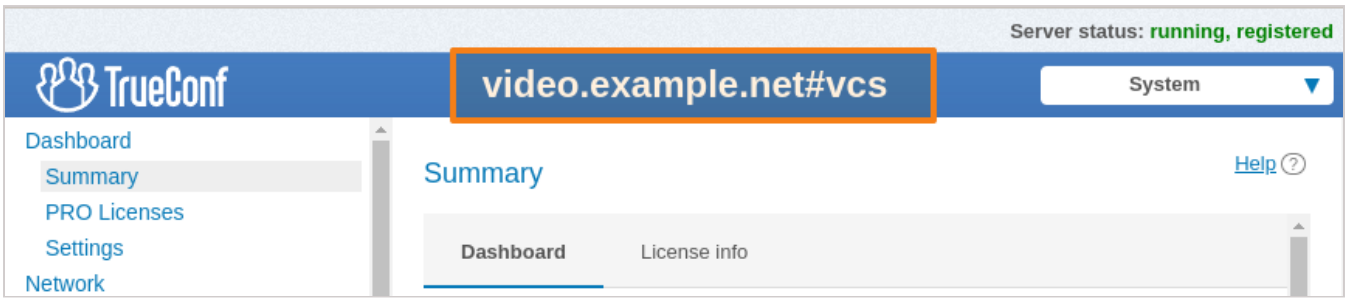
After filling out the form, select your operating system to get access to the corresponding installation guide. When TrueConf Server is deployed, you can register it.

7.2. 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:



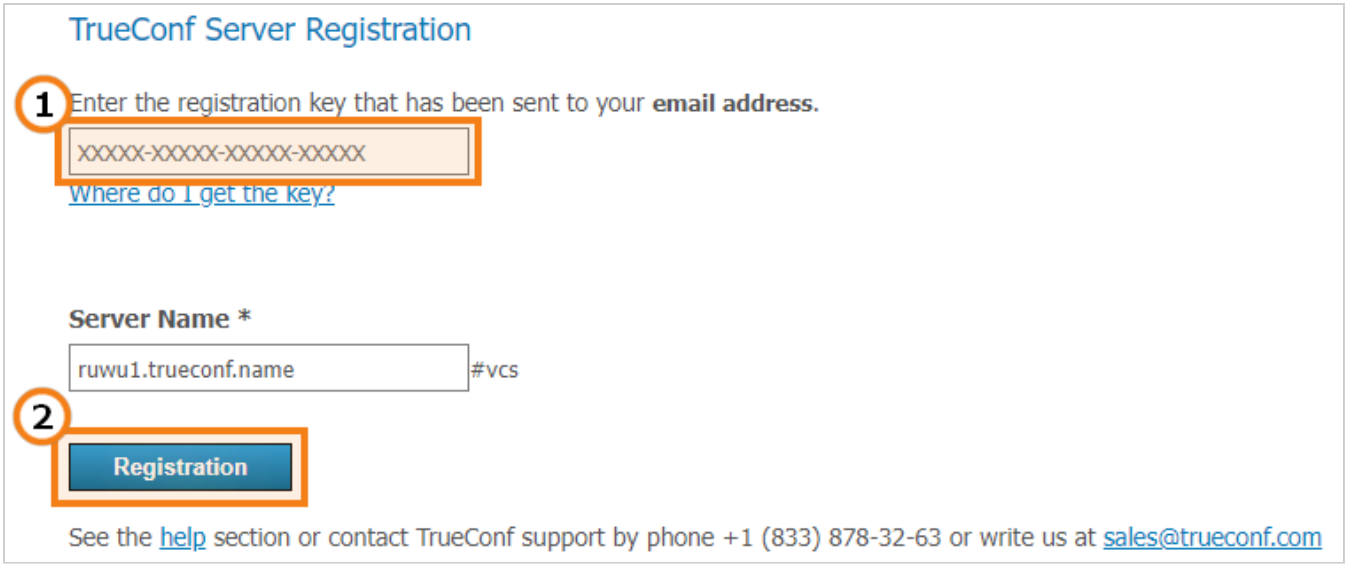
! An IP address cannot be used as the server name.

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

7.3. Registration process

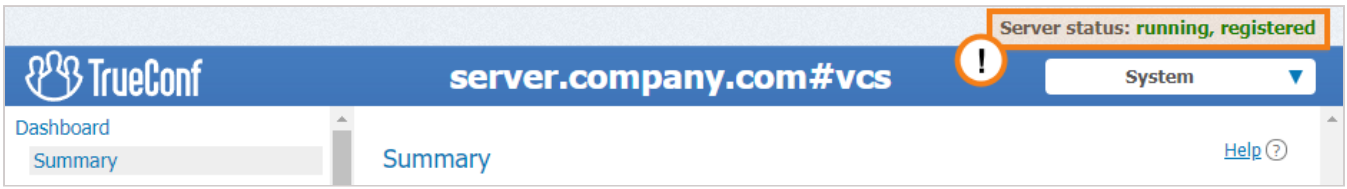
Register the server. To do this, you will need to enter the registration key you have received earlier.

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:



* 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).

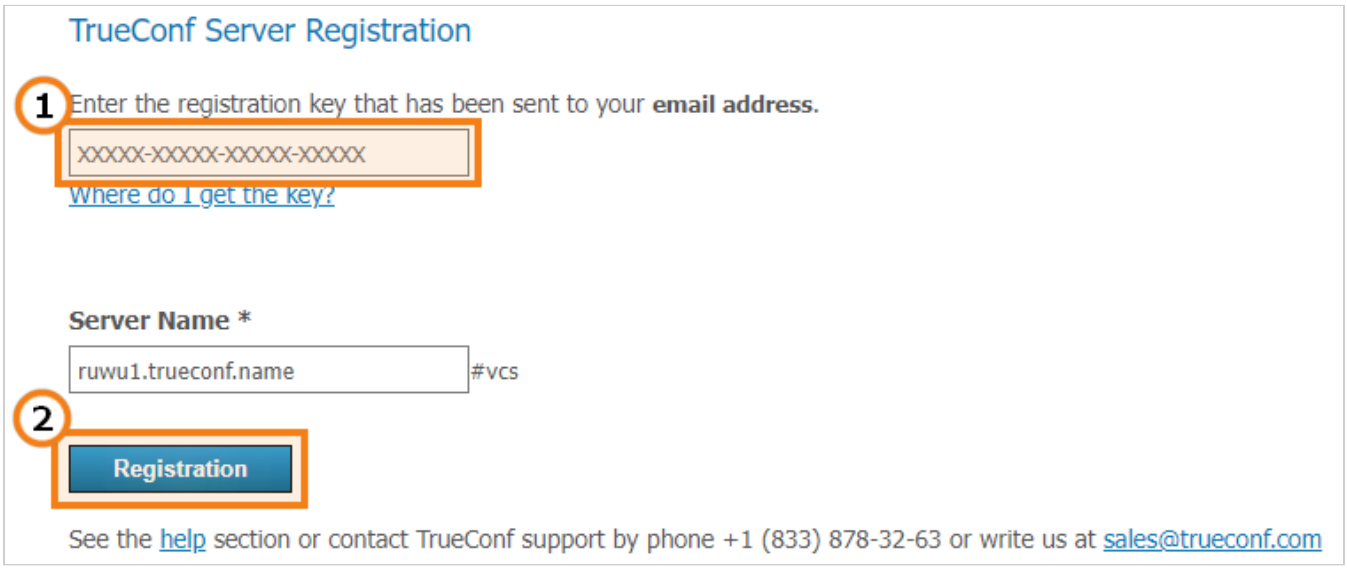
7.4. Offline registration

> *i* 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.

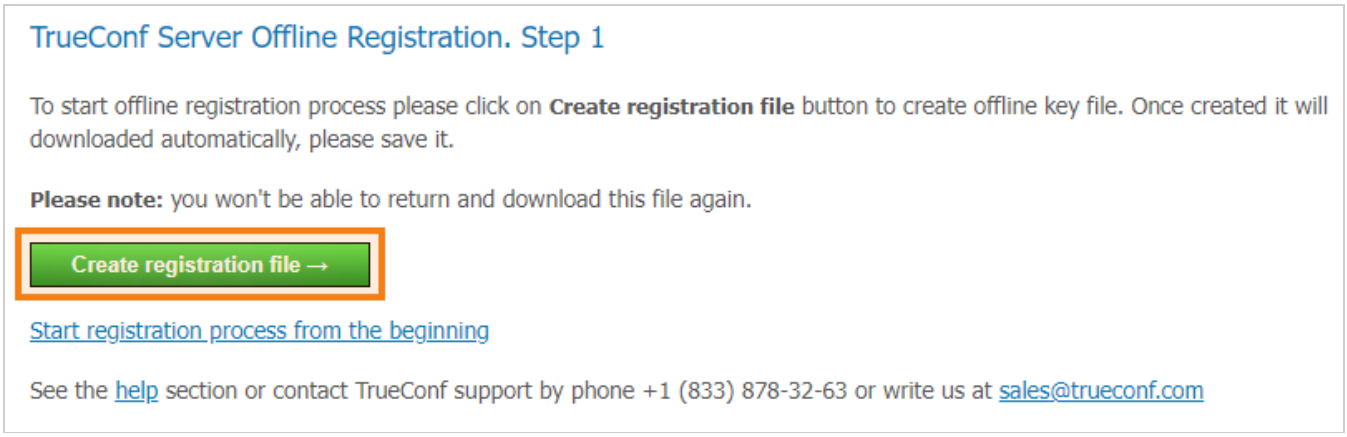
7.4.1. How to register a new server or re-register an existing server after clean reinstallation

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**:



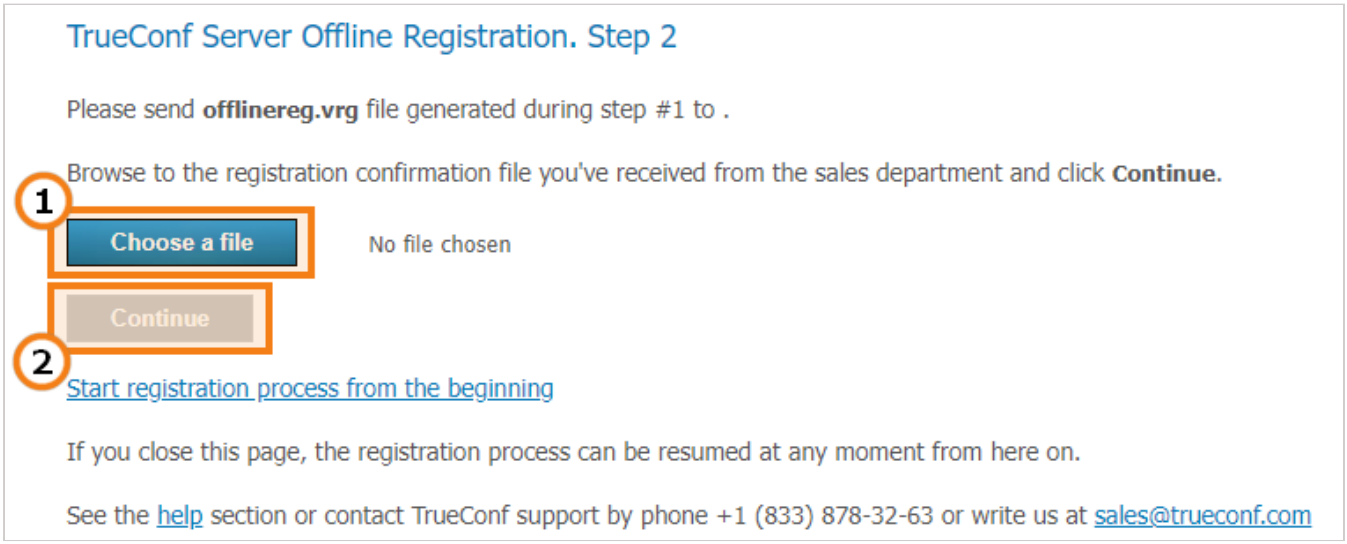
Create registration file button will appear in the registration window. Click on it to generate a file with your registration information:



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 your receive a respond 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**:

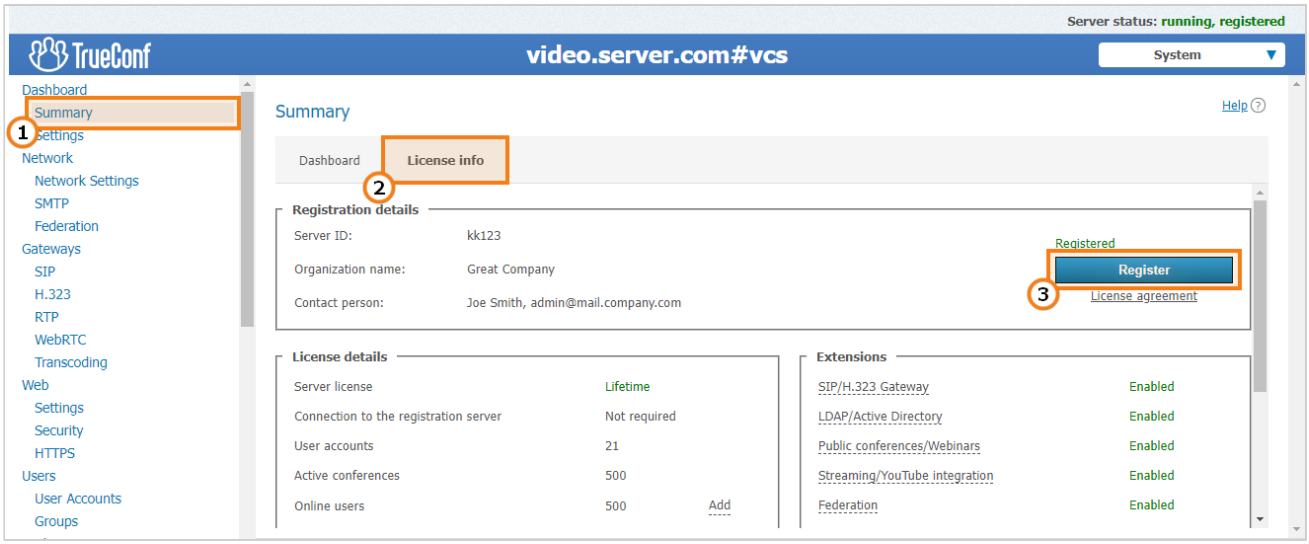


If the offline registration has been successful, you will be notified that TrueConf Server has been successfully registered in the control panel.

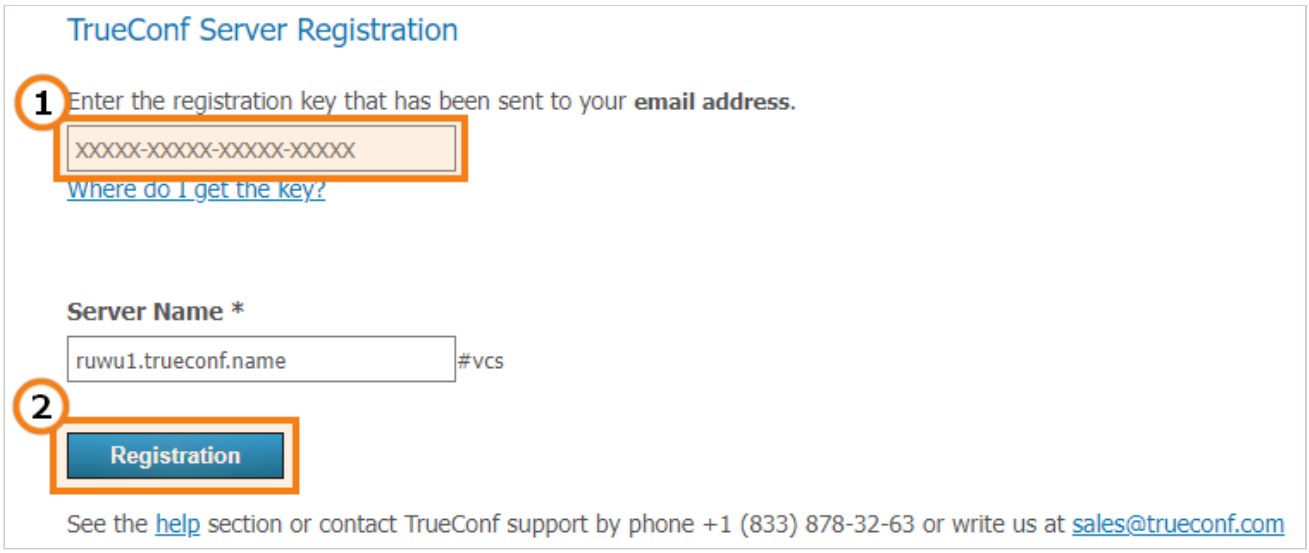
7.4.2. Re-registering the server in a private network

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.

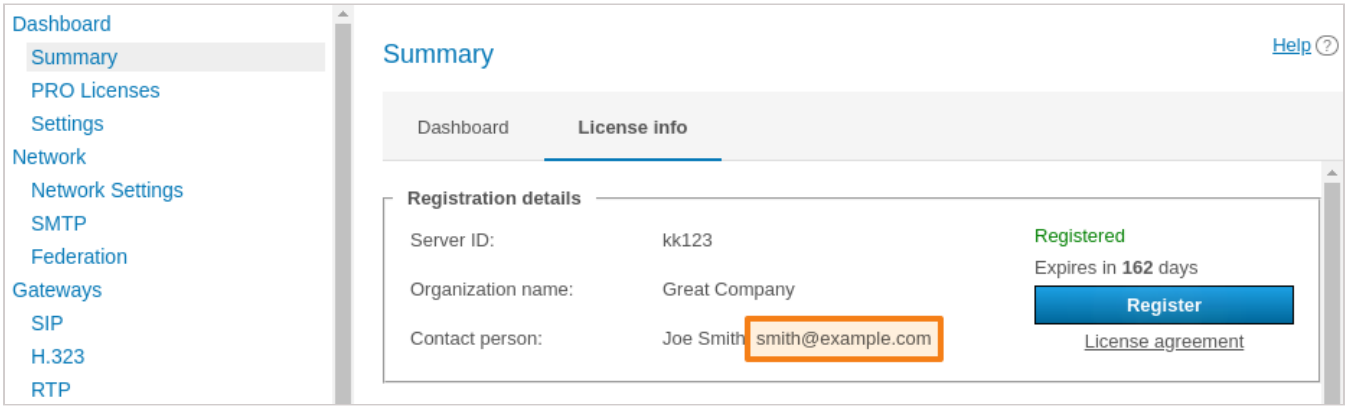
1. Go to the **Summary →License info** section of the server control panel and click the **Register** button:



2. Enter ***your current registration key*** into the appropriate field and click **Registration**:



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:



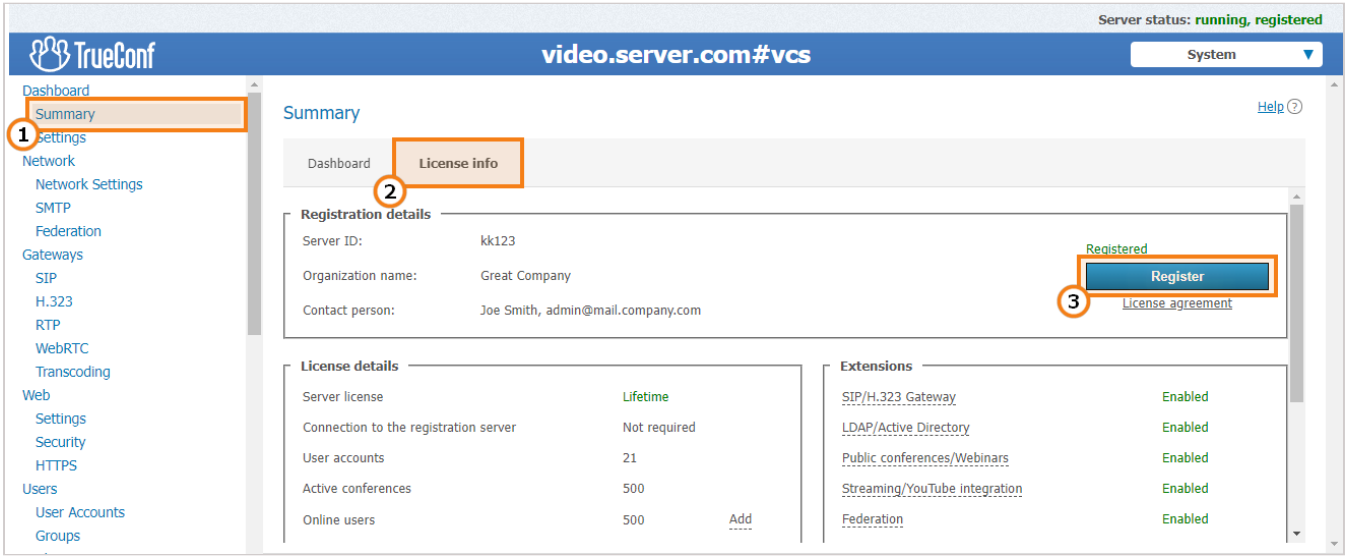
If the email was accidentally deleted, you can request the key from your manager. If you don't have your manager's contact details, just contact us, provide your server ID, and we will help you.

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.

7.5. 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:



7.6. Re-registration with the server name which has already been used

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

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

7.7. 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.

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

* 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.

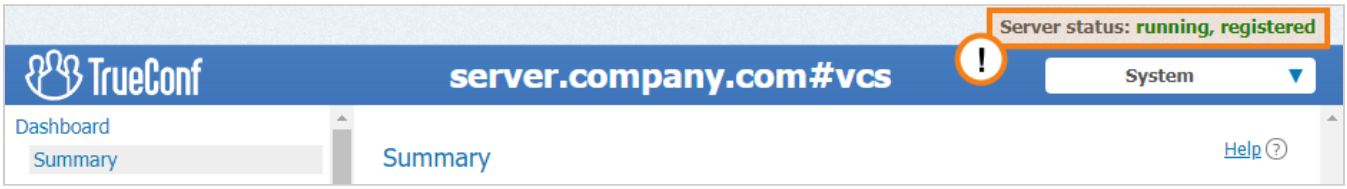
  TrueConf Server does not impose any restrictions on the number of administrators of each type.

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:



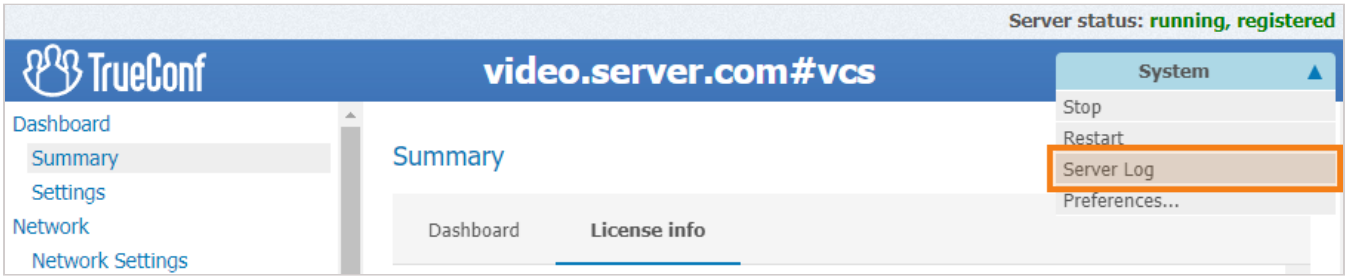
What to do if server is not running?
Stopped status is displayed in the **Server status** string.

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.

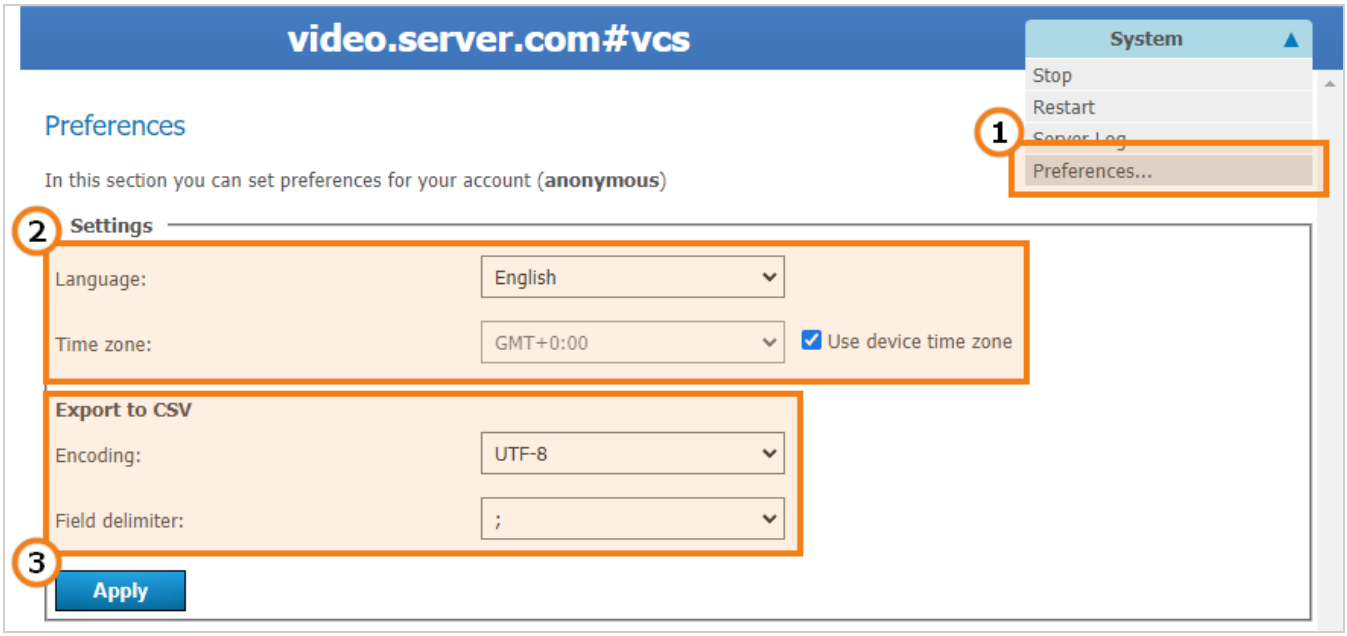


Check **Enable detailed logging** in **Dashboard →Settings** section of the control panel to collect more detailed information in your server logs. Our technical support managers may ask you to do it to ease the troubleshooting process.

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.

If you are using the TrueConf Server version on Linux and change the time zone with the **Use device time zone** checkbox selected, you will need to restart all server services.

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://videoserver.company.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

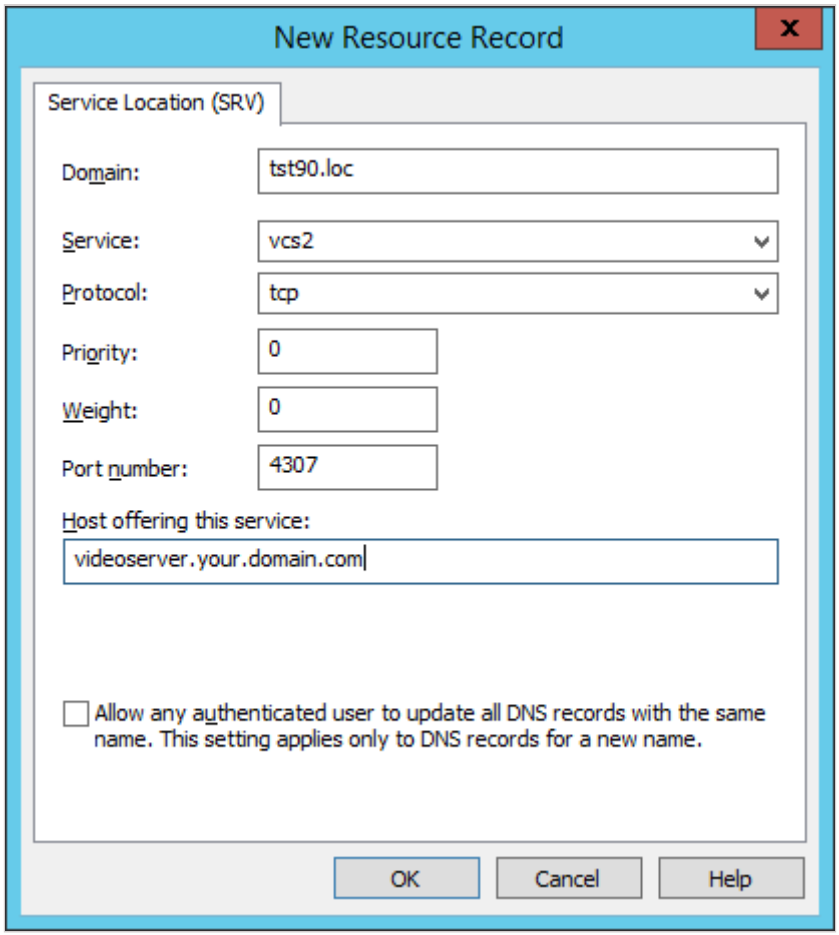
Users can configure connection to TrueConf Server manually. In order to do it, you need to specify the TrueConf Server address and connection port manually in the application network settings menu (or upon the first application launch). You can find detailed instructions on how to connect an application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



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

8.5.3. Configuration of automatic connection to the server by corporate email

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

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

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

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

```sh
vcs2.tcp.[mail-server]. 3600 IN SRV 10 0 4307 [video-server].
```

where:

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

For example:

```sh
vcs2.tcp.mail.example.com. 3600 IN SRV 10 0 4307 video.example.com.
```

For more information about the configuration of this feature and about SRV records, refer to the ***Basic Administration Course*** in the TrueConf certification center.

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.

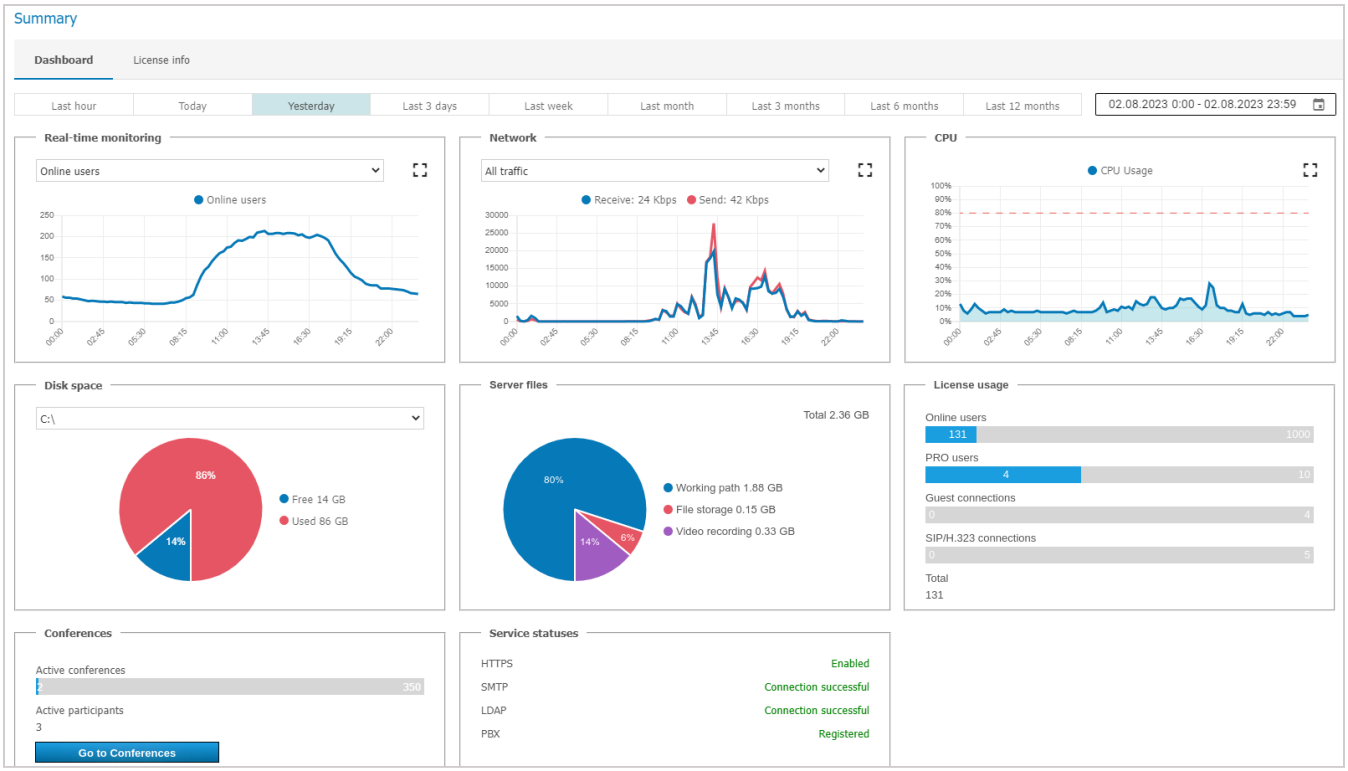
However, you can select any different port after installation both on Windows and Linux. In this case, the port has to be specified in the browser address book right after the colon in the hostname, e.g., `http://localhost:8080`.

9.1. 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:

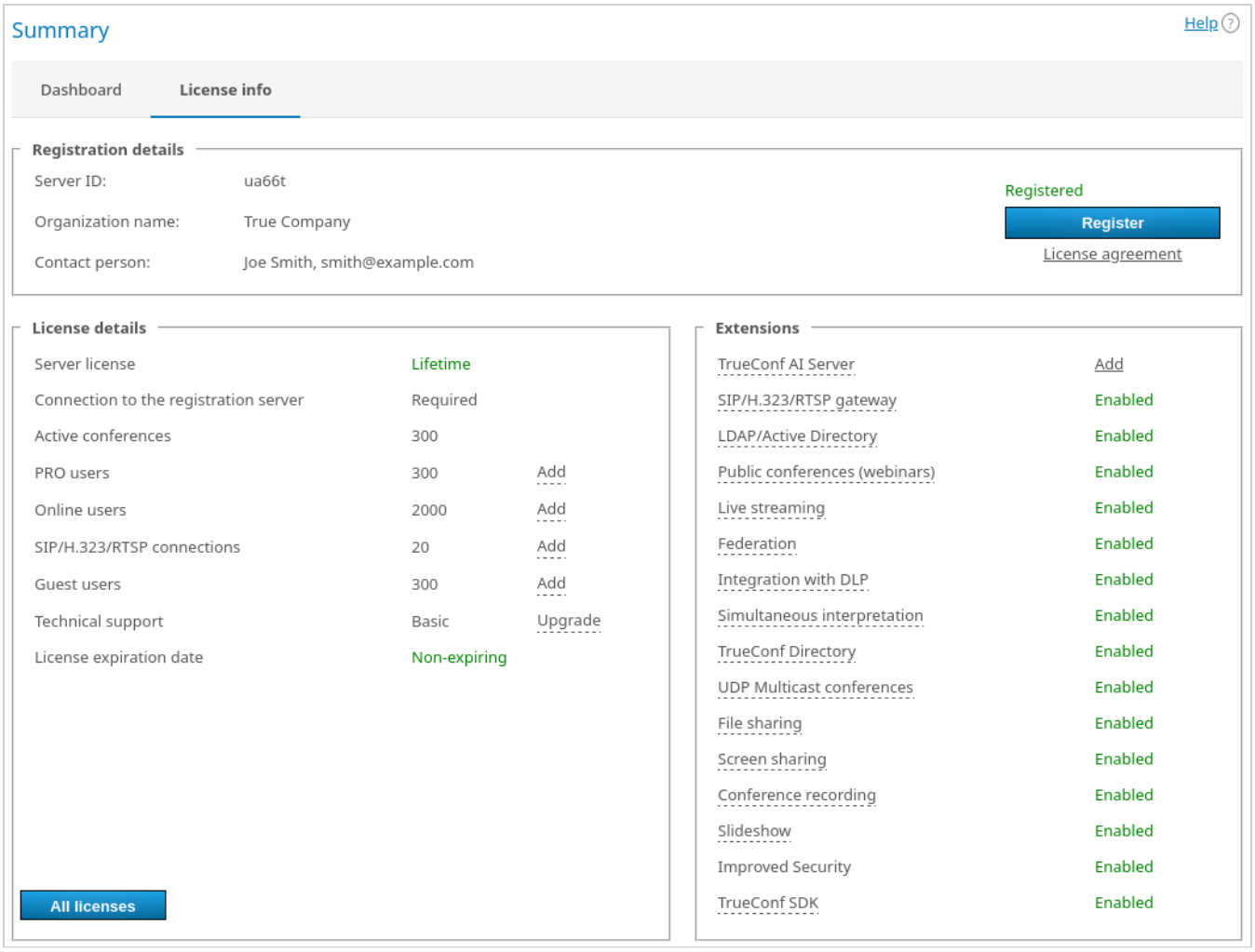
- Real-time performance graphs:
  - CPU usage
  - Network usage (according to the traffic type)
  - Numbers of active conferences and connections of all types
- Available disk space
- Storage space taken by the working directory, chat files and conference or call recordings
- Number of online users, 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 or change the server license with the help of the **Register** button
- Purchase additional features from the **Extensions** section.



By clicking the **All licenses** button, you will open the full list of licenses linked to this TrueConf Server instance. The match is verified by the server ID. Connection to the registration server `reg.trueconf.com` is needed if you want to access this information.

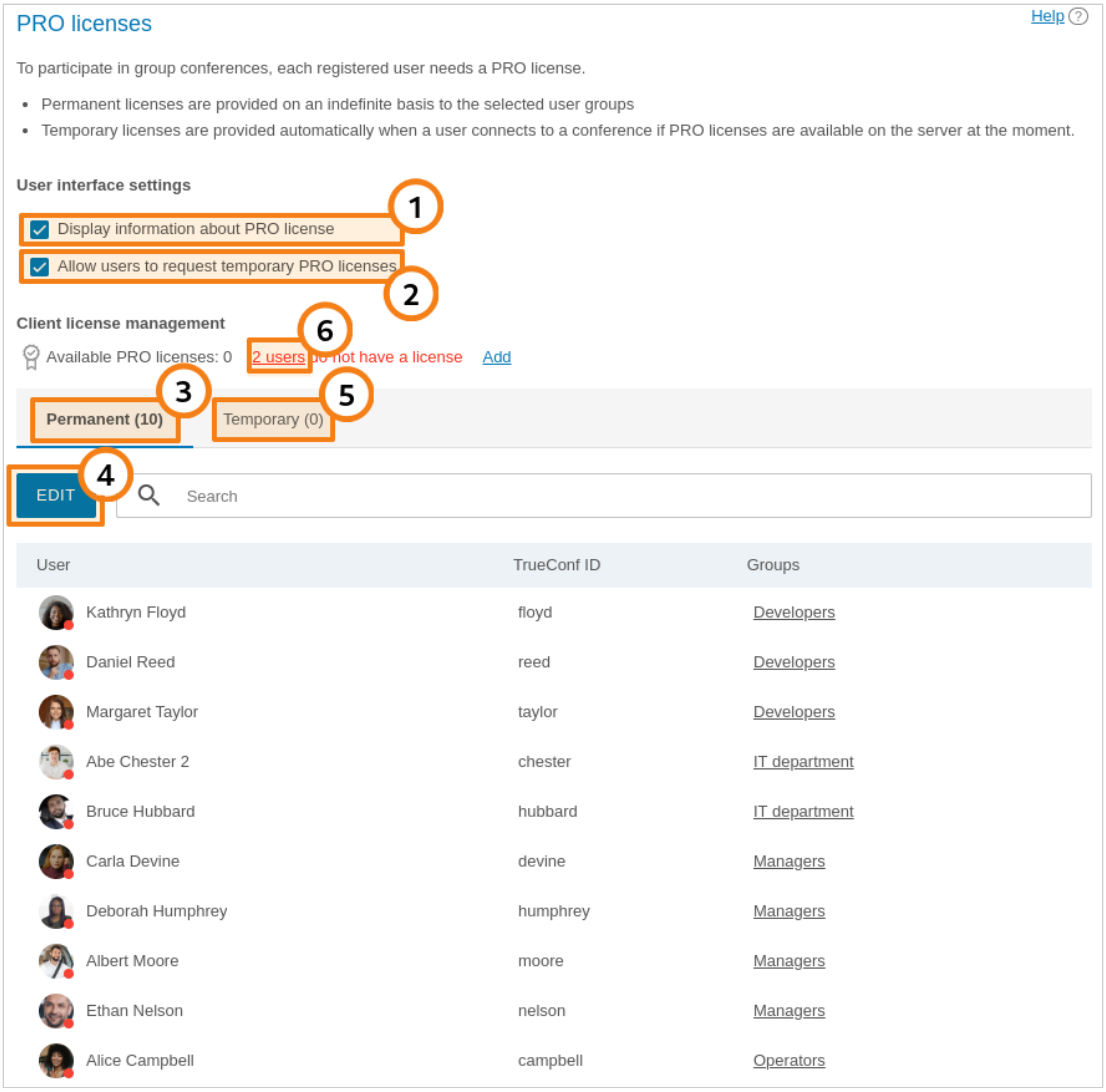
In case of any problems with TrueConf Server registration, the administrator may reach out to TrueConf technical support team via the contacts that will be displayed in case of an error.

! 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.

9.2. PRO licenses

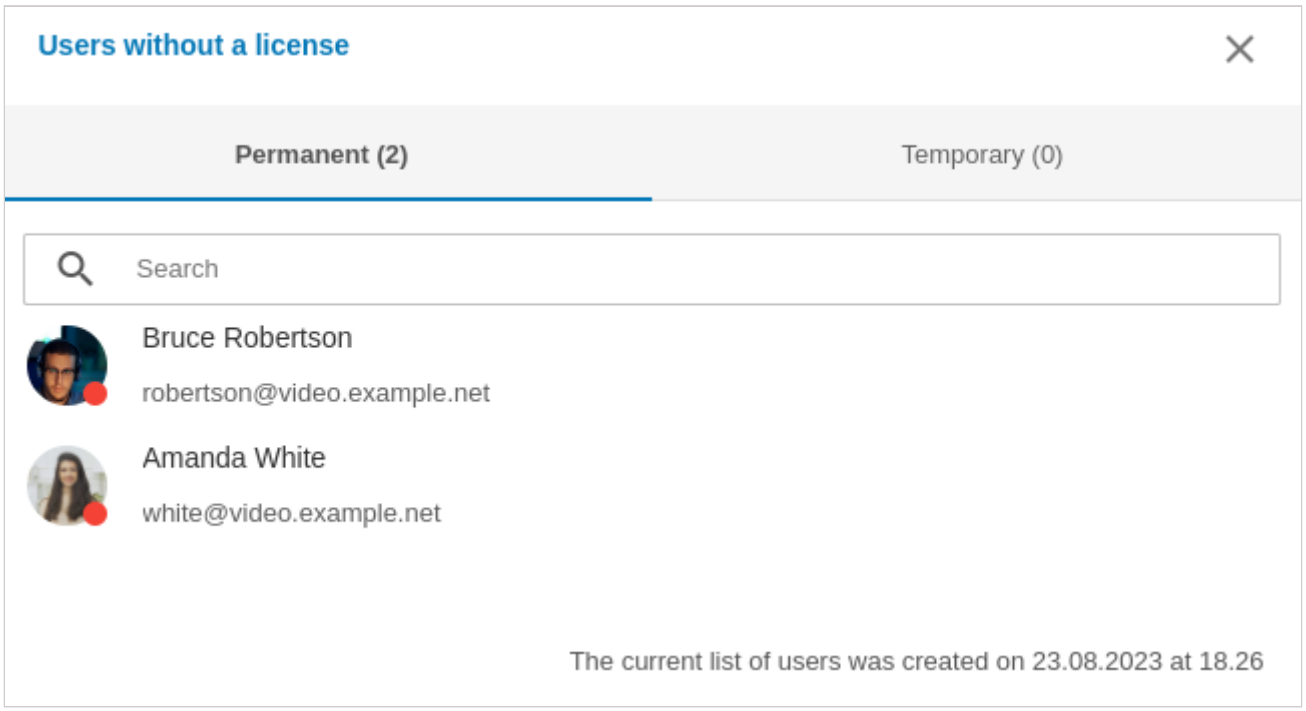
In the **Dashboard →PRO licenses** section, the TrueConf Server administrator can distribute PRO licenses needed for participation in group conferences. The administrator can also view information about the use of these licenses.



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 ✕ 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.

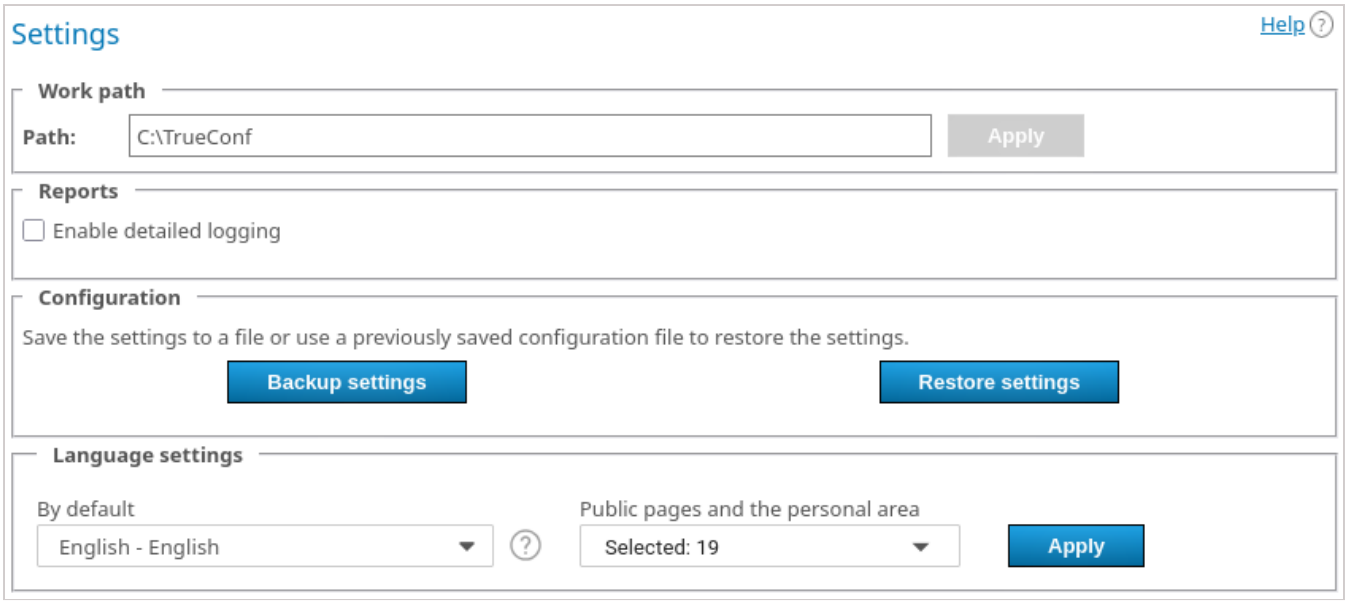
! Please note that the changes in the distribution of PRO licenses are applied either after the server restart or automatically once every 24 hours (check part 5 in the description of license distribution). For example, if a new user is added to the group with permanent PRO licenses, he/she will not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

9.3. Main settings

In the **Dashboard →Settings** section, you can change various parameters of TrueConf Server and some settings of client applications.

9.3.1. Server settings

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



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

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

2. Check the box **Enable detailed logging** to collect detailed information in server logs. Logs may be required when contacting our technical support. This parameter is responsible for the `stdout.log` file.

> * 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. In the **Configuration** section, you can save and restore the backup copy of server settings (to learn more, check below).

4. **Language settings**:

- The language from the **By default** list will be used for email templates (until you select a different language when configuring SMTP notifications), ICS files for adding events to the calendar, page previews on social media, and the connection menu for SIP/H.323 endpoints.
- In the **Public pages and the personal area** list, you can specify, which of the languages supported by the server, will be displayed on the guest page, conference

pages, and in the personal areapersonal area of a user. The **By default** language will always be included in this list of languages.

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

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

Path to `stdout.log`:

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

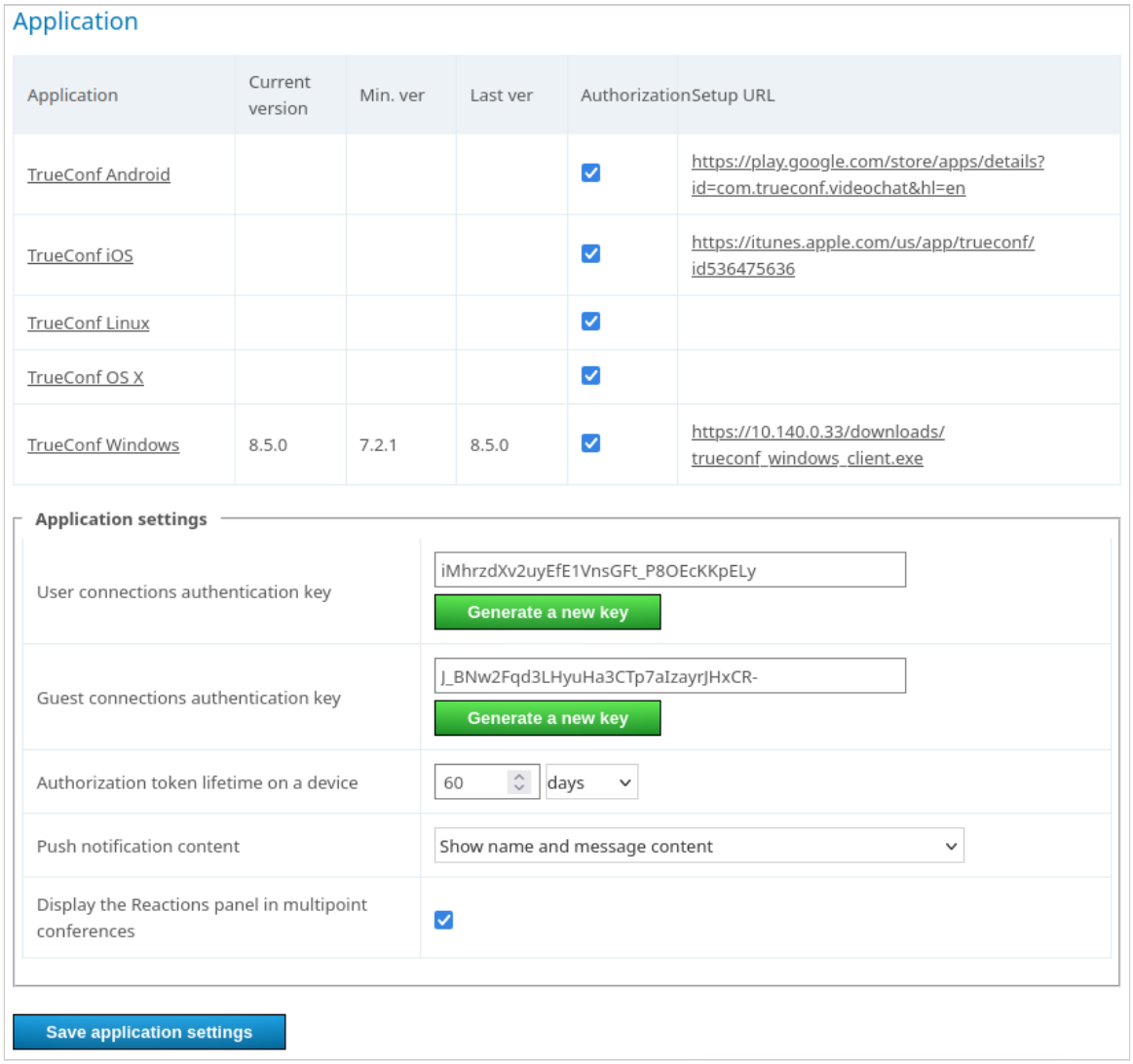
By default, the maximum size of `stdout.log` is 1 GB. When this limit is reached, the file is automatically renamed to `stdout.old.log`, and a new file is created in its place. So, there can be at most 2 main log files of server operation with a total size of 2 GB. The rate at which the file fills up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

Keep in mind that in addition to stdout.log, there are other log files on the server.

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

9.3.3. Applications settings

In the **Application** section, you can change the following settings:



1. TrueConf client applications settings that will be applied when users will be joining your conferences.
2. **User connections authentication key** — used for the generation of session keys, needed for identification of users in a conference. To replace the key, click the button **Generate a new key**. By changing the key during a conference, you can enhance the security of this event (it will be more difficult for unauthorized parties to connect to this event).
3. **Guest connections authentication key** — the key which is similar to the previous one. It controls connection to public conferences via guest accounts.
4. **Authorization token lifetime on a device** determines the duration of the session which starts when a client application is connection to TrueConf Server or a user signs in to the personal area. When the period expires:
5. 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.
6. If a user has been signed in to the personal area, he/she will be logged out after clicking on any button or going to a different section; this person will need to re-authorize according to the current settings.

5. In the drop-down list **Push notification content** you can select the content that will be sent to push notification services (Google, Apple, etc.) and displayed on a user's mobile device. Available options: the message and the sender's name, only the name, or an anonymous notification (both the name and content will be hidden).

6. If you check the box **Display the Reactions panel in multipoint conferences**, users will be able to use special statuses (emojis) during events.

Don't forget to save settings after changing them.

9.3.4. 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.

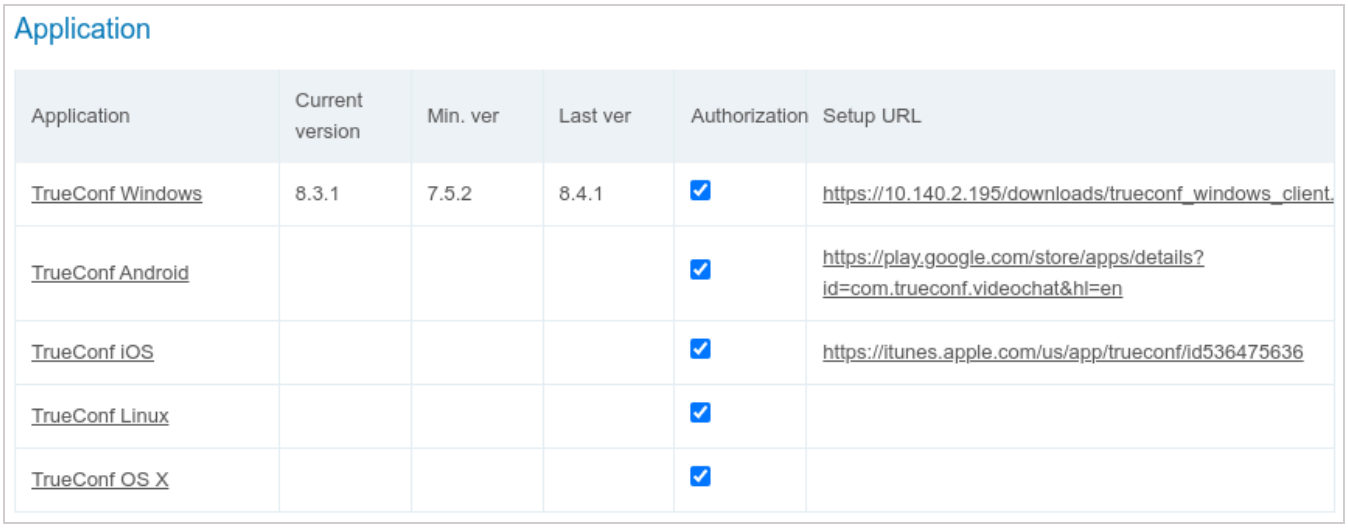
When TrueConf Server settings are saved to a file, the reserve copy of this file will be automatically created in the `[working_path]\registry_backups` folder where `[working_path]` is the working directory of a server. This applies both for Windows and Linux versions of TrueConf Server.

9.3.5. Settings for client application connection

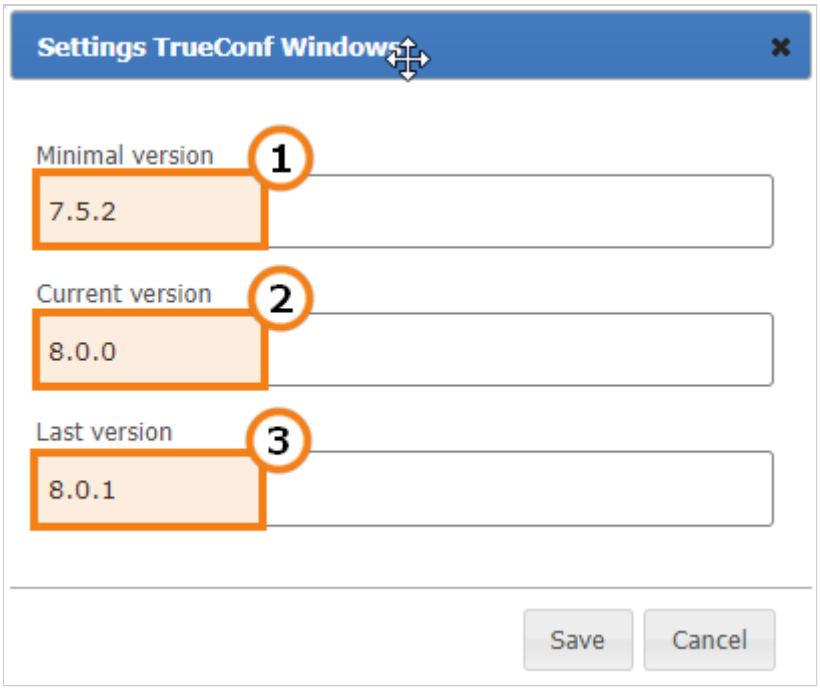
Further down the page, there is a section for configuring restrictions on TrueConf client applications used to participate in calls and conferences held on your TrueConf Server. It is also possible to set separate restrictions for different operating systems: Windows, macOS (previously OS X), Linux,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



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 that 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 then 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.

9.4. How to use other folders on Linux with symlink

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

> *i* 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:

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

- creating a directory for storing files:

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

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

- for recordings

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

- for files

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

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

- copying recordings

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

- file copying

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

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

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

- deleting the directory with files

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

5. Create a symbolic link to the new directory:

- for recordings

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

- for files

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

6. Restart the server main service:

```sh
systemctl restart trueconf
```

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

```sh
unlink [symlink_path]
```

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:

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

9.5. Mounting a network storage on Linux

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

> *i* 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

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

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:

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

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

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

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:


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

* 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:

```sh
mount -t cifs -o credentials=[credentials_path] [remote_path] [local
_path]
```

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`):

```sh
umount [local_path]
```

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:

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

9.6. 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):

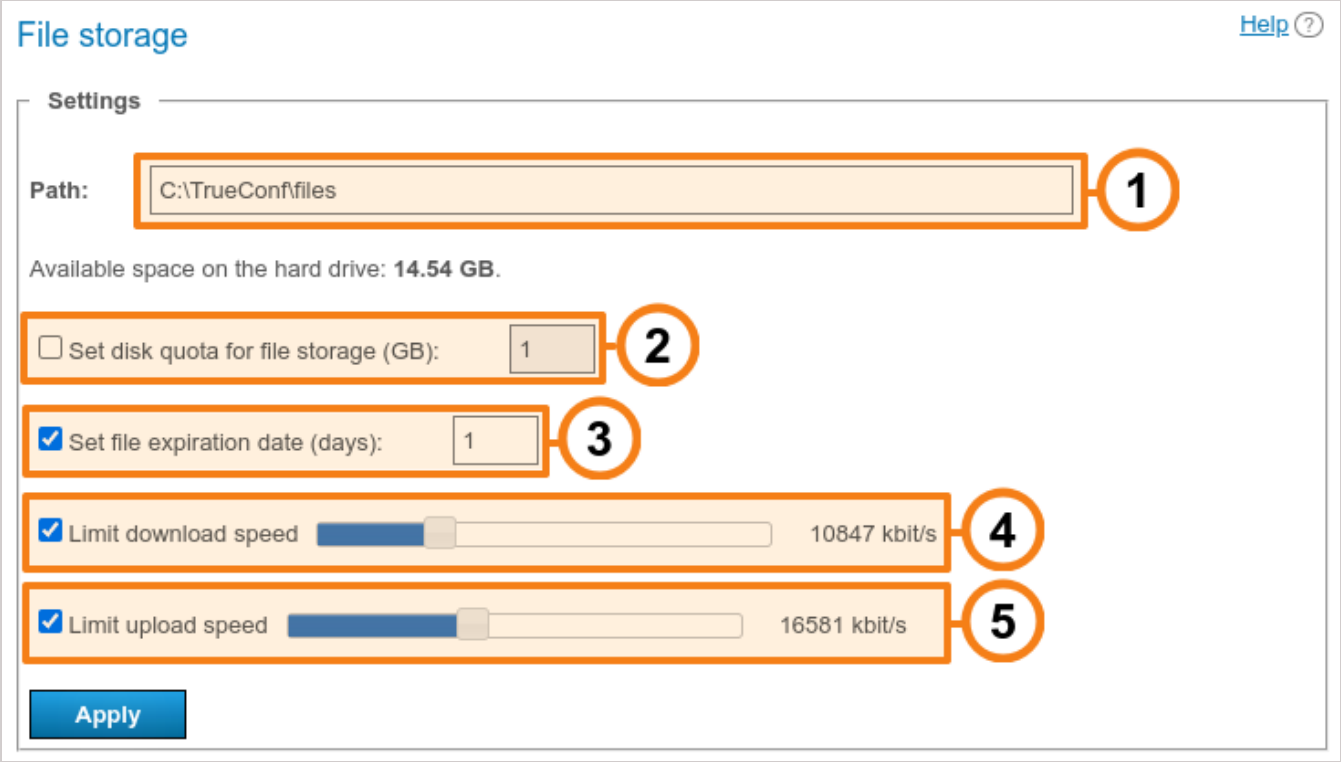
1. Open the list of Windows services. To do it, launch the command prompt (terminal) or PowerShell and run the command `services.msc`.
2. Find the **TrueConf Server** service (the main service of the video conferencing server) in the list.
3. Go to the service properties by double-clicking on the name 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.

9.7. File Storage

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

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

In the **File storage** section you can setup storage settings for files your users are exchanging:



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).

> *i* 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).

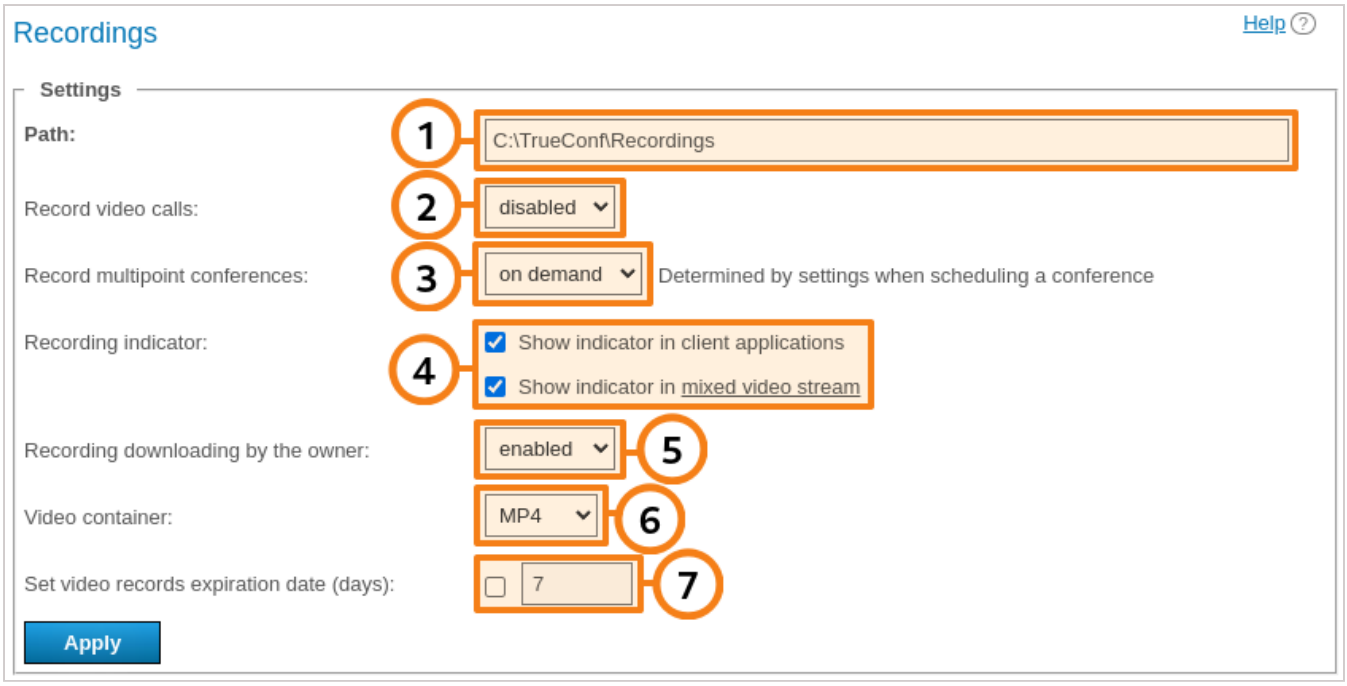
4. Use the slider to set maximum download speed limits to download the files from the server.

5. Use the slider to set maximum upload speed limits to upload the files to the server.

9.8. 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.

i 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 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. Network and federation settings, email notifications

In the **Network →Network settings** section you can configure 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.

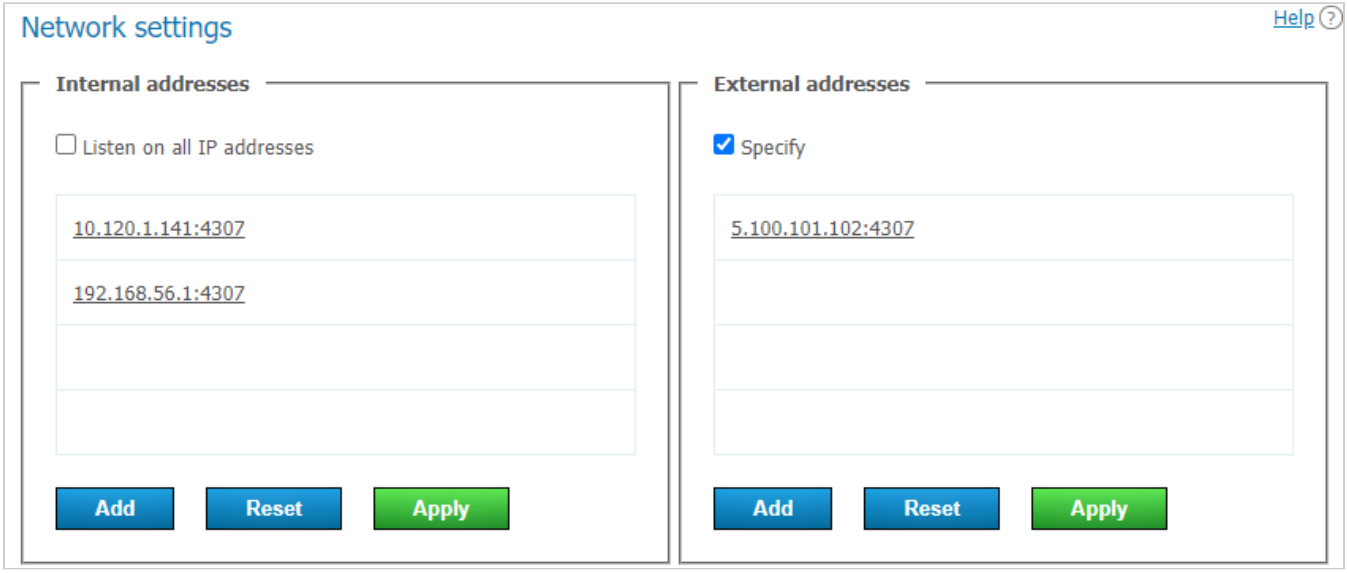
10.1. Network Settings

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

i 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 authentification 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 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.

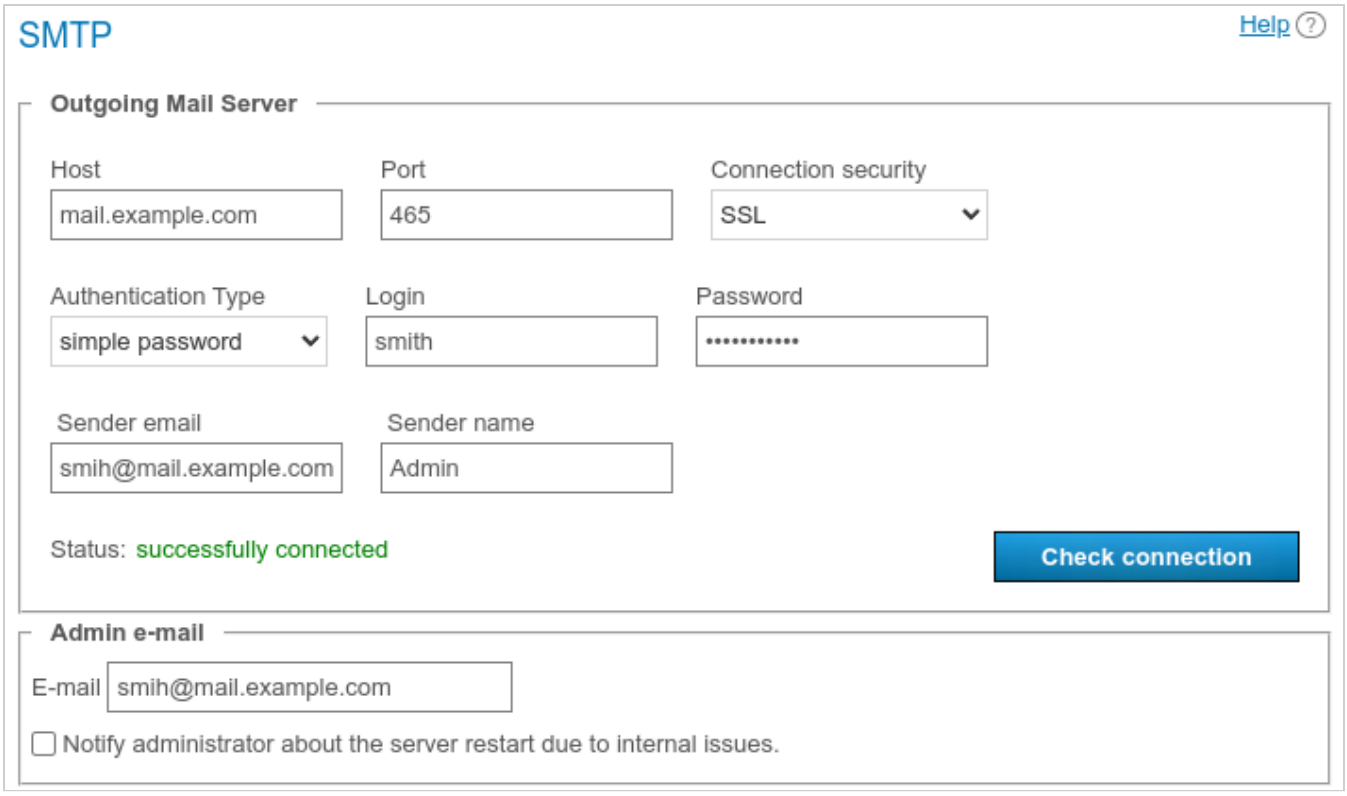
i This guide does not cover TCP port forwarding or DNS names. You can learn more about these topics in your network equipment manuals.

10.2. SMTP (email notifications settings)

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

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

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

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. Confirmations of registration for a public conference

To send notifications about a participant's successful registration for a webinar (this option is available if the corresponding parameter is enabled), use the separate template **Conference registration notification**.

10.2.5. 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.

i 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.

10.2.6. Notifications about conference rescheduling

To notify the participants of a scheduled conference when the start date of this event is changed, check the box **Notification of start time change for scheduled conference**.

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

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

10.2.7. Notifications about the cancellation of a conference

If you want to notify the participants of a scheduled conference that this event was cancelled, check the box **Notification of conference cancellation**. This notification will be sent if:

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

10.2.8. 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.

10.2.9. 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`
  - `%conf_url_app_join` — a link for quick one-click connection via a client application without having to open the conference page. It works as follows: if the link is clicked, when the conference has already started and connection via client applications is allowed, the application installed on the user's device will be launched, and an attempt will be made to connect to the conference. Essentially, it is similar to visiting the conference web page and clicking the button for joining the meeting from a client application. The link looks in the following way: `https://[server_address]/c/CID#app=1`

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

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

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

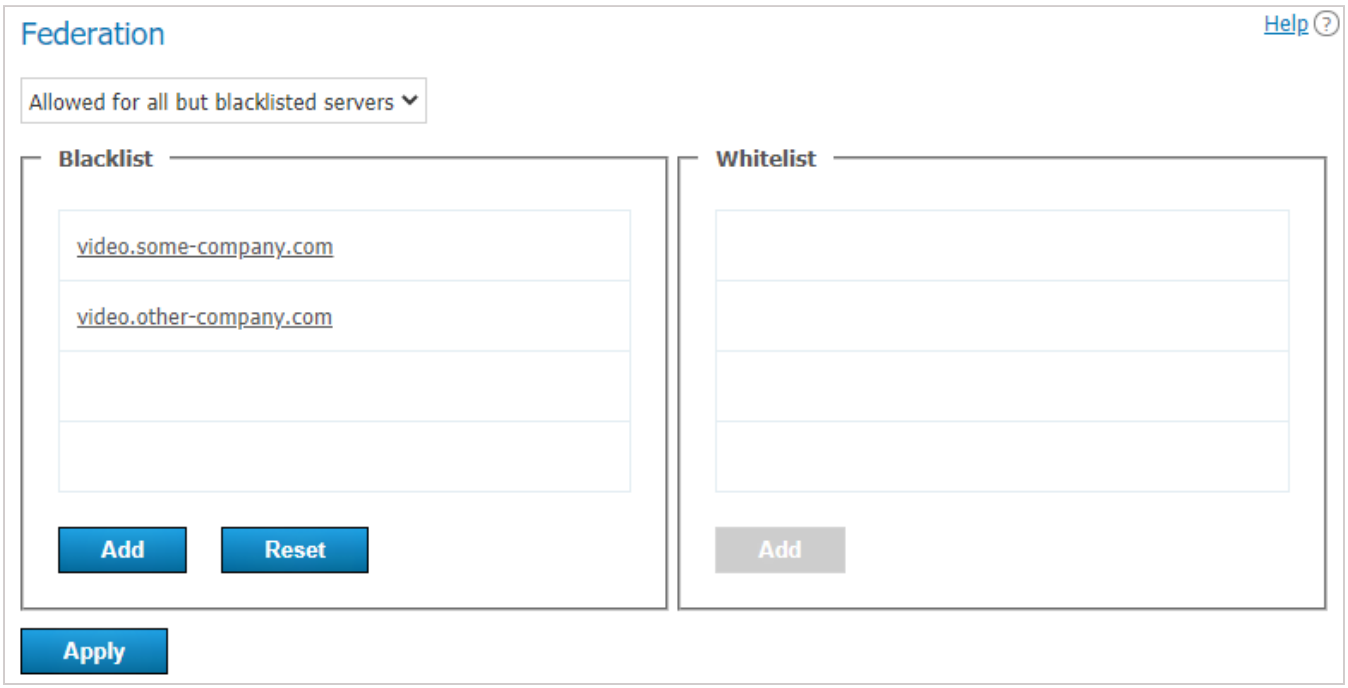
Server administrator contacts parameters:

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

10.3. Federation

Federation mode allows TrueConf Server users to make calls and participate in conferences with users of other TrueConf Server instances. Besides, it enables users from different servers to communicate in chats. Federation is available only in the full version

of TrueConf Server (e.g., when purchasing additional licenses of any type). There is no limit on the number of servers that can be federated. The limits on group conferences will correspond to the limits applied to the TrueConf Server instance which initiated the connection.



Requirements for the correct work of federation:

1. The server has to be registered with an existing DNS name or you have to specify the real server address with the help of DNS SRV records.
2. Each federated server has to be accessible to another server by its DNS (FQDN) name, specified during registration, via the main port for the TrueConf protocol (**4307 is selected by default**). Moreover, it has to be accessible via an HTTPS port (**443 is used by default**). If a different HTTPS port is configured on one of the servers or a different port is selected for the communication protocol, access to this server should be configured via the selected port instead of the standard one.
3. Each federated server has to be available to all users of both servers (whose participation in calls and conferences is expected). Each server has to be accessible via an HTTPS port (**443 is selected by default**) by its domain name which should match the external server name specified during the registration.
4. **IMPORTANT!** If you are using a server which is **below 5.4.0**, it also has to be accessible to all federated users via the main port for the TrueConf protocol (**4307 is used by default**).

* For more information on how a client application can find the server, refer to the section on the configuration of automatic connection.

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

1. In the drop-down list, select the federation mode:
   - **Disabled**
   - **Allowed for whitelisted servers**. 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.

2. Enter the IP addresses or domain names (FQDNs) of the required servers into one of the lists (depending on the federation mode) and click **Add**.

> *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.*`.

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

Let us take a look at some examples.

Case 1

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

1. Add `videoserver.example.com` to the white list
2. Activate federation on the side of `videoserver.example.com` in one of the following ways:
   - Add the domain name of your server to the its white list
   - Allow federation with all the servers that have not been added to the black list (make sure that your server is not added to the black list).

3. Make sure that both servers and client applications connected to them, are accessible to each other by domain names.

Case 2

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

Connection to a conference in federation mode

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

11. 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
- Send [DTMF commands]](#page10-dtmf) to perform certain actions during a conference.

i 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.

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.

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

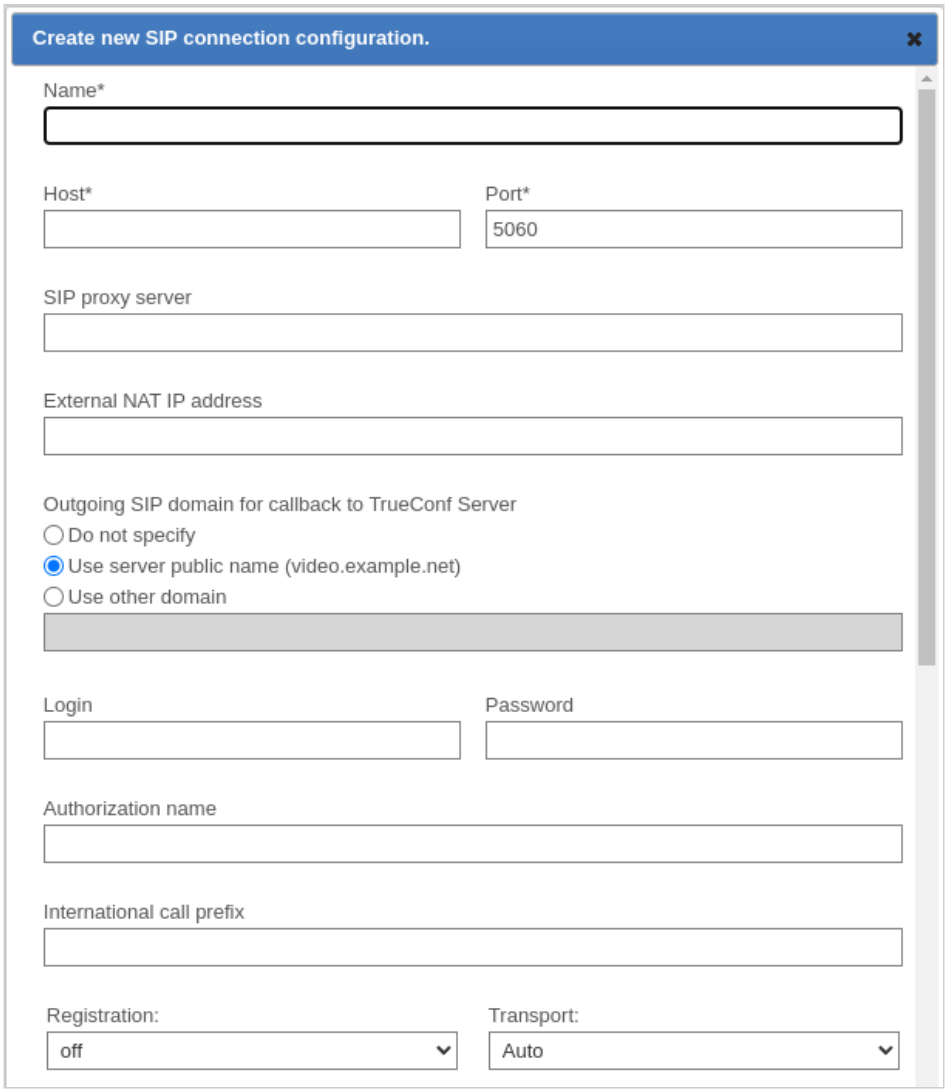
In this section you can create specific rules for certain SIP addresses or call directions. For example, you can use special set of settings to connect to Skype for business servers and another one for PBX connectivity. Every rule is relevant only for target address specified in **Host** field. Every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

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



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.

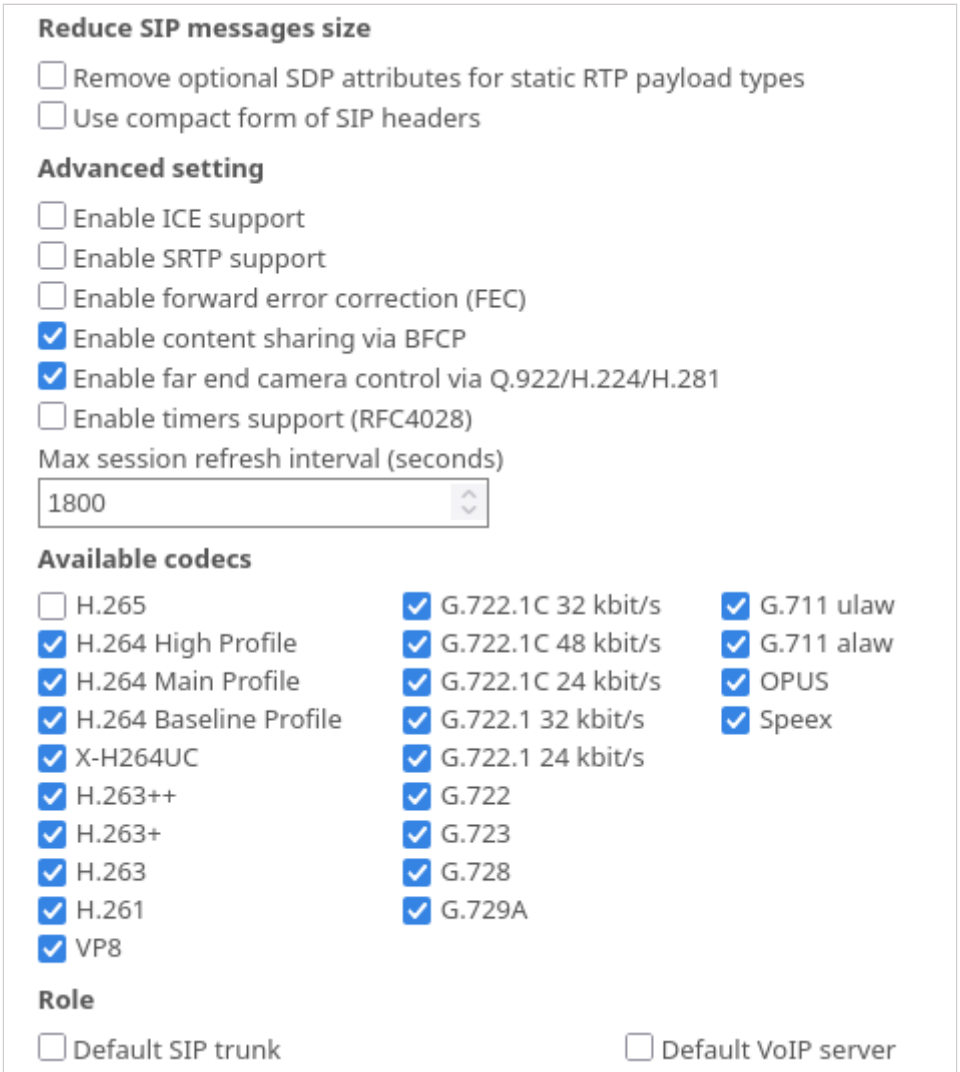
Registration mode defines registration method for the rule:

- **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.

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

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



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).

The box **Enable forward error correction (FEC)** enables you to control the work of error correction when the quality of connection drops in the configured SIP direction. By default, this box is checked, but some devices or MCU servers may not work correctly when this box is checked, and it has to be disabled. If you configure the rules for connecting to TrueConf Group or TrueConf MCU, we recommend leaving the box **Enable forward error correction (FEC)** checked.

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

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.

i 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.

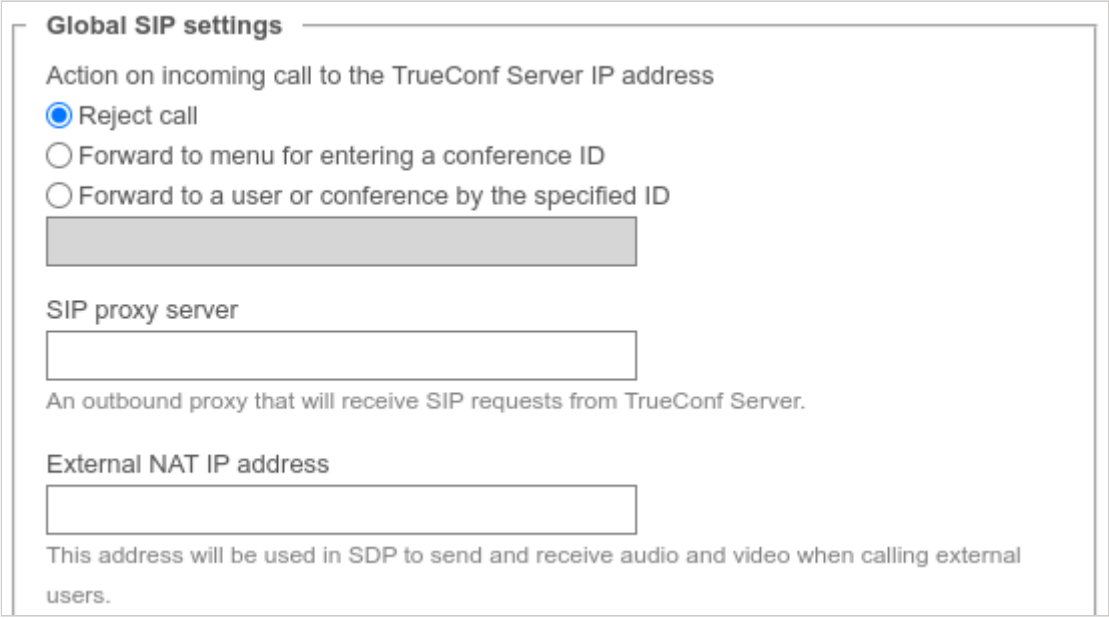
To call Skype for business users from TrueConf client applications, use the following format: `#sip:User`, where `User` is TrueConf username. This user will receive an incoming call from the TrueConf Server account. The same method is used to invite Skype for business users into the conference or add 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.



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`.

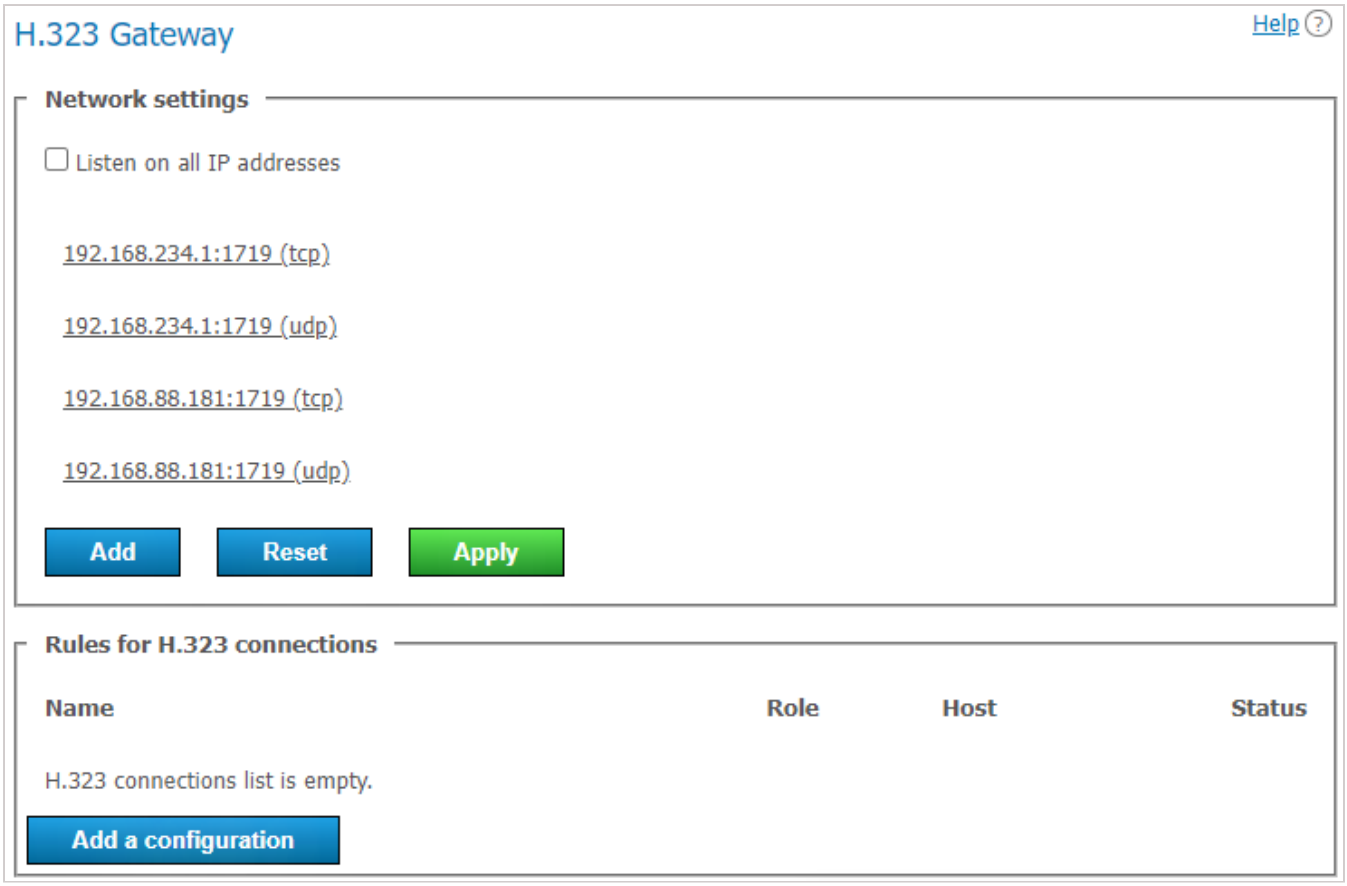
* You can also find an instruction on how to connect to a conference held on TrueConf Server from an SIP endpoint on the conference web page.

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.



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.

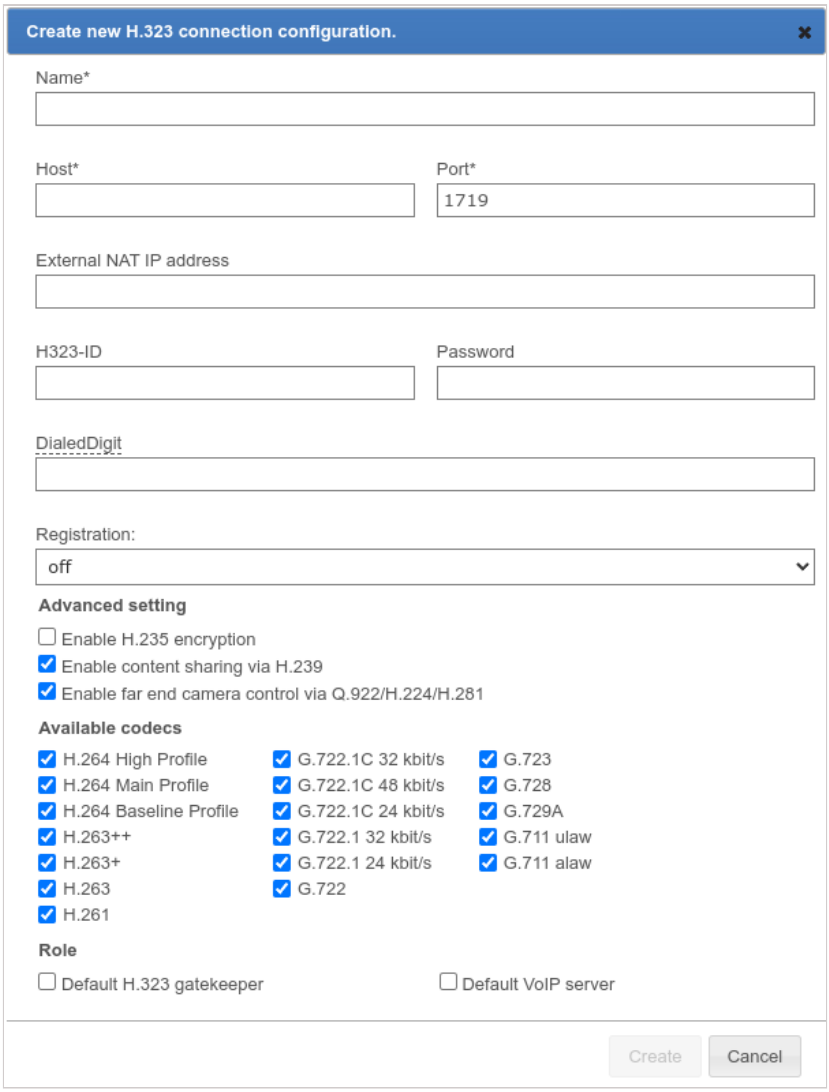
11.2.2. Rules for H.323 connections

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 outcoming from the connected H.323 device will be redirected to a specific user ID or conference ID on TrueConf Server side.

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

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.

i 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.

The parameter **Action on incoming call to TrueConf Server IP address** enables you to choose the behavior in case of a call via SIP 2.0 to any of the addresses from the **Network settings** section:

- 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.

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.

11.2.7. Sending DTMF commands

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.

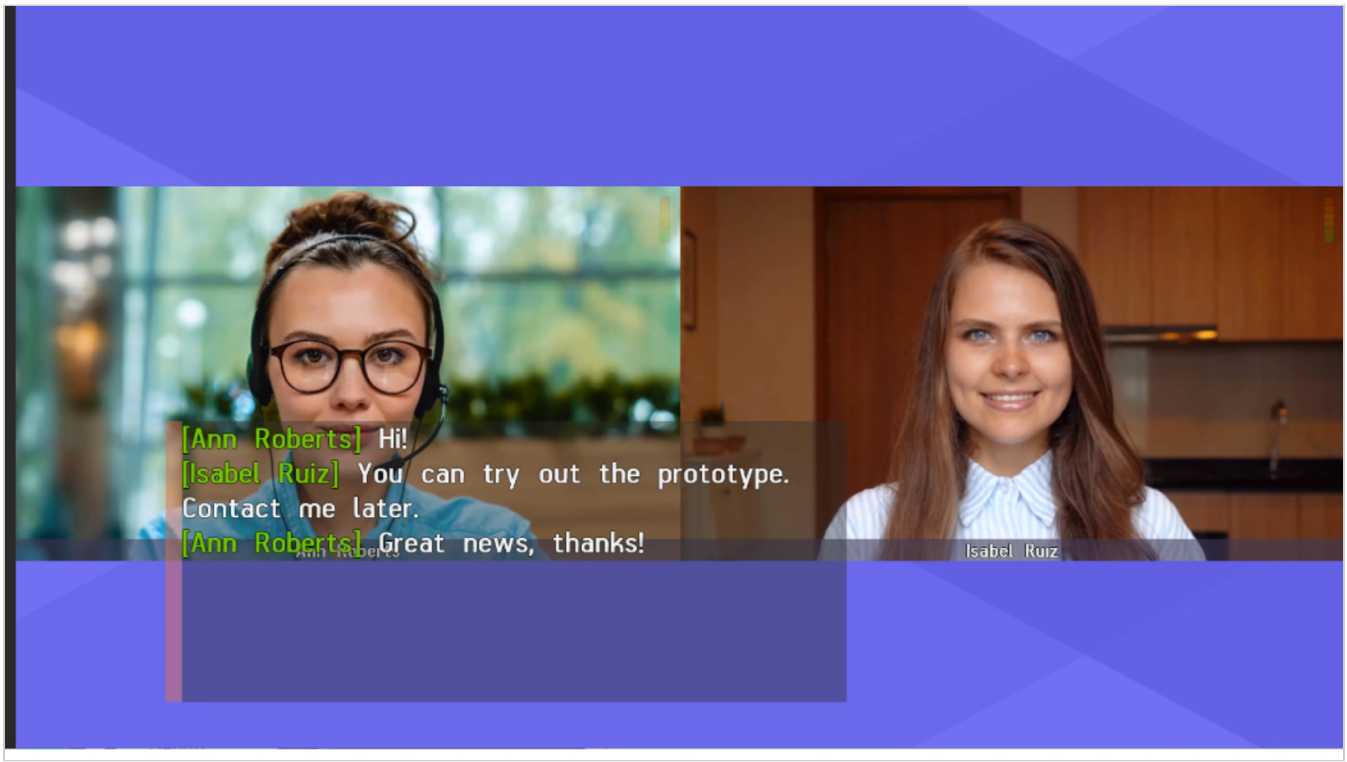
- `2` – to leave the podium.

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.

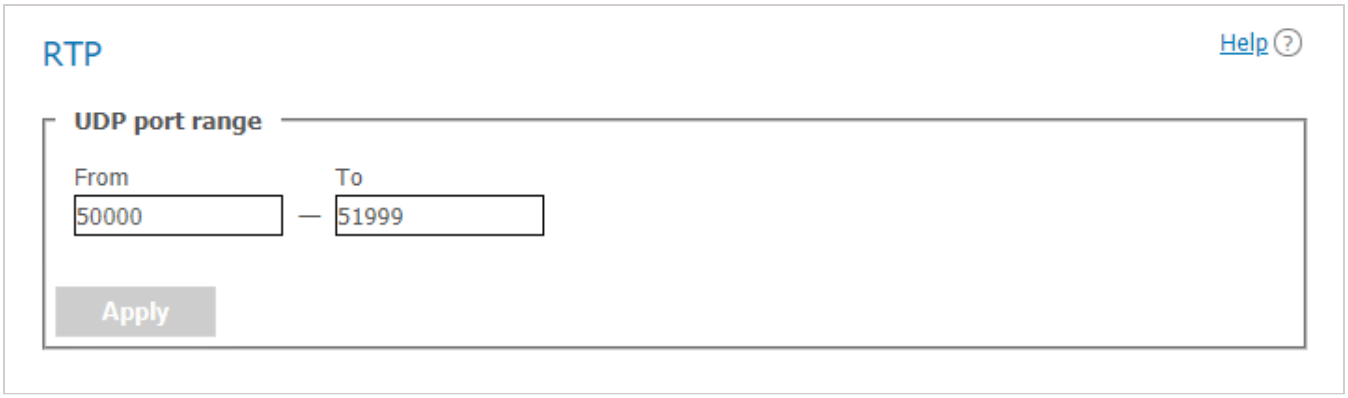
11.3. Chat during calls on TrueConf MCU

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:



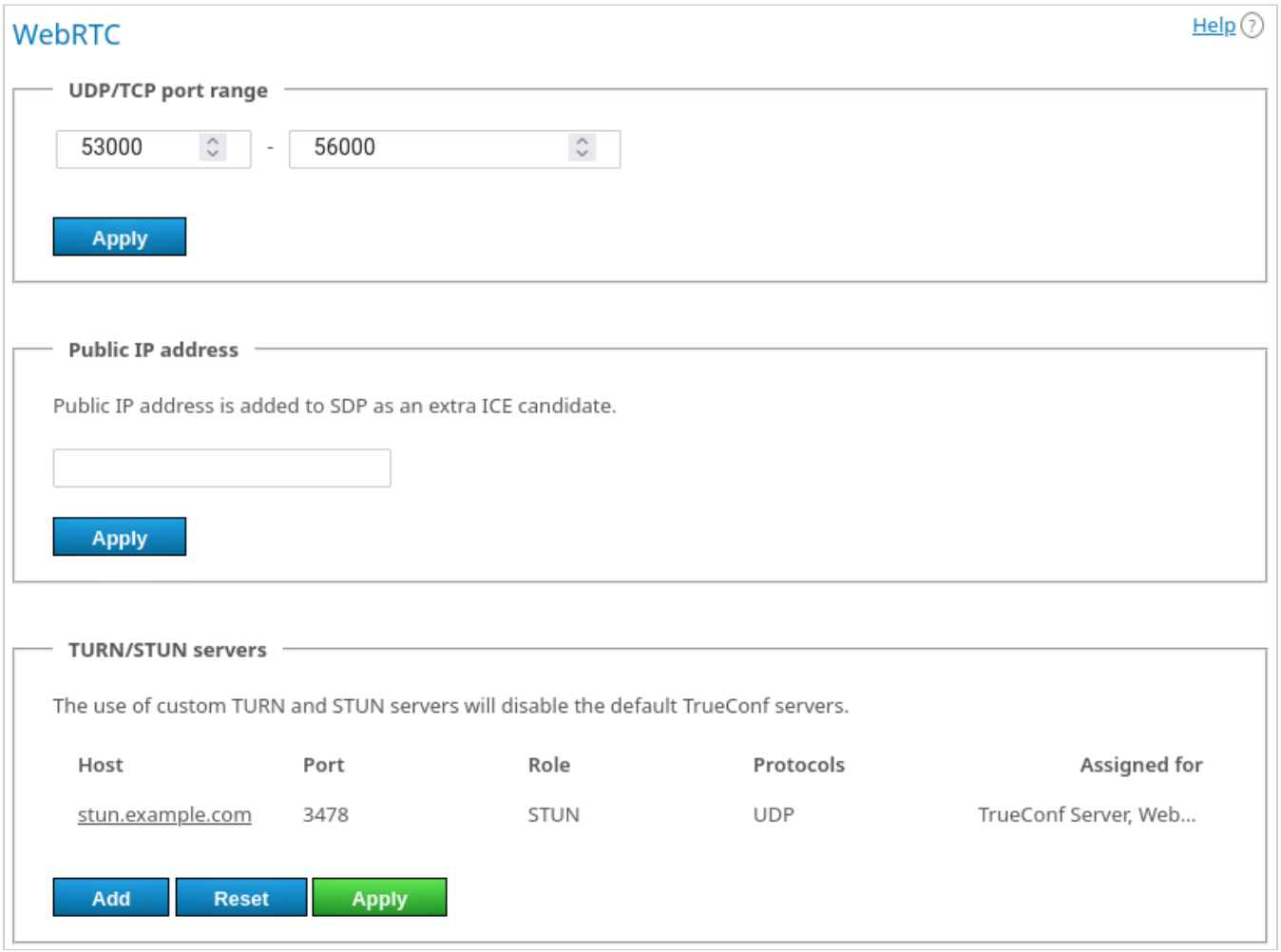
11.4. RTP

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).



11.5. WebRTC

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



- UDP or TCP port range for WebRTC connection (the ports 53000-56000 are used by default).
- In the field **Public IP address is added to SDP as an extra ICE candidate**, you can enter the IP address that will be used for NAT traversal, if automatic detection fails due to some reason.
- Add the addresses of STUN/TURN servers for fine-tuning NAT traversal.

* To learn more about the work of WebRTC, refer to the article on our website.

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

1. TrueConf Server acts both as an authorization server and a WebRTC client (a conference participant) at the same time.
2. The role of a STUN or TURN server can be assigned both to TrueConf Server and the WebRTC client. Depending on your choice, the result will vary:
   - If the role of a STUN/TURN server is given to TrueConf Server, it will be possible for TrueConf Server to receive an external IP address.
   - If the role of STUN/TURN is given to the WebRTC client, participants using browsers will be able to get an external IP address.

3. The role of STUN/TURN can be given to TrueConf Server and the WebRTC client at the same time (both items are selected in the **Assigned for** drop-down list).

4. It is possible to add only 1 configuration in which the role of STUN/TURN is given to TrueConf Server.

5. There is no limit on the number of STUN/TURN servers assigned to a WebRTC client.

The following mechanism is used when a participant connects from a browser:

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

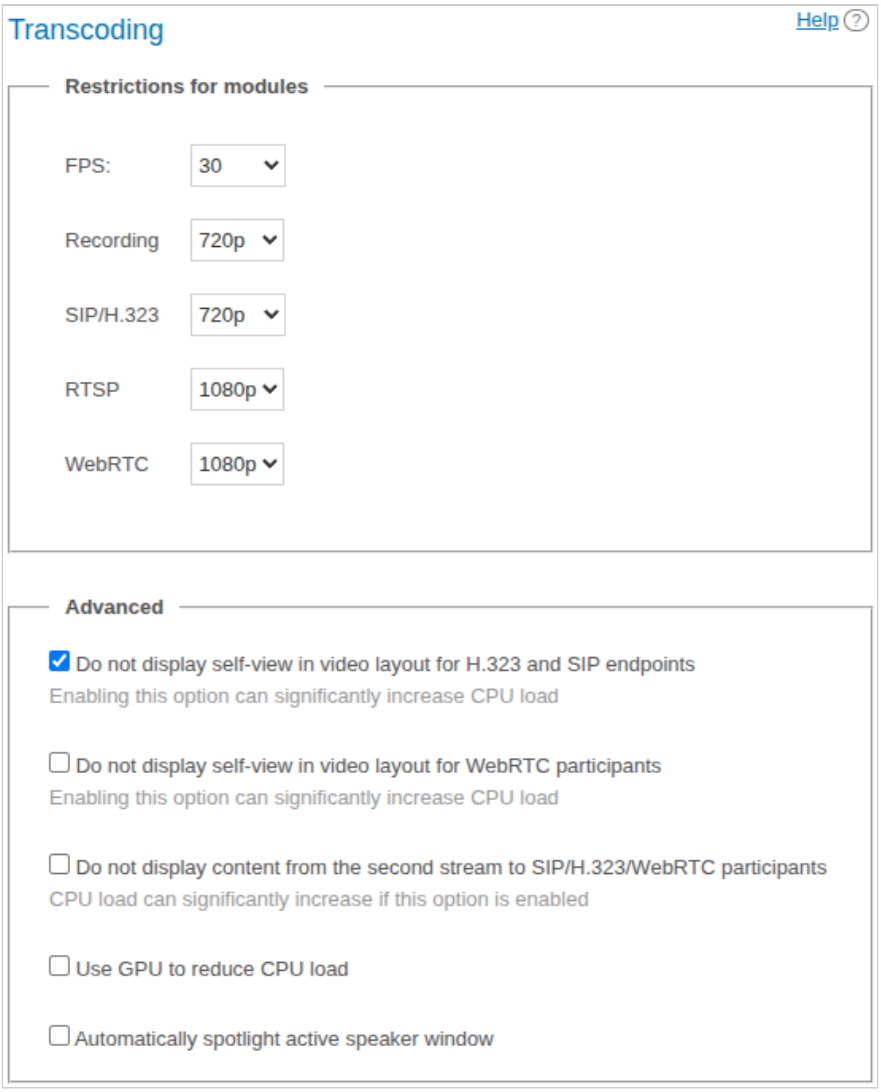
11.6. Transcoding

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.



Cheking 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.

The checkbox **Do not display content from the second stream to SIP/H.323/WebRTC participants** enables you to exclude the second stream (with content or a slideshow) from the resulting video layout for all SIP/H.323/WebRTC endpoints connected to a conferences. However, if a conference is recorded on the server side, the separate mixing process will start, and the second stream will be included in the video recording.

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

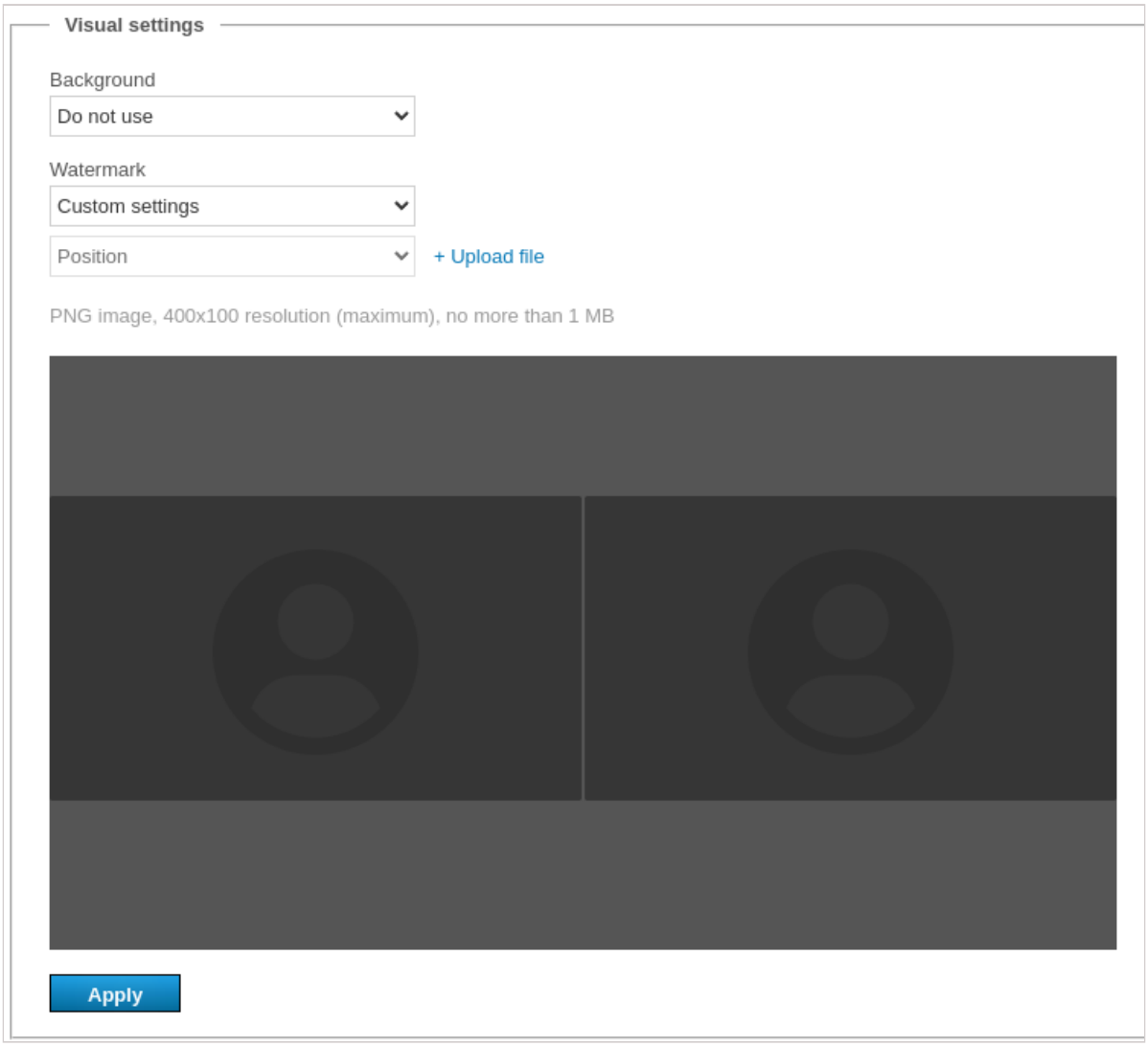
When the box **Use GPU to reduce CPU load** is checked, video conferences will be processed by the GPU of the physical machine with TrueConf Server installed.

i 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.



A watermark cannot be added if TrueConf Server Free is used; a paid license is needed.

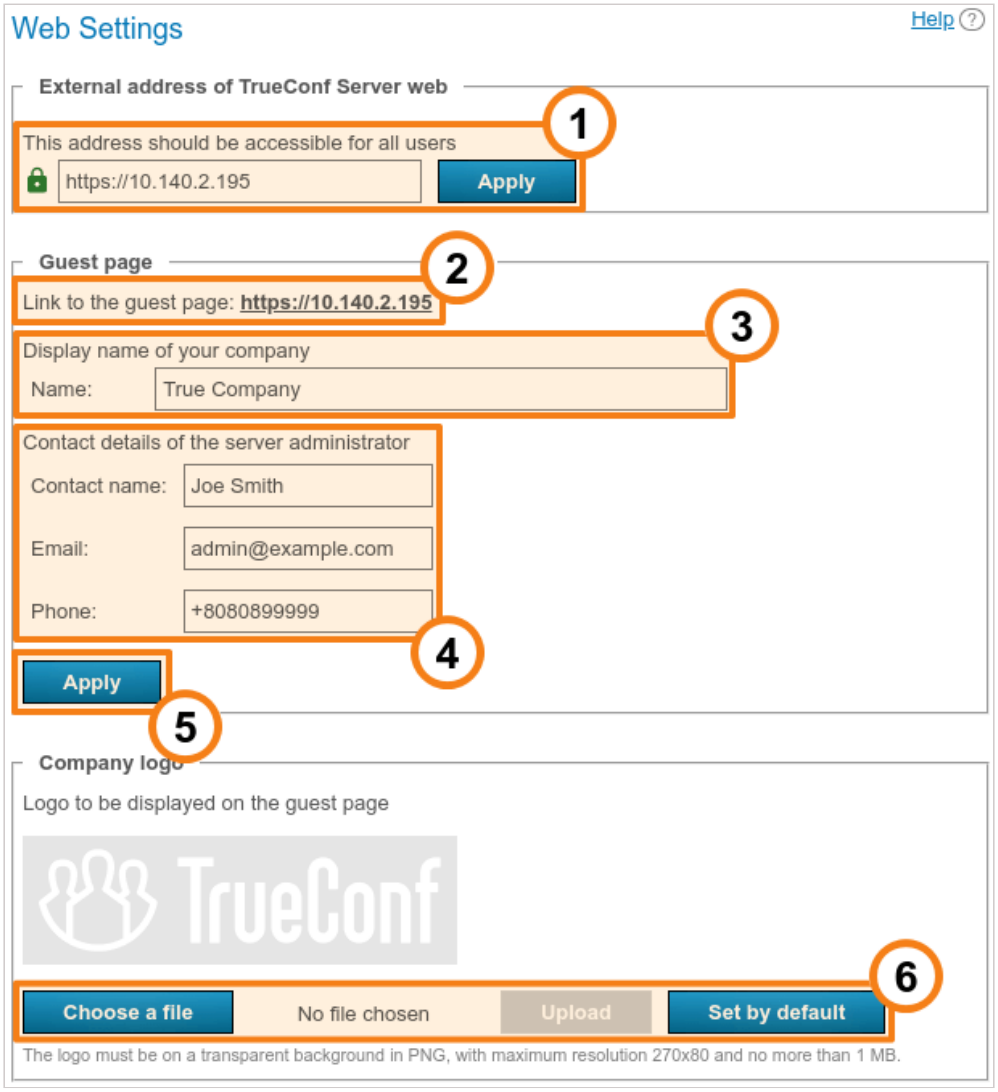
12. Web and HTTPS settings

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:



1. The TrueConf Server address which is used to generate links to the guest page and conference pages. Make sure that it is accessible to all users of your TrueConf Server. If a non-standard port (other than HTTP `80` or HTTPS `443`) is used, it has to be specified in the address field after a colon, for example, `https://video.server.com:4433`. When an external service is used to proxy traffic, the external address of TrueConf Server will be its address. Such a service could be, for example, NAT or TrueConf Border Controller. The specified `address:port` will be used by client applications to receive the widget for real-time conference management, conference scheduler, content shared in the second stream and presentation (slideshow).
2. The link to the guest page which includes guidelines for connecting new users to TrueConf Server. It 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.

i 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.

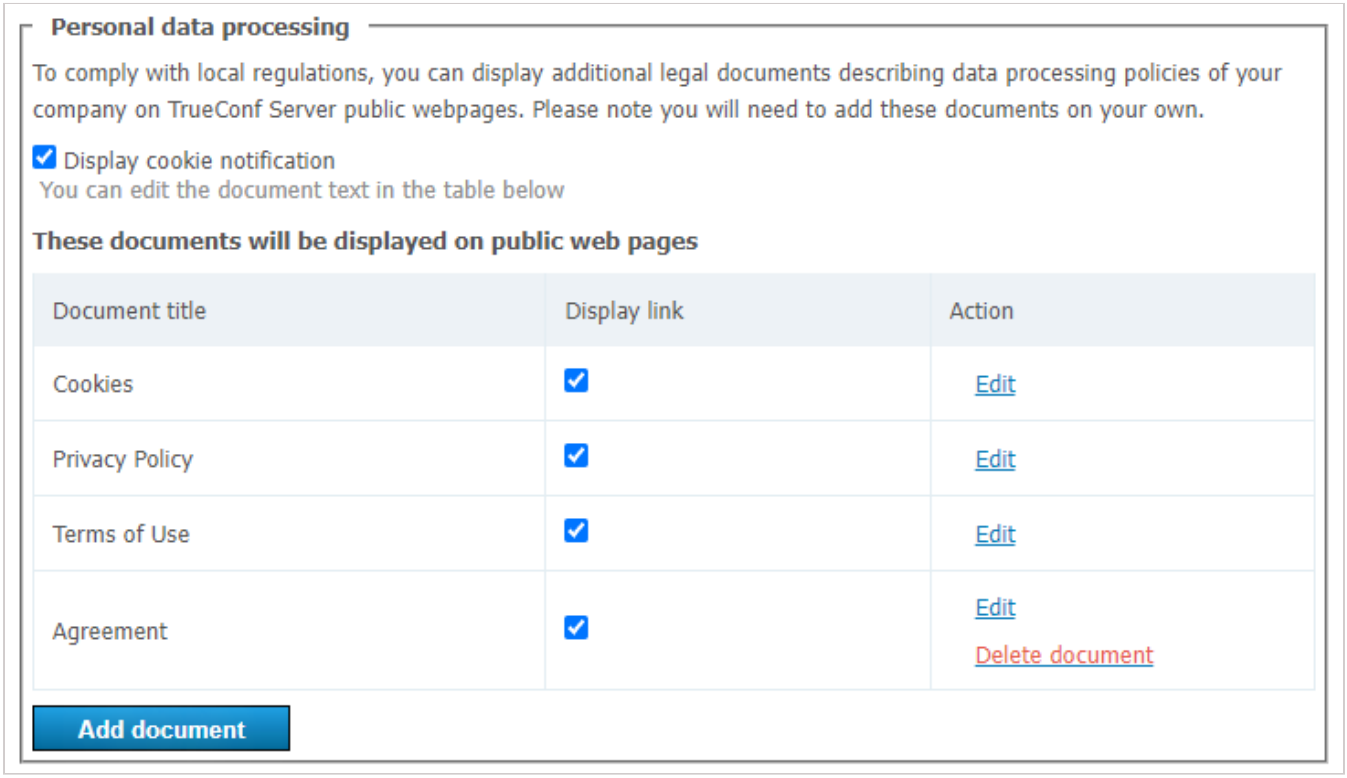
12.1.2. Additional documents

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.

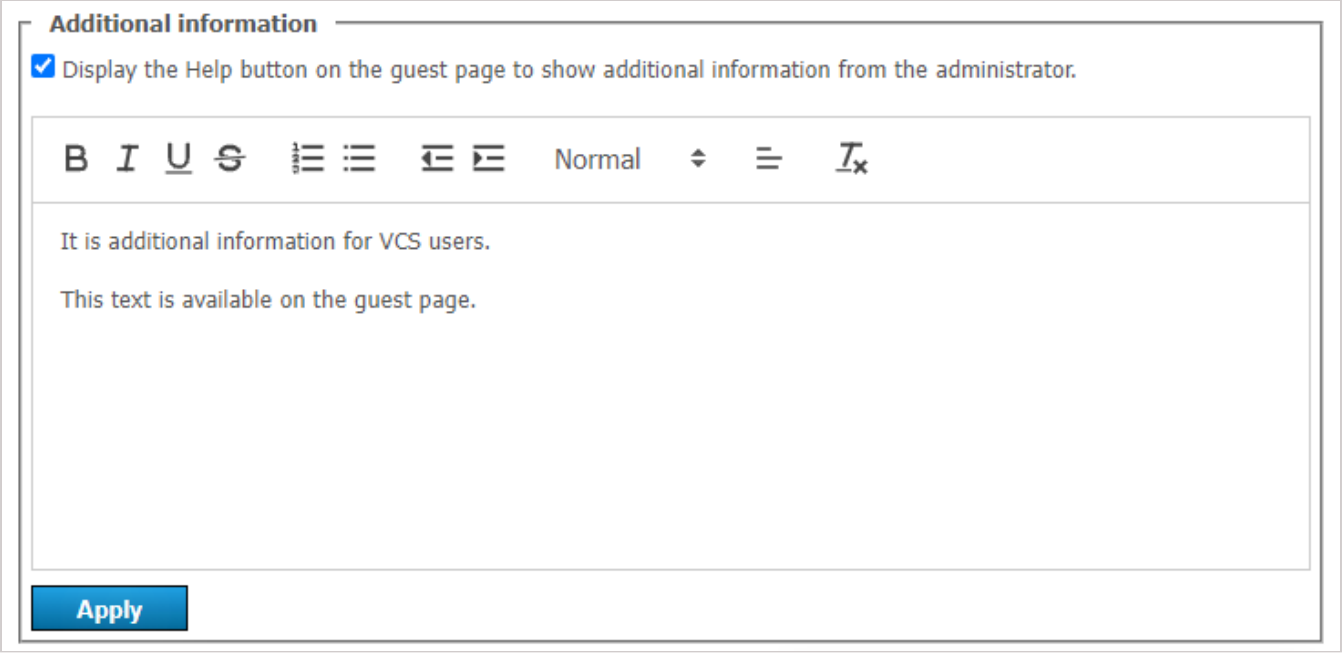
Document links will be displayed at the bottom of your TrueConf Server guest page and conference webpages.



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.

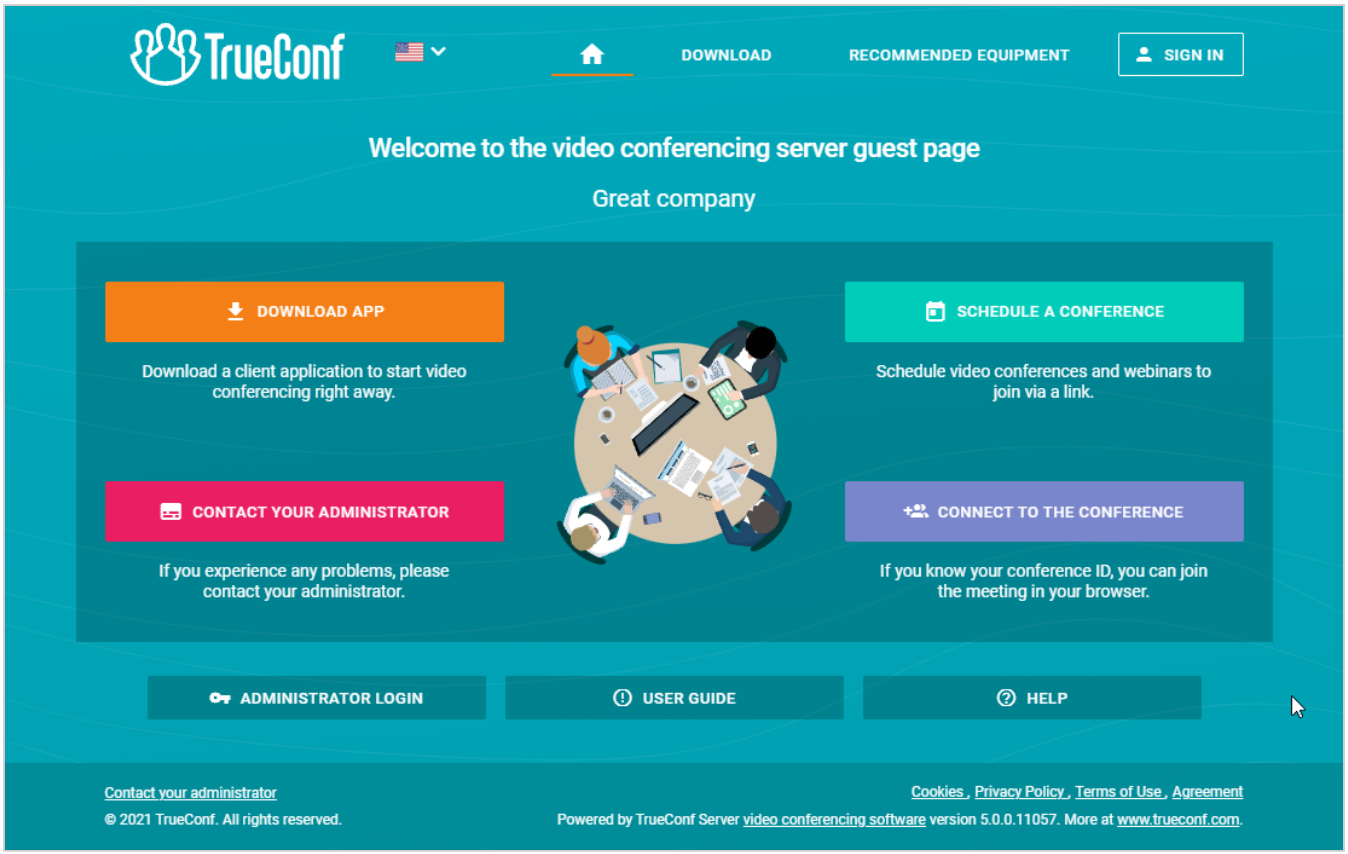
You can also add extra information or a manual for your guest page visitors, which will be displayed once you click on the **Help** button at the bottom of the page. Please note that **Help** is optional and it does not replace the default manual that opens by clicking on the **User guide** button.



To display additional information:

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

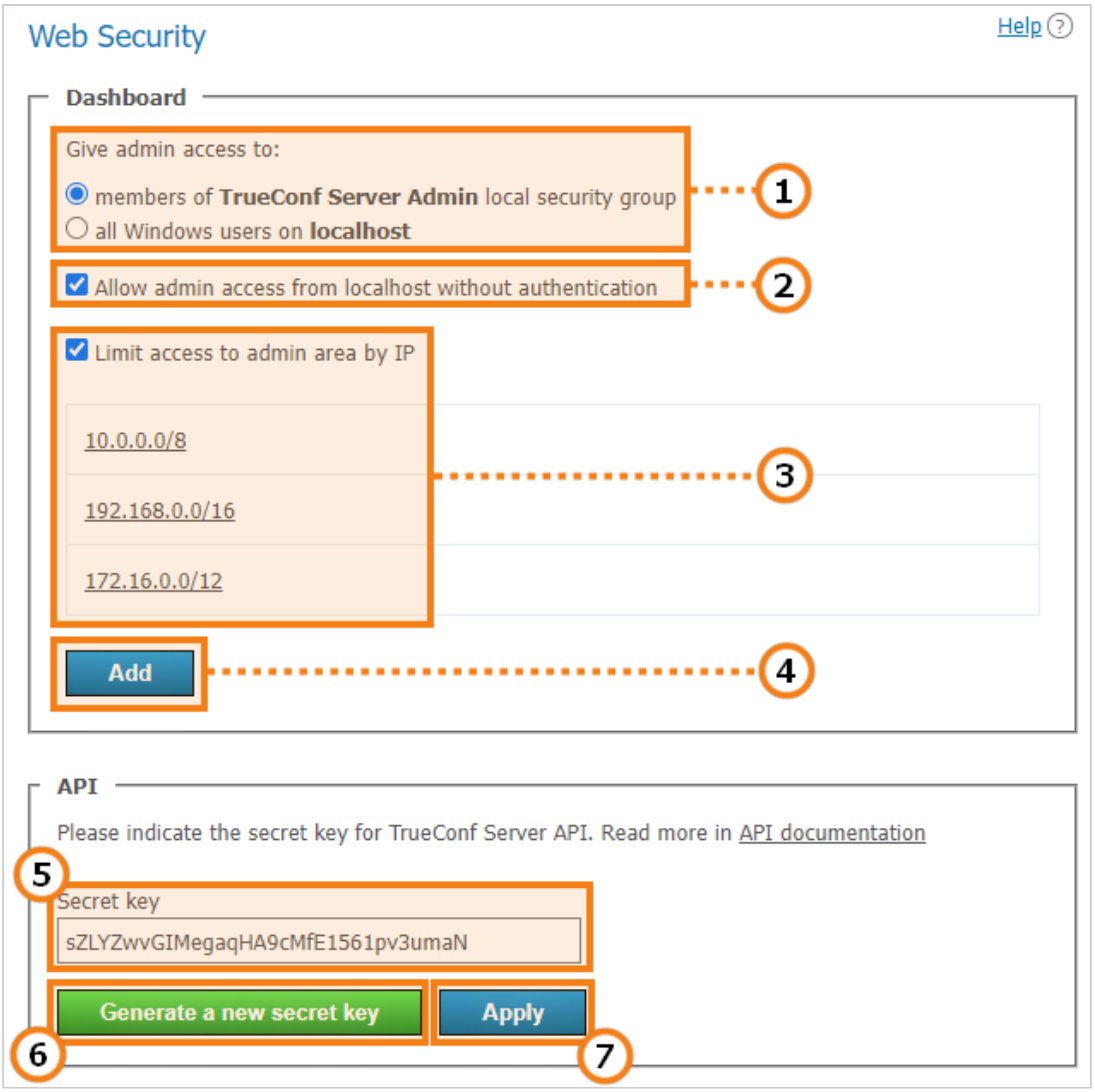
Below you can see an example of a guest page with three default documents, one additional document and a custom **Help** button:



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.

> *i* 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.

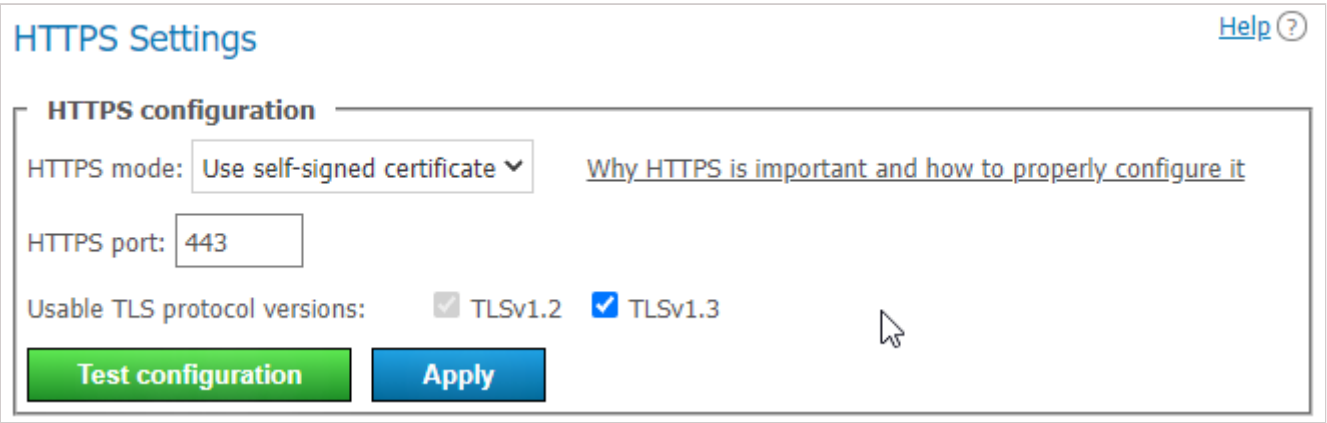
HTTPS is also required for users connected to your TrueConf Server instance from their client applications. Without it, they won't be able to access and use conference scheduler, show slides and manage meetings in real time.

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

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.



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.

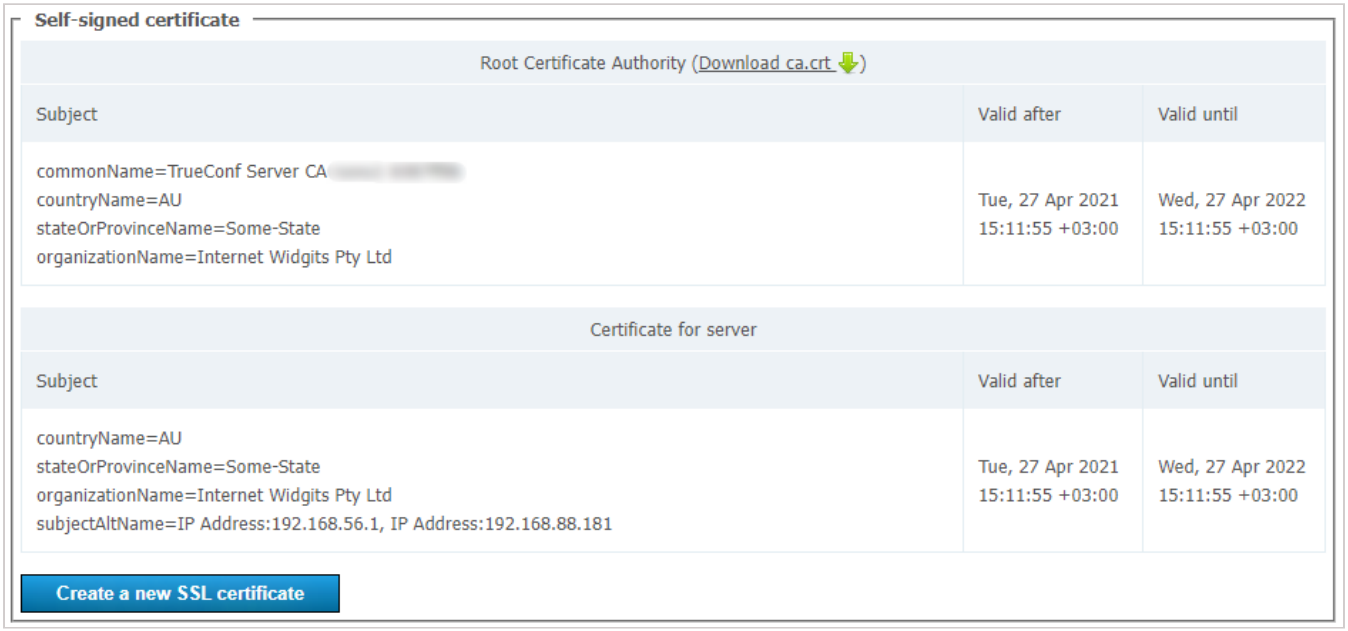
As an alternative you can also use a self-signed certificate:

- 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:

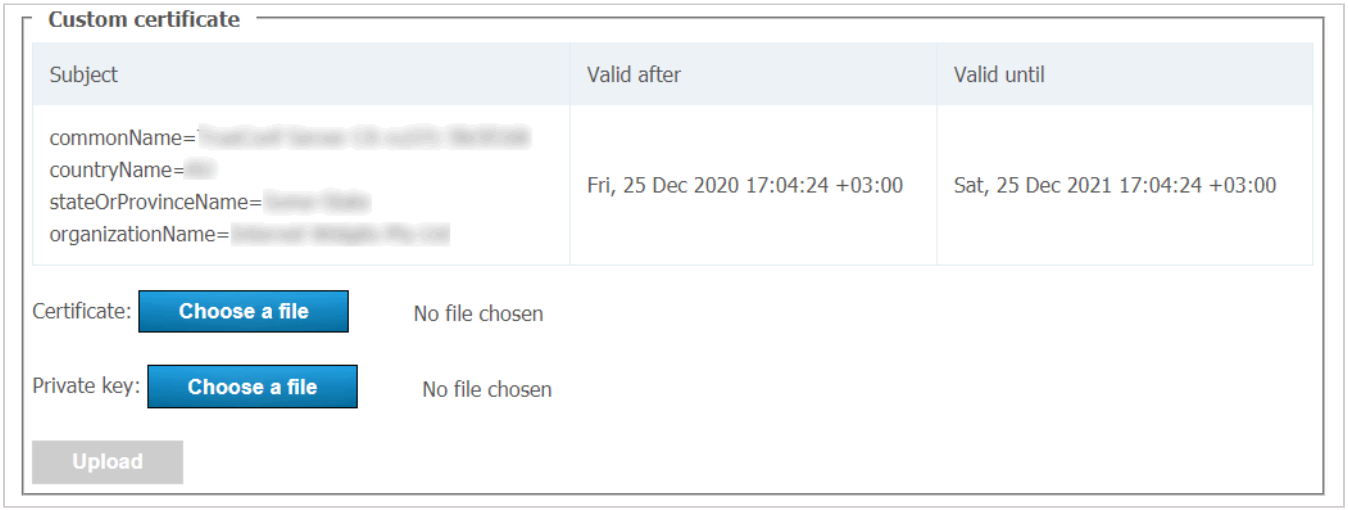


To create a new self-signed certificate, press **Create a new SSL certificate**. You may use this option to renew your certificate for 365 days or to update information about your

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:



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.

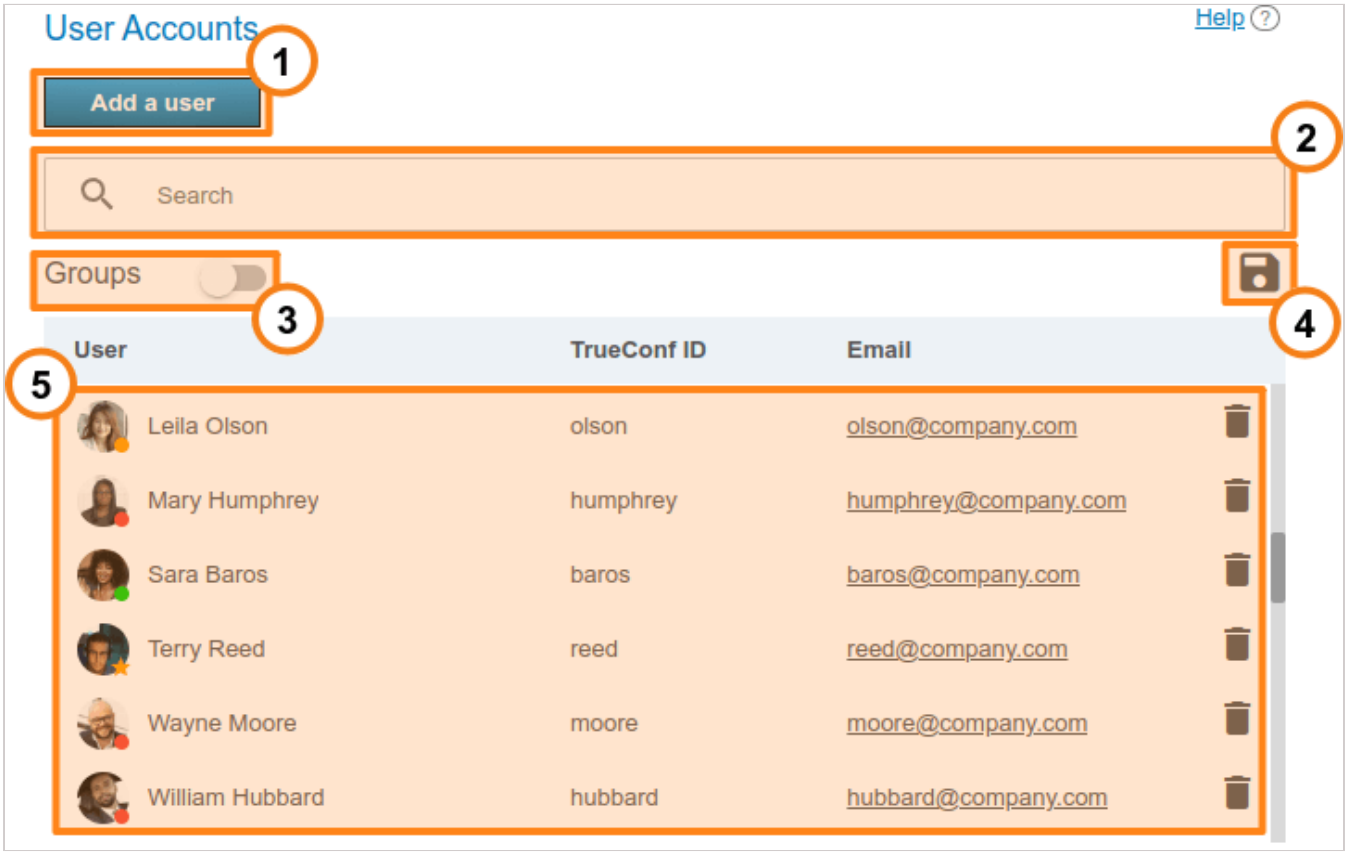
13. Users and groups. Integration with LDAP/Active Directory

13.1. User Accounts

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

i 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.



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 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:

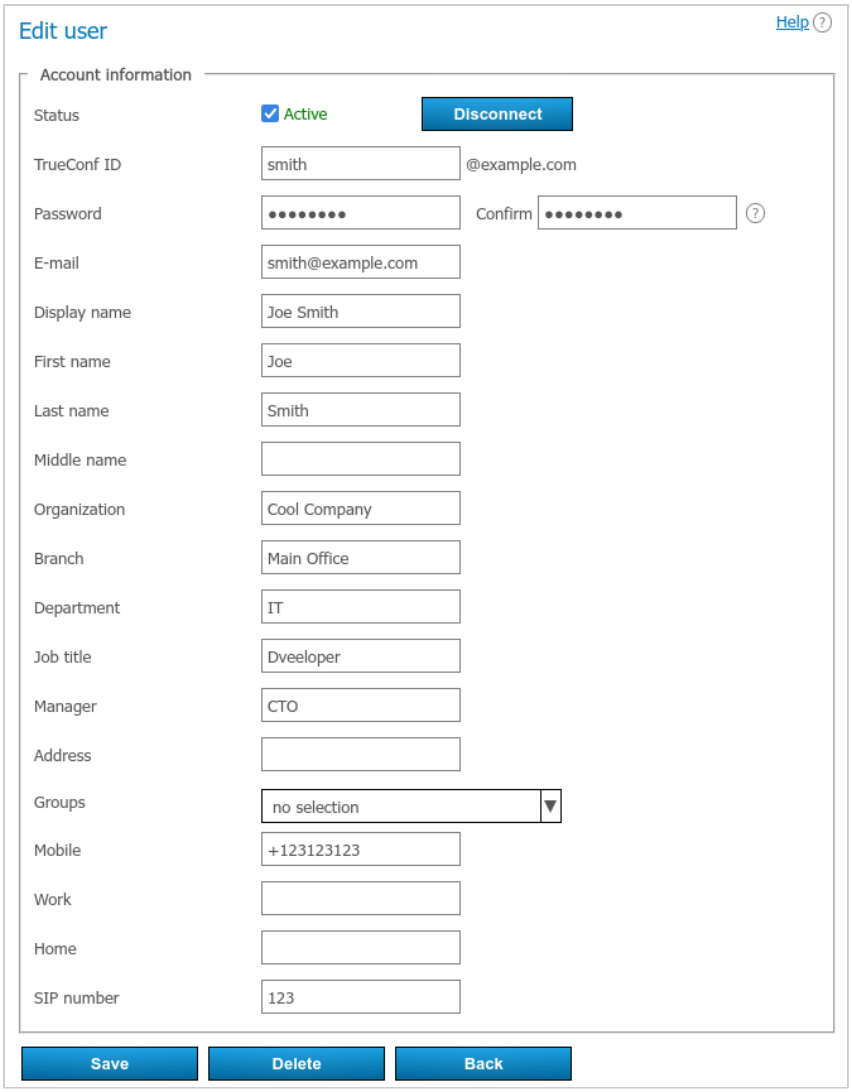
- — the user is online
- — the user is offline
- — the user is in a conference or in a call
- — the user is the owner in the conference
- — the user account is deactivated by the administrator (check the **Status** section in the profile).

> * 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

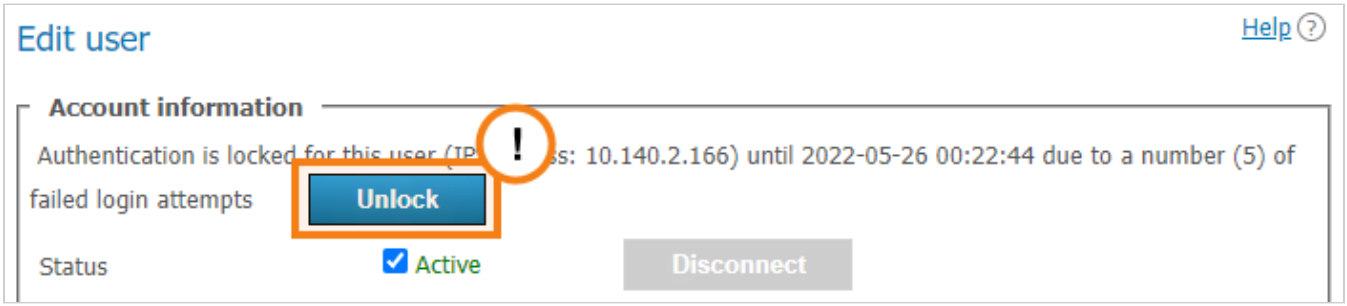
If you create a user or click on any existing user in the list, you will be redirected to the page for entering or editing information about this person:



1. With the **Active** checkbox, you can change a user's status to "active" or "inactive" (see below). Such users will be displayed semi-transparent in the general list with a grey status.
2. Use the **Disconnect** button to disconnect a user from TrueConf Server in all client applications. This feature may come in handy if you need to quickly connect a different user and the maximum number of connections is already reached (according to the license).
3. TrueConf ID is the unique identifier used for authentication in client applications and making calls. The user's login (the part of TrueConf ID before `@`) can include only Latin and Cyrillic letters, digits, underscores, hyphens, and periods. The full TrueConf ID with the server name specified after the login (the extra part in the format `@server` next to the input field) is needed for making calls to a user from a different server. The login is set when a user account is created and cannot be changed later.
4. Enter the user's password. This password cannot be viewed when the account is created or edited, but it can be changed. Use the ⓘ button which is next to the password confirmation field to view the password requirements.
5. Next, specify the email address that TrueConf Server will use to send notifications to the user via the associated SMTP server.

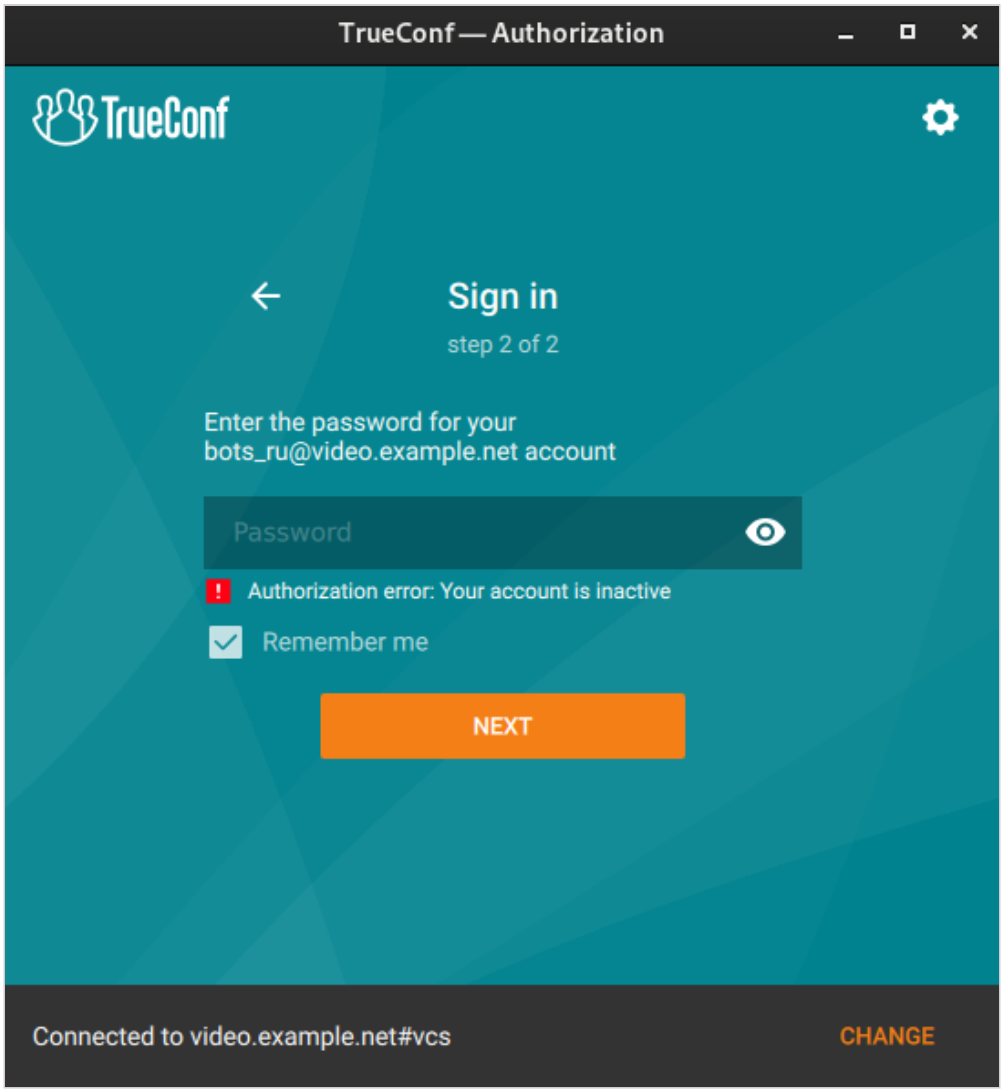
6. **Display name** is another required field which will be displayed in the address book of other users. This field is pre-filled with the username entered during Step 3. However, its value can be changed.
7. Next, comes a group of fields for various data about a user and his/her position in an organization. These fields are optional.
8. In the **Groups** drop-down list, you can add a user to the selected groups. Click on the arrow icon to view the list of groups available on the server. To add a user to one or more groups, just check the box to the left of a group name.
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, it is possible to specify a SIP call number in the corresponding field. If you do it, this field will be displayed in the user profile in TrueConf client application. When a user clicks on this field, the call will be started in the format `#sip:<number>`. The number can be specified as `<number>`, `sip:<number>` or `#sip:<number>`.

If a user has entered an incorrect password multiple times in a row (the exact number will be specified in the **Users →Settings** section), the authorizatin 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:

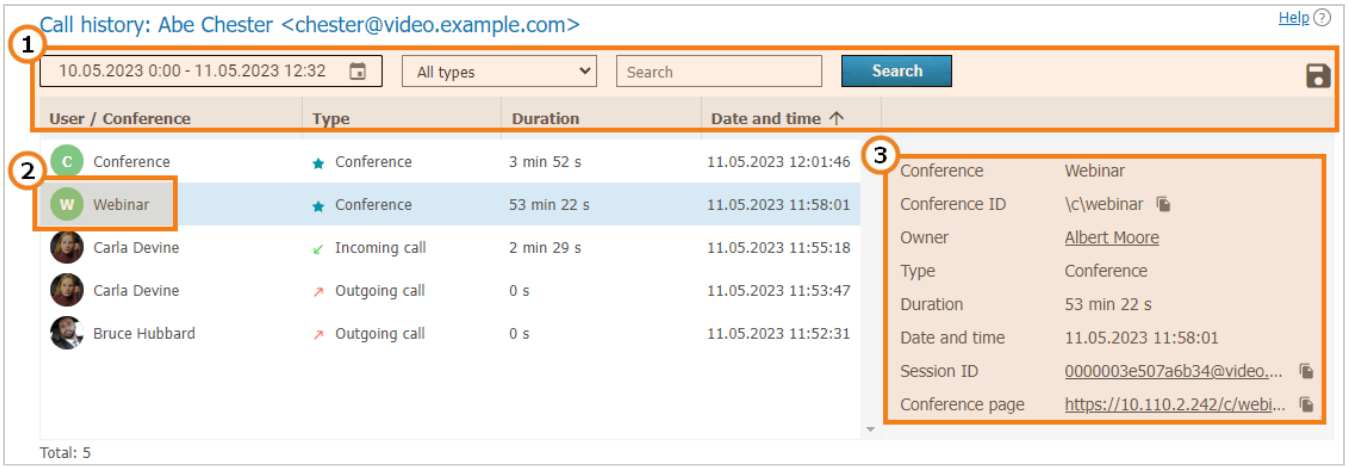


13.2.2. Calls and conferences

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:



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.

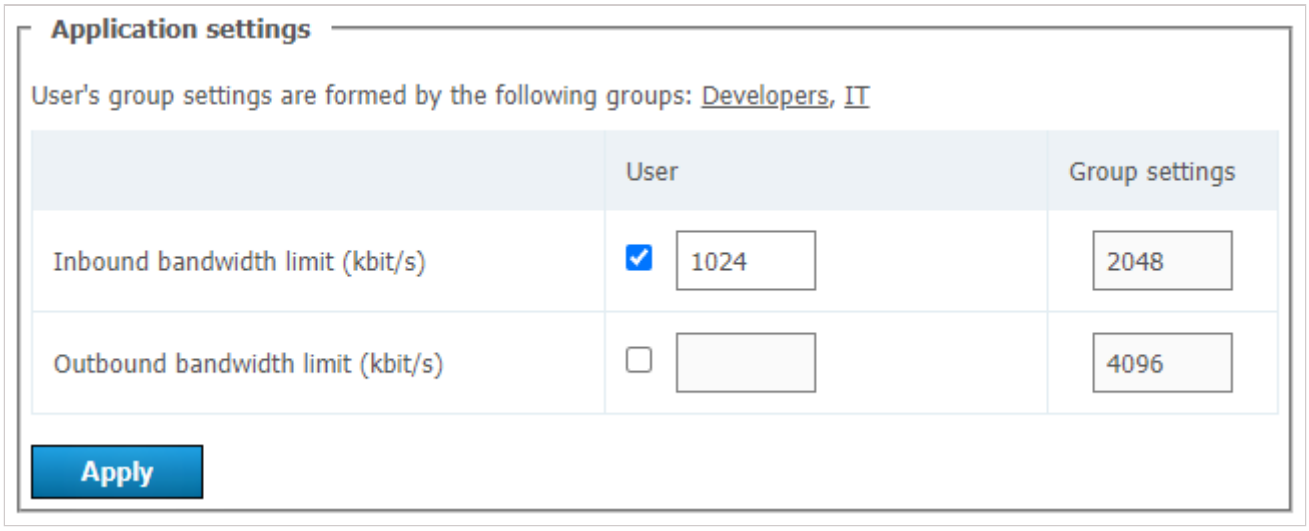
3. When selecting a session linked to the specific conference, you will see the following information in the card on the right:

- 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.



If bitrate restrictions are set at the user or group level, users will not be able to change them in TrueConf client applications, but will be able to see what parameters were selected.

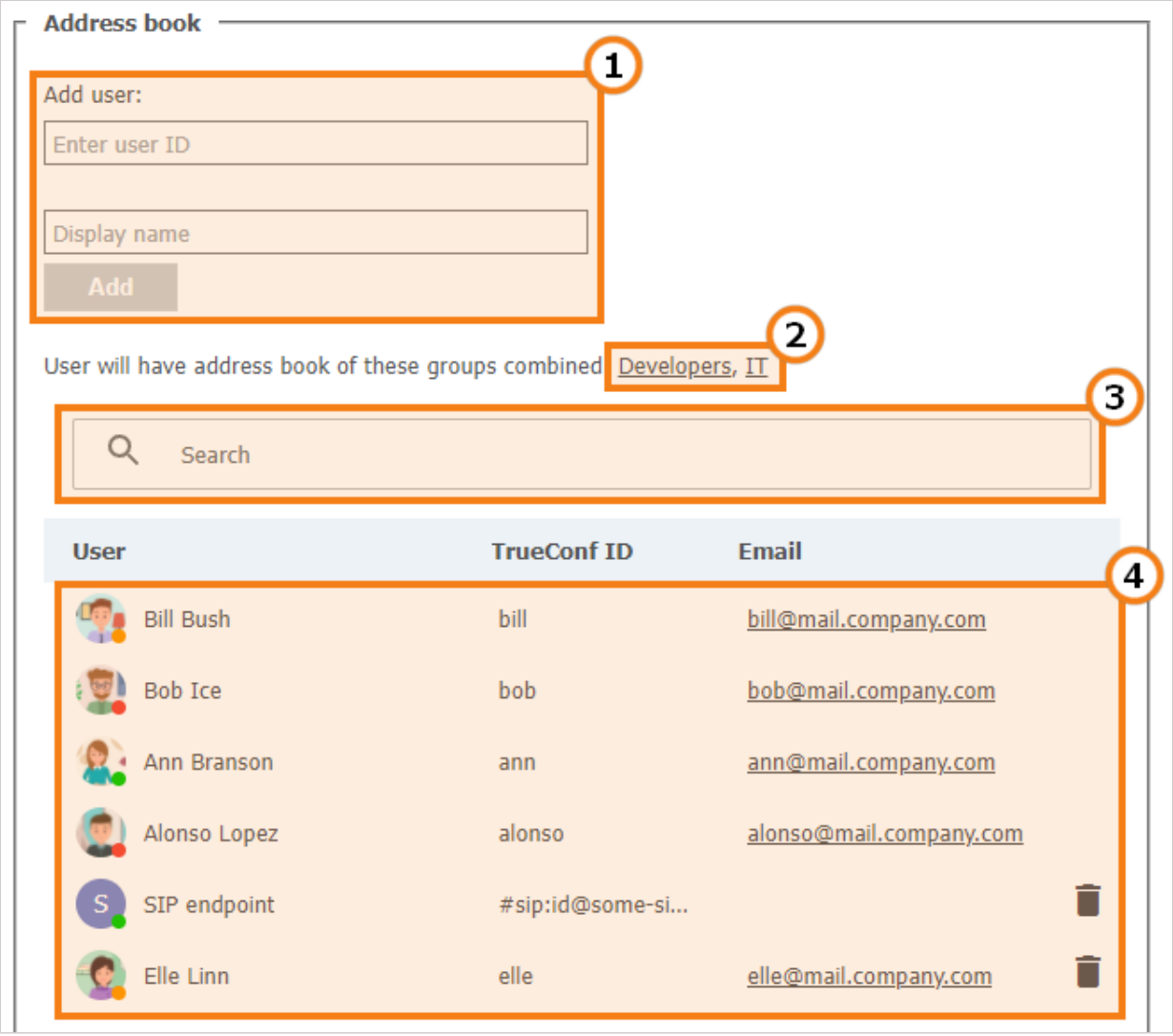
i User application settings have higher priority than group settings: if you put user restrictions lower than group restrictions, user restrictions will be applied.

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.



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.

i Manual editing of the user list and settings (e.g., group name) is not available in LDAP mode. You can only import groups from the LDAP directory as shown below.

Regardless of the data storage mode (Registry or LDAP), the following groups are included in the list by default:

- **Users without group** — 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.

Each user group has specific permissions for using your video conferencing server.

13.3.1. List of permissions for a user group

Please note that certain permissions cannot be given to the groups created by default. This restriction is set for security considerations (e.g., to make sure that operator rights are not available to everyone) and due to application logic reasons (e.g., since guests do not have a permanent account on your server, they cannot create conferences).

Below, there is the list of permissions that can be configured for user groups of TrueConf Server:

Editing address book. By checking this field, administrator allows users to change users display names of the users, delete/add users and perform any other changes in the group's address book. If the box is not checked, group users will not be able to perform the actions mentioned above. In this case, all changes are performed by administrator in TrueConf Server control panel and extend to all address books of the users from this group.

Making point-to-point video calls. However, users can still receive incoming calls.

Creating group conferences.

Sharing the screen and application windows

Ability to request control over a meeting participant's desktop.

A user's ability to give control over his/her desktop.

Slideshows (slides are either imported from files or created by combining multiple images). This permission does not depend on the right to share the desktop or applications.

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.

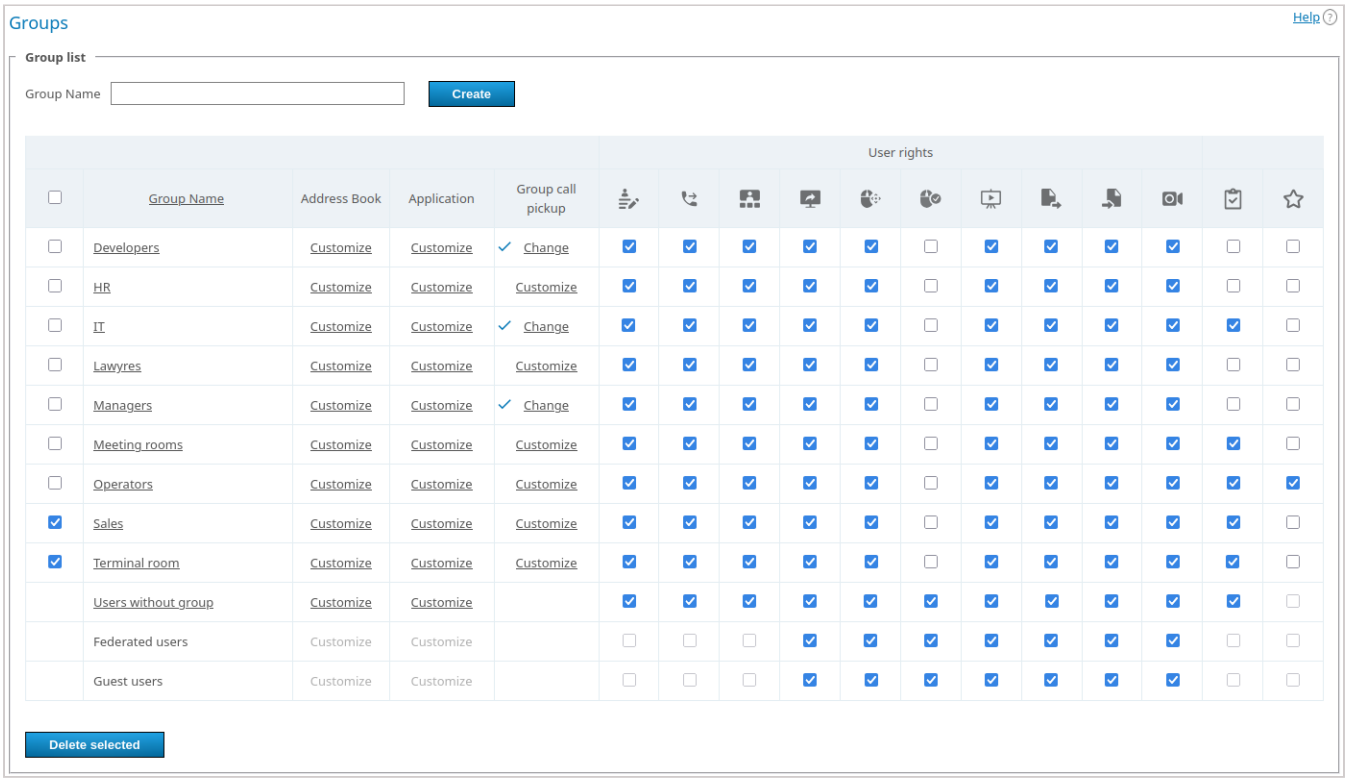
Conference recording in the client application. This feature does not affect the ability to activate video recording when creating a conference in the application scheduler or personal area.

Ability to create surveys and distribute them across campaigns.

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.

13.3.2. Editing groups in Registry mode

Below, you can find an example of group settings for Registry mode, while some parameters will differ for LDAP mode.



1. To add a new group, enter its name and press **Create**.
2. You can enable or disable certain features at the group level in the **User rights** section. These settings allow you to set different rights for users. The full list of these rights is provided above. Besides, read the description of how the rights work when a user belongs to several groups.
3. Click on the selected group in the list to open the menu where one can add or remove participants and change the group name. By clicking on the **Group Name** column, you can sort the list of groups alphabetically.
4. Click the **Customize** link in the **Address Book** column to create the contact list which would be the same for all group members.
5. Click the **Customize** link in the **Application** column to set up bandwidth limits for group participants.
6. The **Customize** link in the **Group call pickup** column allows you to configure group call pickup for the selected group.

7. 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.

13.3.3. Configuration of group call pickup

The administrator can enable group calls for a user group. When this feature is activated, it will be possible to make calls to the entire group, rather than an individual user, so all group participants will see an incoming call. As soon as someone answers this call, it will be automatically declined for other users.

To enable group call pickup, click the **Customize** link in the **Group call pickup** column for the selected group in the general list.

On the opened page, you can configure the following settings:

1. The group for which settings should be configured (if necessary, you can quickly select a different group in the drop-down list).
2. The checkbox for enabling group call pickup.
3. Call ID which must be unique within the server. In other words, it cannot match other group call IDs and TrueConf ID of other user accounts. This ID should be used to start a group call. It can be added to the address book for future use. By default, it is identical to the group ID, but you can specify your own ID (e.g., a short string which is easier to use).

To save settings, don't forget to click the **Apply** button.

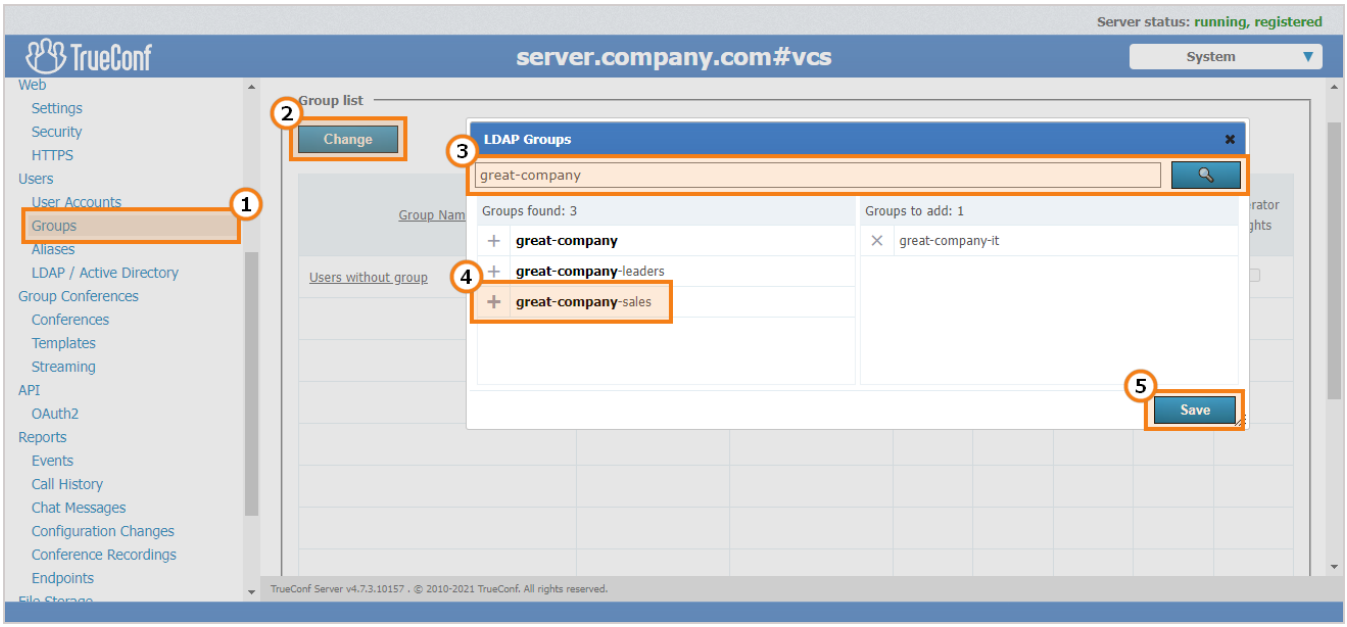
13.3.4. Editing Groups in LDAP Mode

> *i* Manual editing of the user list and settings (e.g., group name) is not available in LDAP mode. You can only import groups from the LDAP directory as shown below.

If you would like to centrally manage user information and enable LDAP synchronization on your TrueConf Server instance, the list of users and groups is imported from the LDAP catalog (e.g., Active Directory). Note that your designated user search catalog object must contain all necessary user groups. For instance, if when configurating 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, just like in Registry mode, you can configure settings for user rights, address book, restrictions for client applications, and group call pickup.

13.3.5. How the restrictions of rights work

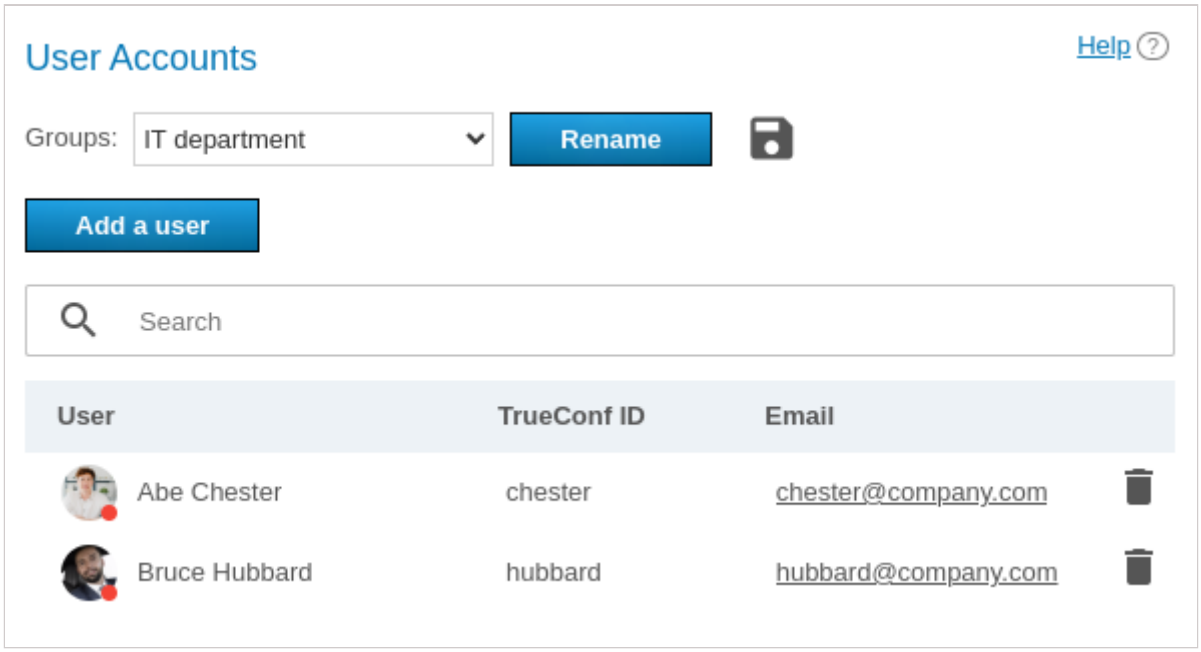
If a user is a member of two groups: the permissive settings will override restrictive ones. For example, the user account is included in such groups as **IT** and **DevOps**. If the members of the **IT** group are allowed to show slides, the user will be allowed to show slides even if this feature is not permitted for the members of the **DevOps** group.

Group-level user rights can also be redefined by restrictions for authentication zones.

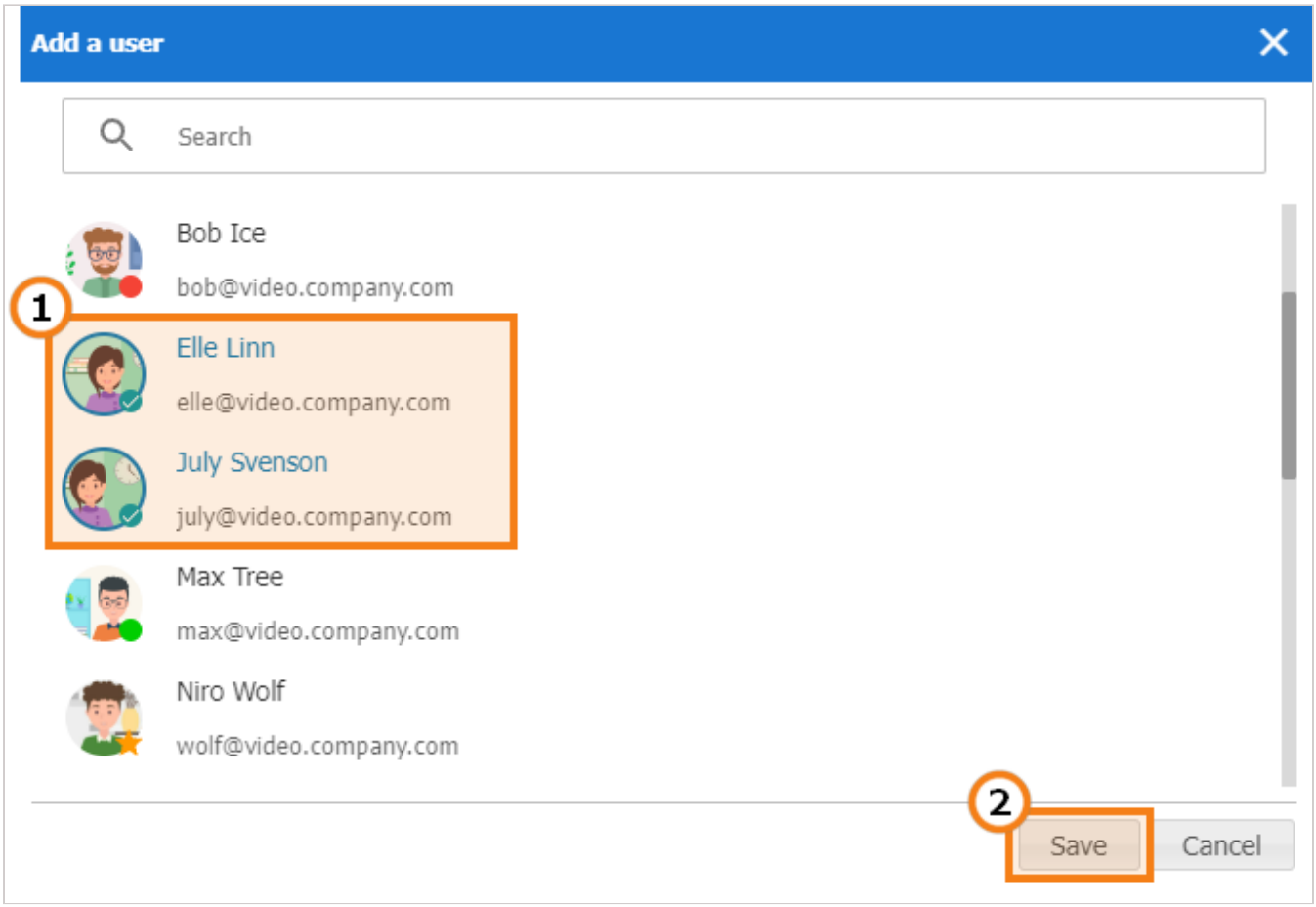
The persons who make a call to the users of your TrueConf Server via federation, will have the rights specified on your side (for the group **Federated users**) and on the side of their own server. For example, if you have disabled file sharing for federated users, they will not be able to send files 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.

13.3.6. Editing group's name and its members

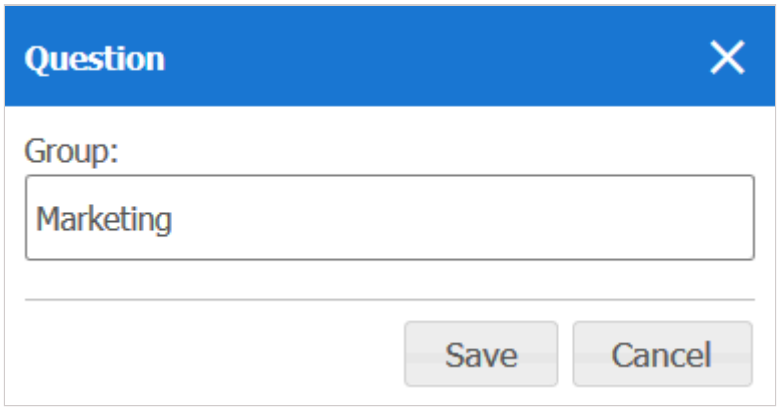
Click on the group name from the list to access the **User Accounts** page. Here you can rename the group and edit the list of members using the corresponding buttons:



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**:



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):

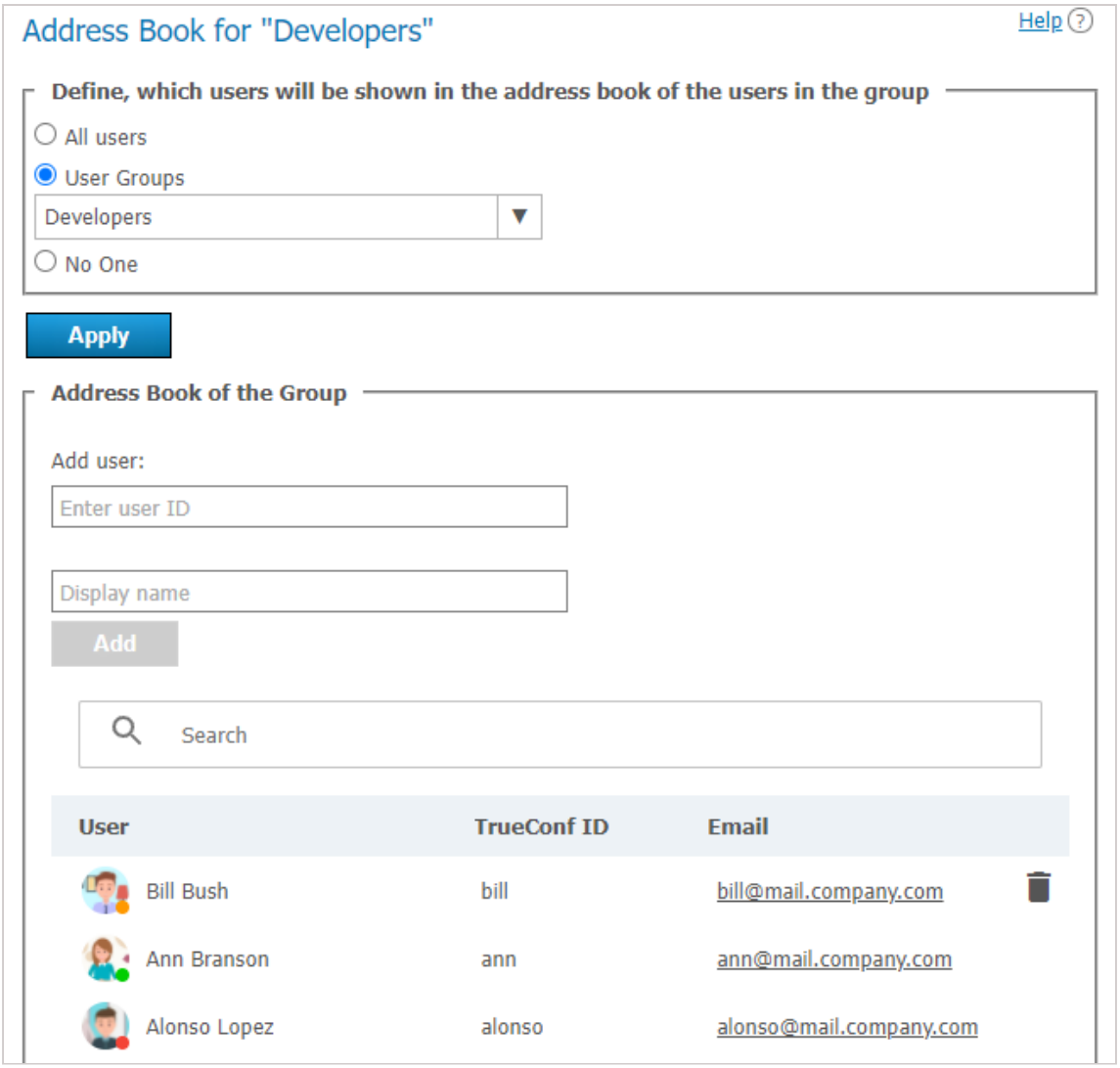


You can also click the button to export the user list of a specific group to a CSV file for subsequent import into the TrueConf Group address book.

13.3.7. 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.

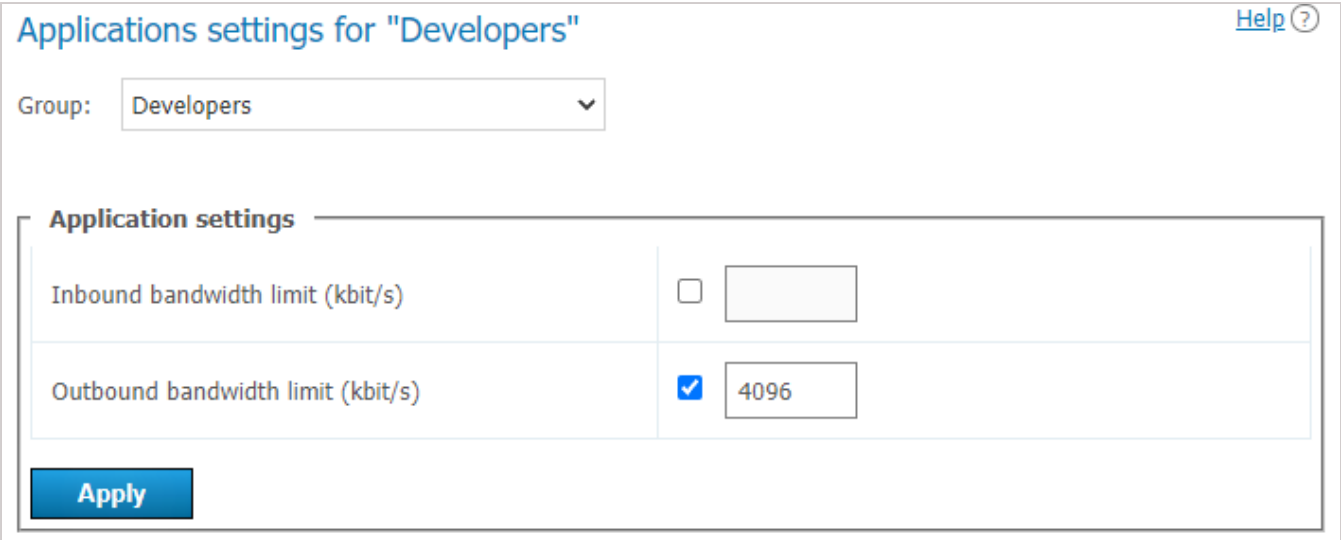


You can also manually add users of different types (this process is similar to adding users to the address book in the user's profile). However, group members cannot delete users themselves, because these contacts are added to the entire group and not to their personal address book.

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).

13.3.8. Setting application settings for group users

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

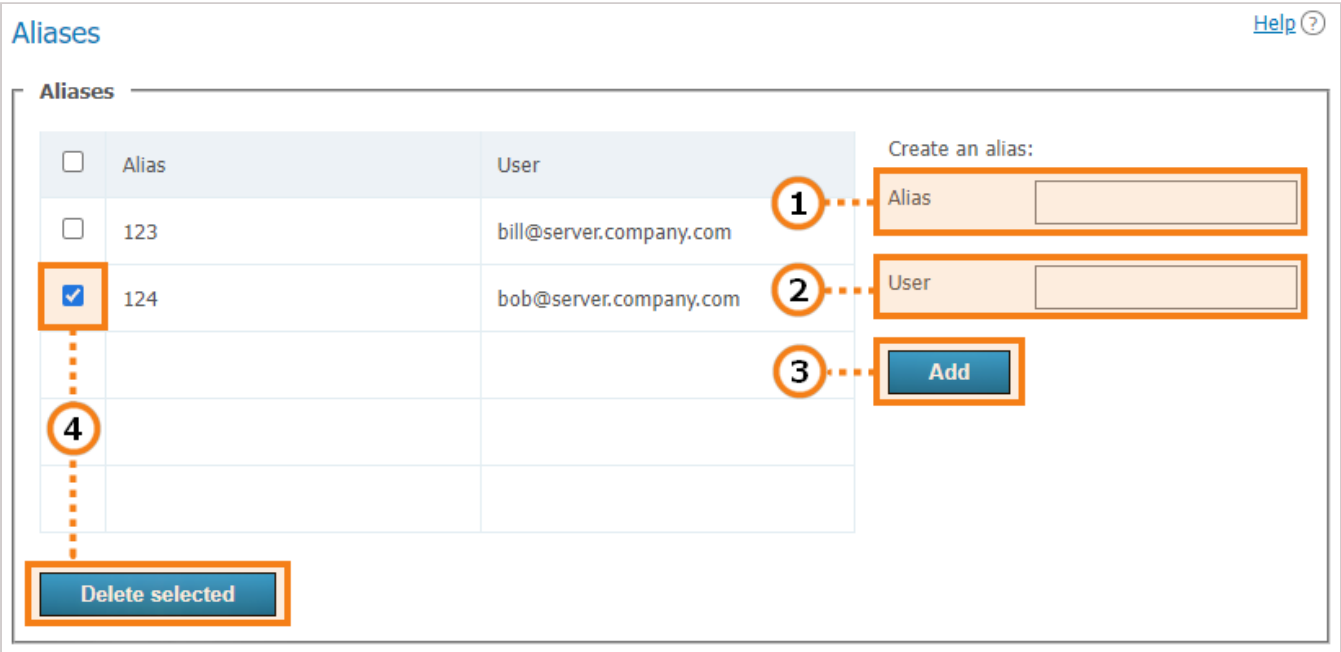


13.4. Aliases

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.



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**.

> *i* 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.

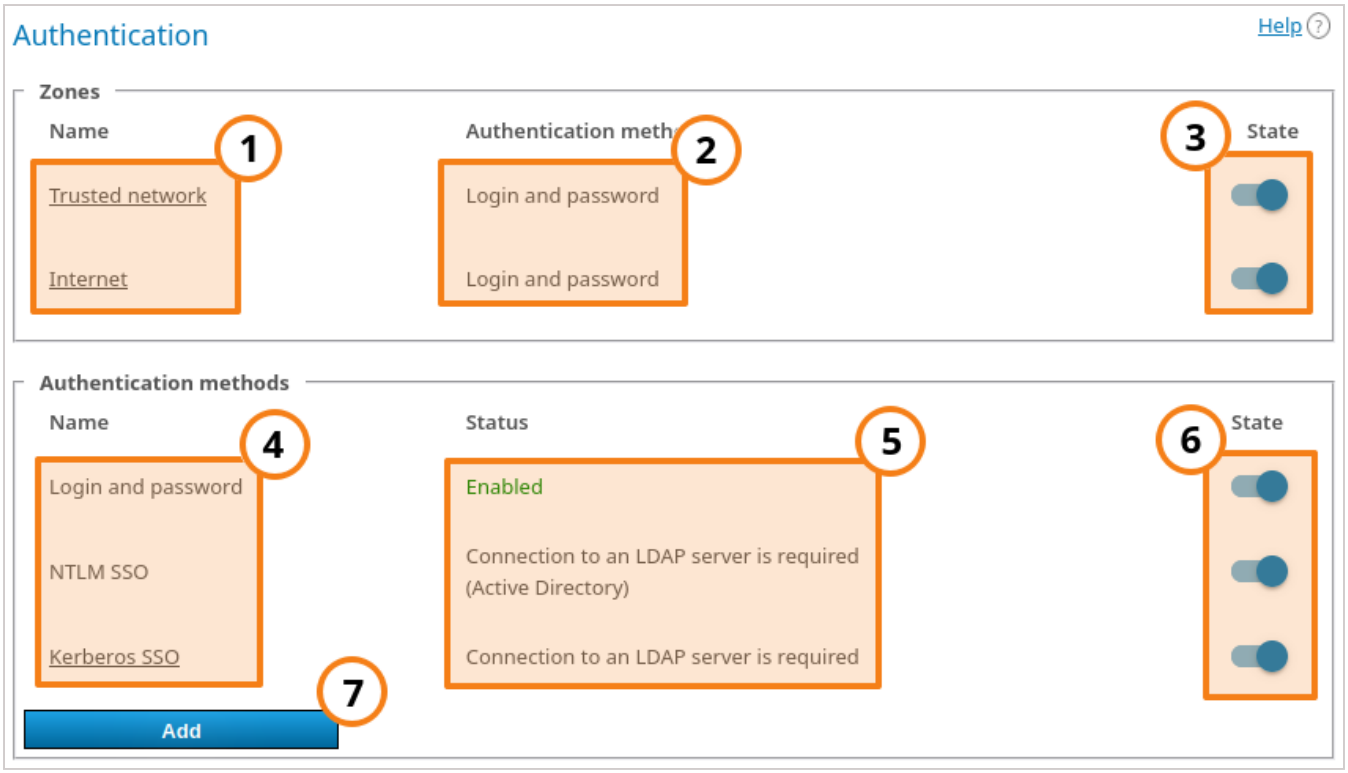
The second option is more transparent for users, but in this case, it will be more difficult to configure a convenient system of aliases.

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.

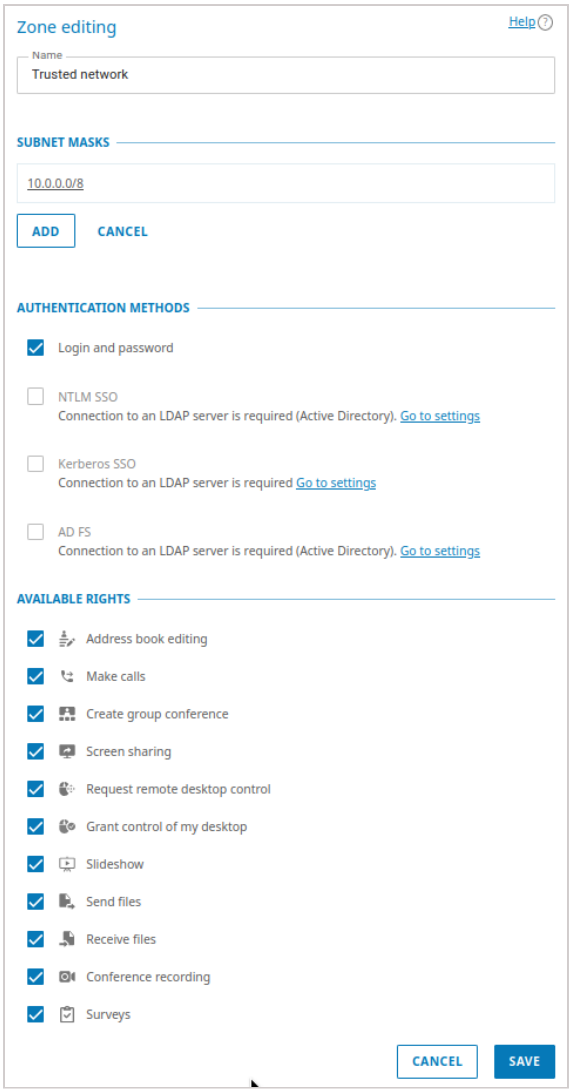


1. Security zones. To open the settings of the security zone, click on it.
2. Authentication methods specified for each zone.
3. Zone activation or deactivation. When a zone is deactivated, the users, who belong to this zone, will receive a notification that authorization is currently unavailable when 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. Authentication methods available for configuration. There are no parameters for **Login and password** and **NTLM SSO** options; they can be simply activated with switchers on the right side. To configure other authentication providers, click on their names.
5. The configuration and work status of each method.
6. Activation of authentication options.
7. Add two-factor authentication: AD FS (Active Directory Federation Services), Keycloak, manual settings for adding a different provider.

i To enable **Kerberos SSO** and **NTLM SSO** 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:



1. You can change the zone name, e.g., to “Corporate network”.
2. In the **Subnet masks** section, specify the network segments that are included in the current zone. By clicking on any entry, you will open the pop-up window for editing the address and subnet mask. Here, you can also delete the subnet. At least, one zone has to be specified for the trusted zone.
3. To add a new subnet to the list, click the **Add** button.
4. In the **Authentication methods** section, select required parameters by checking corresponding boxes. The list of zones is generated from the following options: login and password, NTLM SSO, Kerberos SSO, and other authentication providers which were added manually as shown below.

Below you can find the **Available rights** section, where one can select the rights available for each area. The list of available rights is the same as in the group settings, and restrictions will be added for selected groups which means:

- The right is **given** to a user if he/she is in a zone where this right is allowed, **and** belongs to at least one group that was granted this right.
- The right is **denied** to a user if he/she is in an area where this right is prohibited **or** belongs to groups that were not given this right.

Don’t forget to save changes to apply them on the server.

It is possible to specify the name of the **external zone**, its authentication methods, and available rights, but one cannot specify subnets.

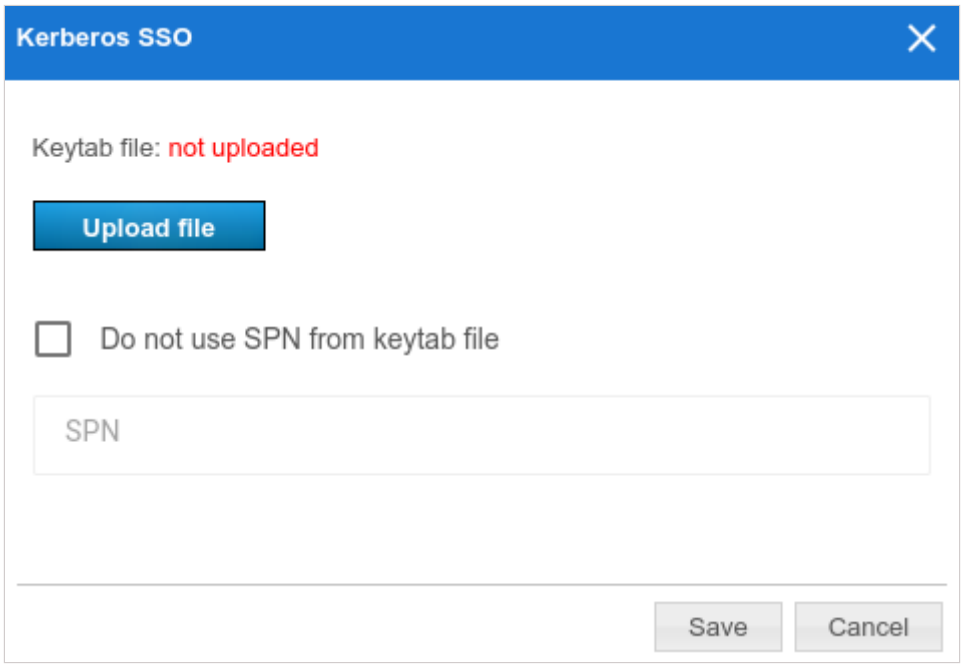
13.5.2. SSO settings

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):

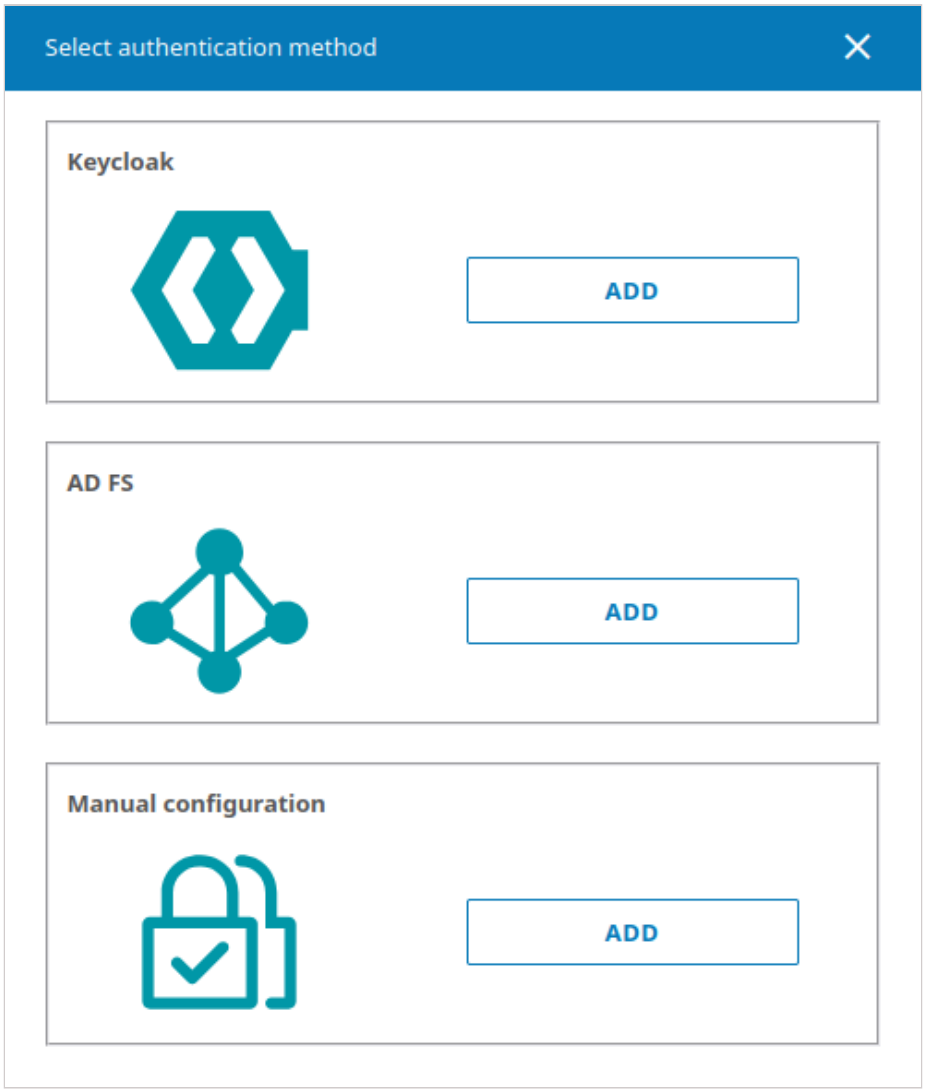


In the pop-up window, select:

- 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.

13.5.3. How to add two-factor (2FA) authentication providers

It is possible to add one or several methods of two-factor authentication (AD FS or OAuth 2.0 providers) to select them later for a certain zone(the number of providers is not limited). To do it, click **Add** in the **Authentication methods** section.



Active Directory Federation Services (AD FS) is the software component of Windows Server which acts as the authentication provider needed for accessing the resources outside the Active Directory corporate system, for example, it may be used for accessing web applications.

To configure integration with the selected authentication provider, click on the **Add** button in the corresponding section and specify the following parameters in the settings window:

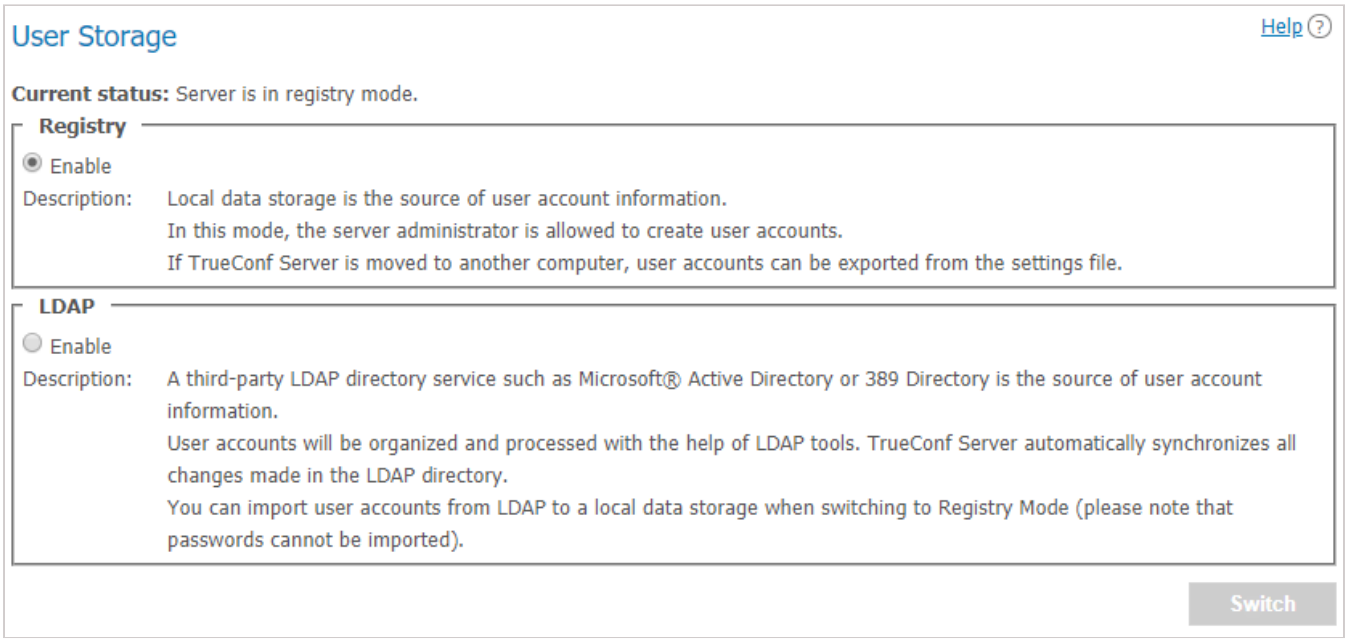
1. The identifier (Client ID) of the OAuth application created on the side of AD FS for receiving the access token.
2. URI on the side of used for receiving the response from AD FS; it also needs to be specified on the federation service.
3. **Authorization form URL** on the provider's side.
4. **Request token URL** required for users' connection to TrueConf Server in case of successful authentication.
5. **Logout URL**.
6. **Scope**.
7. The authentication provider name displayed in the list of authentication options on the page where access zones are configured and in TrueConf client applications when two-factor authentication is used.

8. On the side of TrueConf Server, you can also disable the verification of the SSL certificate received from AD FS.
9. To make it easier to distinguish one authentication method from another, you can set a custom image, by uploading it in the SVG format.

In addition to AD FS, other solutions may be used to implement two-factor authentication based on OAuth 2.0, for example, Keycloak. The list of settings will be identical to the settings for 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:



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:

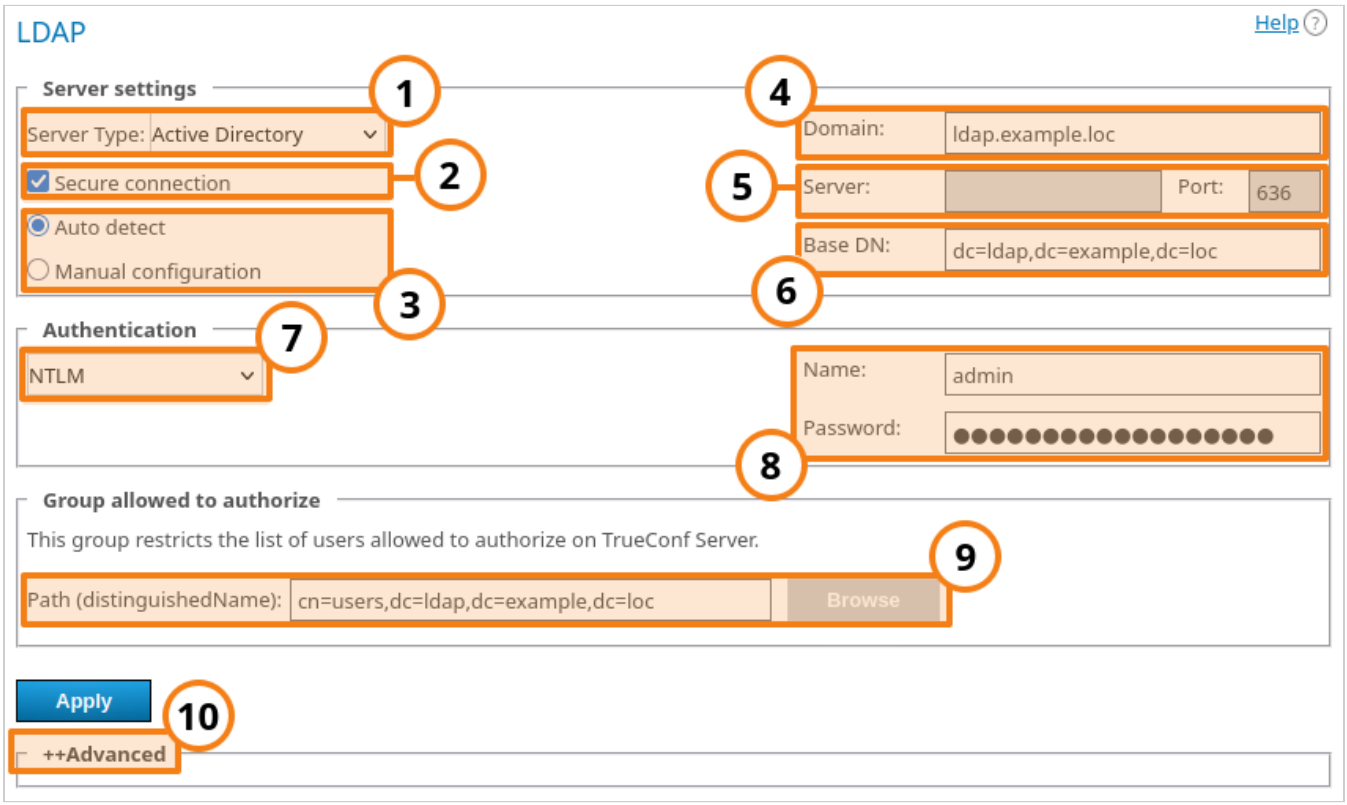
- Automatic syncing of user information
- No need for authorization within the network at the workplace
- Transparency, speed, and ease of administration
- Administration security

- 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:



1. Server type, the following types are supported: **Active Directory**, **OpenLDAP**, **389 Directory Server**, **FreeIPA**. This parameter affects the default attribute names read by the server from the LDAP directory. You can also select the **Custom** option to manually specify attribute names. After choosing the server type, expand the **Advanced** section below and click the **Default** button to switch to the corresponding attribute names. You will see that the attribute names in the **Value** column have changed. If necessary, you can enter required values, and then click the **Apply** button which is also displayed 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).

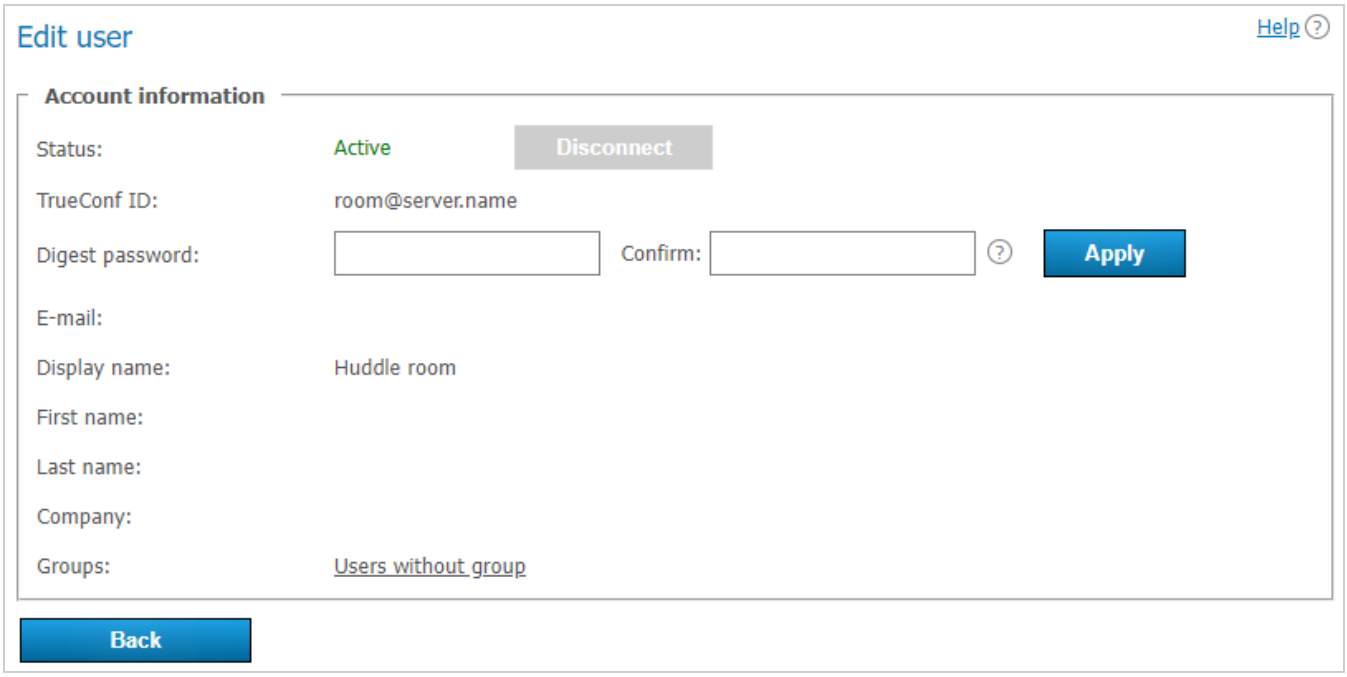
4. In the automatic mode the LDAP server can be chosen among the servers by default of the DNS domain, specified in this field. Default servers are being chosen according to the relevant DNS-notes of SRV type. For Active Directory DNS domain name AD can be indicated here.
5. The address and port of the 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. This will allow you 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:



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. Additional LDAP parameters

Below you can find additional LDAP parameters and their purpose (user fields, filter rules, etc.). Depending on the chosen provider type, some parameters may contain pre-filled values (which can be reset if necessary):

- **Login** — login
- **Display Name** — full display name
- **First Name** — first name

- **Middle Name** — middle name / patronymic
- **Last Name** — last name
- **Email** — email
- **Company** — the name of the organization
- **Branch** — the name of the branch office
- **Department** — department
- **Job Title** — job position
- **Manager** — the manager's name
- **Address** — user's address
- **Max Results** — the total number of pages returned in the search results (5000 is selected by default for all templates of LDAP providers)
- **Max Request Limit** — the number of pages returned by a single request (1000 is selected for all templates by default). This means the server requests data from the LDAP directory in batches of this many pages until it reaches the limit set in **Max Results**
- **Filter Disabled** — ***(for Active Directory only)*** determines whether the user is included or not
- **Group Member** — determines which participants are in a specific group
- **memberOf** — ***(for Active Directory only)*** the parameter which is responsible for linking an object to groups. It includes the list of group DN entries for each user (needed for filtering users by groups).
- **Filter Login** — the filter for searching by logins
- **Filter CallID** — not used, retained for backward compatibility
- **Filter Group** — the filter for searching by groups which prevents other objects with matching names from being loaded
- **Attr primaryGroupId** — ***(for Active Directory only)*** group ID parameter
- **Attr primaryGroupToken** — ***(for Active Directory only)*** group token parameter
- **Attr objectSid** — ***(for Active Directory only)*** object ID parameter
- **Attr SIP Phone** — the SIP number for calling the user
- **Mobile Phone** — mobile phone number for contacting the user
- **Work Phone** — work phone number for contacting the user
- **Home Phone** — a home (personal) phone number for contacting the user
- **User Status Attr** — the attribute that determines the user's absence status across different servers simultaneously
- **User ID Attr** — the attribute that determines the user's absence status across different servers simultaneously by his/her ID
- **Full ID Attr** — the attribute that determines the user’s absence status across different servers simultaneously with the help of the full user ID (with the domain name included)
- **DetailedUserInfo Attribute** — overrides the fields that will be displayed in the user information
- **User Alias List** — the list of attributes that will serve as user aliases after authorization
- **TrustPartner Attr** — ***(for Active Directory only)*** the filter that enables you to combine multiple domains into a trusted domain

- **FlatName Attr** — ***(for Active Directory only)*** the display name for the trusted domain, when multiple domains are combined into a trusted domain
- **TrustedDomain Filter** — ***(for Active Directory only)*** the filter that allows you to combine multiple domains into a trusted domain
- **ForeignSecurityPrincipal Filter** — ***(only for Active Directory)*** the filter that allows you to combine multiple domains into a trusted domain
- **Trust Enabled** — ***(for Active Directory only)*** the filter that allows you to combine multiple domains into a trusted domain
- **FilterClientSearchByLoginGroup** — (`boolean`) used for searching contacts in a client application. If this attribute is not specified explicitly, it defaults to `true`. Moreover, only the users who belong to the login group will be found. If set to `false`, it allows finding other users in the LDAP directory who, for some reason, are NOT yet part of the login group.
- **Use Avatars** — has to be set to `1` to make sure that avatars are loaded correctly in applications
- **Allow Avatar Propagating** — has to be set to `1` to make sure that avatars are loaded correctly in applications
- **AddressBook Refresh** — a timer (in seconds) for periodic caching of relationships between groups and regeneration of address books. When the timer expires, it is assumed that the request did not yield any search results.
- **Filter AddressBook** — the filter that can be used to create a user's address book
- **TimeOut** — the time allowed for connection/request execution (in seconds). When this time elapses, it is assumed that the request did not yield any search results.
- **thumbnailPhoto Attr** — avatar
- **jpegPhoto Attr** — storage location for the avatar
- **Meeting Room Filter** — not used
- **Meeting Room Search Filter Attr** — not used
- **Meeting Room BaseDN** — not used
- **LDAP Login with subdomain** — allow users from subdomains to sign in, their login will be in the format `sub.domain\user`.

13.8.2. 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.

13.8.3. 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:

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

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

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

Ha CentOS:

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

```sh
cp /home/$USER/cert.crt /etc/pki/ca-trust/source/anchors/ && update-ca-trust
```

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):

```sh
telnet [ldap-server] [port]
```

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:

```sh
telnet ldap.example.com 636
```

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:

```sh
openssl s_client -connect [ldap-server]:[port]
```

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

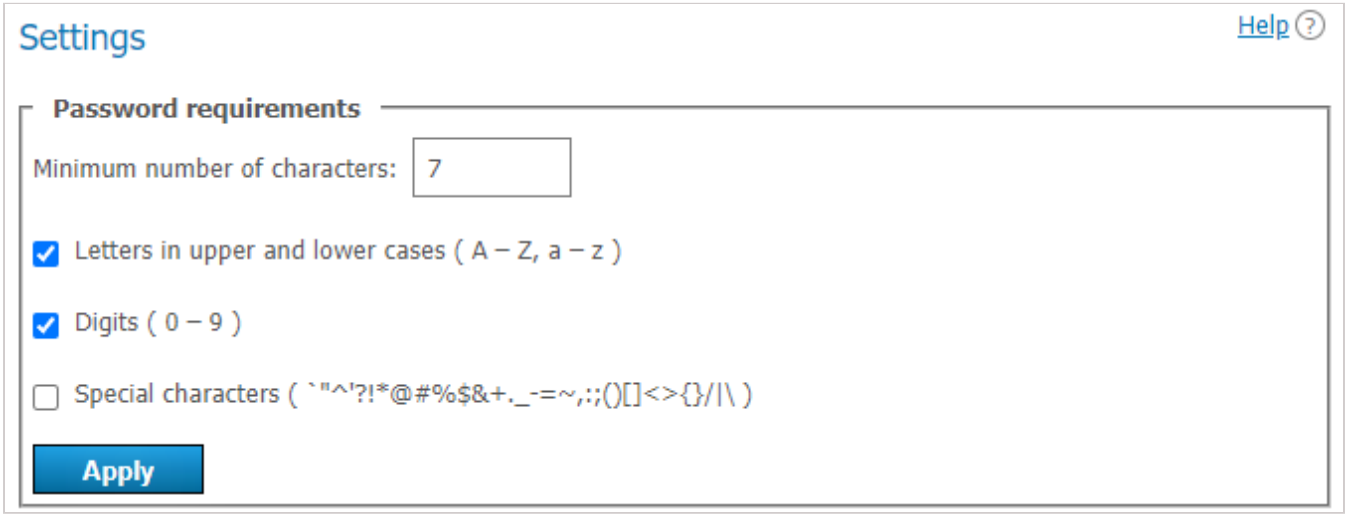
Make sure that:

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**.

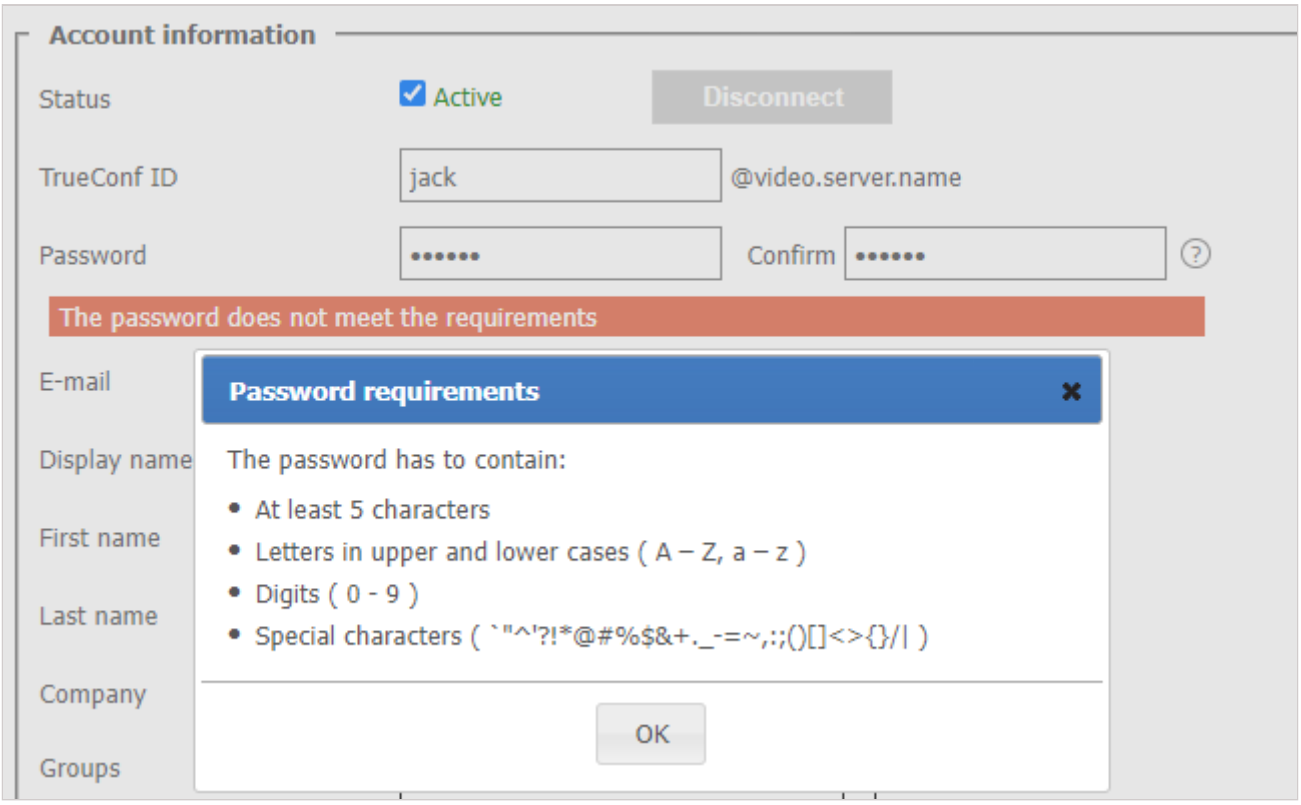
13.10. Password and account lockout settings

13.10.1. Password requirements

If Registry mode is used, in the **Password requirements** section, you can specify the minimum allowable password length (from 2 to 64) and select mandatory characters (upper and lower case letters, numbers, special characters) for users of your TrueConf Server. A password will be checked against these requirements when a new account is added or when the password is changed for an existing account. This includes the cases when a user edits the password in the personal area:



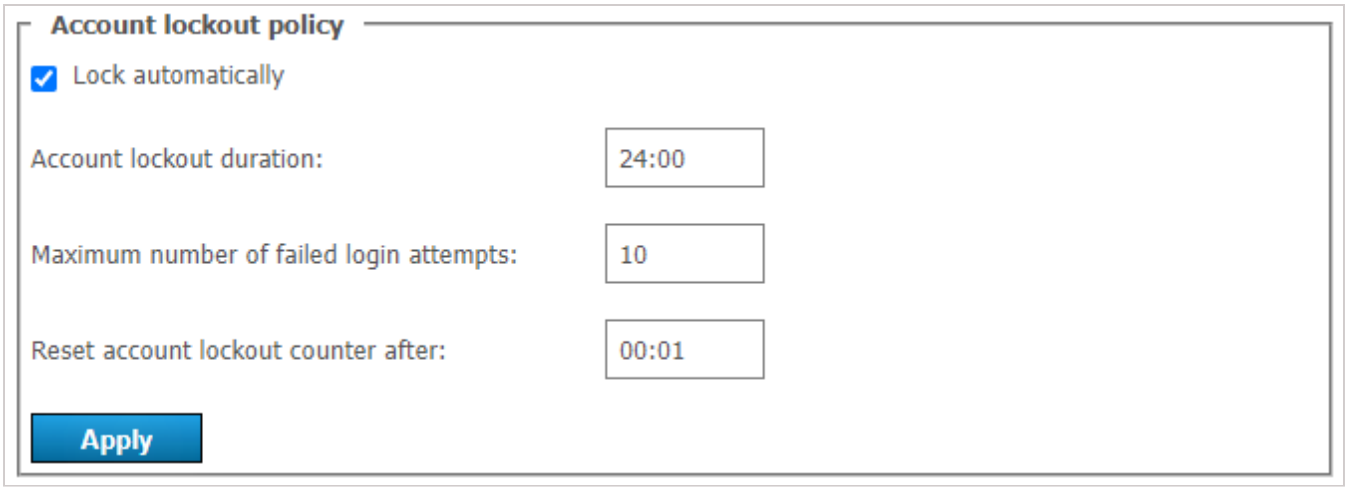
If the password does not meet the requirements, an error message will be displayed. Click on the ⓘ button (which is next to the input field) to view the password requirements:



13.10.2. Automatic lockout

In the **Account lockout policy** section, you can configure the logic for locking a user account in the event of incorrect password entry during authentication.

* 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.



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:

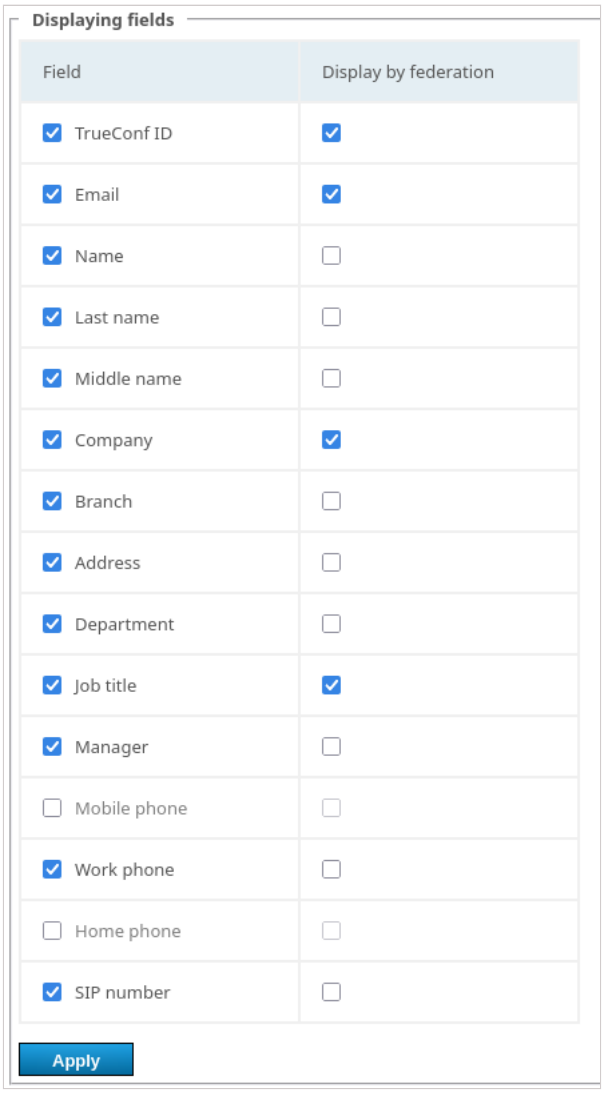
- **Account lockout duration** = ***6:00*** (6 hours);
- **Maximum number of failed login attempts** = ***5***;
- **Reset account lockout counter after** = ***00:10*** (10 minutes).

If a user with an existing server login (TrueConf ID) makes five failed attempts to enter a password with less than 10 minutes between each attempt, the account will be locked for 6 hours. However, if there is a 10-minute gap after any attempt (e.g., after the 4th attempt), the counter will be reset to 1.

13.10.3. Display of fields from a user card

In the **Displaying fields** section, you can select which user profile fields will be visible in the following parts of the UI:

- When users view their profile in TrueConf client applications and in the personal area
- When opening a contact card (information about another user) in the application or in the personal area
- (*Has to be configured separately*) when user information is viewed by the users from a federated server.



In the **Field** column, select which user data from your TrueConf Server will be available to anyone. In the **Display by federation** column, specify which of the selected fields will be shared with federated users who view information about the users of your server.

14. Group conferences and streams

This section enables server administrators to schedule conferences, invite participants, and set other parameters.

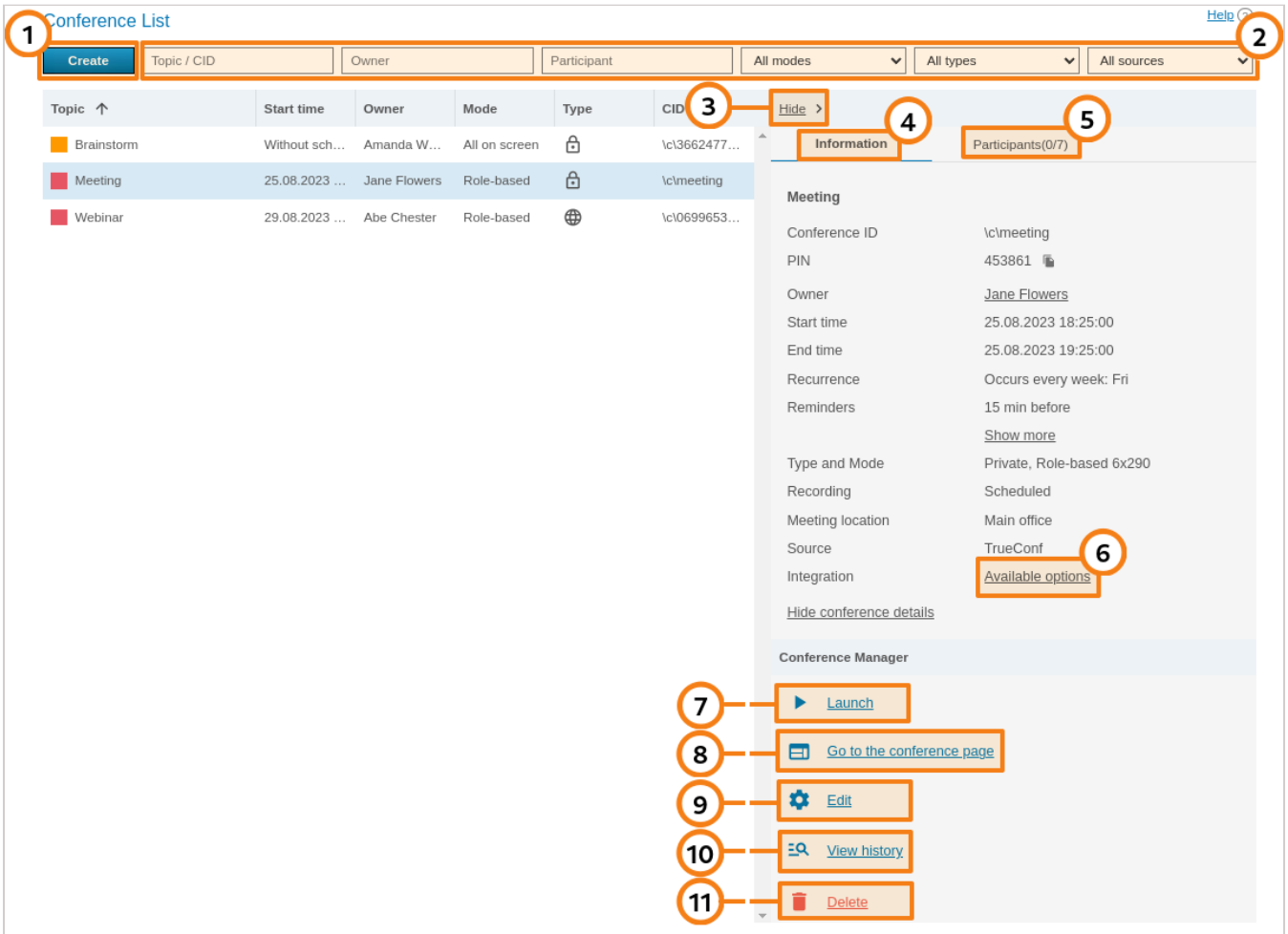
Such conferences can be launched automatically (at a specified time or according to a schedule) or manually by server administrators.

* 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:

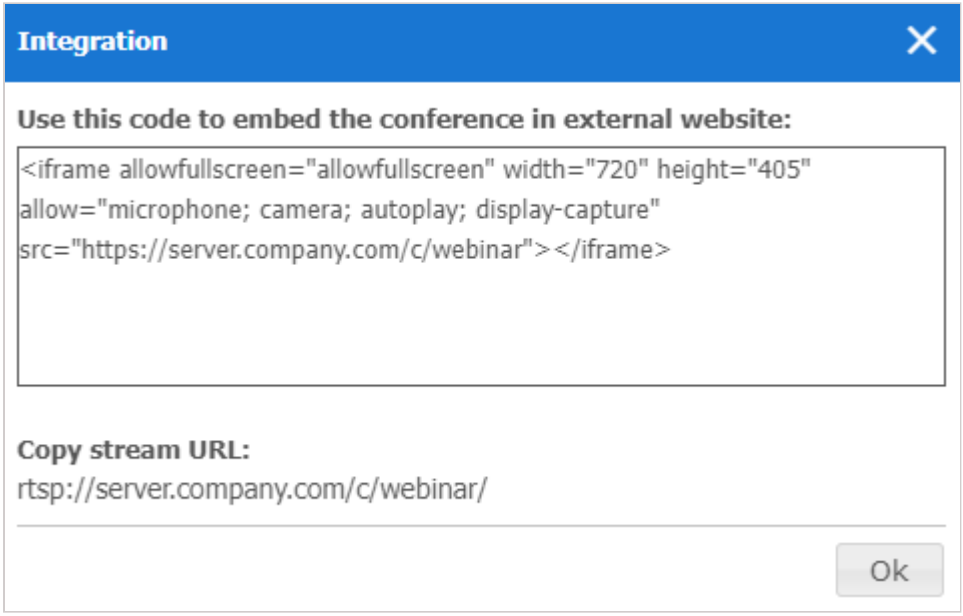
- events created by administrator in this section of the TrueConf Server control panel
- events added by users in the application or personal area
- active conferences created ad hoc in the client applications (they will disappear from the list when they end).



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.
6. Click on the link to get the HTML code of the widget needed for embedding the conference on external websites. It wil 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:

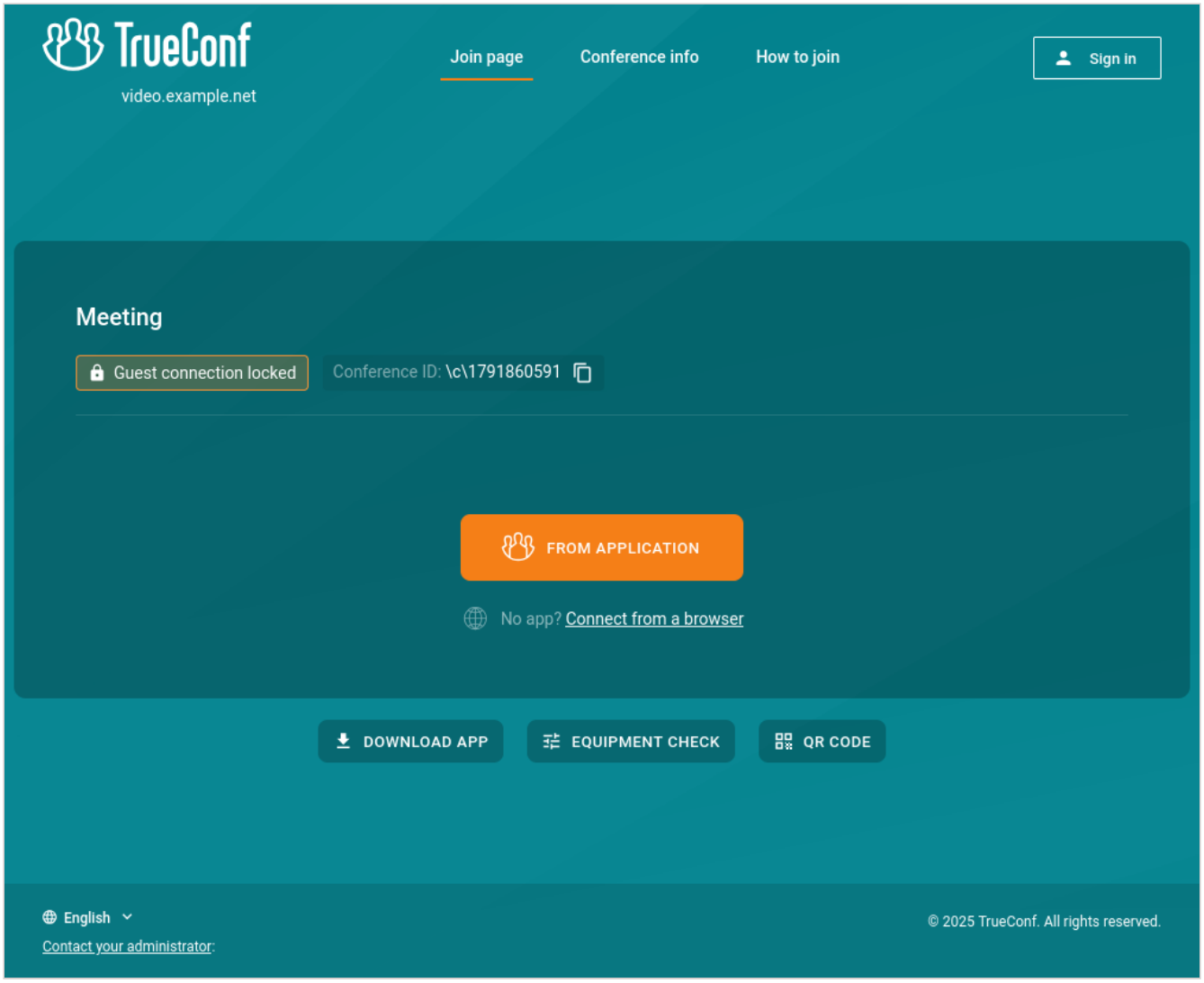


7. Start the conference manually. Before the start you will be offered to invite all the participants to the conference or select particular users. At conference forced start, only online users will be invited to the conference. Email invitations will not be sent out.
8. Go to the conference page.
9. Edit the selected conference (unavailable for an ongoing meeting). In the conference editing menu, you can use almost the same group of features that are available when a conference is created.
10. View the previous sessions (history) of the selected conference in the **Call History** section.
11. 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. Saving guest connection data

There are several convenient features available to the guests who join webinars:

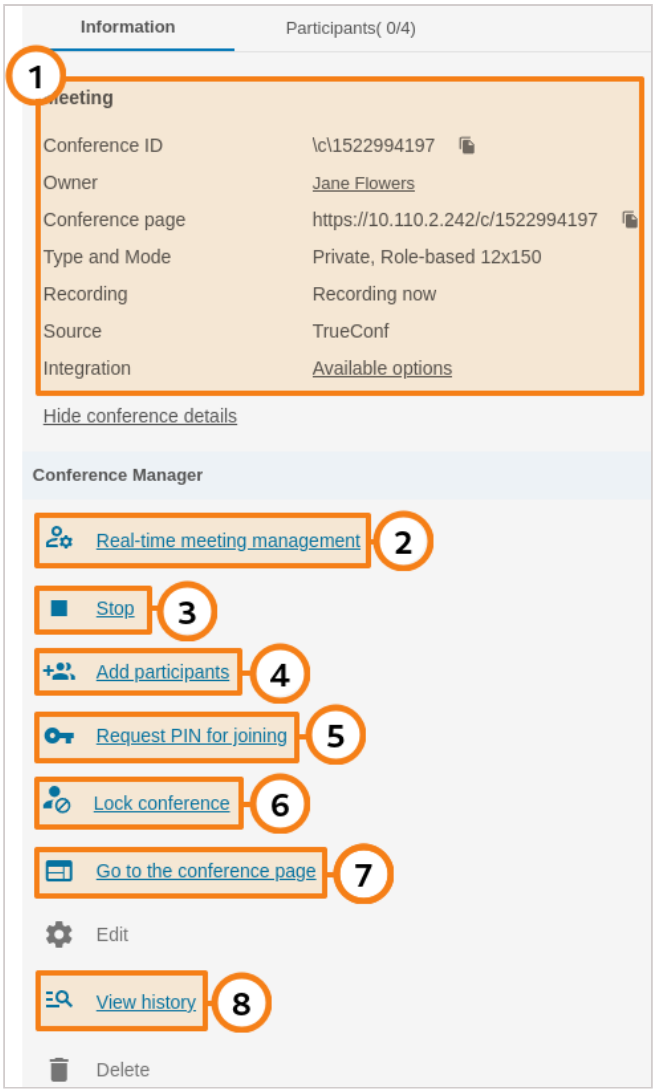
- The temporary internal ID (login) created for a guest is bound to the browser and client application (this ID may be displayed, for example, in the connection list on the page of a session). The guest ID will change if a different application is used (e.g., if a user signs in on a different device), if a different browser is used, or when connecting in incognito mode in the browser.
- Since the ID is saved, it is possible to gather accurate data about the number of participants and other metrics for reports and analytics.
- If a user is suddenly removed from a conference (e.g., if connection is lost) or if the user leaves the conference and then decides to join the meeting again, he/she will see all chat messages, even though these messages were sent when the user was not connected to the conference.
- Thanks to saving the ID, you can leave the conference, quickly change the display name, and join the meeting again (for example, if a typo was made or the name which was entered previously does not meet the requirements set by the administrator). All messages sent under the previous name will also be displayed to all other participants with the new sender's name.

14.4. How to configure an ongoing meeting

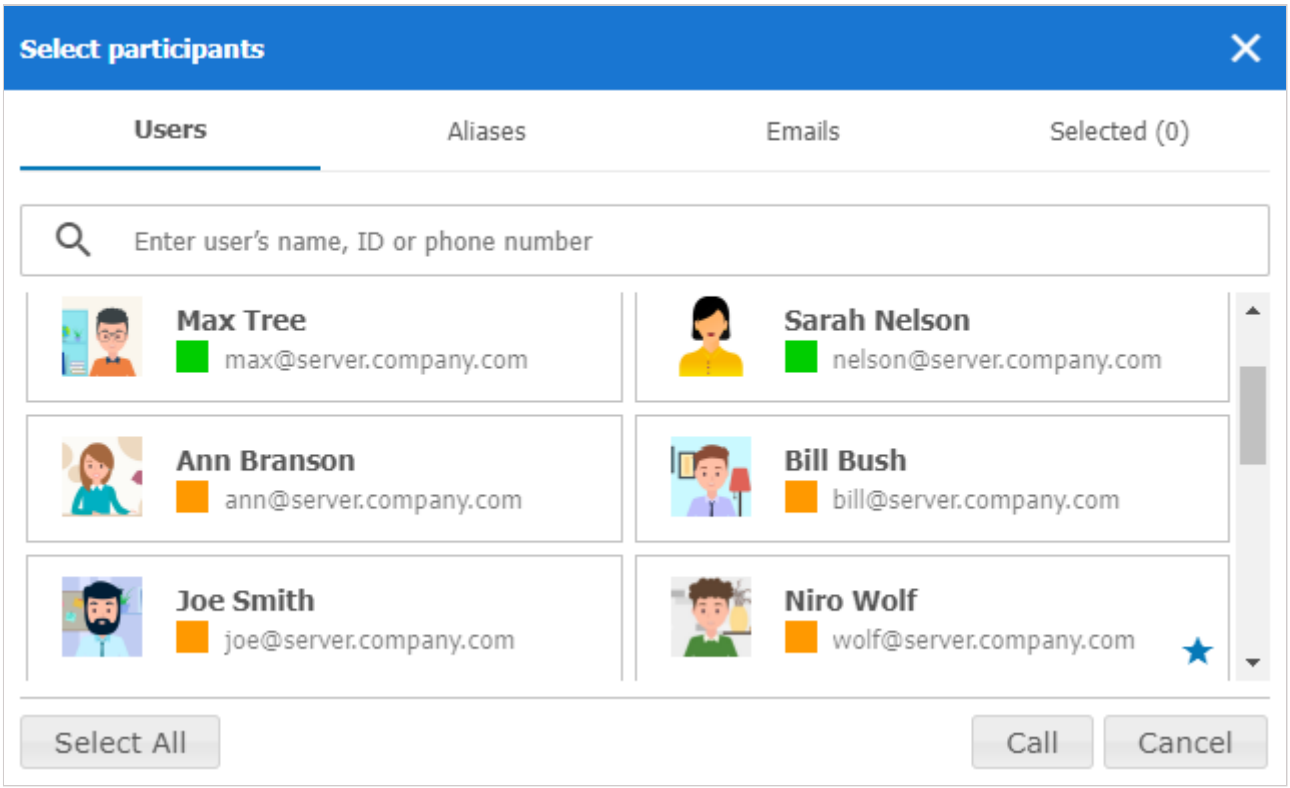
When selecting an ongoing conference, the administrator can view information about it or change some of its parameters (e.g., the layout or PIN code). Standard editing and deletion options will be unavailable.

14.4.1. "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.

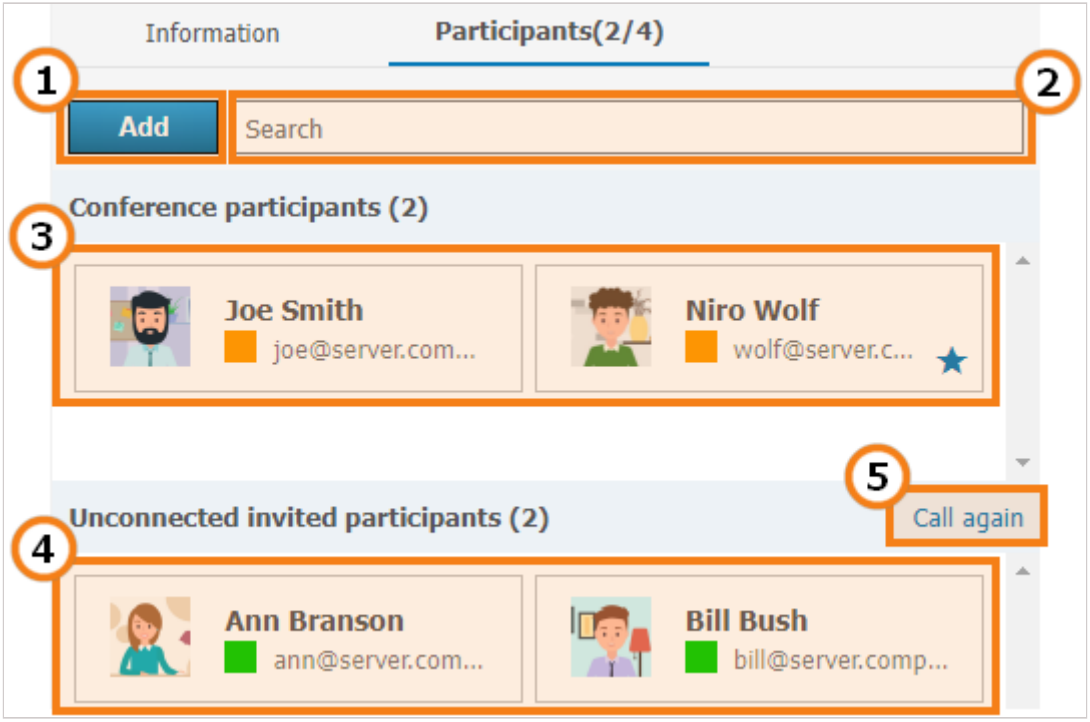
7. Go to the conference page.

* 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.

14.4.2. "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.

14.5. Creating a new conference

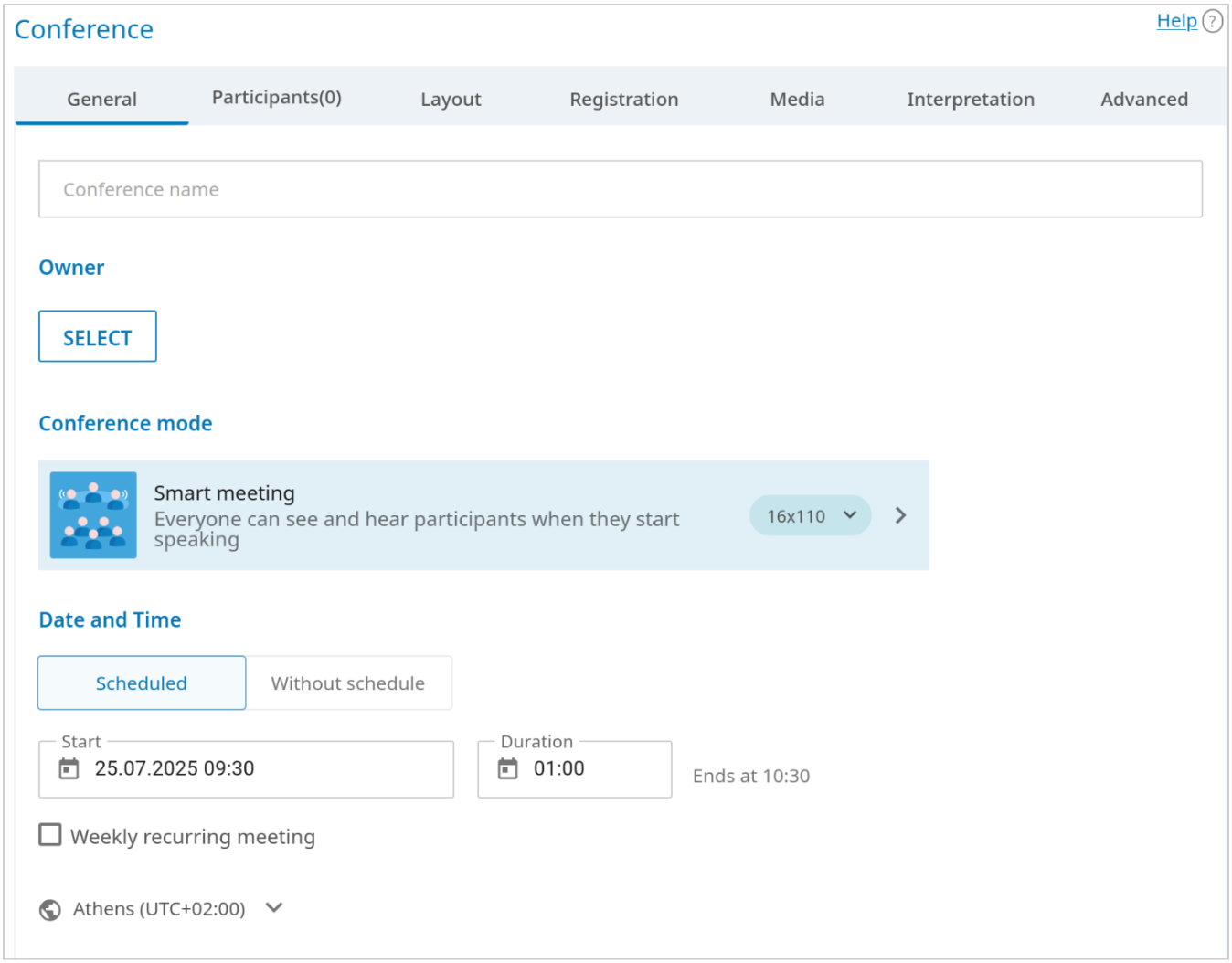
By clicking on the **Create** button in the **Conference List** menu, you will open the **General** tab where one can configure the most widely used settings.

It is also possible to create a conference from one of the templates saved earlier.

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.

14.5.1. "General" tab

At the top of the **General** tab you can find the parameters required for creating a conference:



1. **Conference name** — for example, "Marketing department meeting".
2. **Owner**, see the detailed role description.

> * When scheduling a conference, the administrator selects the owner (who is automatically given the moderator role) and other moderators. The remaining roles are given to users during the conference.

3. Conference **Mode**: all on screen, smart meeting, moderated role-based conference, video lecture. Just click on the option, which is currently selected, to choose a different mode.

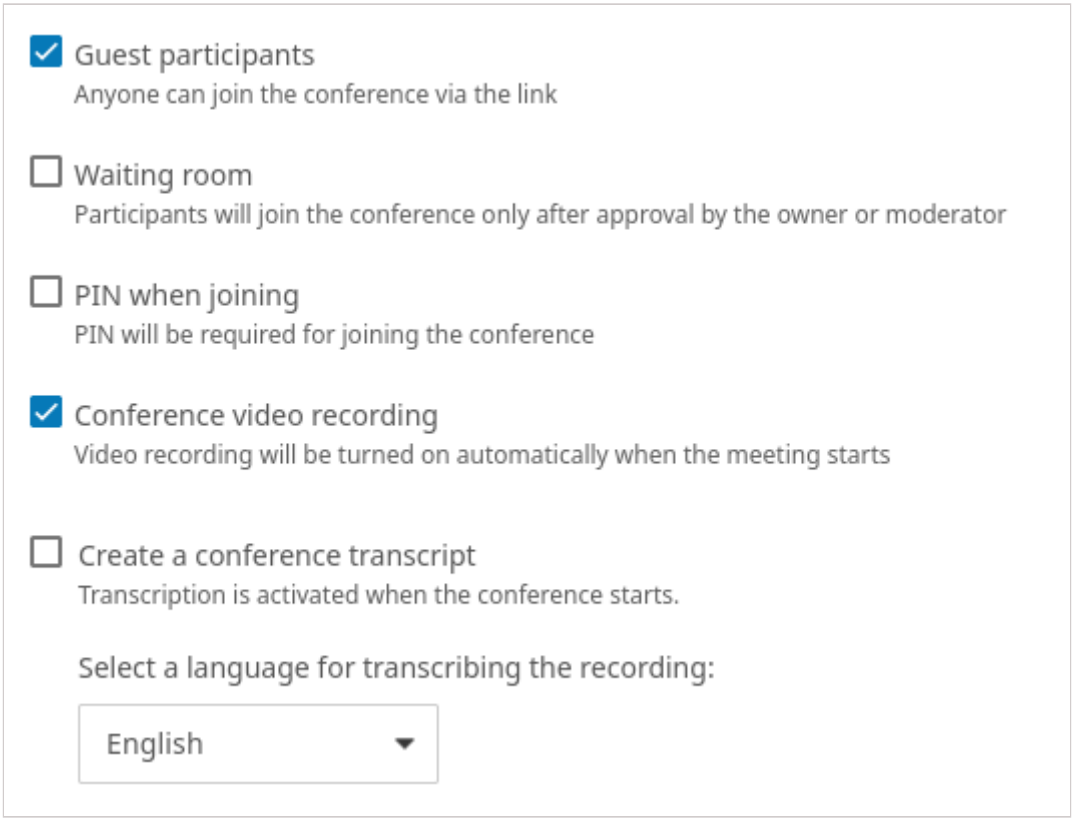
Refer to the documentation on TrueConf client applications to get a better idea of how the layout is filled in a smart meeting with different types of connections.

For moderated role-based conferences and smart meetings, you can specify the number of speakers.

* The maximum number of participants in a moderated role-based conference and smart meeting depends on your license type. The number of participants can reach **2000**. The maximum number of speakers in a smart meeting or moderated role-based conference is **49**.

1. In the **Date and Time** section, choose the conference launch type: unscheduled (virtual room) or scheduled. If you choose to create a scheduled conference, select the time for a one-time or recurring conference. On the **Additional** tab, you can also configure time extension settings for a scheduled conference.

Below you can find access settings, server-side recording settings, and the parameters for speech recognition (available if the integration with the AI server is configured):



To make the conference public (create a webinar), check the **Guest participants** box.

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.

* **Learn more about webinars in our articles and videos:**
  - What is a webinar?
  - Tips for secure webinars
  - How to organize webinars

To activate the waiting room for an event, check the corresponding box. You will be able to select which category of participants will be directed to this room. The list of participants, who can be put in the waiting room, varies slightly for private and public conferences.

SIP/H.323/RTSP connections are always treated as the participants from other servers. For example, if an endpoint makes a call to a conference or is invited to this meeting, it will be directed to the waiting room if all the settings are activated except **Guests only** for a webinar.

i 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**.

If necessary, you can save conference settings as a template so that you could later create an event with the same settings in one click. To do it, check the box **Save as a template** at the bottom of the conference editing window.

Check the box **PIN when joining** to request participants to enter the PIN code when they are joining the conference. This requirement will enhance meeting security by protecting against unwanted participants, even if they have the link, for example, when a webinar is held. If this box is checked, a PIN code will be automatically generated, but you can enter your own PIN in the field below or regenerate it with the help of the button . The use of PIN protection is not available when registration for a public conference (webinar) is enabled.

* To directly connect from an SIP/H.323 endpoint to a PIN-protected event, add the PIN code separated by a comma after the conference ID in the call string:

  `00<conf_id>,pin@<trueconf_server>:<port>`

Check the box **Enable conference recording** to save the video recording of this event on the server (refer to the description of the **Recordings** section). If this feature is enabled, information about it will be displayed on the event page, and the owner can manage the recording (pause and resume) "on the fly" during the conference. Activate the indicator in the **Recordings** section to make sure that all participants (including SIP/H.323 endpoints and participants who join from browsers) know that the event is being recorded.

If your TrueConf Server is integrated with TrueConf AI Server, you can override some of the settings for a specific conference:

1. If the "on-demand" audio recognition option is selected in the general activation settings, you can check the box **Create a conference transcript** to save the audio track of this event for AI processing.
2. Below you can select the main language of the event, which will help the AI server in difficult speech recognition situations. The language is detected automatically, but some languages may be similar in terms of pronunciation, and under such circumstances, it is useful to explicitly specify the main language of the conference.

14.5.2. "Participants" tab

On the **Participants** tab, one can check the number of participants added to the conference (the maximum number depends on the selected conference mode and the server license). It is possible to add participants from the list of server users, by ID, with the call string (for SIP/H.323/RTSP devices) and by email (for a public conference).

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.

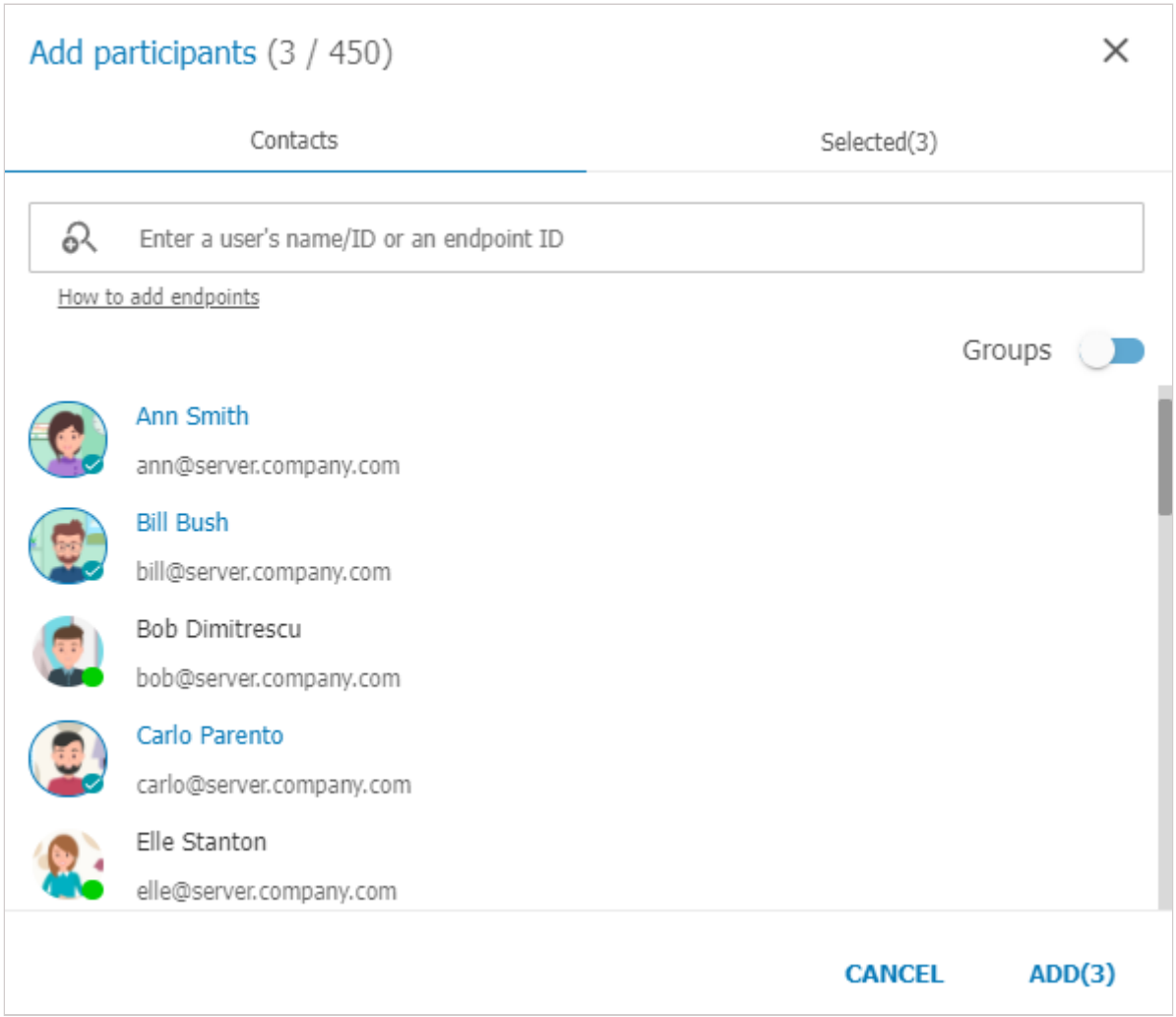
Adding email notification recipients

i This feature is available only in public conference mode.

To invite participants via email, create a list of meeting guests:

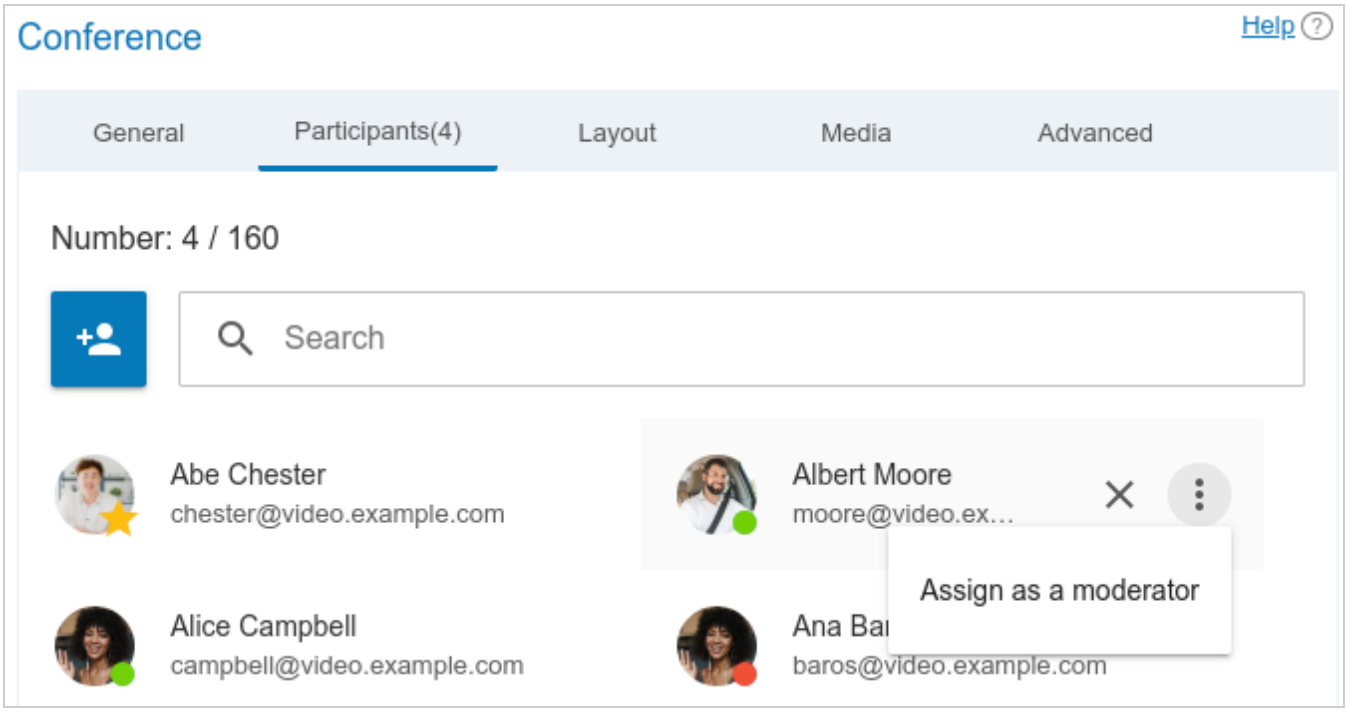
1. Go to the **Email** tab.
2. Fill in the **Name** and **Email** fields with the participant's personal details.
3. Click **Select** to add the user to the guest list.

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



14.5.2.1. 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**.



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

14.5.2.2. Resending email invitations

Sometimes, only some of the participants have to be re-invited to the scheduled conference. To do it, go to the **Participants** tab, hover the mouse over the selected participant, and click on ⋮. Select **Resend invitation email** in the context menu.

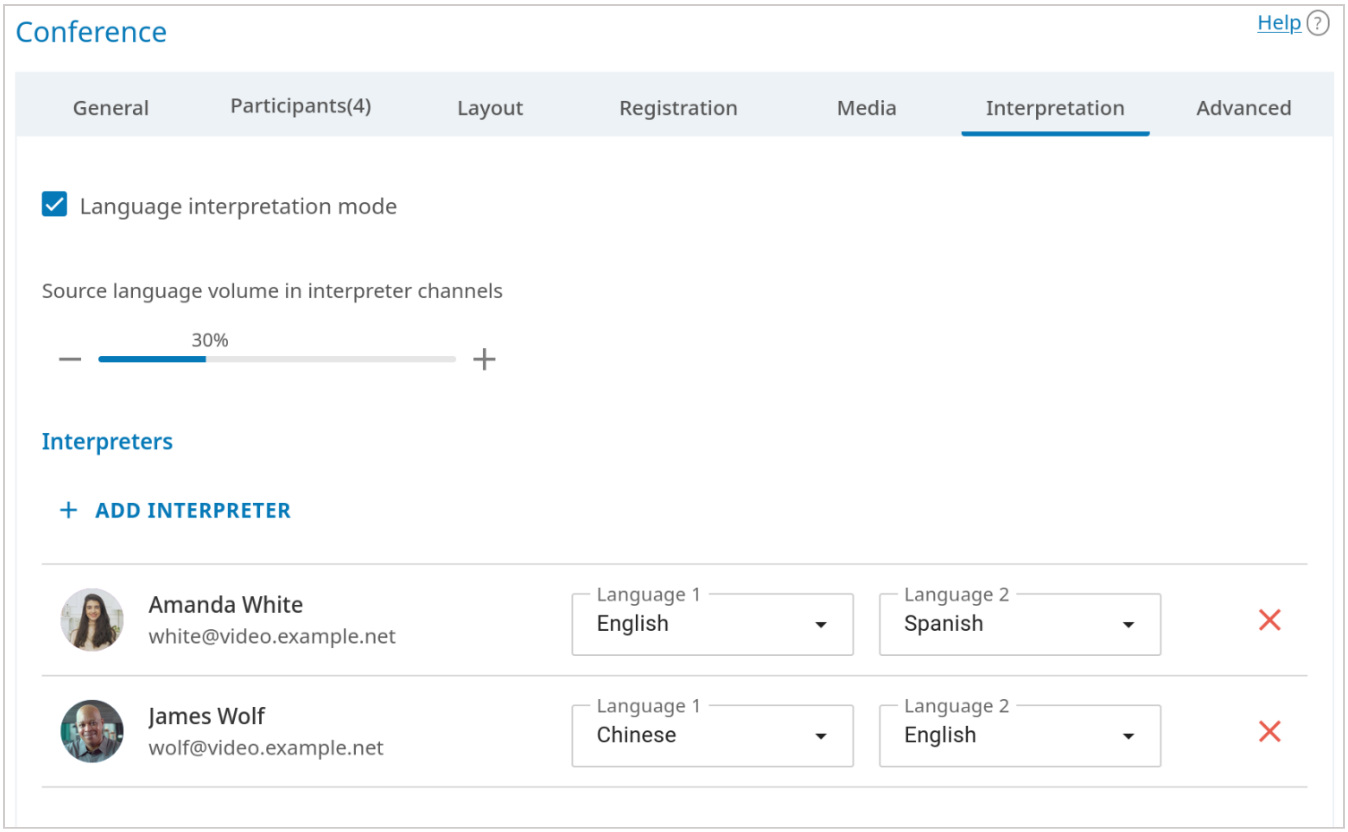
Emails are not sent immediately; they are sent ***only when conference settings*** are saved. So, if you change your mind, you can select the participant again and click ⋮ to cancel the email invitation for this person.

14.5.3. "Interpretation" Tab

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).

Check the box **Language interpretation mode** to create a conference that can be assisted by simultaneous interpreters. When a conference with simultaneous interpretation is recorded, several audio tracks will be created: a general track and separate tracks for each of the languages selected for interpretation.

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:



The role of a simultaneous interpreter can be given to a user from your TrueConf Server or from a federated video conferencing server. Guests who were either added manually when the event was scheduled, or signed up for the event (if registration was enabled), cannot act as interpreters. An interpreter is not displayed in the layout, and cannot send his/her video to other participants during the conference (video settings are simply unavailable).

In this way, you can select several interpreters, including for the same language pairs (for example, one of the interpreters can rest while the other one works with the same languages). At any given time, only one person can interpret the selected language pair in one direction. For instance, only one person will be able to translate from English to Hindi, however, the second person can translate from Hindi to English.

In interpreter channels, participants will be able to hear the original audio track: its volume level will be set at 30 % by default. However, you will be able to reduce the volume level to 0 % (i.e. mute the track).

Please note that you can organize "relay translation" so that multiple interpreters can translate language pairs sequentially one after another for a wider audience. Read more in the client application documentation.

14.5.4. "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.

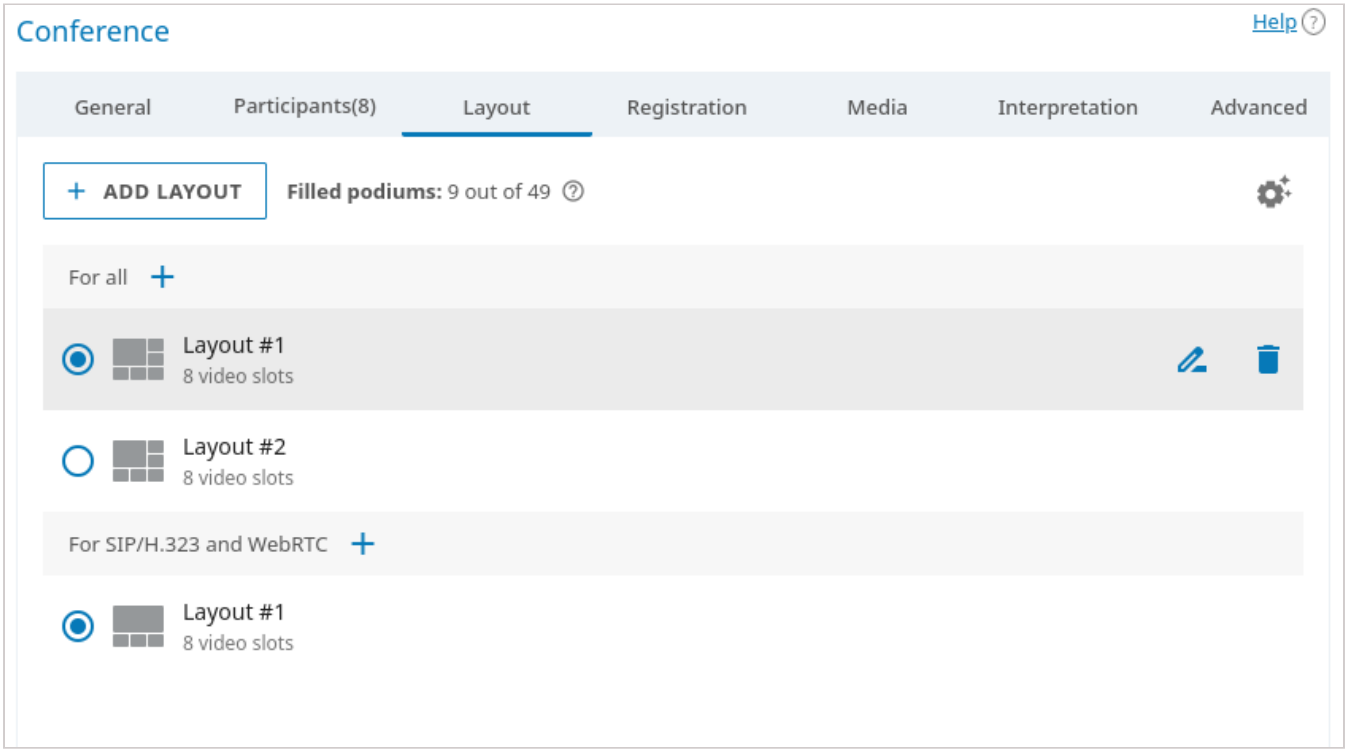
14.5.4.1. General list of video layouts

In the **Layout** tab, you can set up one or more conference layouts (the arrangement of participants' video windows). For more information about the types of video windows and their features, refer to the TrueConf Server user guide.

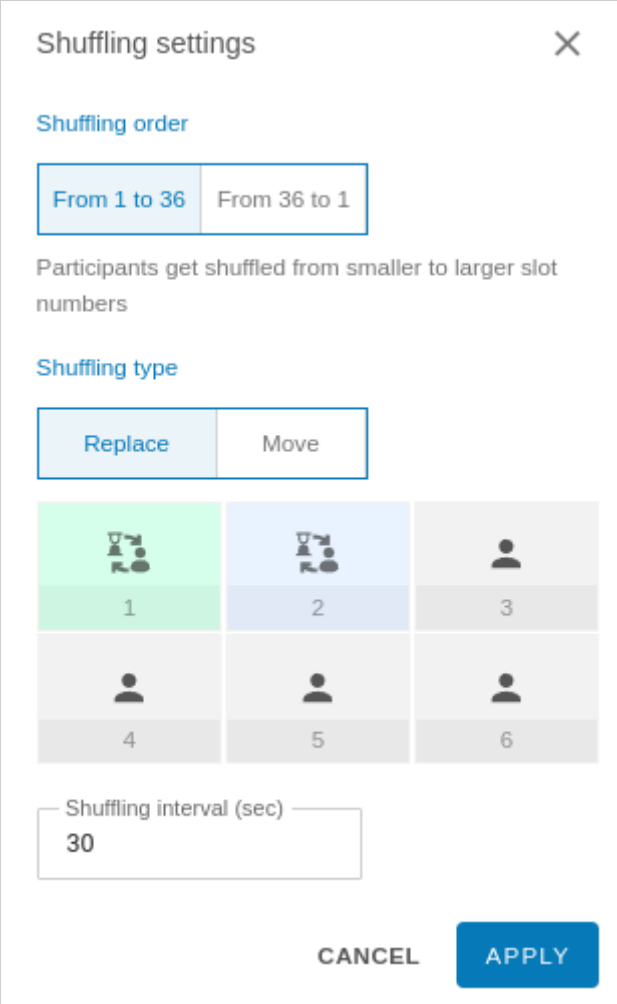
The video layout can be one of three types depending on the category of participants for whom it is created: general (for all participants), individual for a specific participant (including a separate SIP/H.323 endpoint), or the common layout for SIP/H.323 devices and browsers (WebRTC).

The video layout cannot be adjusted in video lecture mode. In smart meeting mode, there have to be at least 2 video windows of the "active speaker" type.

The list of layouts will be displayed if you previously created layouts for the event. When the mouse is hovered over any of them, you will see the buttons for editing the layout name and deleting the layout . The checkbox on the left side of each layout will determine whether this layout should be selected as the main one in its category at the start of the event:

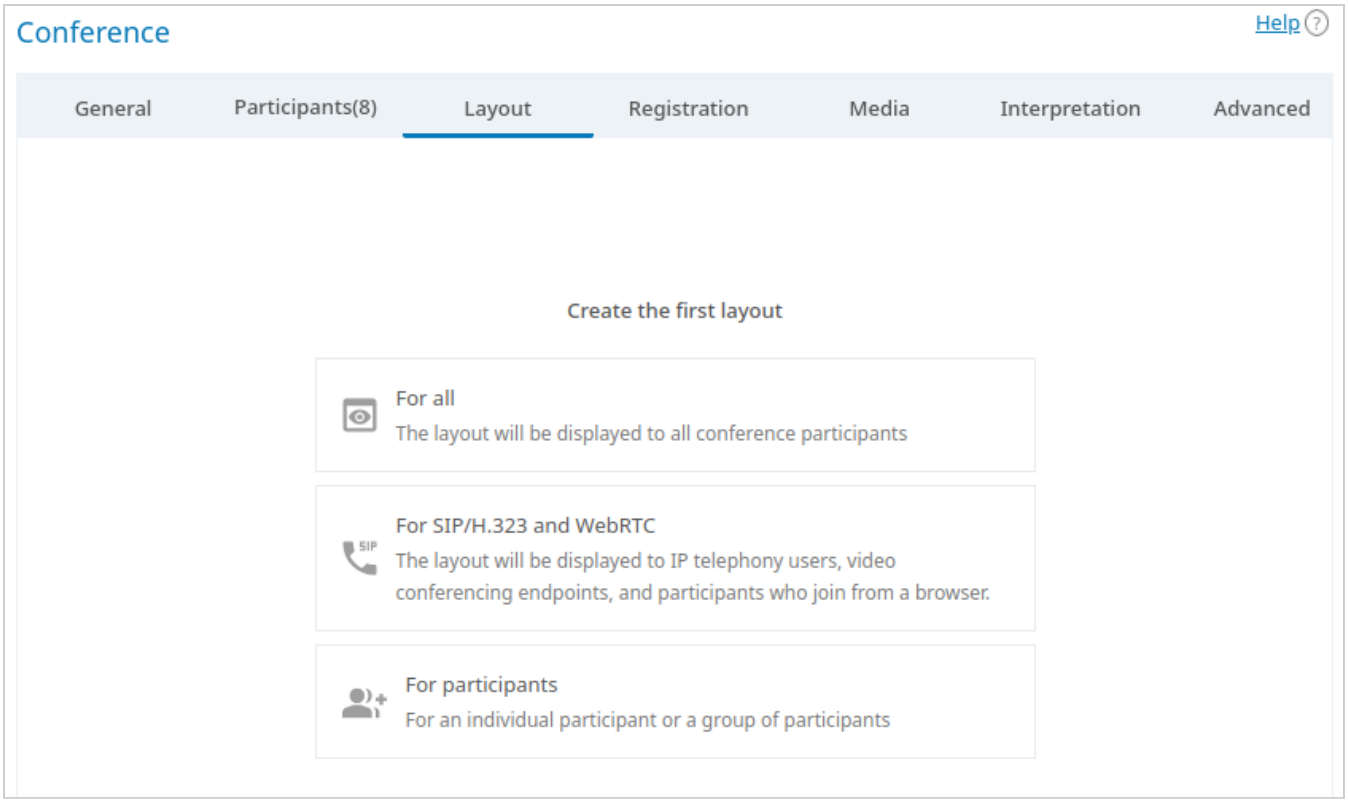


In the general list of conference layouts, you can configure display settings for video windows of the **Time-based shuffling** type. To do it, click the button in the top right corner of the list. These settings will apply to all windows of this type in all layouts of the conference. You can choose the order of displaying participants who were not added to the layout. Besides, it is possible to select the type of shuffling (rotation) and set its speed.

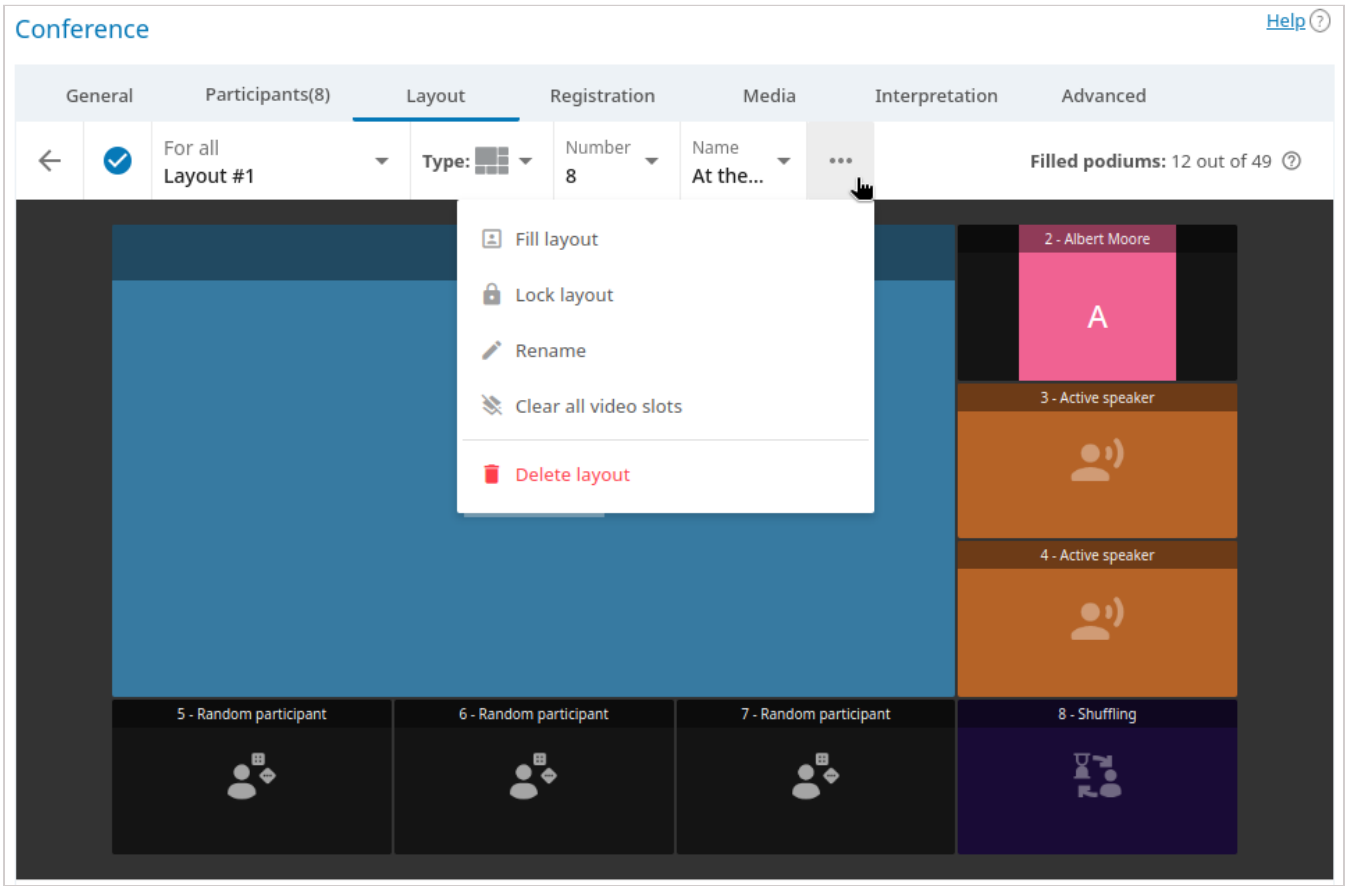


14.5.4.2. Layout editor

If the list is empty, you will first need to choose the category of participants for whom the layout will be created: a general layout (for all participants), an individual layout for a specific participant (including an SIP/H.323 endpoint), or the layout for all SIP/H.323 devices and browsers (WebRTC).



After adding a video layout, you will see the pop-up window where the layout can be edited:



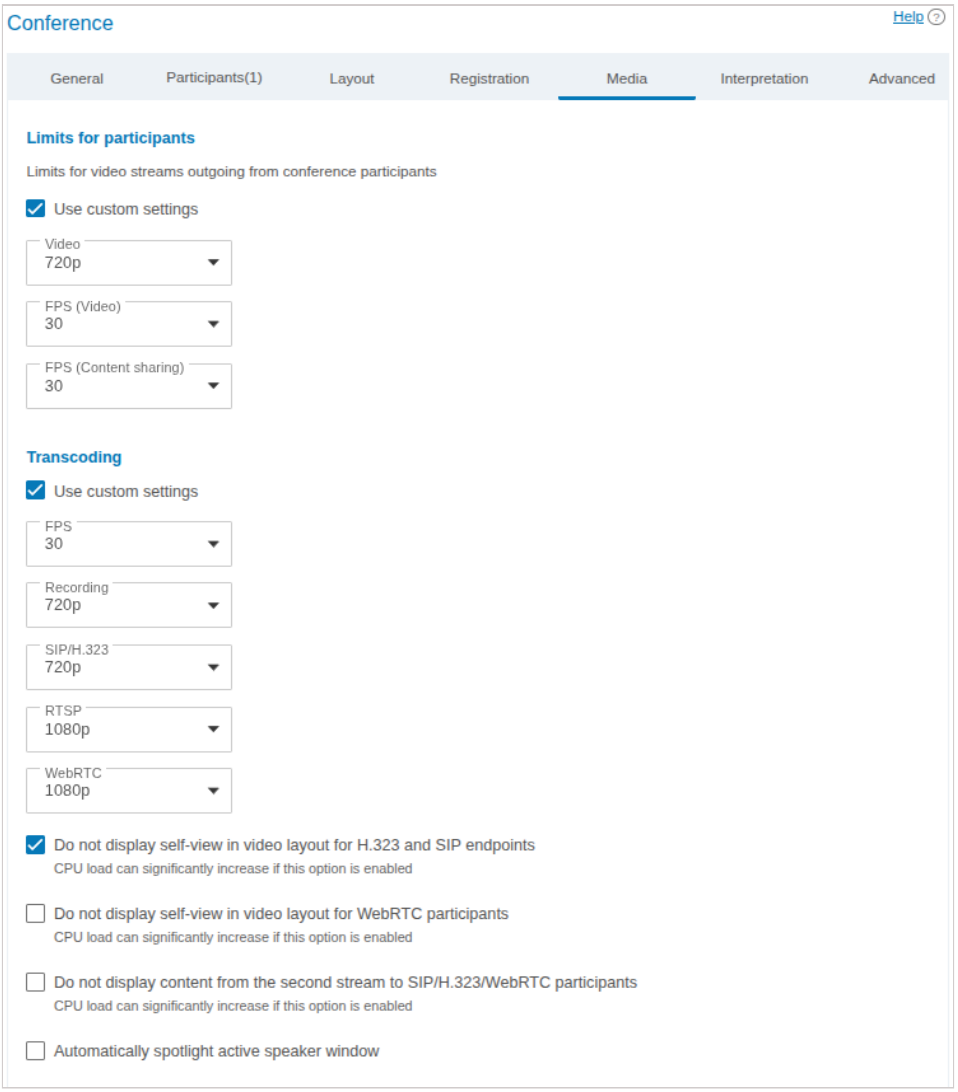
1. Edit the conference layout. You can move a participant's video window and prioritize it (enlarge) by double-clicking. When clicking on any video window, you can choose its type: **Fixed**, **Random**, **Time-based shuffling**, **Active speaker**, **Content**.

2. If the box ✓ at the top of the editor is checked, this video layout will be used by default when the conference starts (this box is checked automatically for the first layout in each category). Click on this box to disable activation of this layout at the beginning of the conference.
3. You can add a new video layout directly from the editor by clicking on the drop-down list next to the layout name and selecting **Add layout**.
4. In the **Type** dropdown list, select the arrangement of video windows in the layout.
5. In the **Number** drop-down list, select the number of video windows in the layout.
6. In the **Name** drop-down list, choose the position of the user's name in the video window.
7. Click the button ••• to open the context menu with these options:
   - **Fill layout** — allows you to automatically fill the slots in the video layout with invited participants (this option becomes available only when the layout is cleared)
   - **Lock layout** — in this case, participants will be required to use this layout when it is activated and will be unable to change it locally. This option is especially useful for connections via third-party SIP/H.323 protocols since endpoints often have fewer options for managing slots.
   - **Rename** — set a convenient name for the video layout (up to 70 characters) so that it can be quickly found in the general list
   - **Clear all video slots** — removes all participants from the video layout so that it can be filled once again
   - **Delete layout** — deletes the selected layout. If the deleted layout was set as the main layout for its category (e.g., for everyone), a different layout will not automatically become the main one after deletion. It has to be selected manually.

14.5.5. "Media" Tab

In this tab, you can set limits on video stream quality for different directions:

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



You can set custom quality parameters for video streams **incoming** to the server from all participants in a given conference: client applications, browser participants via WebRTC, and connections via SIP/H.323/RTSP. To do it, check the box **Limits for participants → Use custom settings** and select values in the drop-down lists. The frame rate limit for content sharing applies when content is displayed in a participant's window and not in a separate stream. So, the quality limit is the same for a participant's video window, but you can specify different frame rates depending on whether the speaker or content is being displayed.

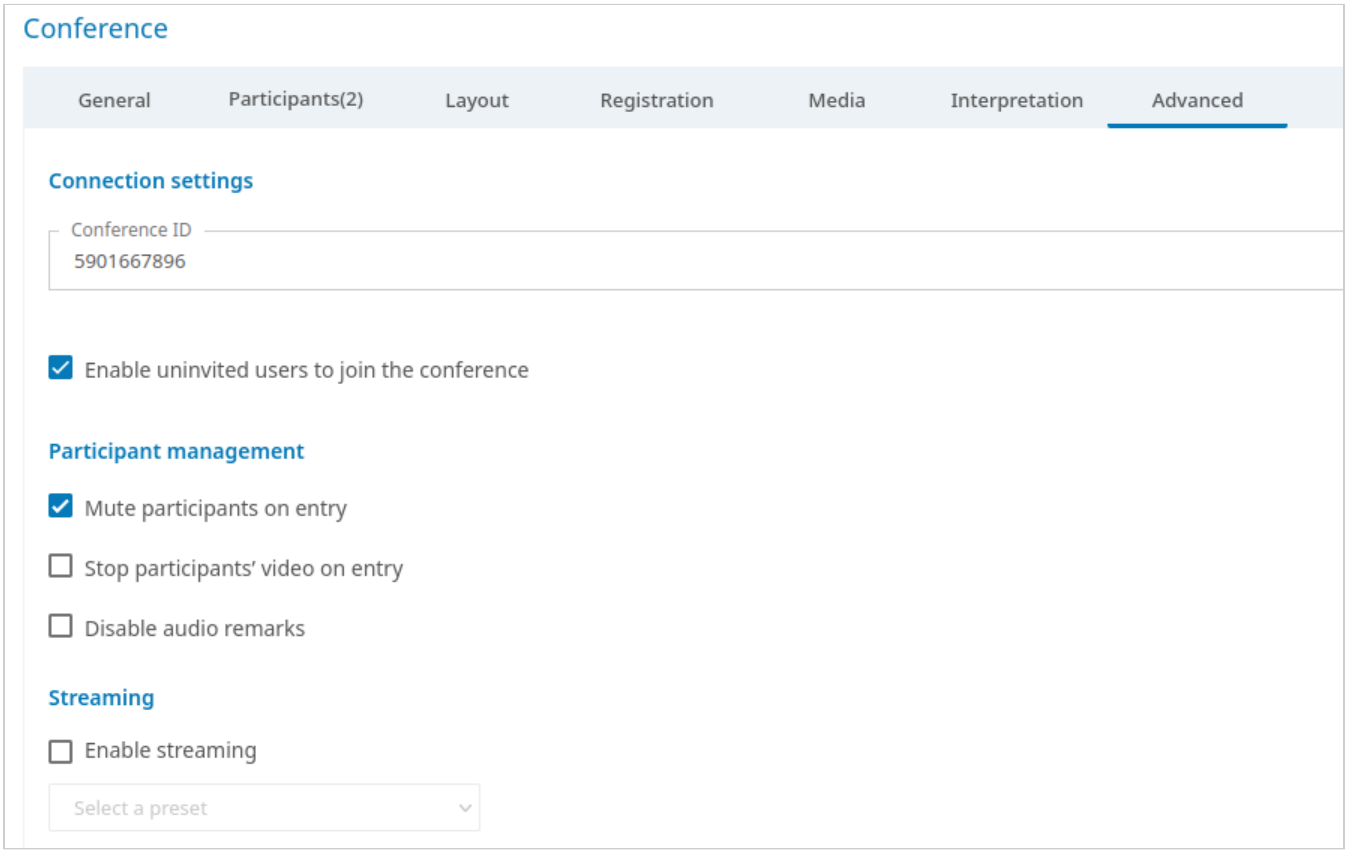
The settings in the **Transcoding** section are identical the settings in the **Gateways → Transcoding** section, except for the GPU acceleration option (this parameter has to be configured only once for the entire video conferencing server). Check the box **Use custom settings** to override resolution settings at the conference level independently for each direction: SIP/H.323 endpoints, WebRTC connections, recording, and streaming. The common frame rate is set for all directions. Below, one can specify additional settings which are activated if no layouts are created specifically for SIP/H.323/WebRTC participants when scheduling a conference or in the real-time meeting management section.

14.5.6. "Advanced" tab

If necessary, you can configure additional conference parameters on the **Advanced** tab.

14.5.6.1. ID, management of participants and streaming

Set the ID and security parameters for the conference:



1. Enter the conference ID manually to make it easier for participants to join the conference. This option can be disabled for all conferences in the **Group conferences →Settings** section.
2. Check the box **Enable uninvited users to join the conference** if you want to allow the users, who were not added the list of participants in advance, to join the event (this option is available only for private conferences).
3. Choose if it is necessary to automatically turn off the cameras and microphones of all participants when they join the conference. If needed, you can also disable audio remarks for participants (this option is available only in a moderated role-based conference).

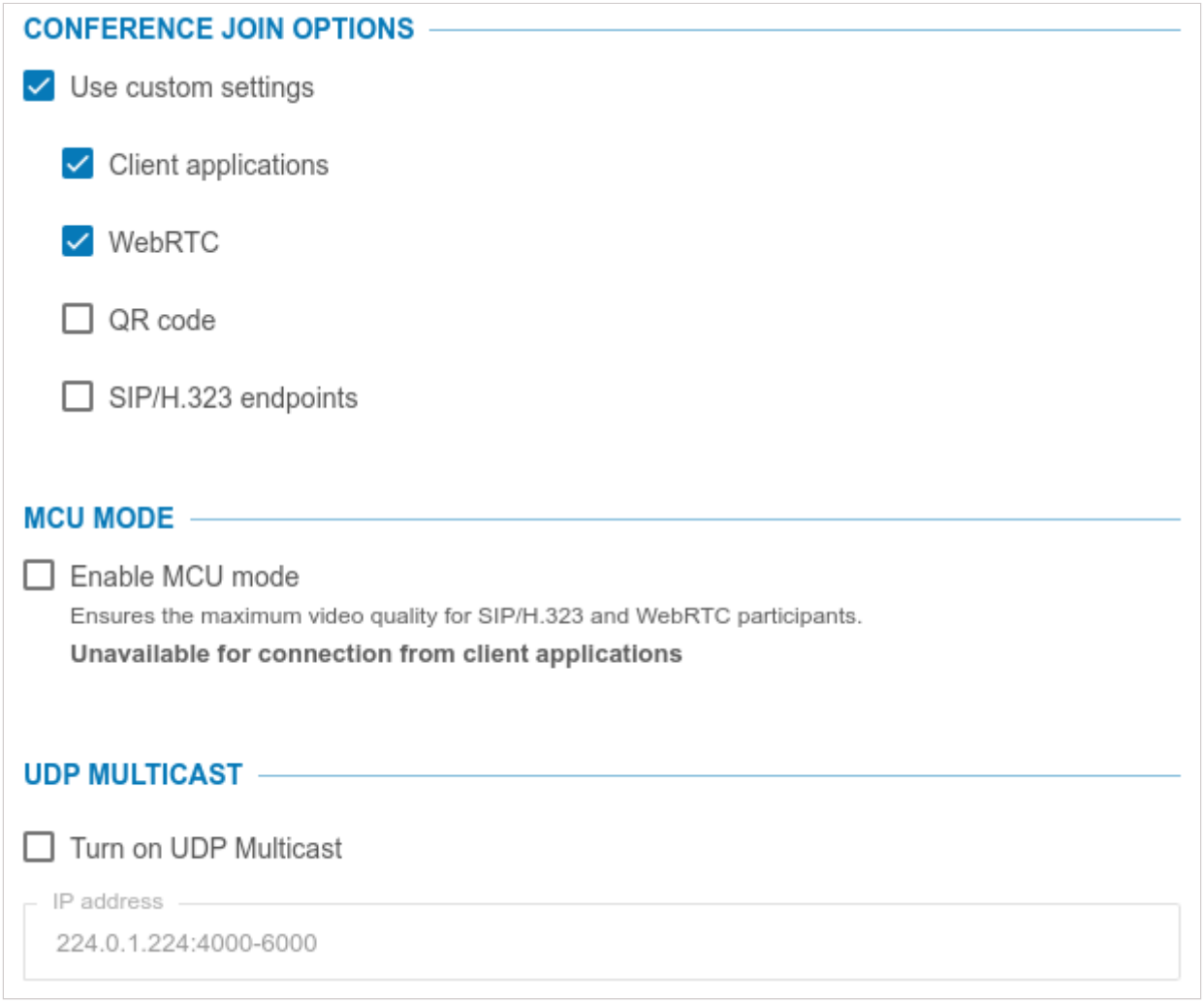
> *i* On/off flag for camera and microphone is now ignored by SIP/H.323 endpoints when connecting to a conference to improve compatibility with smart meeting mode.

4. Below you can enable conference streaming. To do it, select one of the templates created previously in the drop-down list (check the description in the **Streaming** section).

> *i* 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.

14.5.6.2. Connection methods, MCU mode, UDP Multicast

Configure the required parameters:



1. You can bypass general settings and select connection methods for the current conference. For example, if the license limits the number of connections through the gateway and no connections from endpoints are expected, this method can be completely disabled. Please note that this option will be unavailable when MCU mode is activated.
2. In regular conferences, SIP/H.323/WebRTC/RTSP streams from participants are transcoded on the server side into SVC streams for optimal distribution among other participants. If TrueConf applications will not be connected to the conference, this transcoding is not necessary and you can check the box **Enable MCU mode**. In this case, stream processing on the server will be optimized for handling streams without SVC support, and participants will not be able to choose a connection method. They will be able to join the conference **only** from a SIP/H.323 endpoint or browser; it will also be possible to connect an RTSP camera. Please note that if you activate MCU

mode and then disable this option, the list of available connection methods will not be restored to its previous state. In other words, you will need to check the boxes for client applications and the QR code manually.

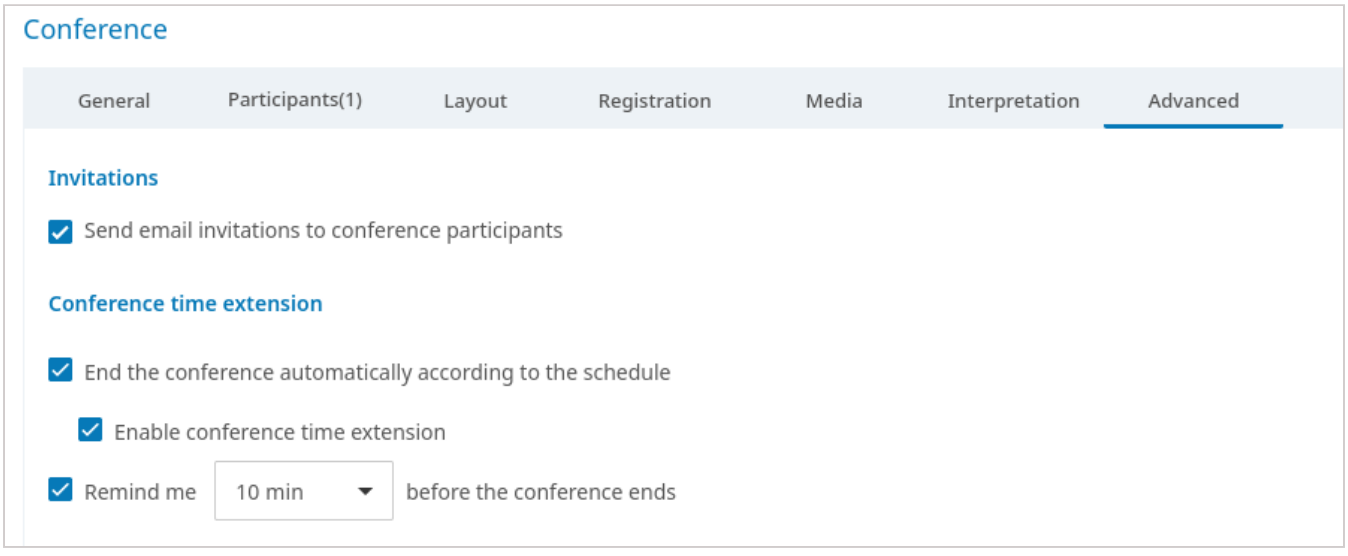
3. If necessary, enable UDP Multicast mode, more details on this mode are provided in the description of extensions. This feature will allow you to increase the number of speakers regardless of the number of podiums. For example, you can create a moderated role-based conference or smart meeting for 2000 participants and 36 podiums for speakers. However, there are many limitations listed below.

> **!** If UDP Multicast mode is enabled while you are trying to connect to the conference using third-party protocols (WebRTC, RTSP, SIP, H.323, etc), video conference recording and streaming will be unavailable.
>
> Enabling this function is recommended **only** for those users who have hands-on experience in the sphere of network administration. Please note that it is your responsibility to check if this technology is available in your network.
>
> If your network equipment is not configured to work in UDP Multicast mode, participants will see only a black screen during a conference.

4. If UDP Multicast mode has to be activated, specify the multicast/broadcast IP address. By default, this field is filled with the value **224.0.1.224:4000-6000**.

14.5.6.3. Sending invitations and conference time extension

It is possible to activate automatic email invitations to a scheduled conference and allow time extension for this event:



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.

> *i* 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.

1. By default, a scheduled conference will not end automatically when its allocated time expires. However, you can enforce automatic ending of the event by checking the box **End the conference automatically according to the schedule**. In this case, the option **Enable conference time extension** will become available so that moderators could extend the duration of a conference. This option will be accessible in the personal area, real-time meeting management section in client applications, and by clicking on the button in the notification about the upcoming end of the event (if this notification is enabled, see below).

3. You can configure notifications about the upcoming end of the event (see above) by checking the box **Remind me 10 min before the conference ends**. The notification time can be changed in the drop-down list. This option is available only for scheduled conferences. All moderators, not just the owner, will see such notifications.

A scheduled conference without a time limit will automatically end when certain conditions are met.

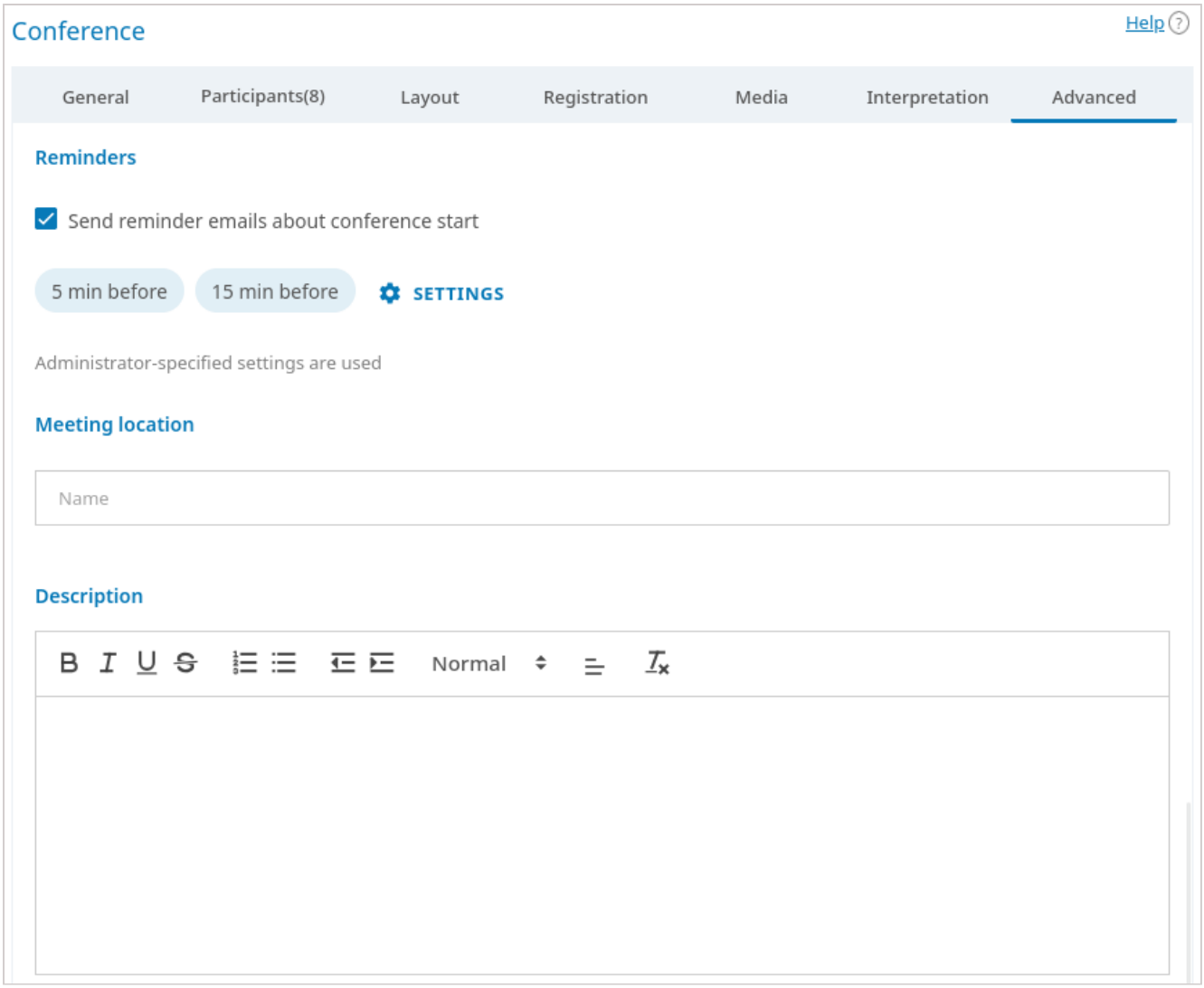
14.5.6.4. Visual settings

In the **Visual settings** section, you can configure the settings for the conference background and watermark.

Here, the administrator can configure the same settings that are available in the **Gateways →Transcoding** section. The only difference is that one can use general settings or specify different settings only for a specific conference.

14.5.6.5. Reminders and description

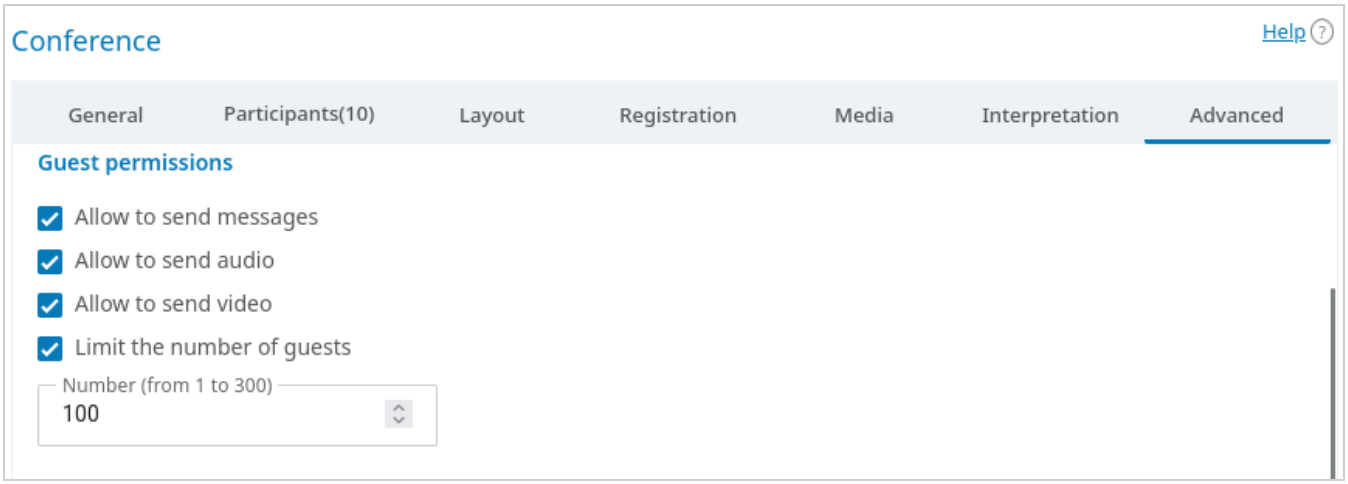
Below you can find the settings for conference reminders and description:



1. By checking the box **Send reminder emails about conference start**, you can enable email reminders that will be sent to event participants. This feature has to be enabled in advance in the SMTP settings. You can add up to 4 reminders for one conference by using the **Settings** button. To use global notifications settings, click the link **Use administrator specified settings**.
2. In the **Meeting location** field, you can enter the text that will be displayed on the **Information** tab on the meeting page and in the conference list.
3. In the **Description** field, you can add supplementary text for the scheduled event (for example, descriptions of participants' presentations or the event agenda). This text will be displayed on the conference page.

14.5.7. Restrictions for webinars

If the box **Public conference (webinar)** was checked on the **General** tab, you can configure the following settings in the **Advanced** tab:

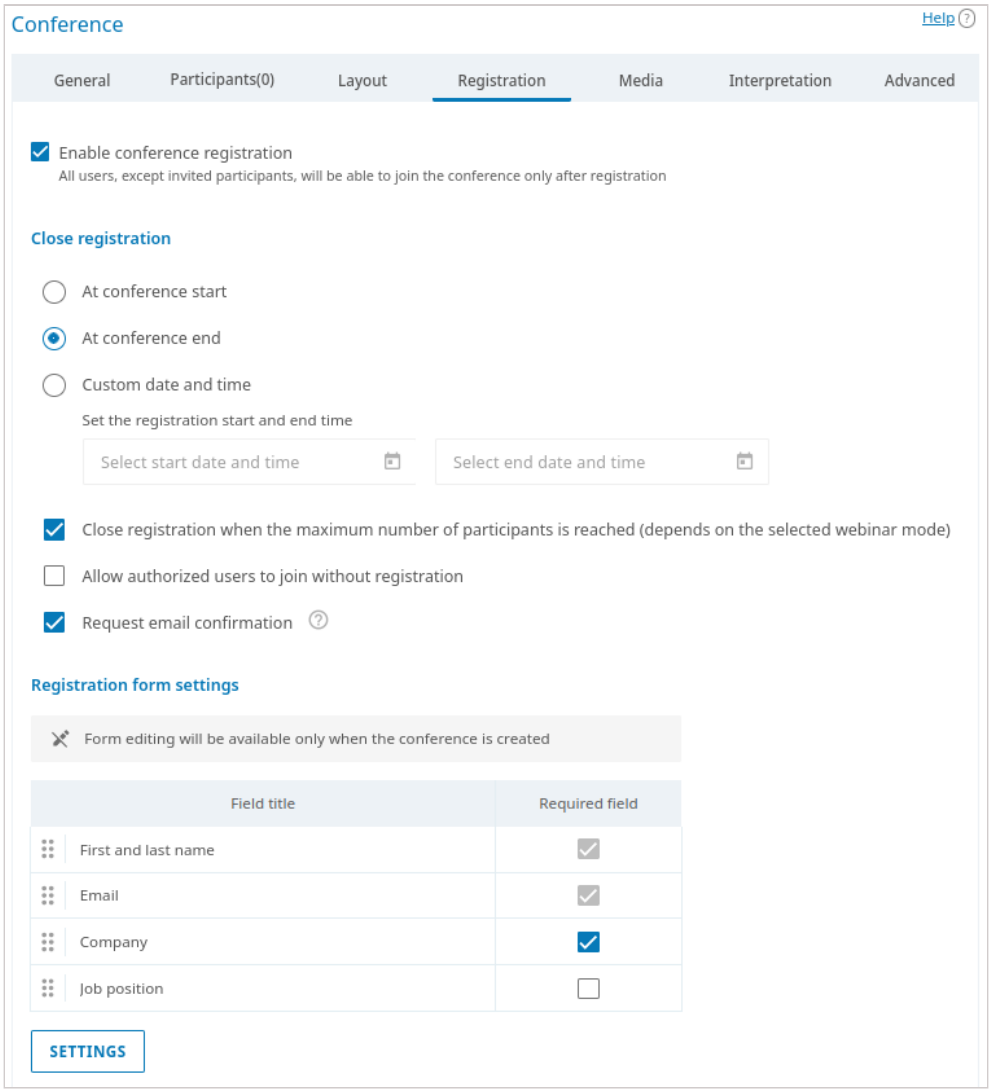


1. Permission settings for guest users
2. The **Number** parameter is used to restrict the number of guests in a webinar (by default they can join an event up until the moment when the license limit for guest connections is reached). This option may be helpful when multiple webinars are held at the same time, and it is necessary to distribute guest connections between them or if the rules of your event impose restrictions on the number of attendees (e.g., if it is a lecture).

i 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.

14.5.8. "Registration" tab

If a public conference (webinar) is created, you will be able to set the parameters on the **Registration** tab. Here, you can configure settings for self-registration of guest participants for your online event (available only for a scheduled conference):



1. Check the box **Enable conference registration**.
2. In the **Close registration** section, you can select when registration will be closed and it will no longer be possible to sign up for the event:
   - **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.

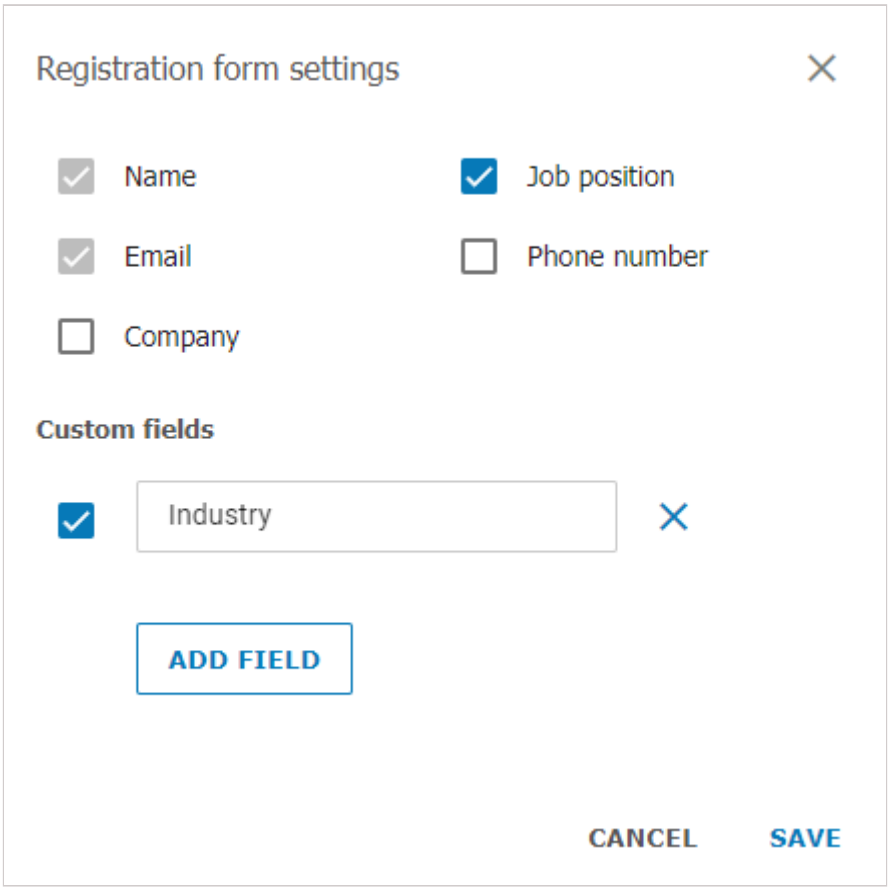
3. To limit the number of participants in a webinar, check the box **Close registration when the maximum number of participants is reached (depends on the selected webinar mode)**.

4. Check the box **Allow authorized users to join without registration** to enable users from your server to join the conference without filling out the registration form. In this case, any user from your server can authenticate on the conference page and add oneself to the list of invited participants by clicking the **Attend** button.

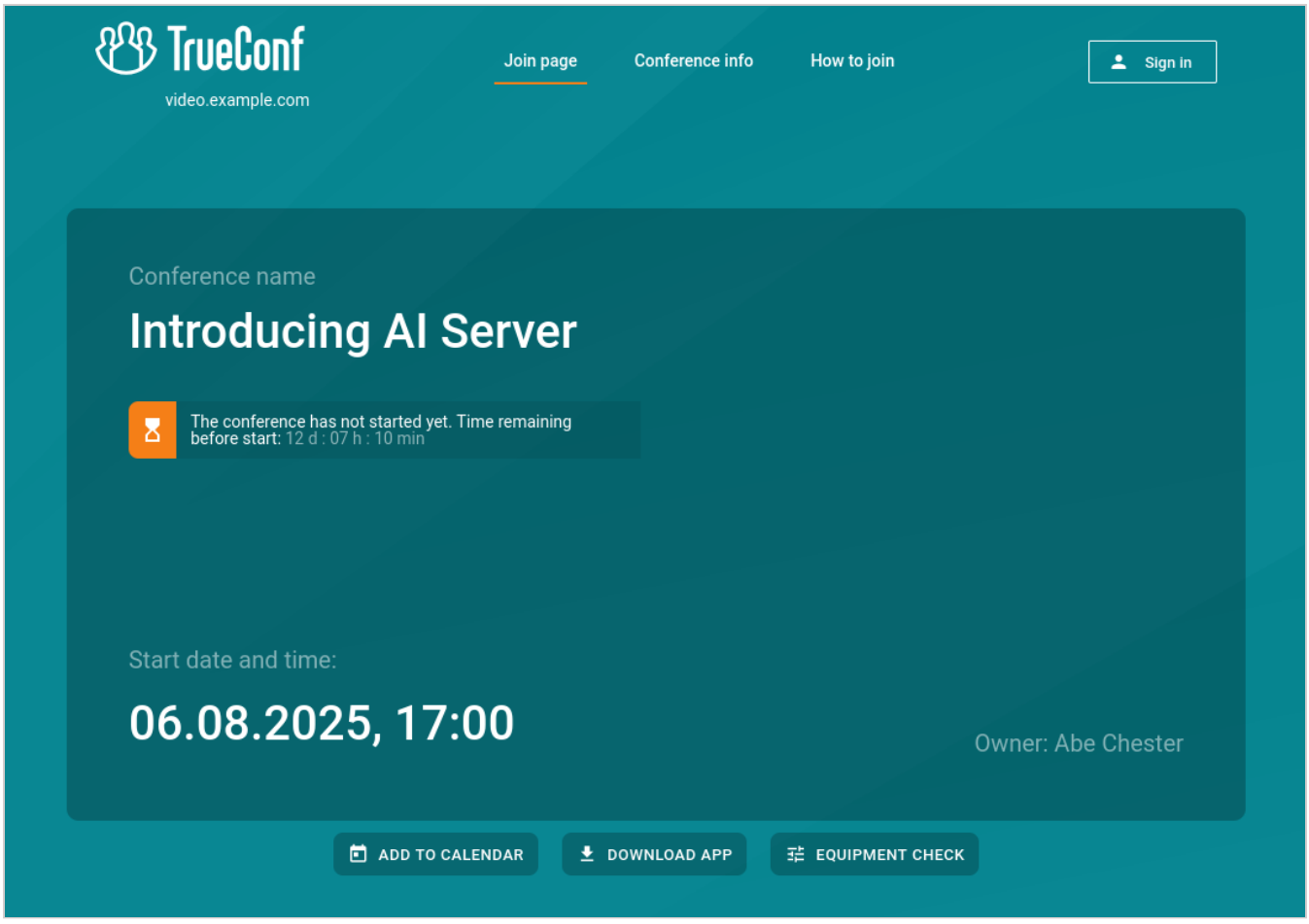
5. Settings for the input fields in the registration form. You can drag and drop input fields to create a custom registration form. Besides, you can mark the corresponding

checkboxes to make sure that certain fields must be filled by participants. The customization of registration form is available only when a conference is created. This feature is not available when the conference is edited.

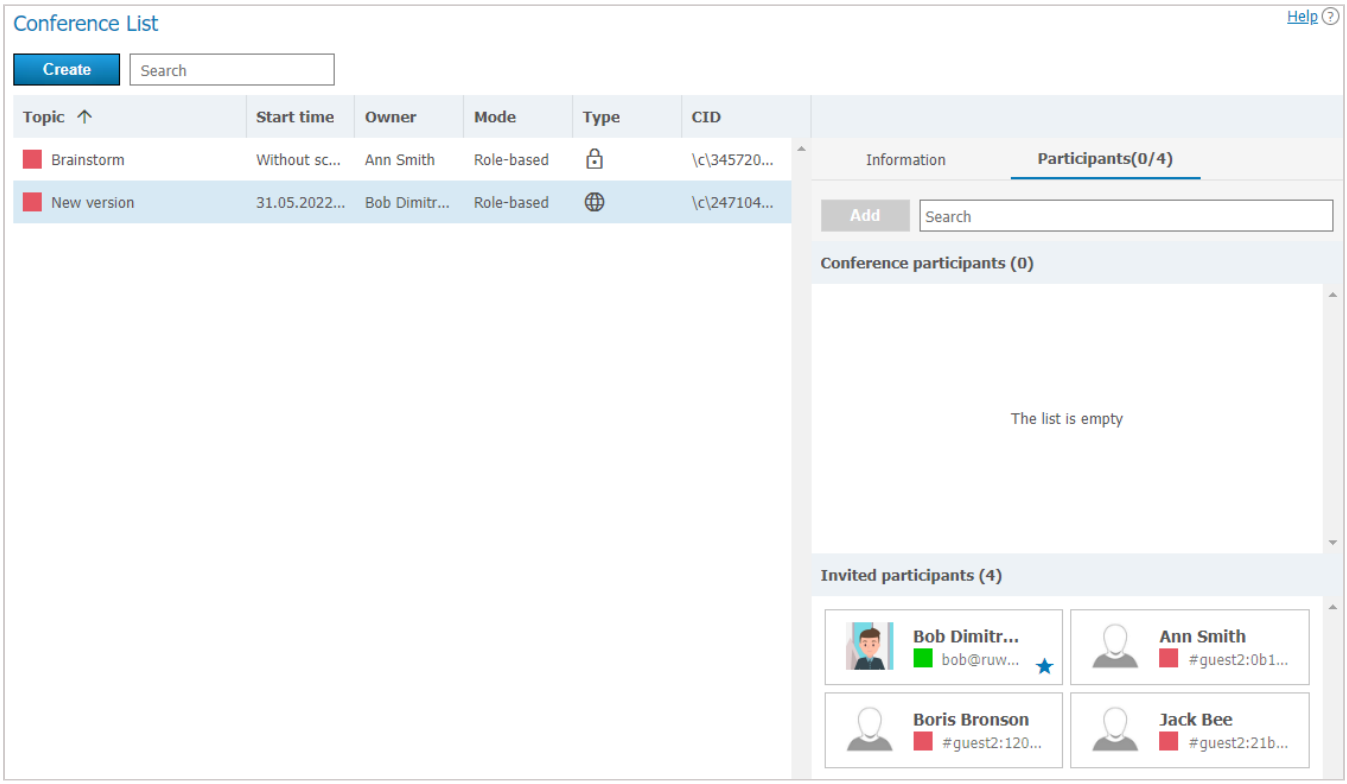
6. You can select the input fields that should be displayed during registration only when creating a conference. Click on the **Add field** button to specify both standard and custom fields (up to 10):



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:`:



> *i* Please note that registration for the webinar is not available for SIP/H.323 terminals and RTSP devices (e.g., IP cameras). They will only be able to participate in such a public conference if the host adds them to the list of participants when creating/editing it, or invites them after it has started.

14.5.9. Automatic conference ending

By default, scheduled conferences do not end at the specified time, but this behavior can be changed in the settings for each event.

To optimize the use of server resources, a scheduled conference will automatically end in two cases:

1. Time-based automatic conference ending is enabled. If it is possible to extend conference duration, but this option is never used, the meeting will also end.
2. Automatic conference ending is disabled, but only one participant remains and no one else joins the meeting for 15 minutes.

14.6. Templates

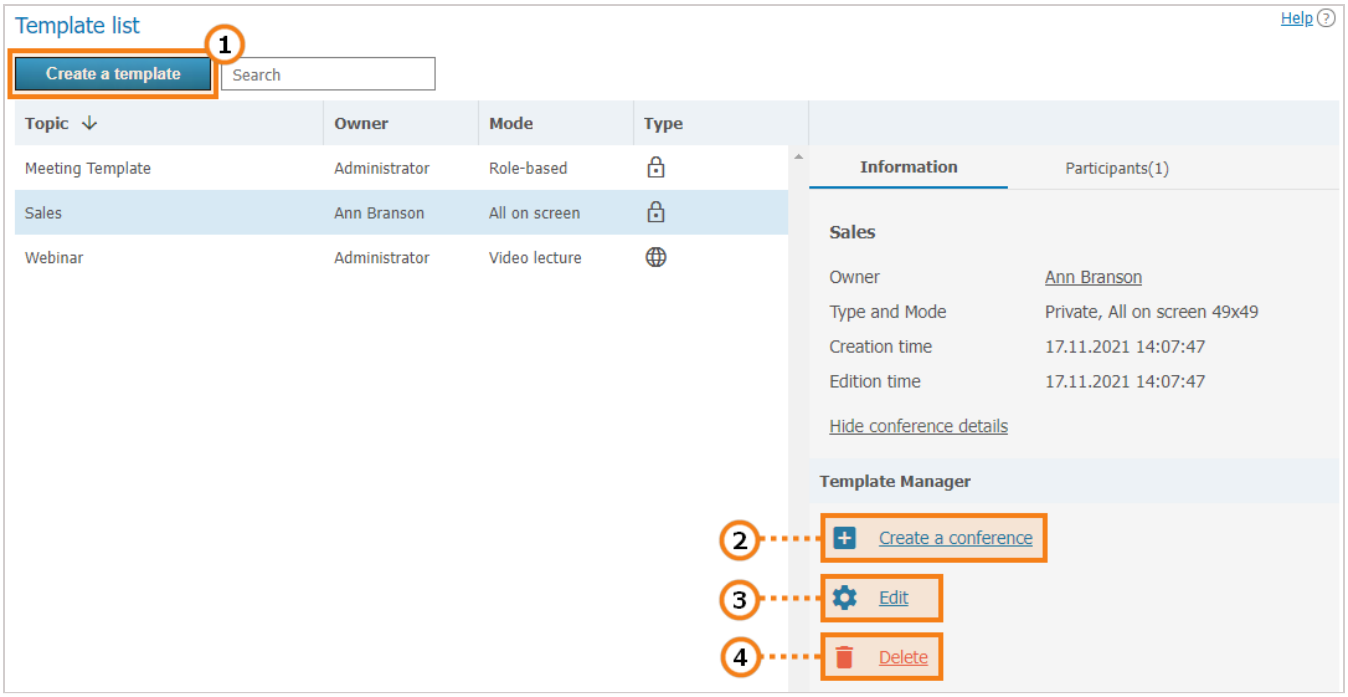
This section allows server administrator to create new conference templates and edit saved ones. Templates can also be saved while editing conference.

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.

> *i* 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.



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.

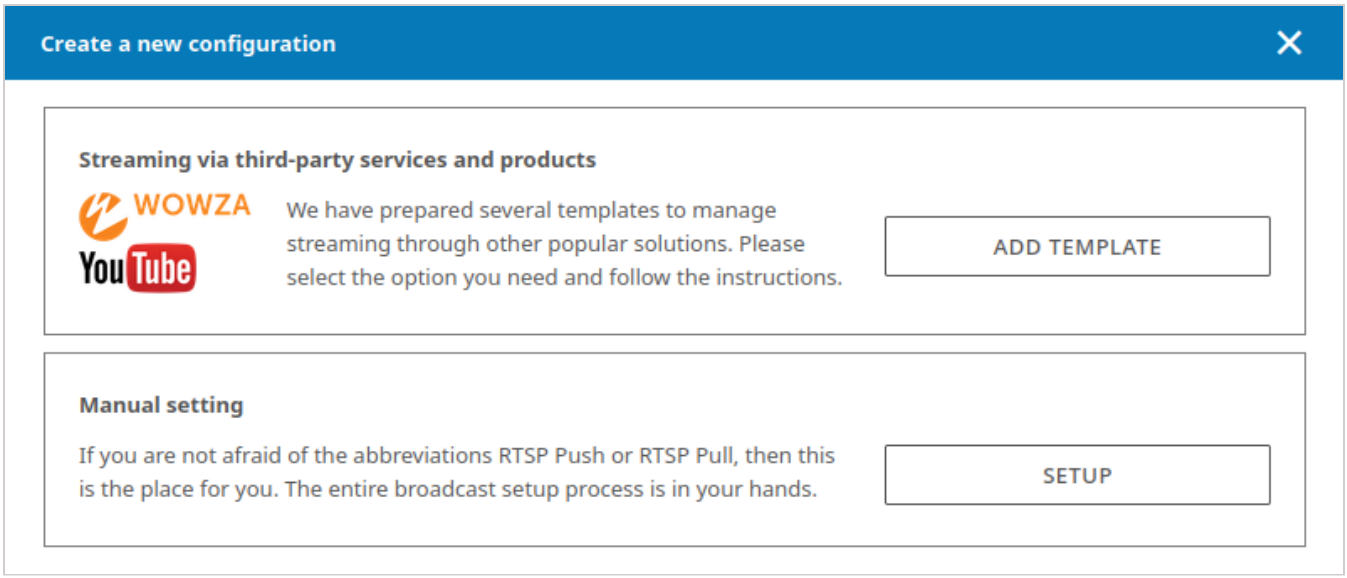
14.7. Streaming

In this section, you can create and set streaming configurations used for setting up a conference.

* The knowledge base TrueConf contains ready-made instructions on how to organize broadcasts to the main sites:
  - YouTube
  - Wowza

  You can also manually set up conference streaming to other third-party services, for example, Facebook.

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



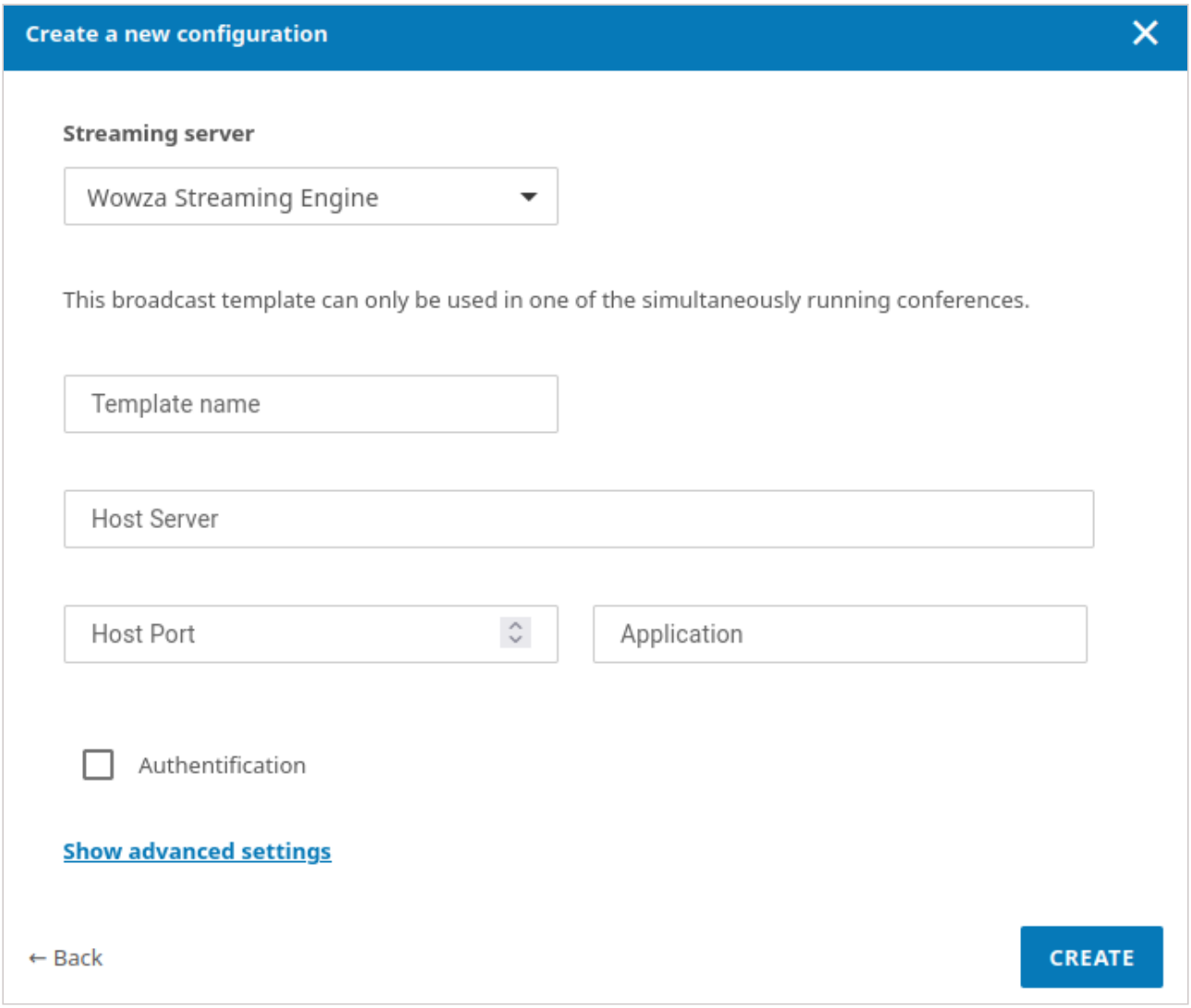
14.7.1. Streaming via third-party services and products

The section **Streaming via third-party services and products** includes our default configuration templates for popular streaming solutions both within corporate networks and over the Internet. To open additional settings, click the **Add preset** button.

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

14.7.2. Wowza Streaming Engine

To stream video to Wowza Streaming Engine, specify the following parameters:

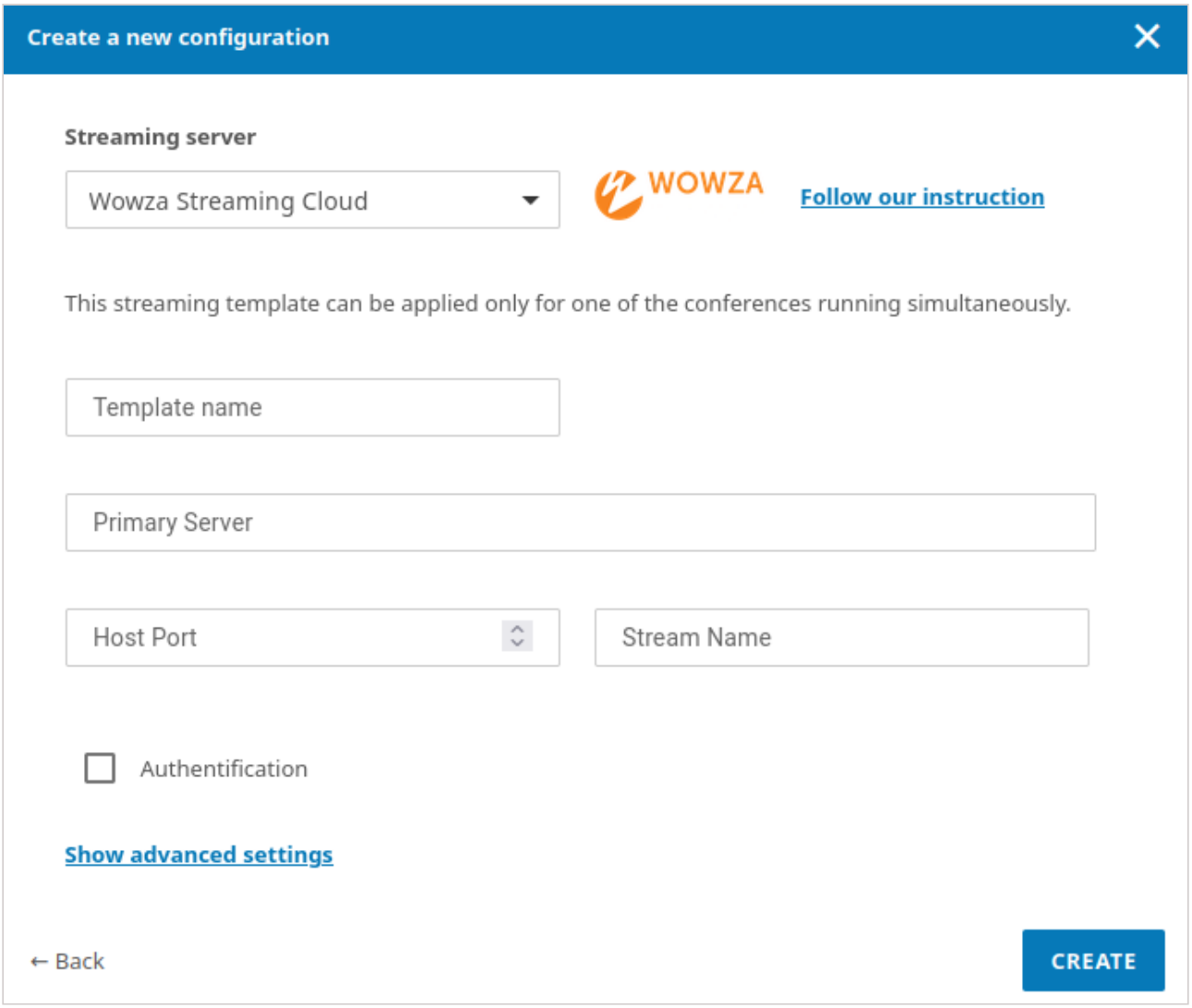


1. **Template name** — will be displayed in the list of stream configurations when a conference is created or edited.
2. **Host Server** — the address of the Wowza Streaming Engine server.
3. **Host Port** — the port through which the Wowza Streaming Engine accepts connections. As a rule, the ports `1935` or `1940` are used.
4. **Application** — refer to the Wowza Streaming Engine documentation for the description of this field.
5. Check **Authentication** to enter username and password to access Wowza Streaming Engine if required.
6. Click the link **Show advanced settings** to open the block with additional parameters for the current configuration (check the documentation section **Additional streaming configuration settings**).

Next, click the **Create** button to save your changes.

14.7.3. Wowza Streaming Cloud

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

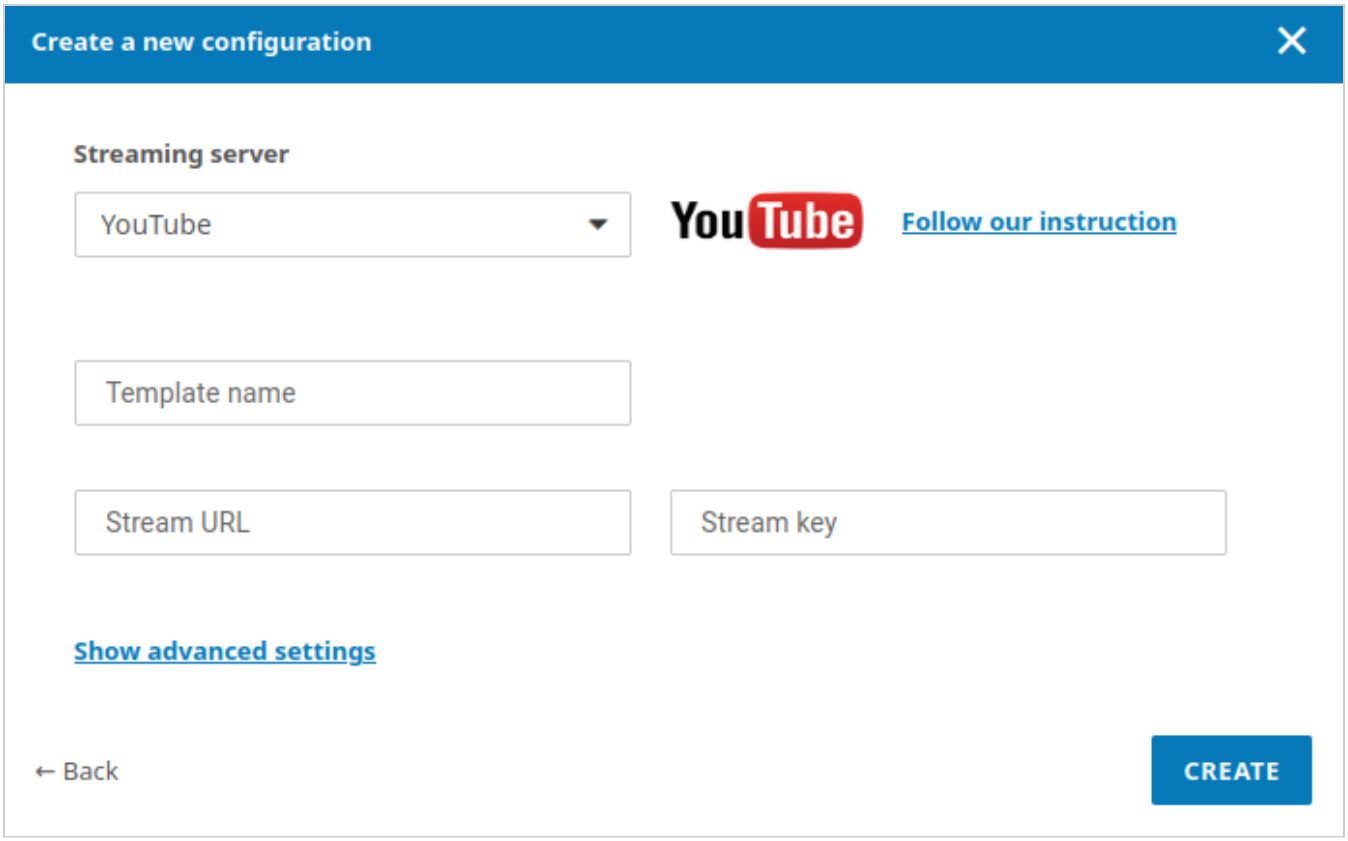


1. **Template name** — will be displayed in the list of stream configurations when a conference is created or edited.
2. In the fields **Primary Server**, **Host Port** and **Stream Name**, enter the stream data received from the Wowza Streaming Cloud service when configuring the stream.
3. If the **Authentication** box is checked, you can enter the login and password required for accessing Wowza Streaming Cloud.
4. Click the link **Show advanced settings** to open the block with additional parameters for the current configuration (check the documentation section **Additional streaming configuration settings**).

Next, click the **Create** button to save your changes.

14.7.4. YouTube

Specify the following parameters for YouTube streaming:



1. **Template name** — will be displayed in the list of stream configurations when a conference is created or edited.
2. **Stream URL** — the server address from the stream creation page on YouTube.
3. **Stream key** — the stream name/key from the stream creation page on YouTube.
4. Click the link **Show advanced settings** to open the block with additional parameters for the current configuration (check the documentation section **Additional streaming configuration settings**).

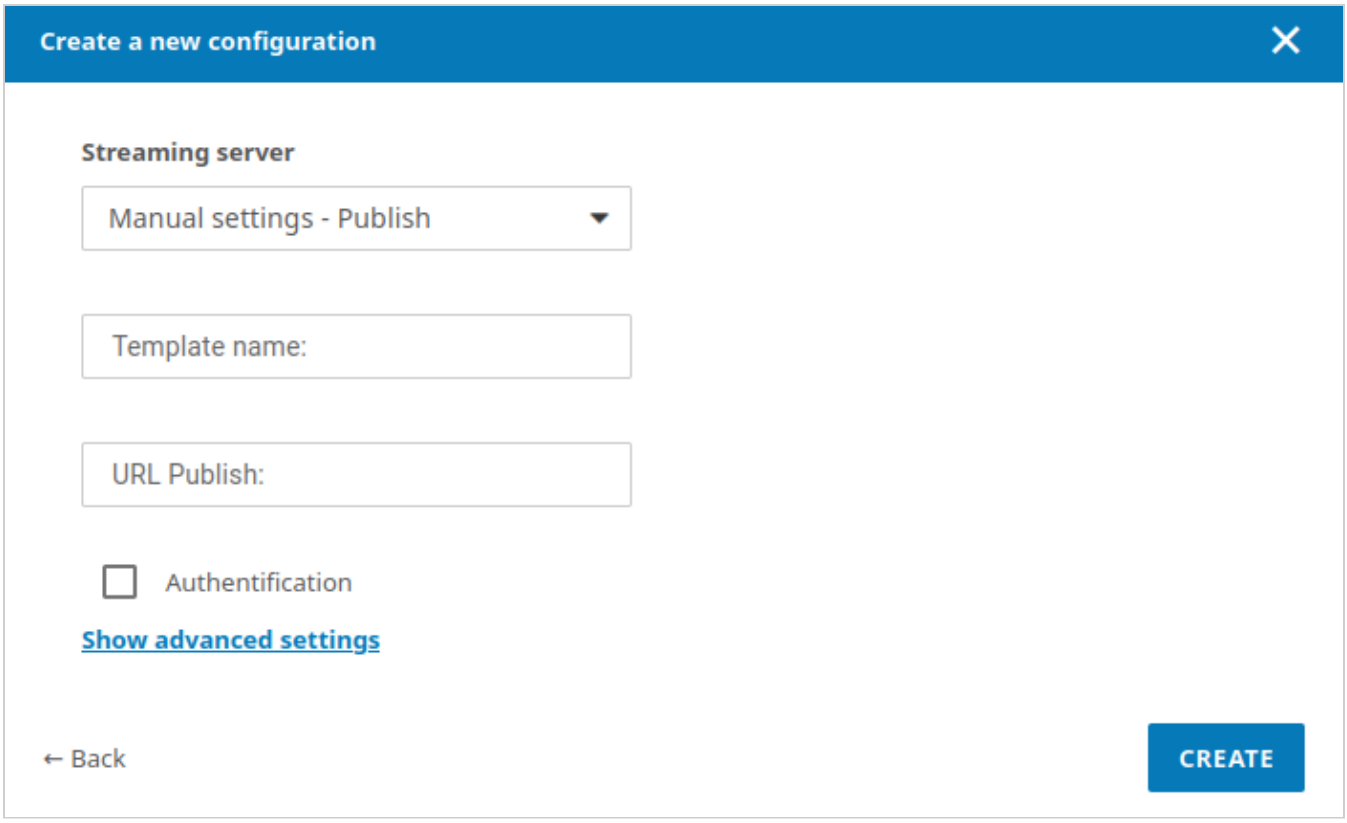
Next, click the **Create** button to save your changes.

14.7.5. Manual settings

Select the **Manual setting** option to manually configure streaming to the majority of existing solutions, including those listed above. TrueConf Server supports two content transmission methods: RTSP Publish (also known as RTSP Push) and RTSP Pull. If the first method is used, your server notifies the streaming system about the availability of a stream, while in the second case, the system retrieves (pulls) the stream from your server.

RTSP Publish manual settings

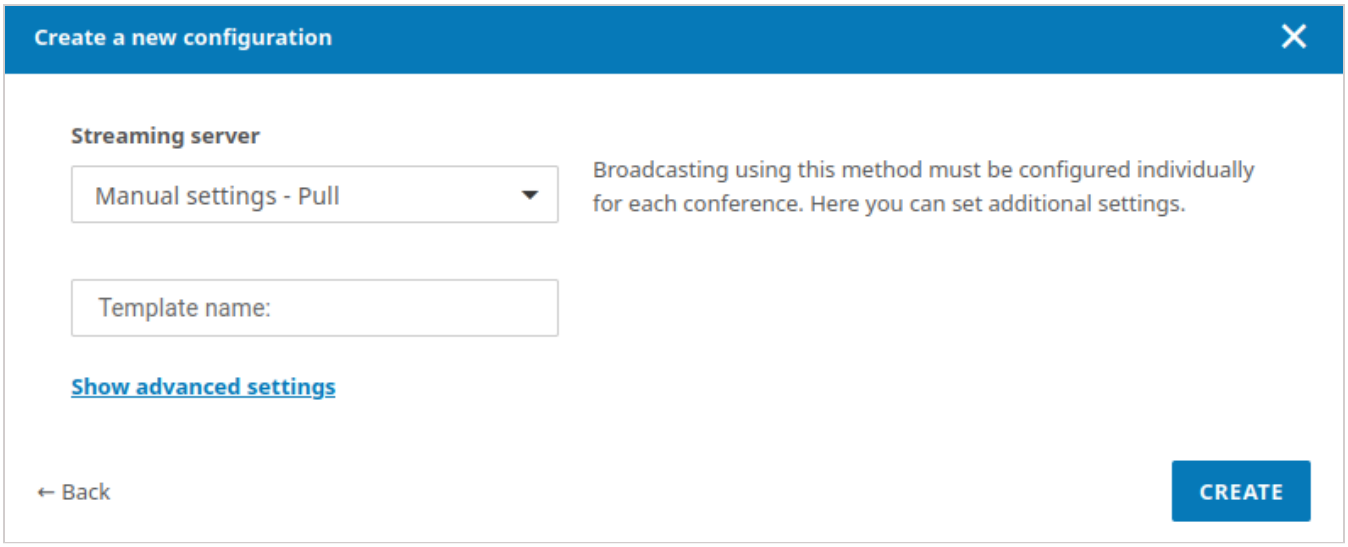
Available parameters:



1. **Template name** — will be displayed in the list of stream configurations when a conference is created or edited.
2. **URL Publish** — the address used by our server to notify about available streams via the RTSP ANNOUNCE protocol.
3. Check **Authentication** to enter username and password and gain access to the service.
4. Click the link **Show advanced settings** to open the block with additional parameters for the current configuration (check the documentation section **Additional streaming configuration settings**).

RTSP Pull manual settings

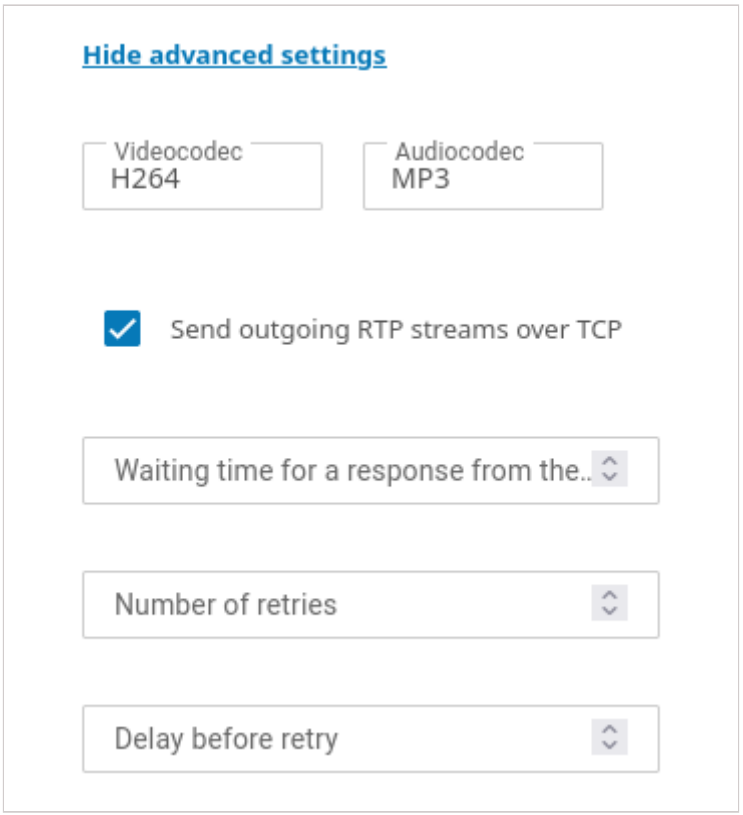
This method can used to get an RTSP link to the conference stream and to specify this link directly on a third-party service or convert the stream with additional software, e.g., OBS Studio.



1. **Template name** — will be displayed in the list of stream configurations when a conference is created or edited.
2. Click the link **Show advanced settings** to open the block with codec settings for the current configuration (check the documentation section **Additional streaming configuration settings**).

Additional streaming configuration settings

The availability of certain parameters depends on the selected template.



1. You can change video and audio codecs used for the stream encryption.
2. Check the box **Send outgoing RTP streams over TCP** if you need to send outgoing RTP streams via TCP instead of UDP.

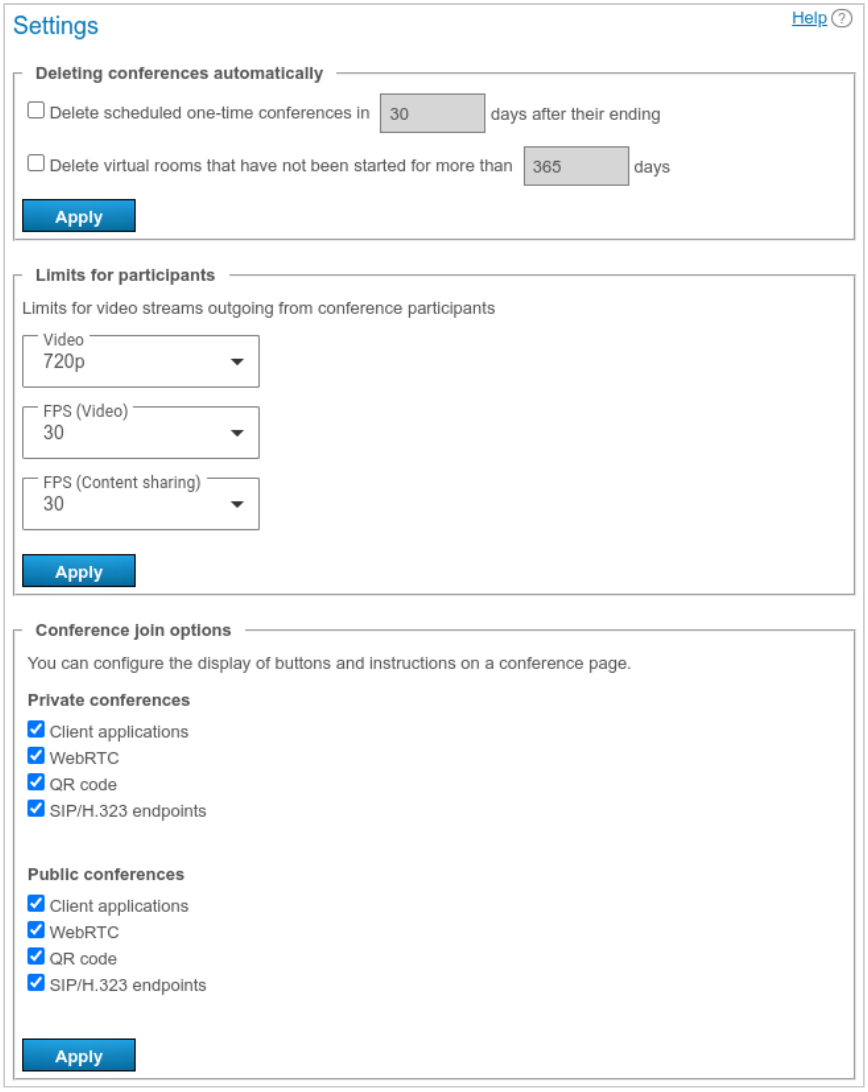
3. In the field **Waiting time for a response from the server**, you can set the waiting time (in seconds) for the external streaming system to confirm the reception of information about the published conference stream.
4. The **Number of retries** parameter enables you to specify the maximum number of reconnection attempts in cases when connection with the streaming system is lost. This will allow TrueConf Server to restart stream publication.
5. The parameter **Delay before retry** is needed for setting the delay (in seconds) between attempts to publish stream information.

14.8. Conference settings

In the **Group Conferences →Settings** section, you can configure automatic deletion of conferences and select meeting connection methods available to participants.

14.8.1. Automatic conference deletion

Sometimes, it may be helpful to delete events from the general list if they were held a long time ago, and are no longer needed. TrueConf Server allows you to configure automatic deletion of such conferences:



The 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.

14.8.2. Limiting the quality of outgoing video from participants

You can set general quality parameters for video streams **outgoing** from all participants in all conferences. This includes client applications, participants, who join from a browser via WebRTC, and connections via SIP/H.323/RTSP. As a result, the server will explicitly instruct participant's devices/applications on the quality of the video to be sent. This will be the upper limit on the incoming video quality. The resolution limit applies only to the quality of the camera video, but not the content which is being shared in a participant's window. Content (screen/application window) is always shared with the resolution at which it is captured, with a maximum quality of FullHD 1080p. SVC works for fps/bitrate but not for resolution.

You can set the frame rate limit for two different scenarios: when a speaker is displayed in the video window or when this person is sharing content in the same stream. This limit does not affect content sharing settings for the second stream, where FullHD 1080p quality is always used with a low FPS, prioritizing resolution.

The server administrator can set individual quality settings for a conference when creating or editing this event.

14.8.3. Ways of joining conferences

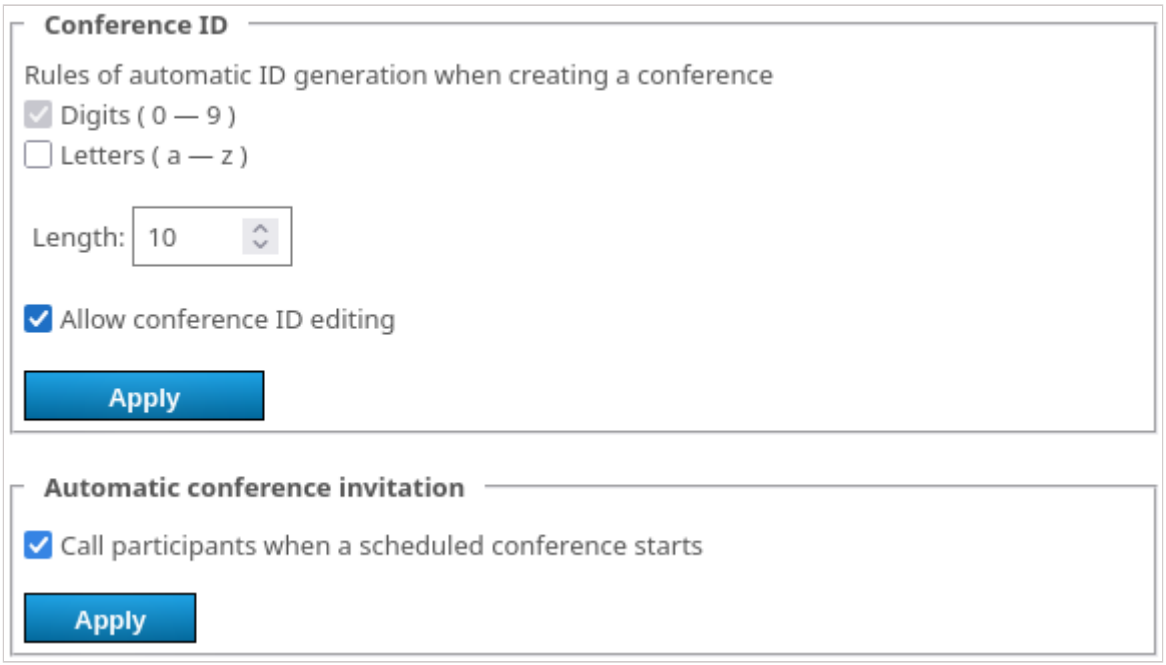
In this section, you can choose which ways of joining conferences should be available to all participants. These general settings will apply to the following conferences:

- 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. Please note that quick conferences created in client applications are always private. Conferences can be joined from client applications, browsers (via WebRTC), by QR code from the event page, and from hardware or software SIP/H.323 endpoints.

14.8.4. Conference ID and the rules for calling participants

In the **Conference ID** section, you can set rules for automatic generation of unique IDs when events are created. It is also possible to disable ID modification, so that neither an administrator nor a user can change the ID in the scheduler on the **Advanced** tab.



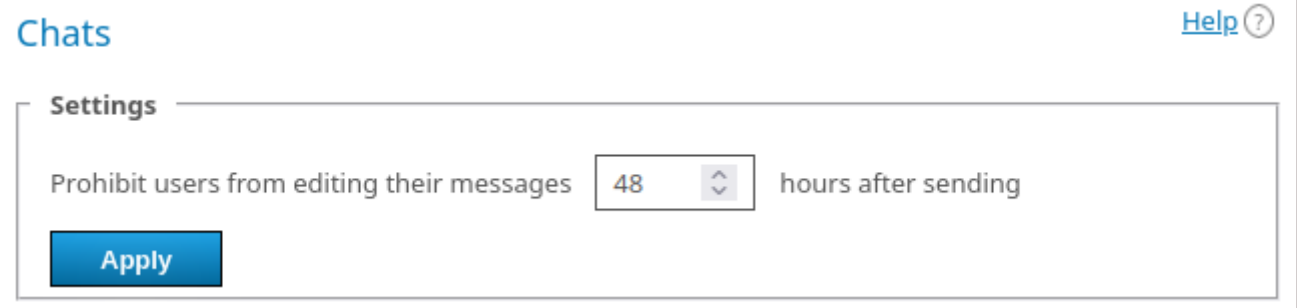
Below you can disable the automatic invitation of all users who were added to the list of participants for a scheduled conference. To do it, uncheck the box **Call participants when a scheduled conference starts** (enabled by default).

15. Chat settings

In the **Chats** section, you can configure chat settings for the users of this TrueConf Server instance.

* There is only one parameter in this section so far, but in the future versions of the video conferencing server other settings will be added.

15.1. Timeout settings for editing messages



To limit the time available for editing messages, check the box **Prohibit users from editing their messages** (checked by default). In this case, users of your server will be able to edit their messages only within the specified time range (48 hours by default). When this time period expires, the edit option will not be available in TrueConf client application when a user right-clicks on a message.

Limits apply to:

- Authenticated users of your TrueConf Server (their application will request the information about the restriction from the server and apply it)
- Guest participants of your conferences since a temporary user account is also created for them on the server.

Users of the external federated server will comply with the restrictions of the server where they are authenticated.

15.2. Automatic deletion of empty conference chats

In some cases when a conference ends, empty chats may remain, for example, if there was a meeting, but users discussed everything verbally without sending any messages to the chat. The developers of TrueConf Server made sure that such empty chats were not added to the chat list and were automatically deleted.

How it works:

1. You need to have TrueConf Server 5.5.0 or above.
2. About once in 15 minutes, the system checks if a chat was automatically created for a one-time conference which has already ended (in other words, it is not the chat of a virtual room or the conference was started based on a group chat, but was unlinked from this chat). The system will also delete the chats of quick conferences created in a

single click in TrueConf client applications. So, this chat will no longer be available to any user when the conference ends.
3. The system checks if the chats do not include any messages from users (however, a chat may include some service messages, e.g., notifications about a user's connection to the conference).
4. All the chats, which match these criteria, will be deleted; so, they will not be displayed in the list of chats in users' TrueConf client applications.

Please note that if some conference participants were from a federated server, the chat will be deleted depending on the settings of the server where the conference was created (for example, if the servers with different versions were used).

16. Surveys

Users of TrueConf video conferencing systems can create surveys to collect people's responses and examine their opinions. This feature does not require a separate license and is available even in TrueConf Server Free.

What features does the built-in polling (survey) module offer:

- Ability to configure survey access (available only to the users of your server or to everyone)
- Anonymous surveys
- Configuration of respondents' permissions to view the survey results
- Ability to retake the survey
- Permission to change responses
- Ability to use images as one of the response options for a multiple-choice question
- Add images to a question
- Ability to mark any questions as required which ensures that a user cannot skip these questions when completing the survey
- Create survey campaigns which will allow you to easily segment results by respondent groups
- Export results as a CSV file.

The server administrator can manage all surveys. The users, who were given the right to create surveys at the group level, can also manage them; however, such users can manage only the surveys that they created (in other words, they are the owners of these surveys). However, users cannot manage all surveys.

16.1. Types of questions and limits

Each survey may include questions of the following types:

- **Short answer** — an open-ended response that a user has to type instead of selecting from available options (***up to 255 characters***)
- **Paragraph** — a type of an open-ended response which can include a larger number of characters (***up to 4096***)
- **Single answer** — a question with multiple answer options, of which only one can be selected. When creating a question, a user can add the **Other** answer option.
- **Multiple answers** — a question with multiple answer choices, from which several options can be selected at the same time. When creating a question, you can add the **Other** answer option.

The following limits apply to TrueConf surveys:

Maximum number of surveys — unlimited.

Maximum number of questions in one survey — 5000.

The maximum number of answer options for each question — 20.

The maximum length of a single response option — 255 characters.

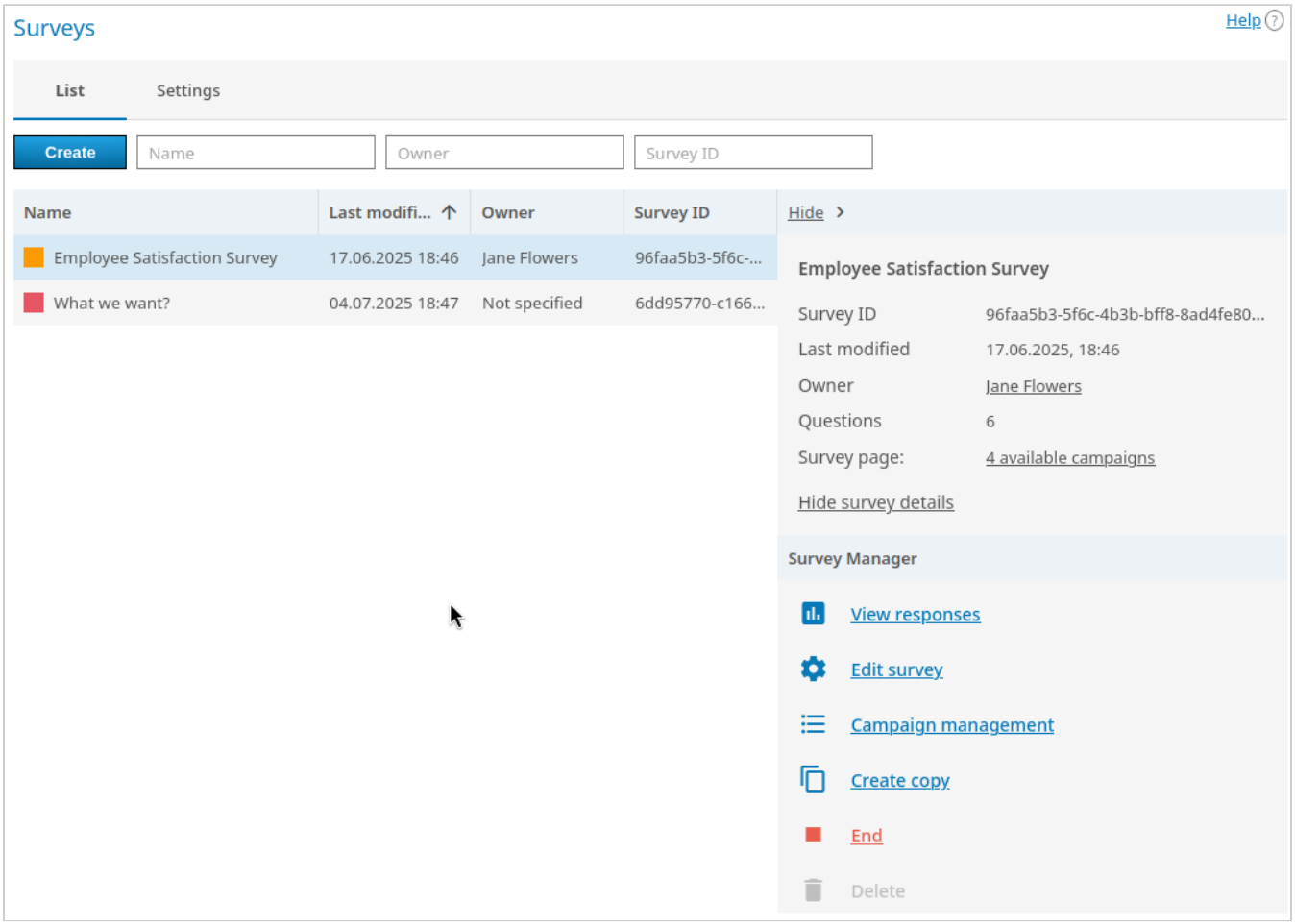
The maximum length of a question — 255 characters.

Allowed formats for an image that may be uploaded for a survey — JPEG, PNG, GIF, BMP.

16.2. Creating and editing a survey

To work with surveys, go to the **Surveys** section of the TrueConf Server control panel.

You will see the list of surveys (by default, it is empty):



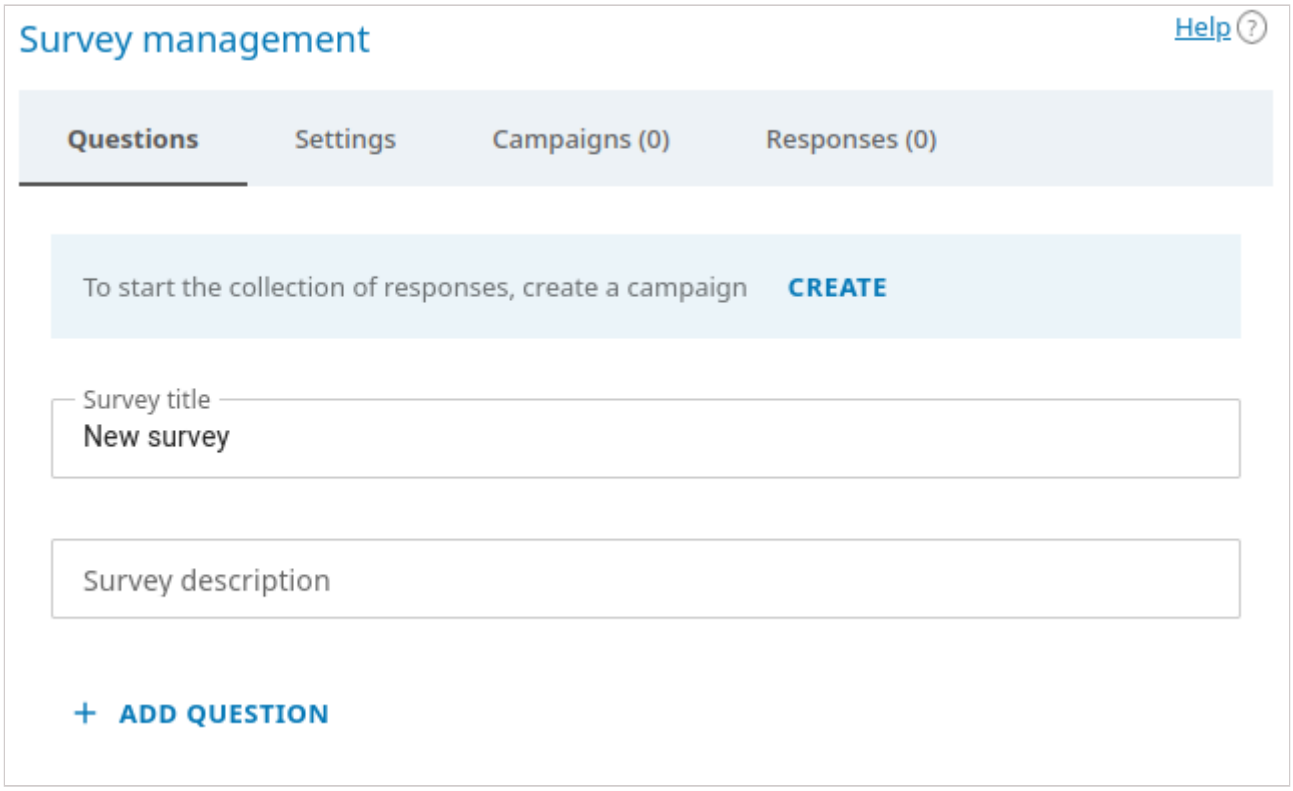
By clicking on a survey, you will open the card with general information about it: survey ID (which may be helpful when you need to find its change history in the logs), the last modified time, the owner's name, the number of questions, and a direct link to the campaign (if it was created).

Survey owner is a user of your TrueConf Server who has full access to manage the survey and its campaigns. A survey can be held even without the owner; however, in this case, it has to be created by the administrator. Moreover, only the administrator will be able to manage the survey and view its results.

A **campaign** is a specific survey session that allows you to segment participants for analyzing results across different groups. At least one campaign is **required*** for holding a survey since users essentially participate in a survey campaign. Each campaign includes all the questions created for the survey and differs only in terms of its link and access settings (see below). Multiple campaigns can be created for a single survey, and there are no restrictions on the number of active campaigns that can be held at the same time.

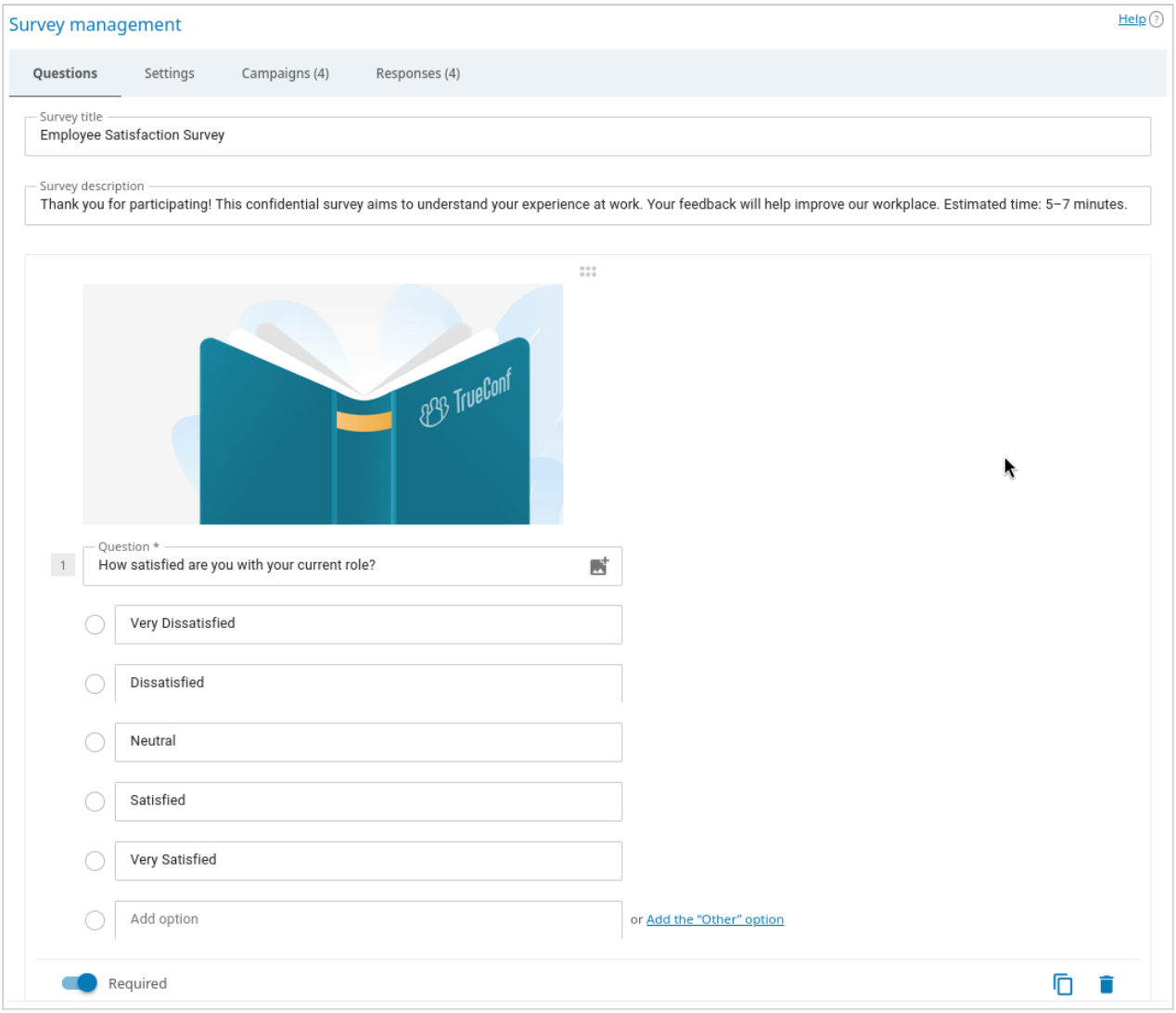
16.2.1. How to create a survey

To create a survey, click the **Create** button in the general list. The **Questions** tab will be opened. Here, you should specify the survey name (required), description (optional, will be displayed to participants on the survey page). Plus, below you need to add survey questions:



To create a question, click the **Add question** button and select its type. Next, enter the question text and fill in the answer options, depending on the question type. If necessary, you can add an image to the question text and to any of the answer options. It may be necessary to give a better illustration of the question or to use images as answer options. Changes to the list of questions are saved automatically, so you don't accidentally lose your work when creating a survey with a large number of questions.

Below, you can find an example of a question which is of the **Single answer** type:



16.2.2. Settings

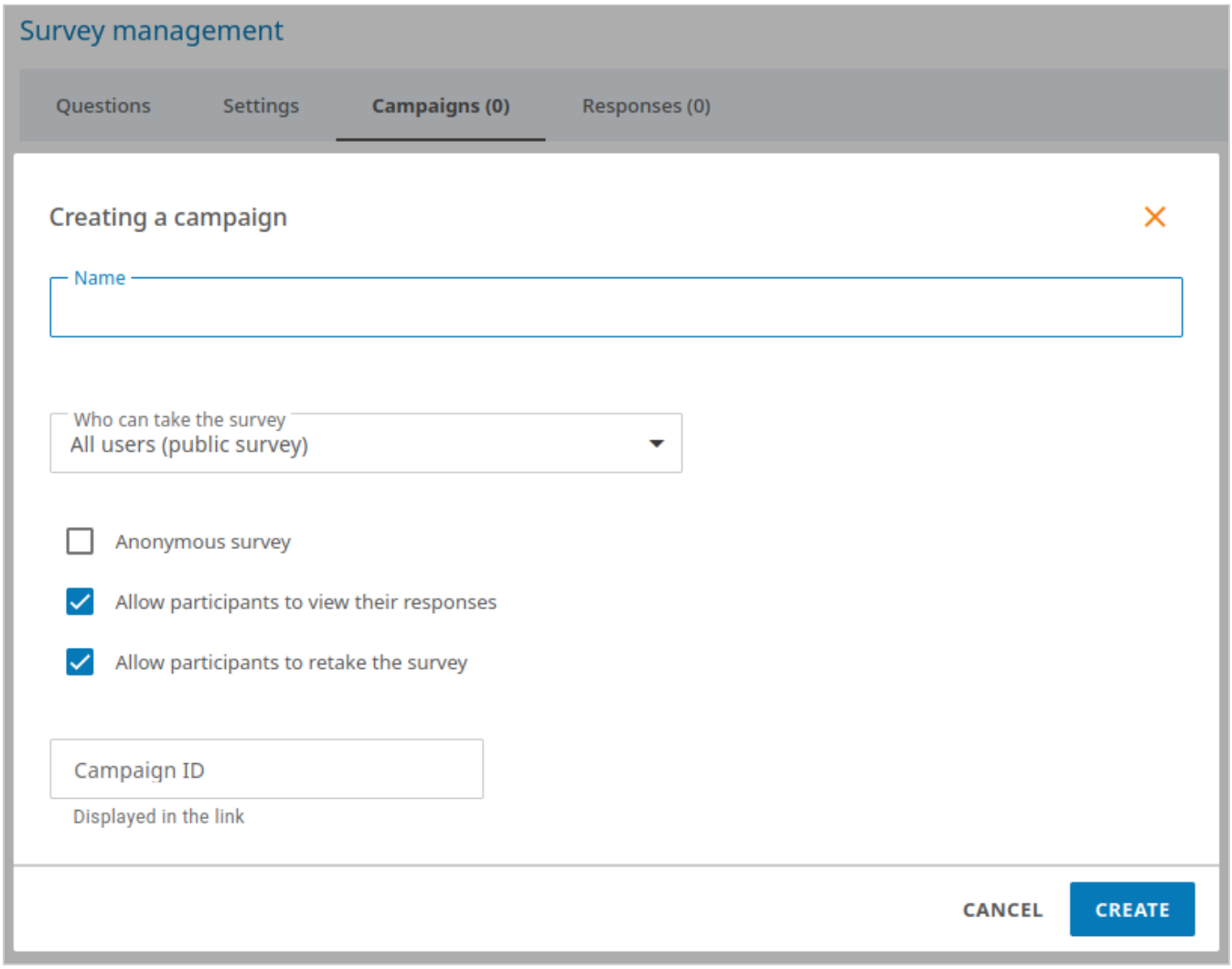
In the **Settings** tab, you can assign the owner to a survey. To do it, just click the **Select** button and choose one of the users on your video conferencing server. Other types of users such as guests or federated users cannot be selected as the survey owner. The user, who creates a survey in the personal area, automatically becomes its owner.

After adding the owner, you will be able to select a new one at any time (even when a survey campaign is running). However, you cannot remove the owner.

16.2.3. Survey campaigns

To hold a survey, you need to create and start at least one survey campaign. Go to the **Campaigns** tab to do it. By default, no campaigns are added, and they have to be created manually. If campaigns already exist, you will see the list of campaigns.

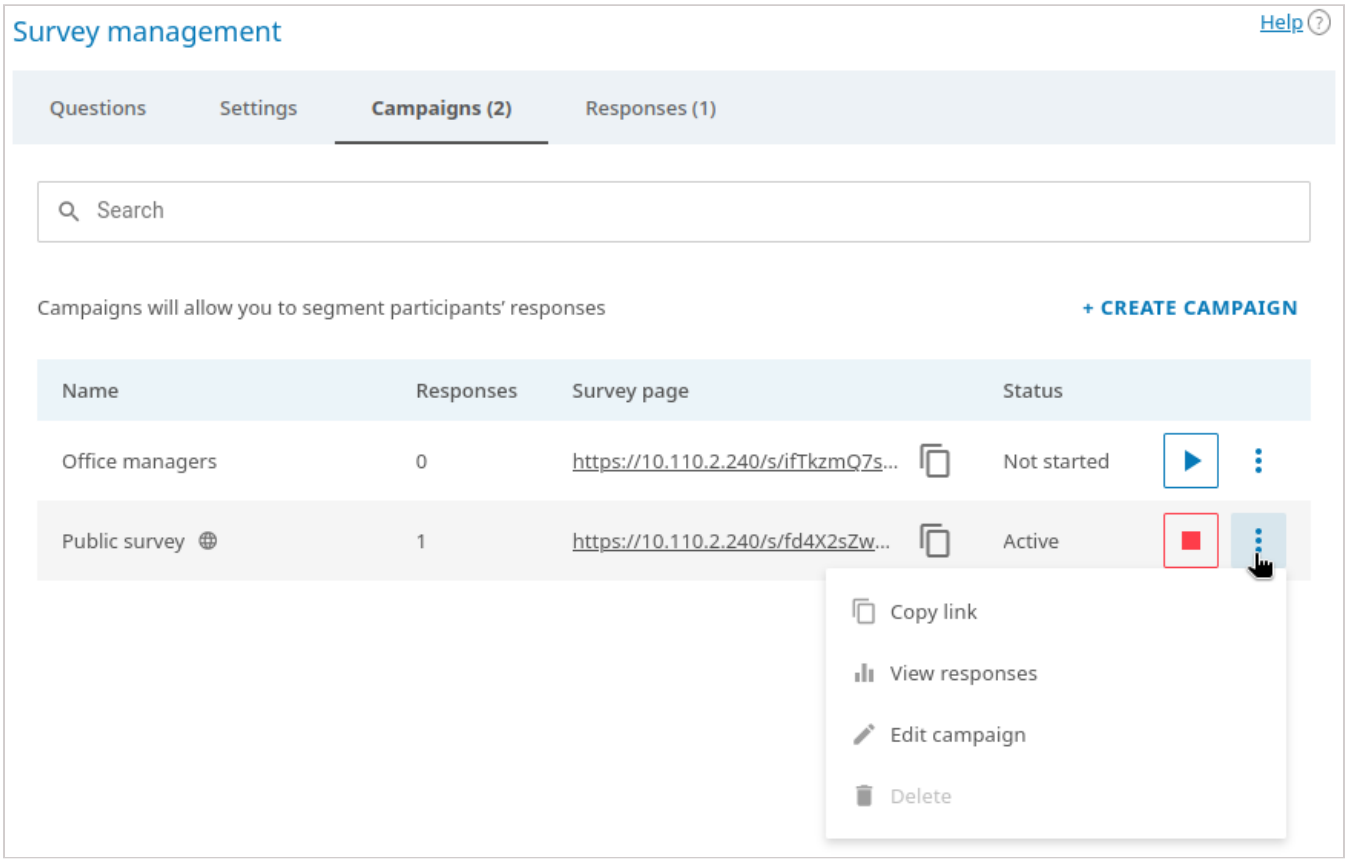
16.2.3.1. How to create a campaign



1. Click the **Create campaign** button.
2. Enter the campaign name in the **Name** field. It is not visible to participants and is used only for quickly finding campaigns in the list.
3. Choose the level of campaign accessibility for participants in the drop-down list **Who can take the survey**: everyone can follow a link and complete the survey (public campaign) or the survey will be available only to the users of your TrueConf Server.
4. Check the **Anonymous survey** box if you need to collect anonymized responses without participants' names. The results of an anonymous campaign will be displayed for each response option in each question, but without participants' names. No hidden analytics will be saved in the server database.
5. The checkbox **Allow participants to view their responses** enables participants to review their answers after submitting them.
6. Check the box **Allow participants to retake the survey** to let participants submit their responses again.
7. To provide participants with a neat campaign hyperlink, enter its suffix (the last part of the link added to your server address) in the **Campaign ID** field. For example, if you specify `office`, the link will look in this way: `https://example.com/s/office`. The ID must be unique within your server.

16.2.3.2. List of campaigns

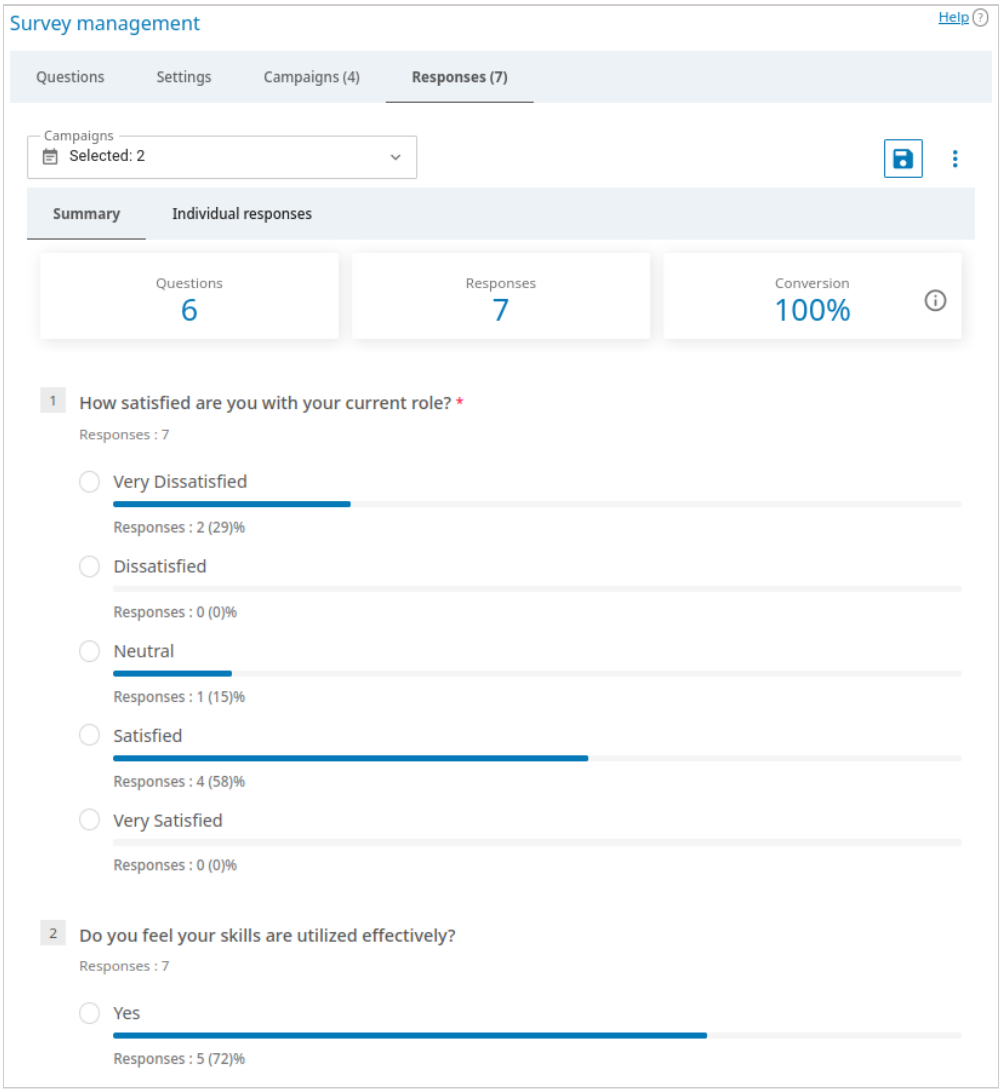
If multiple campaigns are created, they will be displayed as a list with several available actions (public campaigns are marked with the icon):



1. To copy the campaign link, click the button.
2. To launch an inactive campaign, click the button.
3. To stop the campaign, click the button . The survey will be paused and can be resumed if needed.
4. To go to the **Responses** tab with the results of the selected survey campaign, click the button in the row of this campaign and select **View responses**.
5. You can change the settings of a campaign regardless of its current status (active or paused); for example, a campaign can be made anonymous. To do it, click the button and select **Edit campaign**.
6. A paused campaign can be deleted which will also delete all the responses given specifically for this campaign. To do it, click the button and select **Delete**.

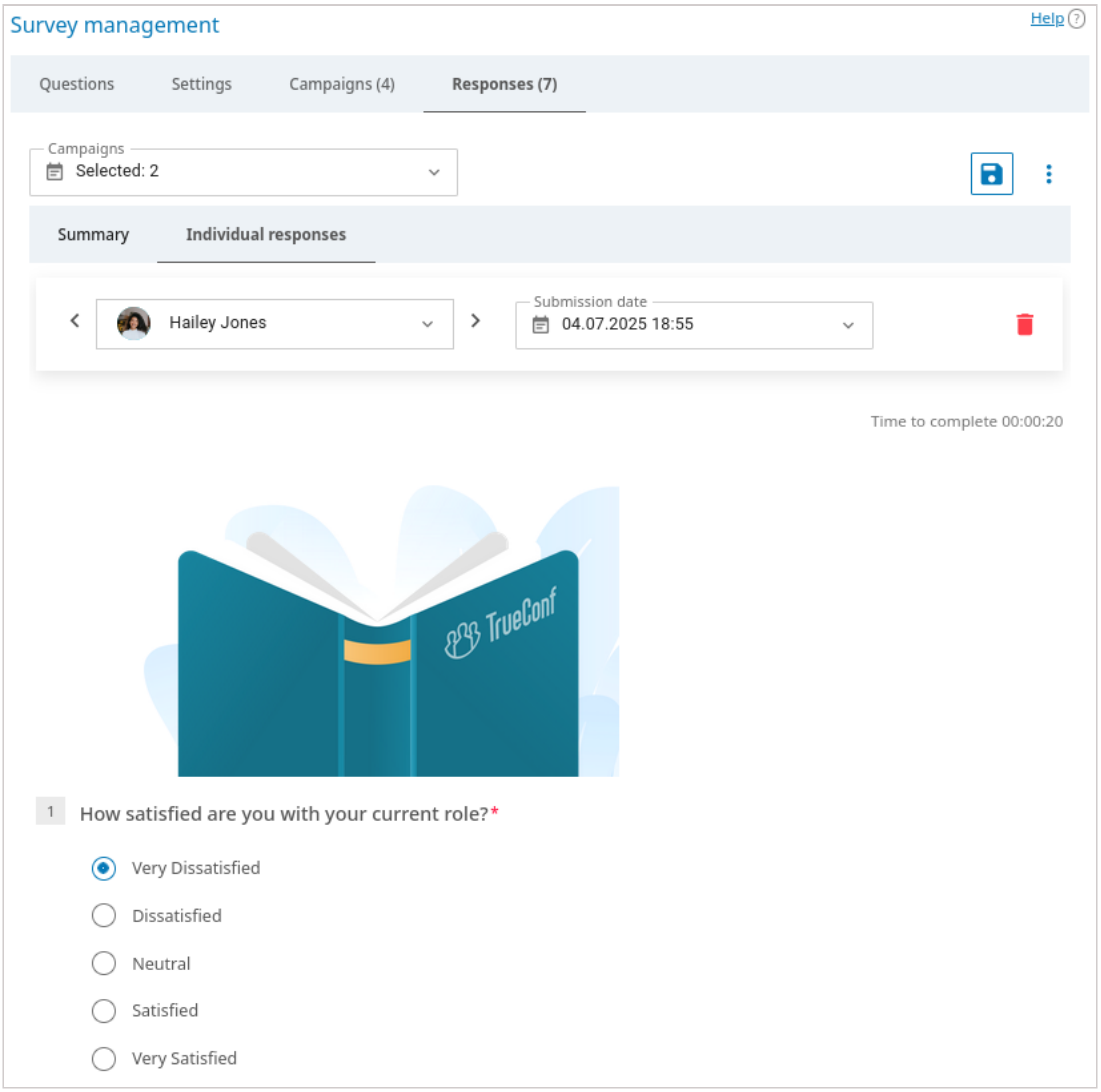
16.3. Results of survey campaigns

To view the results of survey campaigns, go to the **Responses** tab when editing the survey, or click the **View responses** link in the survey card in the general list. The opened tab will display the number of all responses across all campaigns:



1. In the **Campaigns** drop-down list, select the campaign for which you want to view the summary, and click **Apply**. You can select multiple campaigns to view the general summary for these campaigns.
2. The summary of results shows the number of responses, in other words, it shows how many users filled out the form and submitted responses. The conversion rate is also useful since it indicates the percentage of respondents who filled out the form after accessing the survey page.
3. To download the responses for one or several campaigns selected from the **Campaigns** list as a .csv file, click the button .
4. To delete the results of selected survey campaigns, click the button and select **Delete all responses**. All responses received for selected campaigns will be deleted.

By default, the results are displayed in the **Summary** tab, but you can switch to the **Individual responses** view. This allows you to select a participant to view this person's responses and the time taken to complete the test:



If the campaign was launched as ***anonymous*** (see campaign settings), the **Individual responses** list will display **Anonymous user** instead of names.

17. 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.

17.1. 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	Server wide	*Access token* valid for 1 hour is issued.

recommended for trusted applications only.		
User Credentials (a.k.a. *Resource Owner Password Credentials Grant*) 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 *(refresh token)* valid for 7 days are issued.
Authorization Code *Access token* 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 *access token* based on your existing *refresh token*.	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.

17.2. Permissions

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

The list of permissions expands with each new version of the API as new features are added to the video conferencing server. Refer to the API documentation for the list of APIs available in each version.

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.

17.3. 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.

17.4. 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.

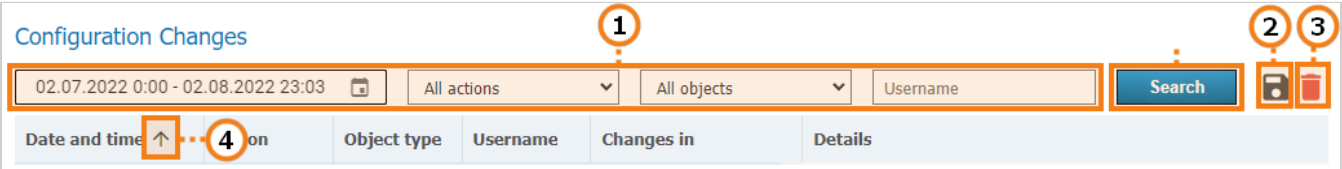
18. Server logs (reports)

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:



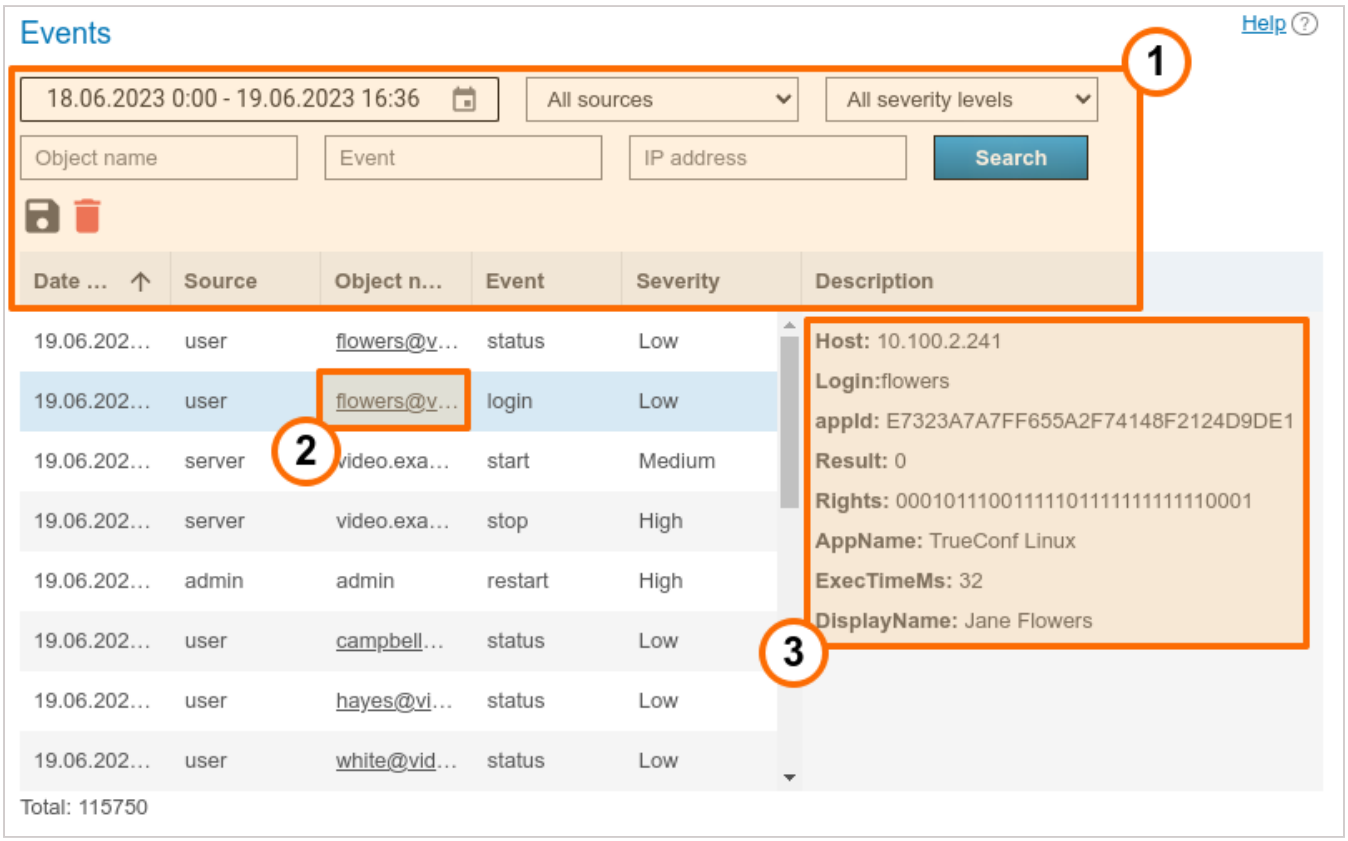
1. Filter entries.
2. Save a table in the CSV format (the export format can be selected in the preferences section).Please note that in this case, you will save the selection obtained after applying filters and clicking on the **Search** button.
3. Deleting the user accounts selected through filtering.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

18.1. 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)
- Results of the actions taken by OAuth applications (refer to the server API description for more details)
- Revocation of a user`s PRO licenses due to one of these reasons:
  - No PRO licenses were available when a user tried to join a group conference.
  - Revocation of a user's PRO license (either permanent or temporary) as a result of license redistribution after server restart or automatic revocation by timeout.
  - 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.



1. General UI for working with the table (check the description above). The **Event** drop-down list can be used to select one or multiple event types for more flexible search and analysis.
2. Link to an active user profile.
3. Event details. Contains detailed information required for the technical support department to solve possible issues you may face. The most common event details:
   - **Users:** 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.

18.1.1. 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: • a user by login and password in the client application or personal area in the browser • a TrueConf Serveradministrator 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: • 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)

18.2. Call History

This section contains history of video calls and conferences hold on the server.

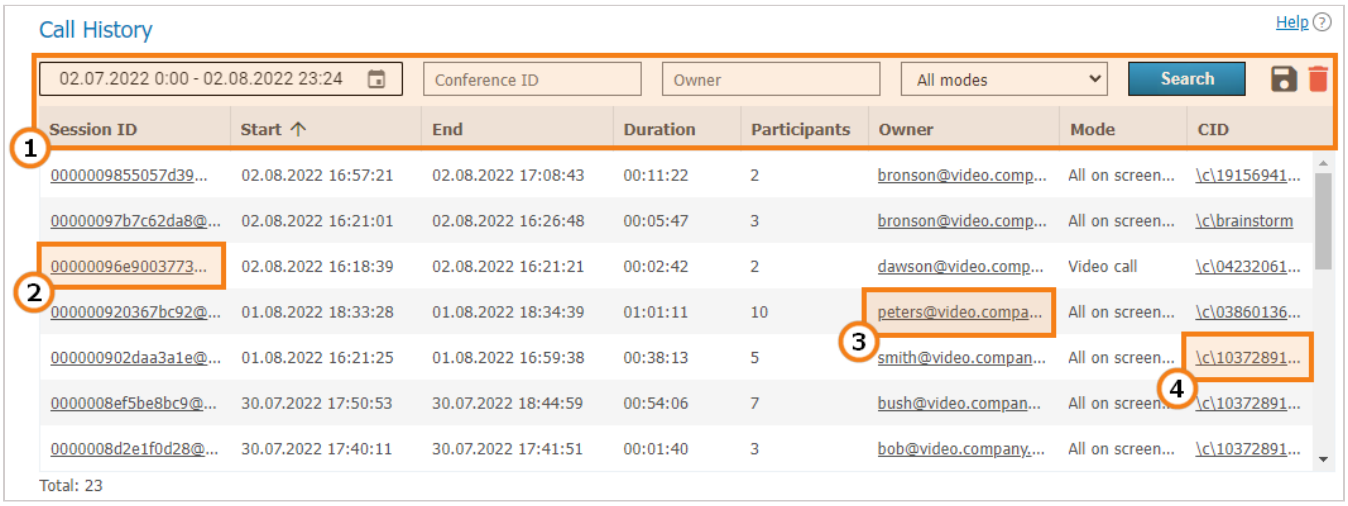
Please note that each time you start the same conference, a new conferencing session with its own identifier is initiated. This is relevant for scheduled recurring events or for

virtual rooms. For this reason, there will be several entries in the call history table with details of each independent conferencing session.

18.2.1. 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.

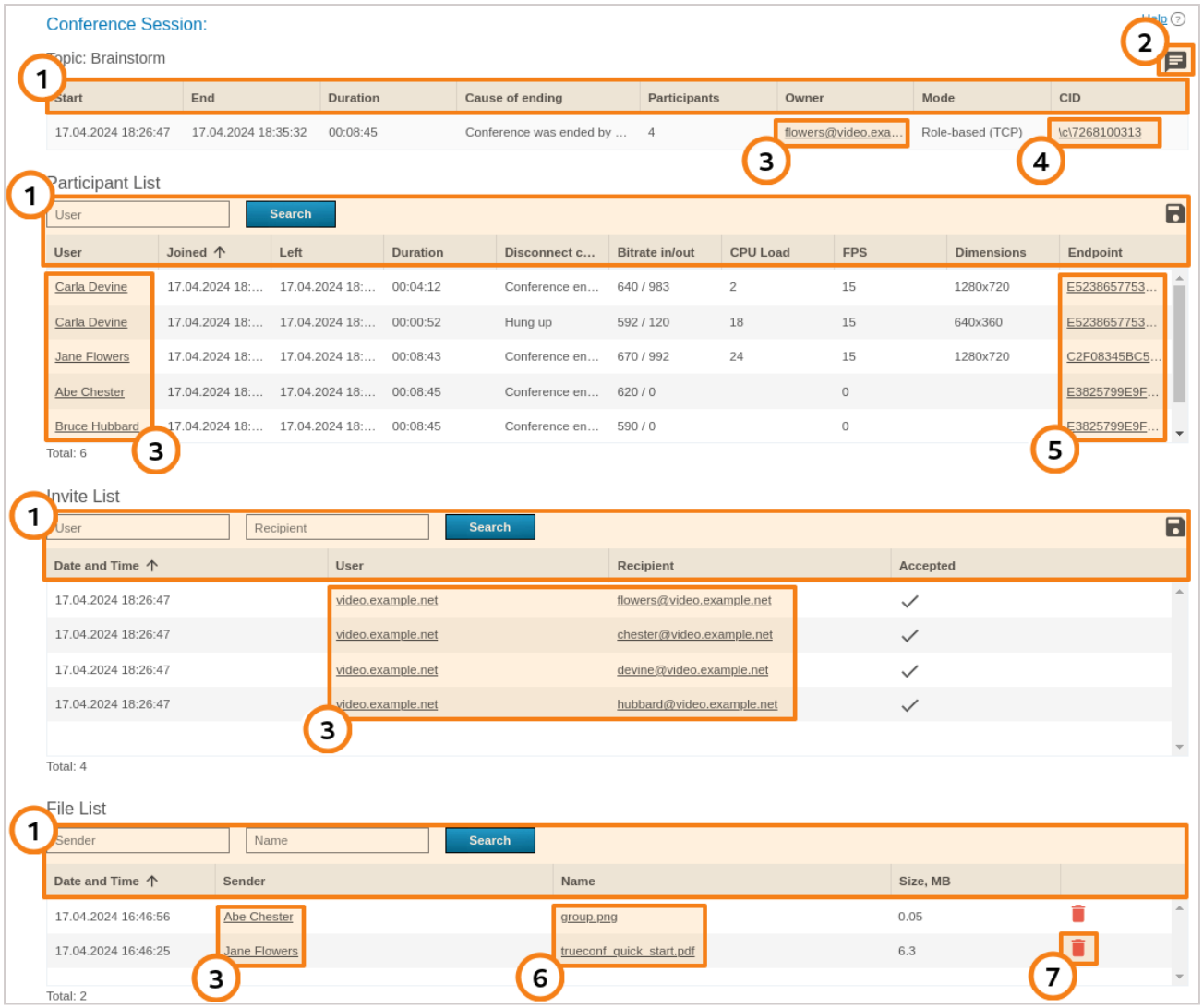


1. General table interface (see the description above).
2. Link to the page with detailed information about a session.
3. Link to a profile of the conference or call owner.
4. If this session has a parent server-side conference (not created ad hoc in the client application), you can find it in the general list.

18.2.2. 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.



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.

i 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).

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

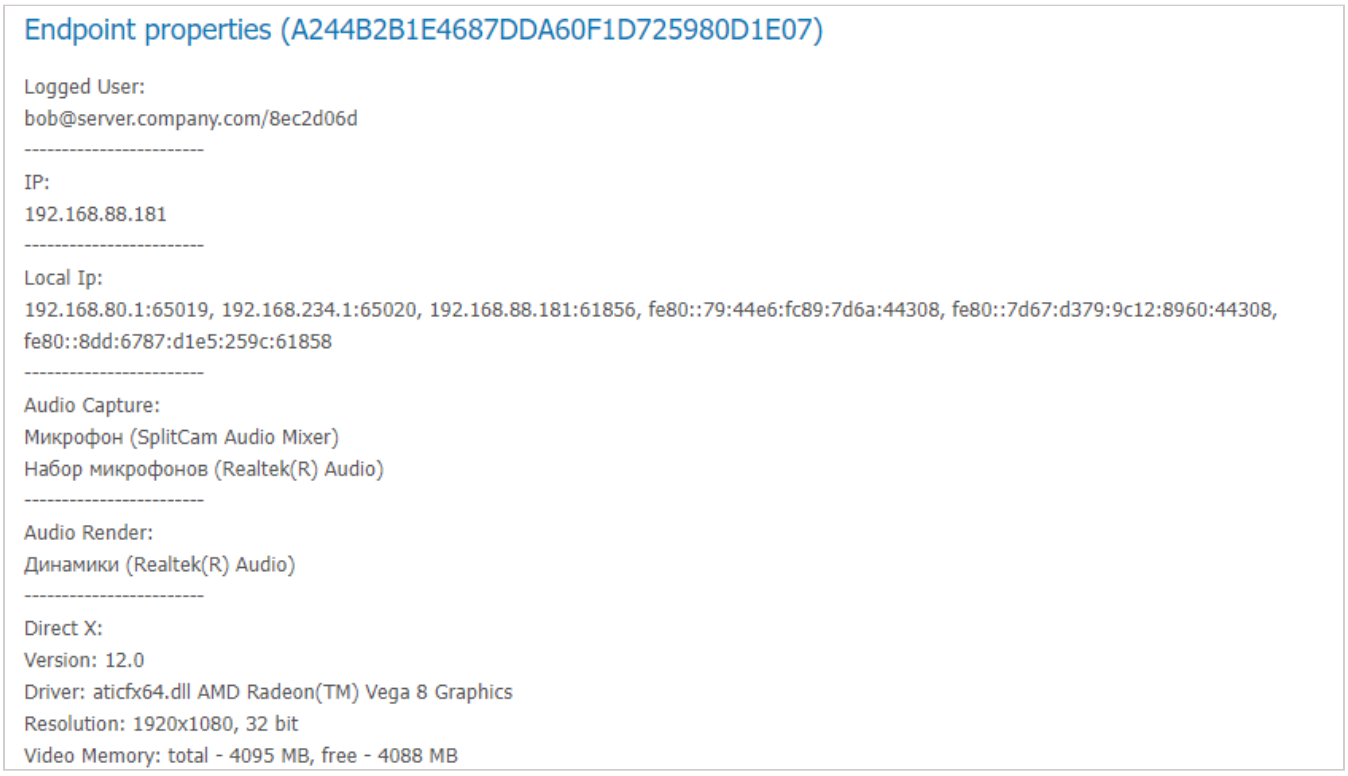
may differ. In the example above, we see that at least one user **Carla Devine** joined twice.

A guest, who reconnects to the webinar from the same application or browser, will not be counted again, even if he/she enters a different display name. For more details, refer to the section describing the peculiarities of guest IDs. However, the history of name changes will be displayed along with conference reconnection events.

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).

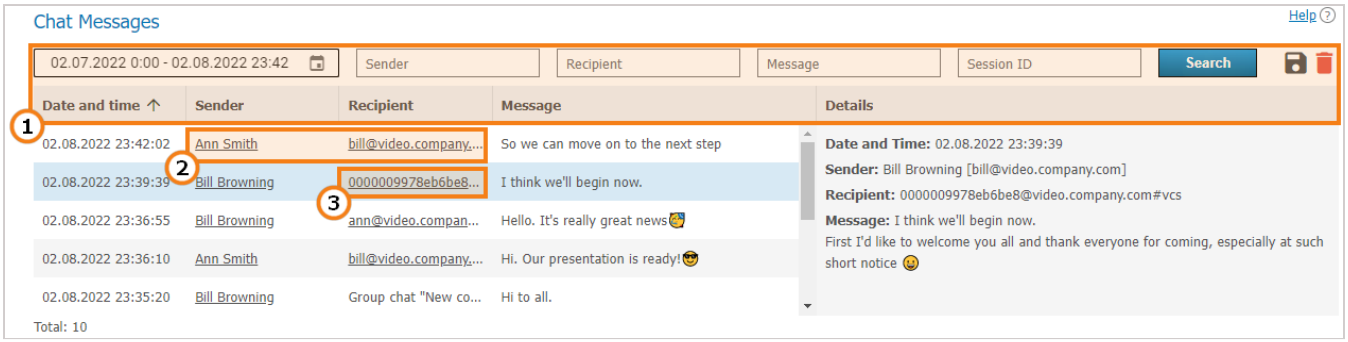
18.2.3. Connection properties

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:



18.3. 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.



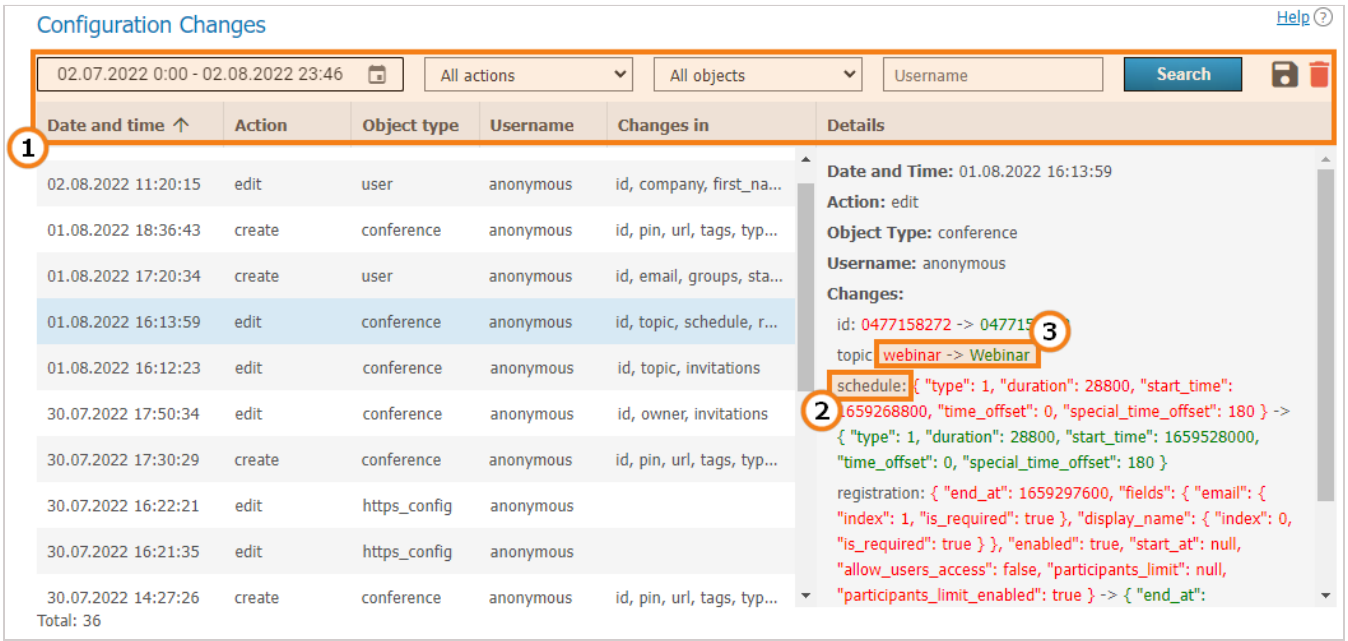
1. General table interface (see the description above).
2. Links to user profiles of the sender and recipient of a private message.
3. Link to a page with detailed information about the session to the common chat of which a message was sent.

18.4. 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
- Modification of external systems integration settings (LDAP, DLP, corporate email)
- History of creating and modifying surveys (but not responses to the surveys)
- 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.



1. General table interface (see the description above).
2. Name of the modified parameter.
3. Parameter values: **previous** (before change) -> **new** (after change).

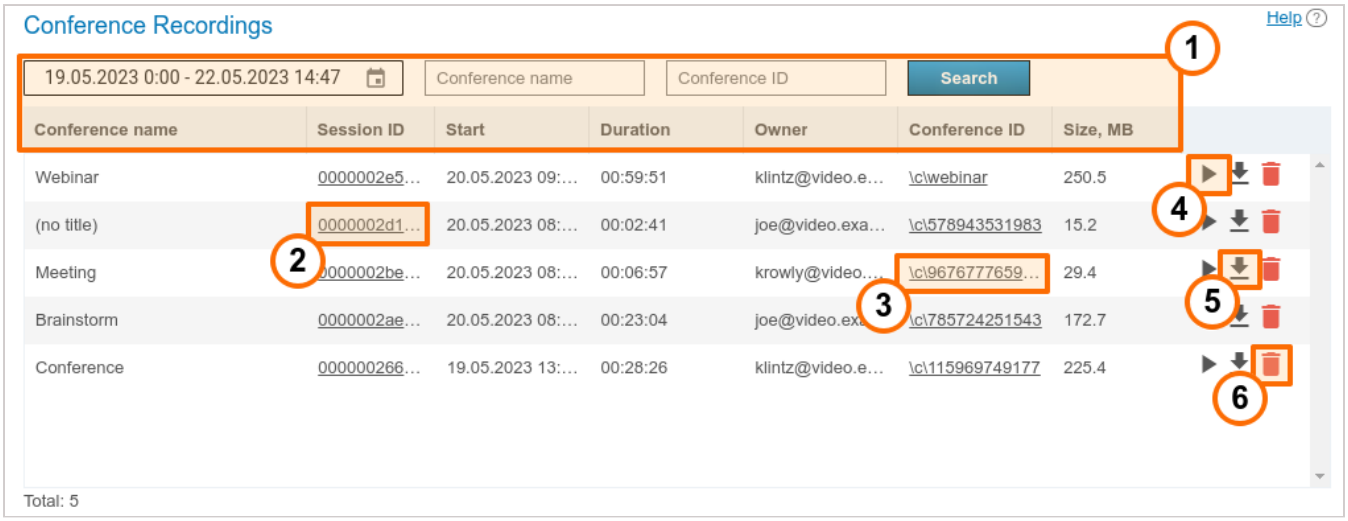
For example, the picture above illustrates an event involving some changes in the conference settings. The following parameters were changed:

- Name (`topic` parameter)
- Schedule settings (`schedule` parameter)
- Conference registration settings (`registration` parameter).

18.5. Conference Recordings

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

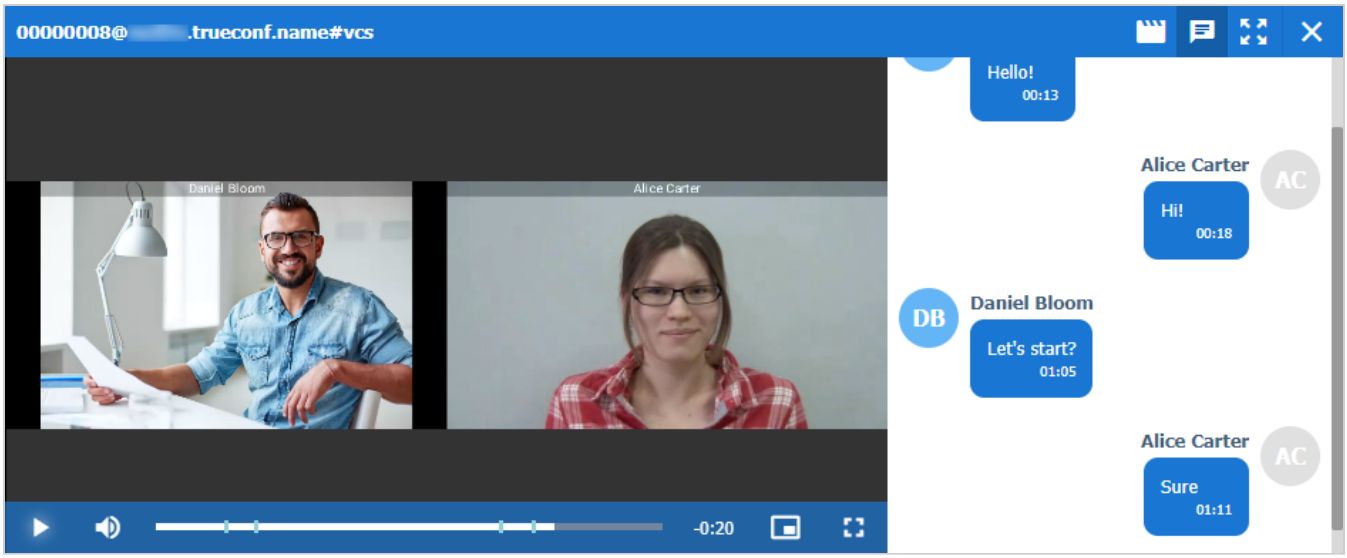
The parameters for storing conference recordings are set in a different section, **Recordings**.



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):



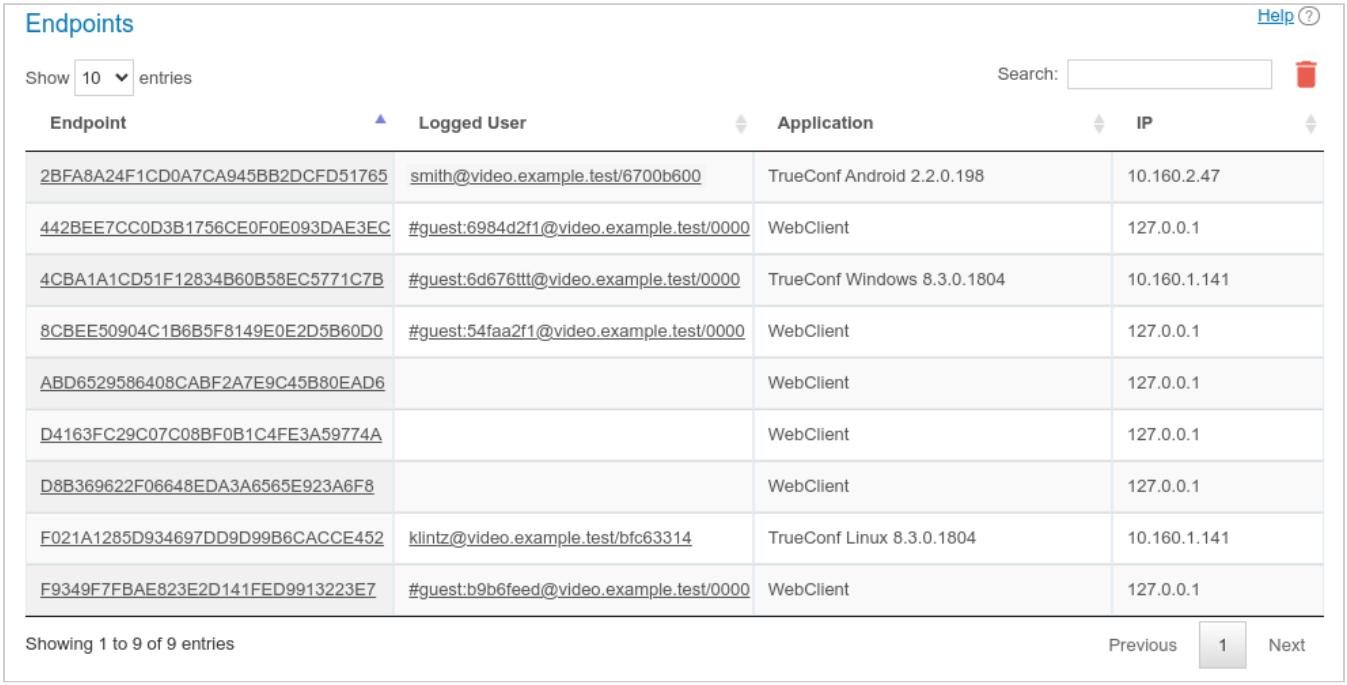
Can the video recorded with TrueConf Server be played using third-party programs?

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.

18.6. Endpoints

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



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):

18.6.1. Events that update device information

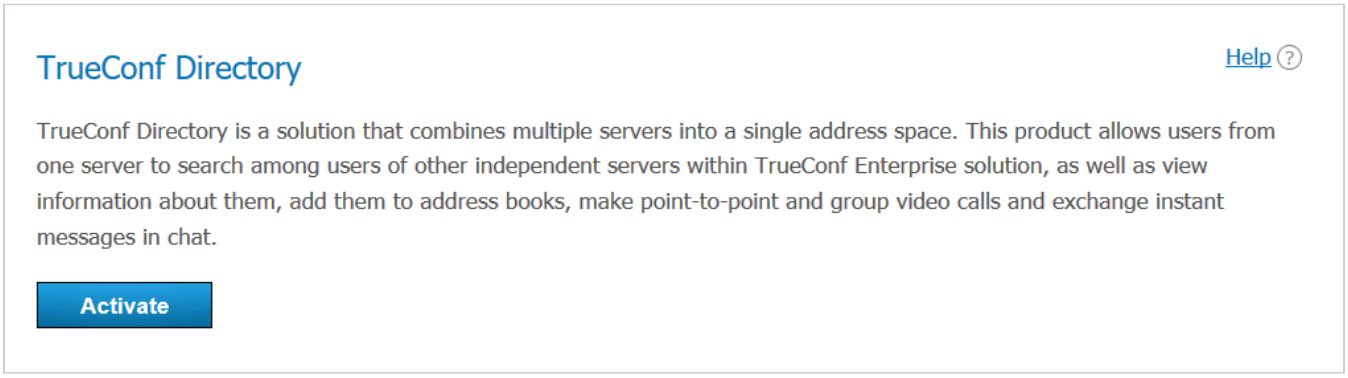
Event	Variable Fields
Connecting or reconnecting device to the server	• Network Info Type • Audio Capture • Audio Render • Video Capture • Direct X • Hardware Config
Conference end	Last Conf Name
Taking network test (by clicking a corresponding button in the client application)	Network Test
Authorization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

19. Configuration of extensions

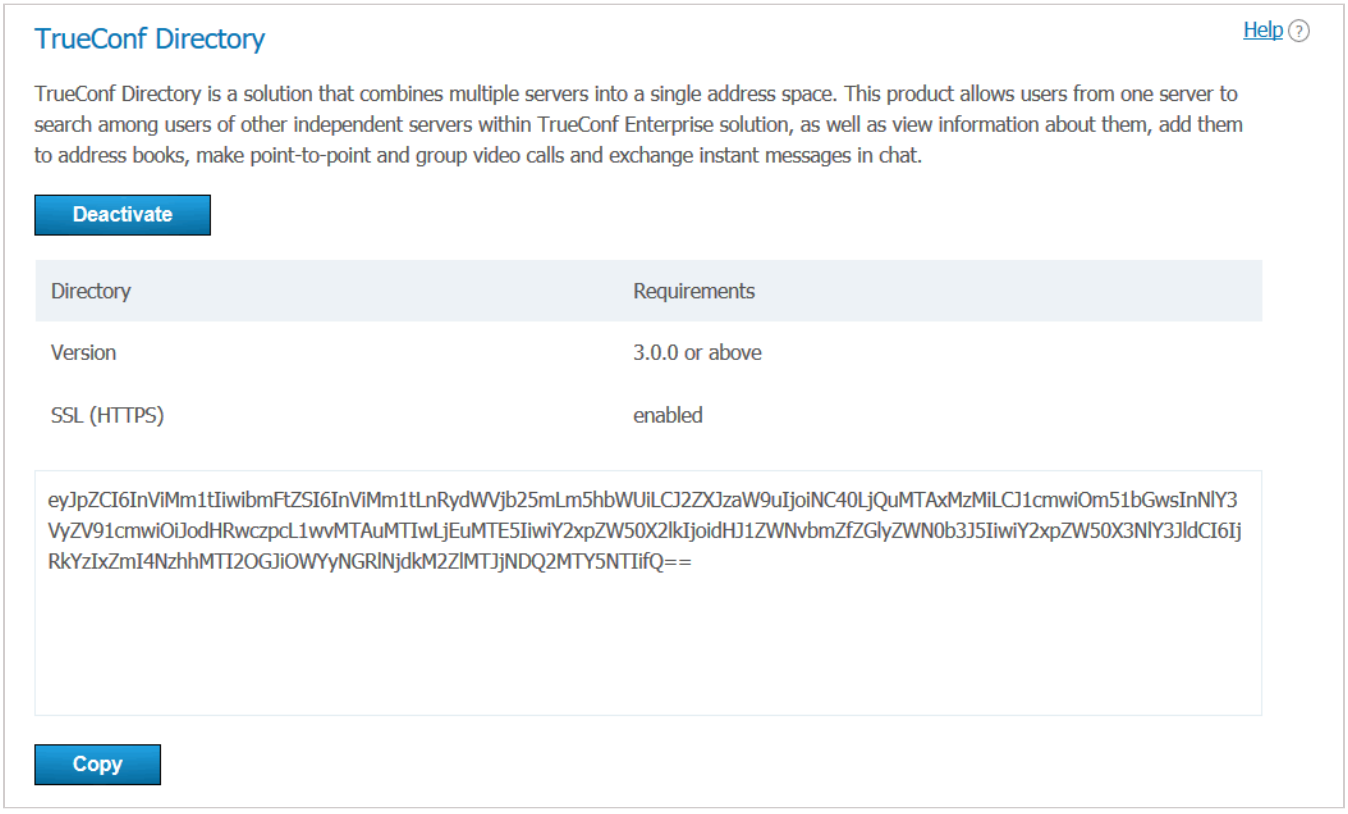
19.1. TrueConf Directory

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.



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

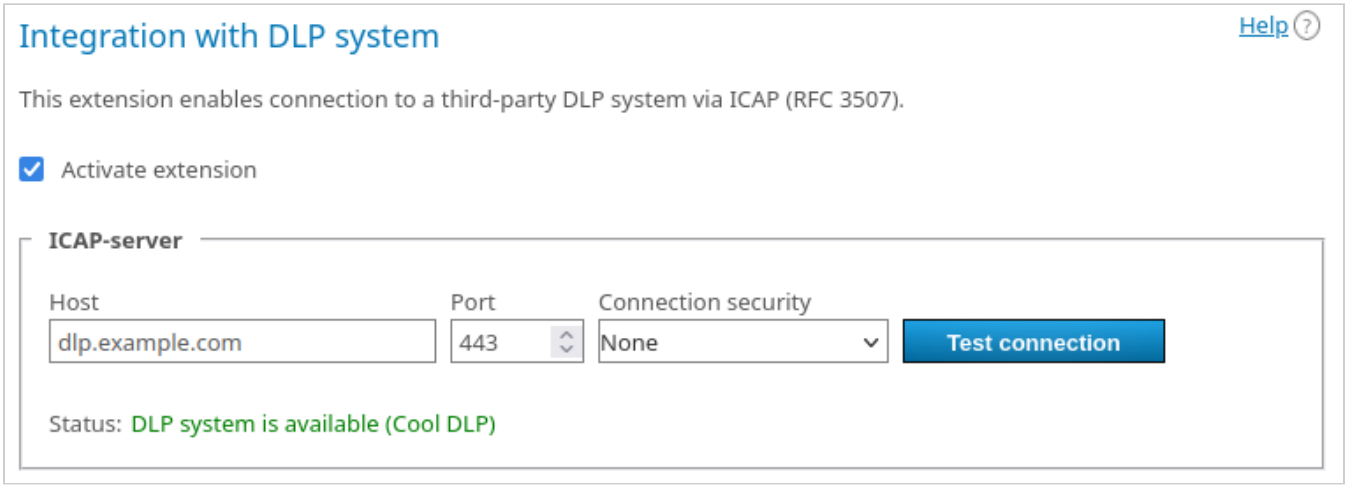


If you want to learn more about TrueConf Directory extension, as well as how to purchase and set it up, please contact us in any convenient way.

19.2. 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.

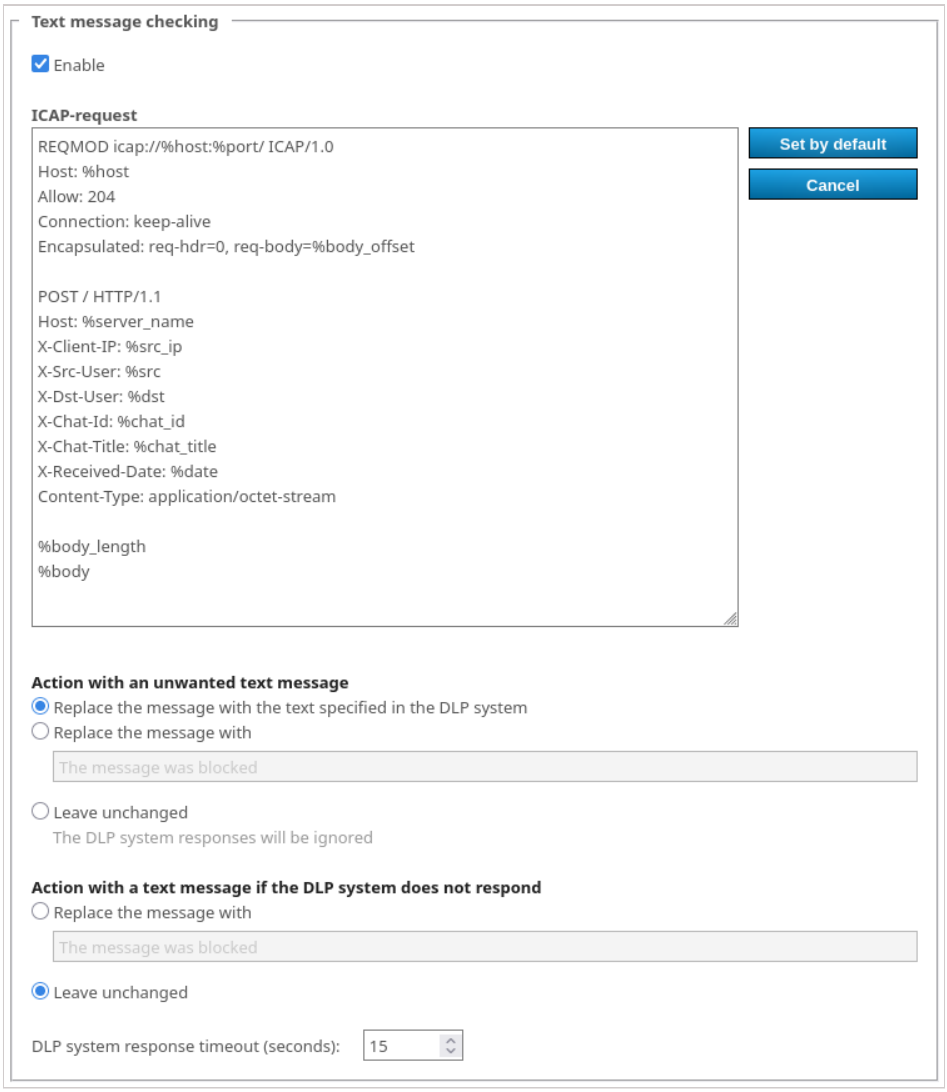
19.2.1. DLP system connection settings



1. Before using a DLP system, you need to check the **Activate extension** box. Until the box is checked and the settings are saved with the **Apply** button at the bottom of the page, no checks will be made by the DLP system.
2. In the **ICAP-server** section, configure the parameters for connecting to the DLP system: host (IP or FQDN without the 'http: / https:' prefix), port, and connection type (standard or TLS-secured).
3. Click the **Test connection** button to check if the system is available. The test result will be displayed in the status line below.

19.2.2. Message verification settings

In the **Text message checking** section, configure the parameters for handling regular messages:

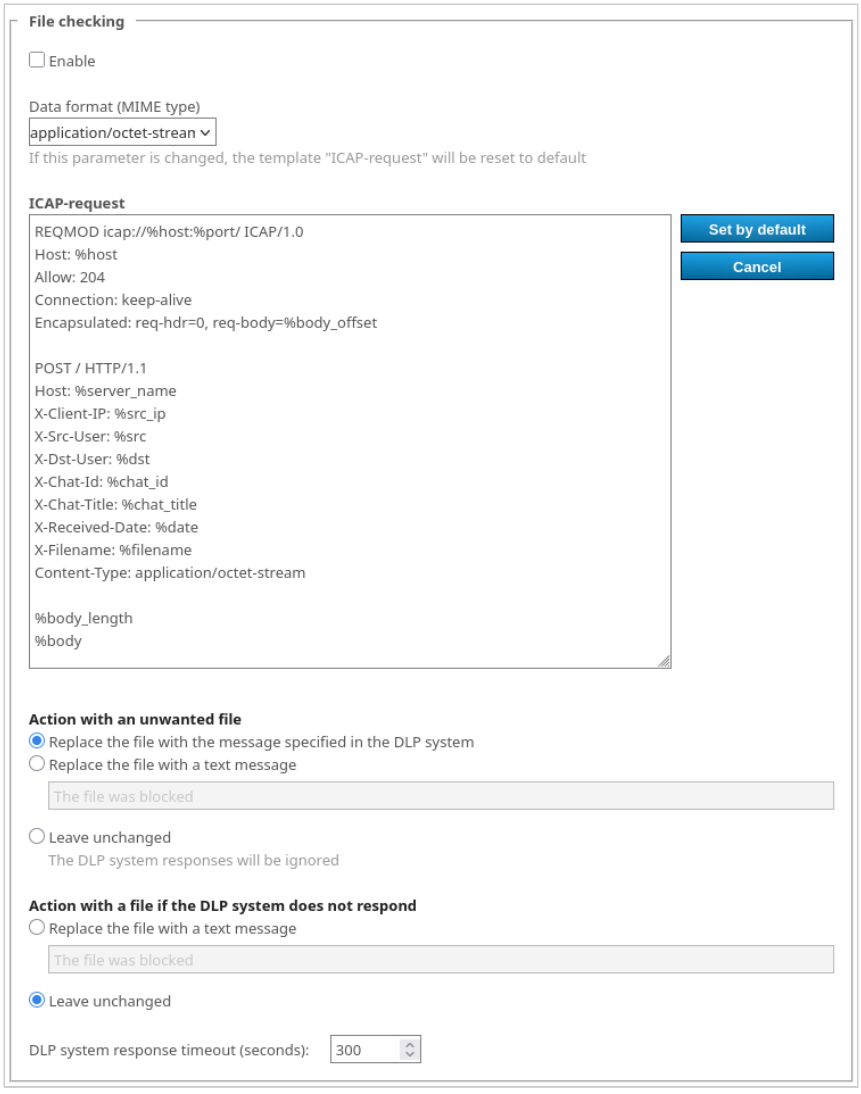


1. Check the **Enable** box. Until the box is checked and the settings are saved with the **Apply** button at the bottom of the page, the verification will not work.
2. In the **ICAP-request** input box, enter the fields required for sending data to the DLP system. The request format depends on the specific system; below, you can find the variables used in the template which will be replaced with actual values when data will be sent for analysis.
3. To reset ICAP request settings, click the **Set by default** button.
4. The **Cancel** button enables you to discard the changes in the request text which were not saved with the **Apply** button.
5. In the section **Action with an unwanted text message** choose the action to be taken if a message fails the DLP check. You can replace the message with the text chosen in the DLP system, enter your own text, or leave the message unchanged. In the latter case, users will receive all messages, but the DLP system logs will record the sending of unwanted messages.
6. In the section **Action with a text message if the DLP system does not respond**, choose what to do if the DLP system is not available. For example, you can enter the text ***No connection with the security system*** so that no messages can be delivered to recipients until the integration issue is resolved.
7. The parameter **DLP system response timeout (seconds)** is used to set the waiting time for applying the settings from the previous sections. If the connection to the DLP

system is disrupted, the time specified here will have to elapse before the action selected in the section **Action with a text message if the DLP system does not respond** is taken (since attempts will be made to restore the connection). Later, the connection check will be carried out in the background, and messages will be sent or blocked almost instantly.

19.2.3. Checking the files sent in chats

In the **File checking** section, set the parameters for handling the files sent in chats:

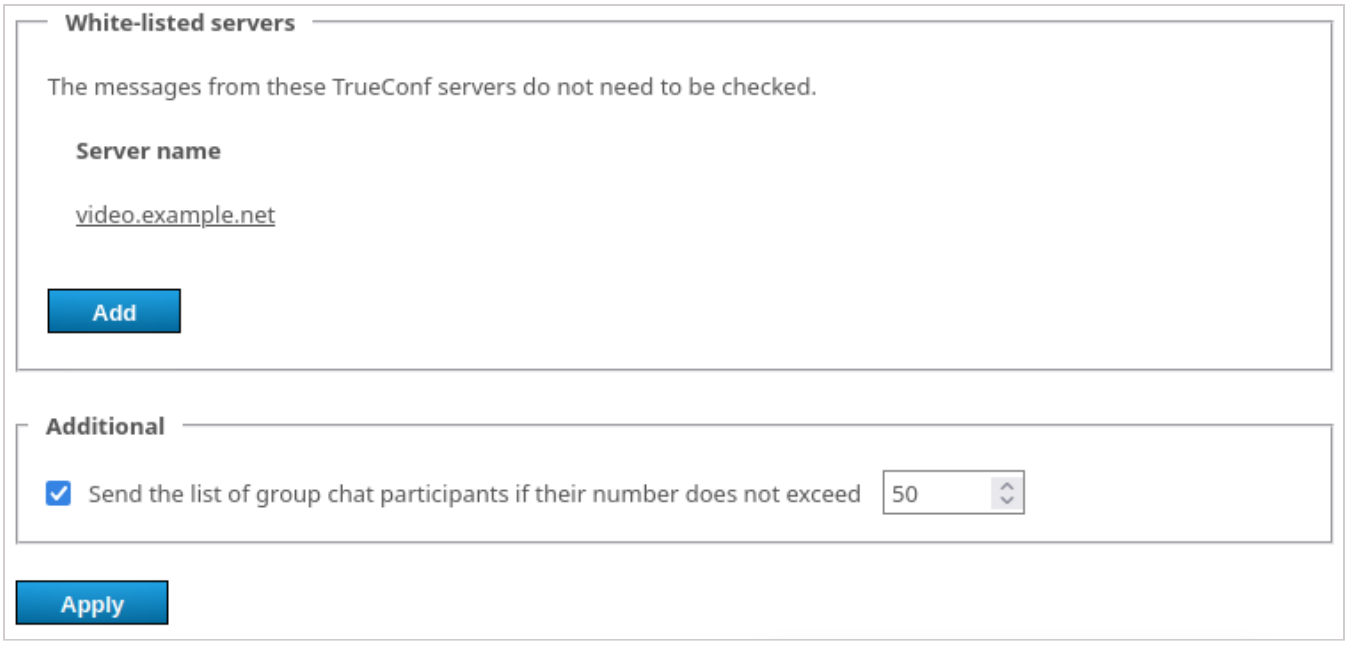


The list of settings is similar to those ones for message checking, but an extra parameter was added for selecting the request body type which improved compatibility with various DLP systems.

Don't forget to click the **Apply** button to save changes.

19.2.4. Trusted servers and advanced configuration for sending the list of chat participants

In the **White-listed servers** section, you can add addresses (only FQDNs, not IP addresses) of the video conferencing servers for which there is no need to verify messages and chats. This will speed up the verification process, but please be careful when using this feature. You can also include the address of the current TrueConf Server instance in this list. To change an address, just click on it in the list:



Example of how the activated parameter **Send the list of group chat participants if their number does not exceed** works:

1. Let us suppose that the template includes the `%dst` and `%dst_user` parameters.
2. A limit of 30 participants is set for group chats.
3. For each chat with 30 users or less, the list of full TrueConf IDs and the list of logins will be sent in this format `domain\user`.
4. If the number of chat participants exceeds the limit, the list will not be generated (an empty list will be sent to the DLP system).
5. If you uncheck the box **Send the list of group chat participants if their number does not exceed**, and include the `%dst` parameter in the template, the full TrueConf ID of a meeting participant in private chats will be sent to the DLP system, but the list of participants in group chats will not be sent.

19.2.5. 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` is the recipient's full TrueConf ID specified in the format `user@server`. For group chats, the list of all participants will be sent if the limit from the parameter **Send the list of group chat participants if their number does not exceed** is not exceeded.

This rule applies to all parameters described in this format `%dst_YYY` except `%dst_size`.

- `%dst_size` — the number of participants in a group chat. If the limit on the number of participants is exceeded (check the parameter **Send the list of group chat participants if their number does not exceed** at the bottom of the page) and the full list of recipients is NOT sent, this number can be used to estimate the size of the data leak.
- `%dst_base64` — `%dst` in base64 format
- `%dst_user` — the recipient's login (part of TrueConf ID up to the `@` character) with the domain specified as `domain\user`
- `%dst_user_at_domain` — the recipient's login in the `user@domain` format (`@domain` may be omitted if the recipient is in the main domain)
- `%dst_user_at_domain_base64` — `%dst_user_at_domain` in base64 format
- `%dst_user_base64` — `%dst_user` in base64 format
- `%dst_user_no_domain` — recipient's login
- `%dst_user_no_domain_base64` — `%dst_user_no_domain` in base64 format
- `%host` — the value taken from the **Host** field
- `%message_id` — unique message identifier
- `%multipart_boundary` — the value of the `boundary` parameter in the message header (intended to be used in the following way: `Content-Type: multipart/form-data; boundary=%multipart_boundary`)
- `%port` — the value 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

19.3. Mail plugins

The **Email plugins** extension provides access to the settings of TrueConf plugins for integration with popular email applications. To learn more about them, refer to the section on corporate calendars and email applications.

20. Integration with calendars and email

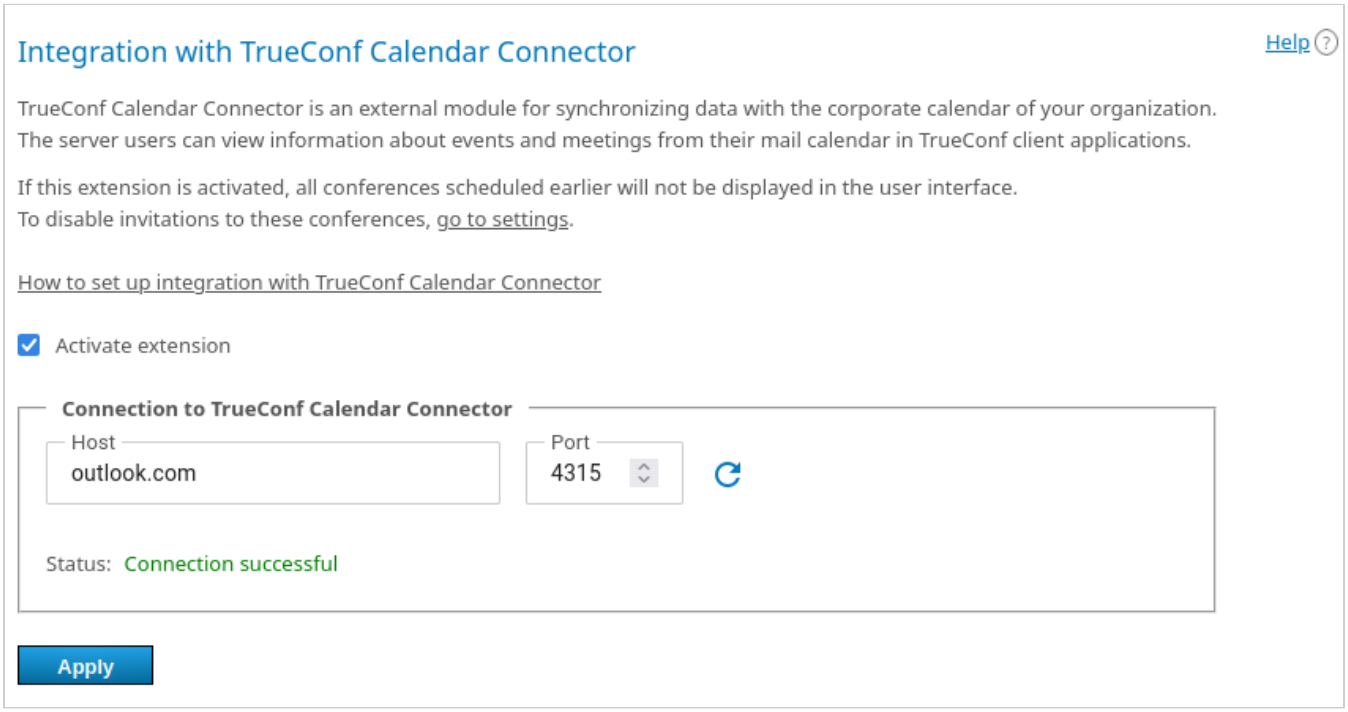
TrueConf offers a special module for seamless integration with corporate calendars and email plugins for popular mail and calendar applications: Microsoft Outlook, Mozilla Thunderbird.

20.1. Integration with a corporate calendar

To integrate your video conferencing server with corporate calendars, you need to use **TrueConf Calendar Connector**, a software module that acts as a link between the server and the corporate calendar software (e.g., Microsoft Exchange). It is installed on a separate machine and can act as a gateway for multiple instances of TrueConf Server.

Before integration, make sure that TrueConf Calendar Connector is installed on a machine that can access your TrueConf Server (see below). Moreover, a separate license is needed for the work of TrueConf Calendar Connector, but no additional licenses are needed on the side of connected video conferencing servers.

To set up integration, refer to the **Manage add-ons →TrueConf Calendar Connector** section.



1. First, you need to check the **Activate integration** box to enable information exchange with TrueConf Calendar Connector.
2. Specify the domain name (FQDN) or IP address of the machine where TrueConf Calendar Connector is installed. To set up correct integration, you need to make sure that both servers can communicate with each other. The domain name (FQDN) or IP address of your video conferencing server instance must also be configured on the side of TrueConf Calendar Connector.
3. Specify the TCP port for connection with TrueConf Calendar Connector (**4315** is used by default).
4. Click the **Apply** button to activate the integration and view the connection status.

! To make sure that everything works correctly, you need to activate TrueConf Calendar Connector and configure integration on the side of this solution as it is described in the documentation.

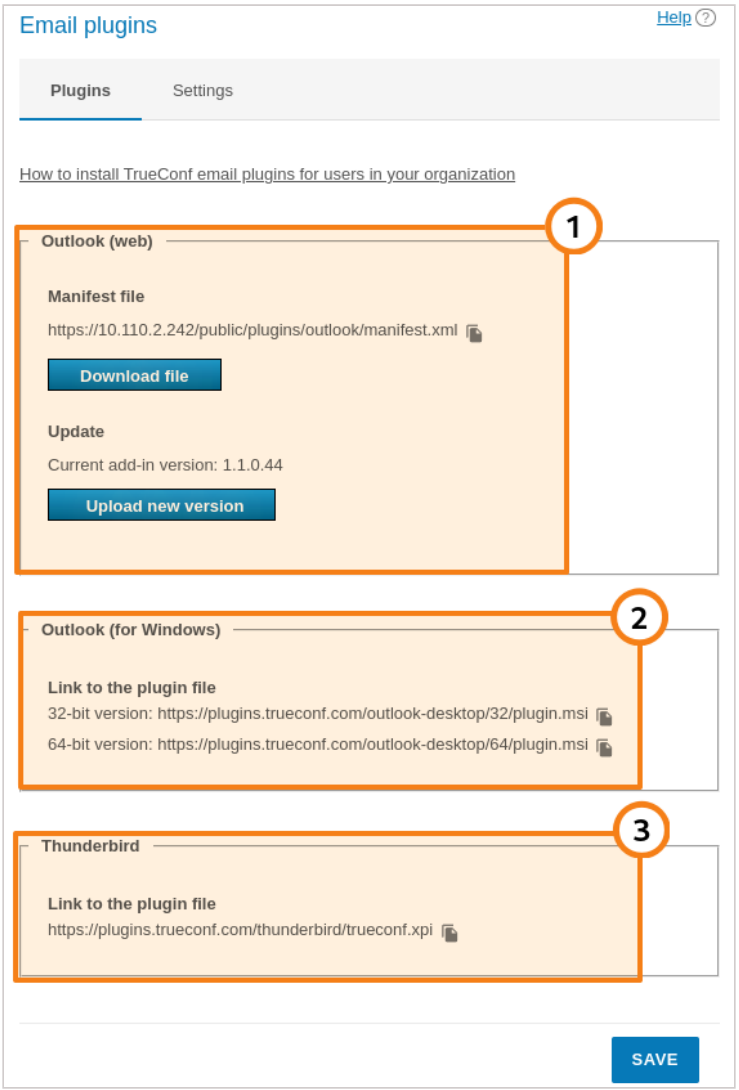
20.2. Mail plugins

The **Email plugins** extension allows 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).

Go to the **Manage add-ons →Email plugins** section. In 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

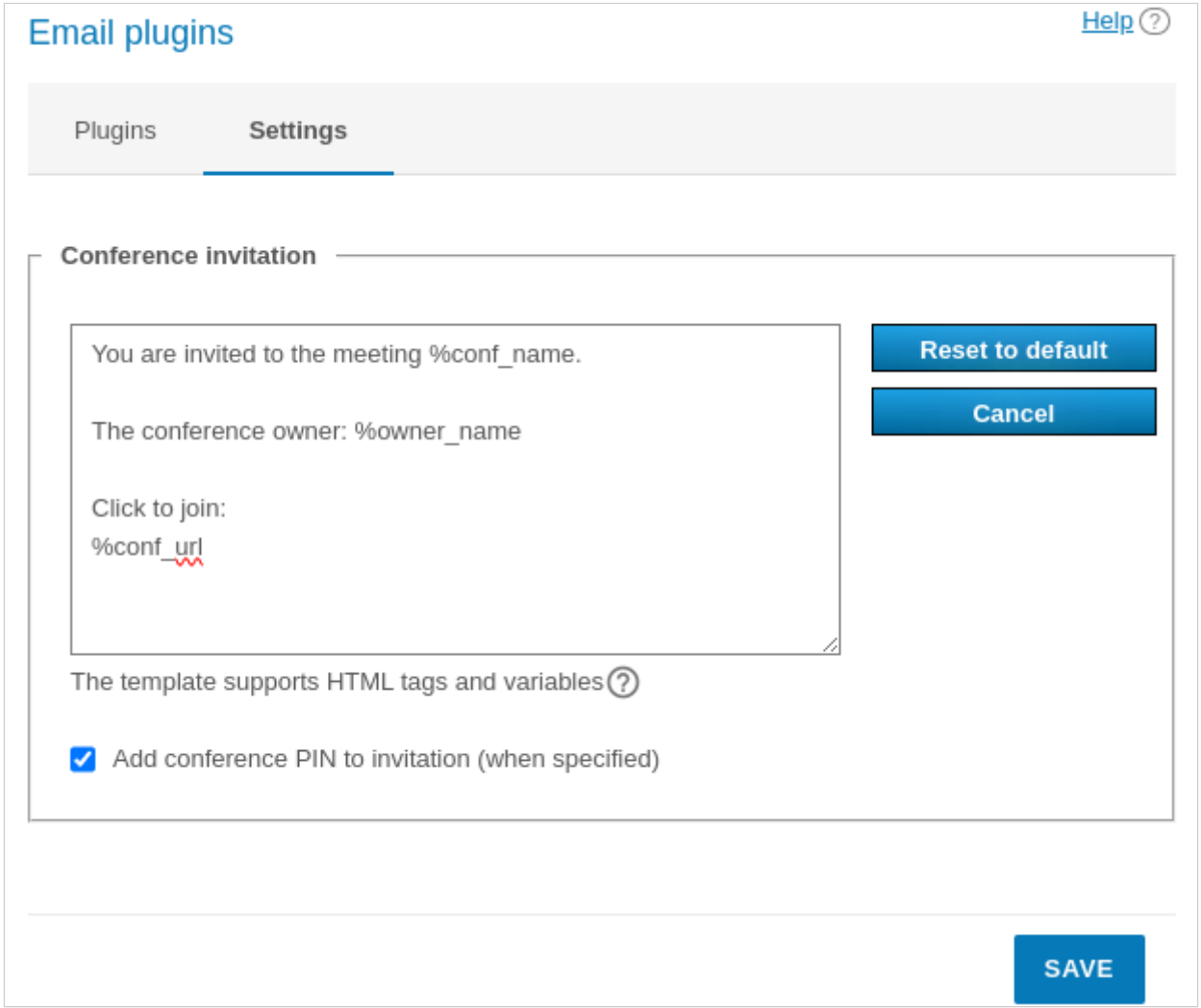
corporate network (including the private network that does not have access to the Internet) so that these users could install the plugin directly from your TrueConf Server.

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):



20.2.1. Invitation template settings

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

- `%owner_name` — display name of the conference owner
- `%conf_id` — ID of the conference, e.g. `\c\df0a2adebe`
- `%conf_url` — the link to the conference page, e.g.,: `https://example.com/c/CID`
- `%conf_name` — name of the conference
- `%conf_type` — the access type of the conference (private or public)
- `%max_speakers` — the maximum number of speakers (for a moderated role-based conference and a smart meeting, this is the left value in the pair of numbers *M x N*)
- `%max_participants` — the maximum total number of participants (for moderated role-based conferences and smart meetings, this is the right-hand value in the pair of numbers *M x N*)
- `%conf_mode` — conference mode
- `%conf_pin` — the PIN code for joining the conference
- `%conf_url_app_join` — a link for quick one-click connection in a client application without having to open the conference web page
- Server administrator contacts parameters:
  - `%admin_name` — display name
  - `%admin_email` — email address
  - `%admin_phone` — phone number.

20.2.2. Plugin configuration when using a self-signed certificate

If a self-signed certificate is used on the side, additional settings will be needed:

- If the Outlook plugin is used: no action is needed for the COM plugin, while for the web plugin, a user only needs to go to the server guest page in the browser and trust the self-signed certificate.
- If the mail plugin is used for the Thunderbird application, the certificate should be imported to each user's PC in the following way:
- Export the TrueConf Server certificate from the control panel. To do it, go to the **Web → HTTPS** section and click the **Download ca.crt** link. Next, choose where to save the **ca.crt** file. Distribute this file to users' PCs in any convenient way.
- On a user's PC, open the settings in the Thunderbird application.
- Go to the **Privacy & Security** section and click the **View Certificates** button.
- In the new window, go to the **View Certificates** tab and click the **Import** button.
- Select the **ca.crt** certificate file that you moved to this PC during Step 1.
- Check all the boxes in the certificate trust settings window and click **OK**.

21. Integration with AI server

Let us discuss separately how to add AI capabilities for meeting transcription and summarization to your video conferencing server.

To integrate AI features into the video conferencing system, you need to use the stand-alone solution TrueConf AI Server. A transcript is a text generated when the audio recording of a conference is recognized. If transcription is enabled for a conference, its audio is recorded during the video conferencing session and sent to the AI server according to the settings specified below.

* Recording of the audio file that will be sent to the AI server does not depend on the video recording feature. Separate files are created for transcription purposes and stored in a separate directory on the server.

This integration offers the following features:

- Transcription (writing meeting minutes) of a past conference
- Access configuration for a transcript
- Send notifications when a transcript is ready and when a user is allowed access to a transcript
- Ability to start transcription automatically or manually.

To set up the integration of TrueConf Server with TrueConf AI Server, go to the **Manage add-ons →TrueConf AI Server** section.

21.1. Levels of access to conference transcripts

You can connect only one instance of TrueConf AI Server to the video conferencing server with full access and an unlimited number of instances in read-only mode.

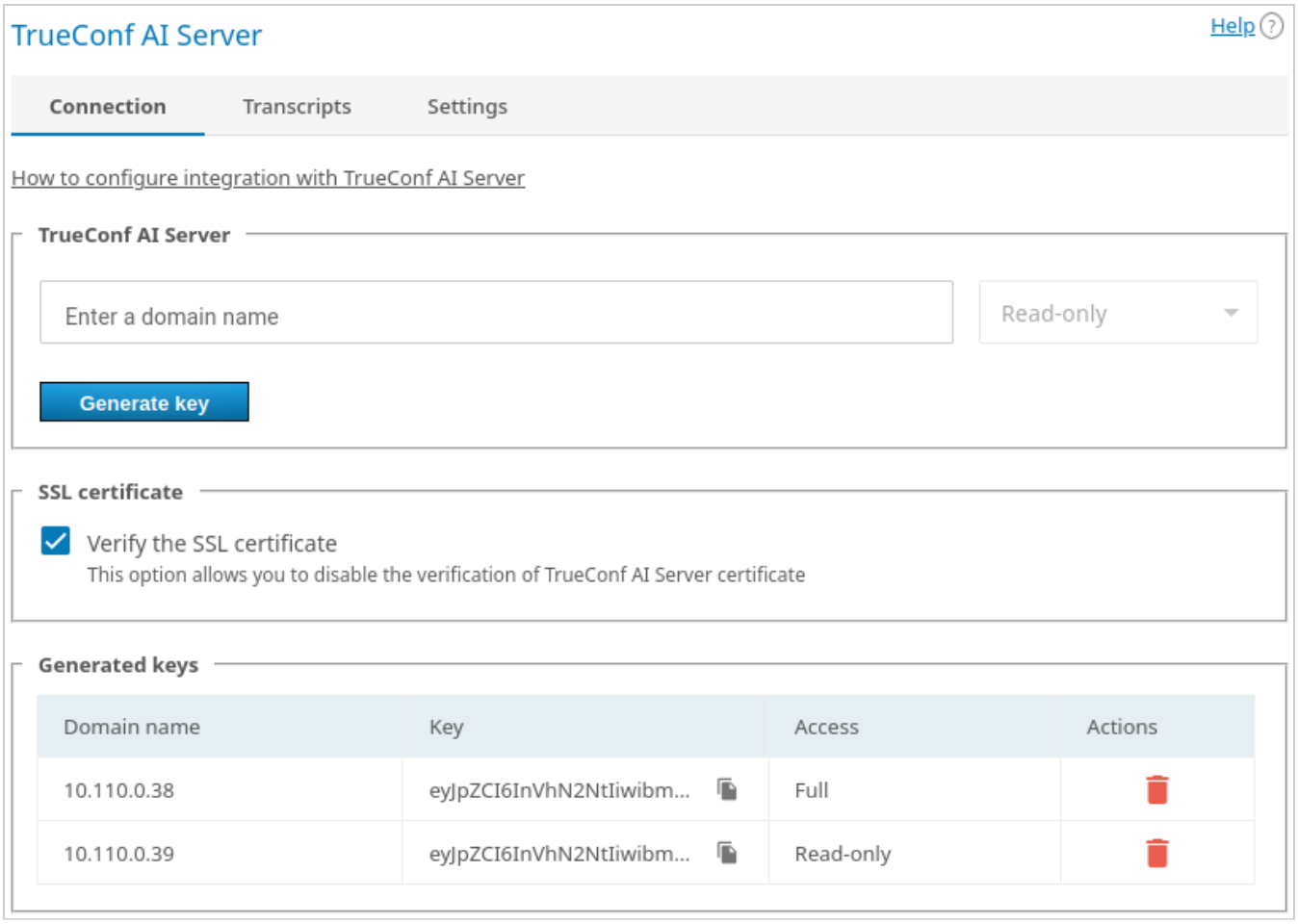
Read-only is the mode for integrating TrueConf Server with TrueConf AI Server. In this mode, users of the video conferencing server can only view and download transcripts.

Full access — in this mode, all users of the video conferencing server can get all permissions for working with transcripts. In addition to viewing and downloading these files, they can grant other users access to them, start transcription, and delete the recording.

Access to each transcript can be configured individually and can override the default settings (see below).

21.2. AI server connection settings

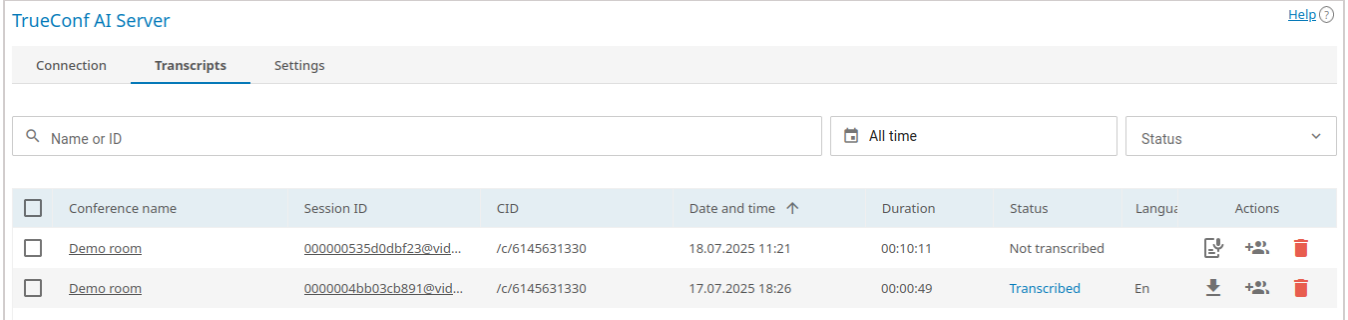
The parameters for connection to the AI server are configured on the **Connection** tab.



1. Enter the domain name of the AI server in the corresponding field (without the `http:/ https:` prefix).
2. In the drop-down list, select the maximum access level for your users when they will be connecting to the AI server.
3. If you do not need to verify the authenticity of the SSL certificate (for testing purposes or due to the use of a self-signed certificate on the side of TrueConf AI Server), uncheck the box **Verify the SSL certificate**.
4. Below you will see the list of added AI servers, their keys, and buttons for deleting unnecessary configurations. It is impossible to edit the settings of the servers which were added previously. They can only be deleted and added once again.

21.3. Viewing the list of completed and pending transcripts

On the **Transcripts** tab, you can see the list of transcripts for all conferences held on your server and for which the transcription feature was activated.



For each entry, you can follow the link to the corresponding conference and even to the page of a specific session (call session). Please note that a single conference may have multiple sessions if it was started more than once.

The **Status** column shows the current state of each transcript and can have the following values:

- **Added to queue** — the audio recording has been sent to TrueConf AI Server and is awaiting transcription
- **Not transcribed** — the recording has not been sent to the AI server; so, it was not transcribed (for example, meeting transcription has to be started manually **On request** and this process has not been started yet)
- **Transcribed** — the audio recording was successfully sent to the AI server and transcribed
- **Transcribing** — the audio recording is being transcribed (an approximate completion percentage will be displayed).

To quickly find required transcripts, filter the list by name or conference ID, as well as by event time and the status of the transcript.

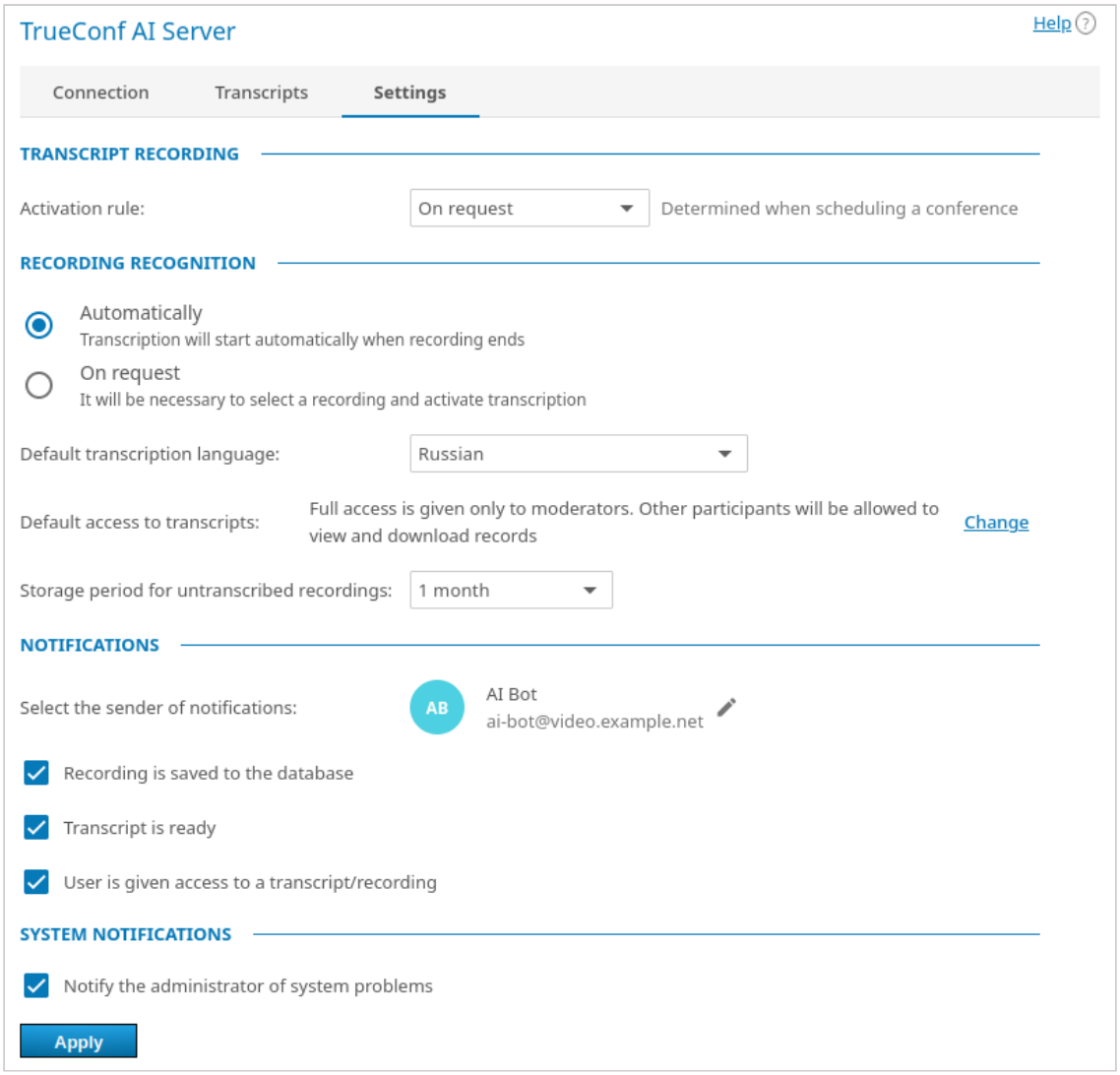
To start recording transcription, click the button (displayed if this process has not been started yet). To download the text of a transcript, click the button . You will be able to choose the export format for the transcript: a ***csv*** table, a ***txt*** file, or a ***pdf*** document. The transcript can also be downloaded as an archive with the original audio recording of the conference.

To delete a transcript, click the button . In this way, you will delete both the transcript and the original recording of the corresponding conference.

You can select multiple transcripts with the help of checkboxes and either download or delete them all.

21.4. Conference transcription settings

In the **Settings** tab, you can set general rules for sending audio files that will be transcribed and for sending notifications.



1. Select the rule for starting conference audio recording in the **Activation rule** drop-down list: you can choose to record all conferences, only those ones selected on the **Advanced** tab, or disable recording altogether.
2. When the conference ends, the recorded audio is sent to TrueConf AI Server, but transcription has to be started separately. If you activate the **Automatically** toggle in the **Recording recognition** section, transcription will automatically start for all conferences (queued on the AI server). If you choose **On request**, transcription of a specific recording has to be started manually in the personal area of the video conferencing server or in the AI server.
3. Choose the default language that will be used when transcribing all conferences. Please note that the AI server can detect when conference participants switch to a different language. Moreover, it will correctly recognize different languages spoken by event participants. However, by selecting the main language spoken by participants, you can make transcription more accurate.
4. In the drop-down list **Default access to transcripts**, you can select which conference participants will have access to the transcript. These are not final settings since the users, who were given full access, can override permissions for other users for each conference in the personal area of the video conferencing server or the AI server. The following access options are available by default: full access for moderators and read-only access for other participants; full access for all participants; transcripts are

available only to moderators and the server administrator, but not accessible to anyone else; transcripts are available only to the server administrator, who can configure access for participants, if necessary.

5. The parameter **Storage period for untranscribed recordings** determines how long every audio recording will wait for transcription before it is automatically deleted to reduce the disk space used by the video conferencing server. Files are deleted only on the side of TrueConf Server. Besides, only the recordings that have not been sent to the AI server will be deleted.
6. In the **Notifications** section, you can select the account on whose behalf notifications about transcription events will be sent to users. This step is optional but it will help users to work with transcripts because all involved participants will receive relevant notifications. You can send notifications about the following events: an audio recording is added to the database of the AI server, a transcript is ready, and a user is given access to a recording or transcript.
7. Additionally, you can check the box **Notify the administrator of system problems** to send notifications about integration problems to the administrator's email (specified in the main server settings). For example, the administrator can be notified if the storage allocated for audio files of this video conferencing server is running out on the side of TrueConf AI Server.

* There is no need for a continuously running chatbot to send notifications; so, no additional online licenses are used. You just need to create a separate account for notifications.

22. Permissions of the administrator with the Security Admin role

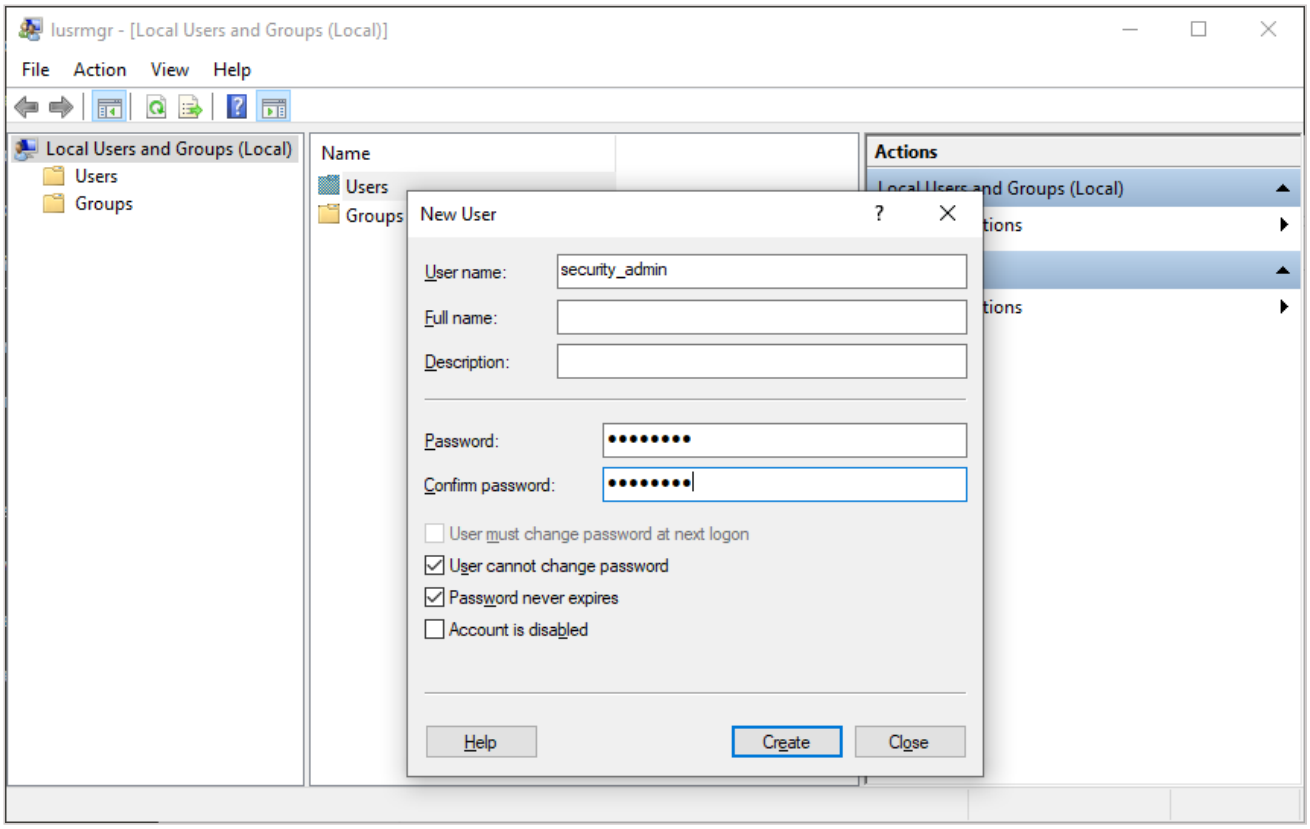
To enable limited access to the TrueConf Server control panel, a local **TrueConf Server Security Admin** user group on Windows and **tcsecadmins** on Linux is automatically added to your operating system during the server installation process. TrueConf Server administrators can add to this group the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

22.1. How to add a Windows account to the Security Admin group

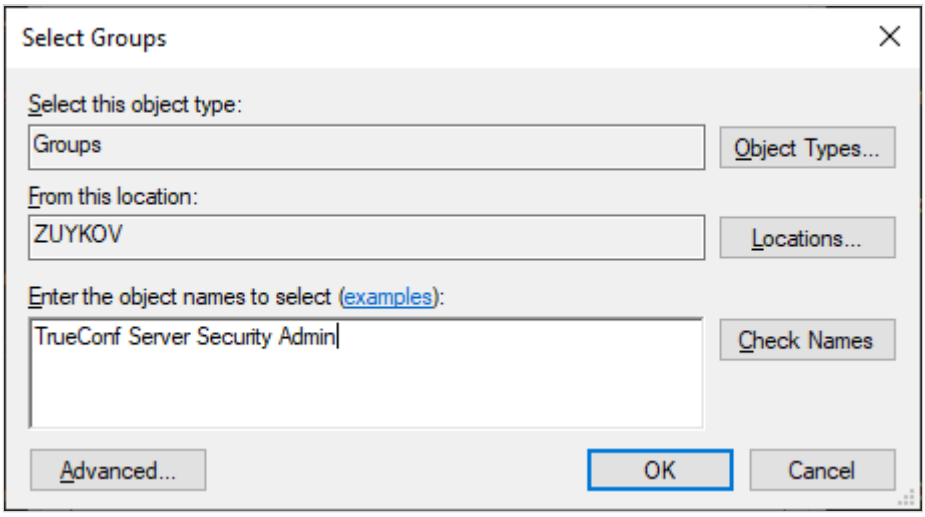
To create a new local Windows account with necessary rights:

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.

22.2. 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:

```sh
adduser --ingroup tcsecadmins [new_admin]
```

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.

22.3. 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.

```sh
usermod -aG tcsecadmins [user]
```

On Linux, one can view the list of user's groups or check if the user is actually available by running a single command:

```sh
groups [user]
```

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.

22.4. 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**.

22.5. 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.

22.6. 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.

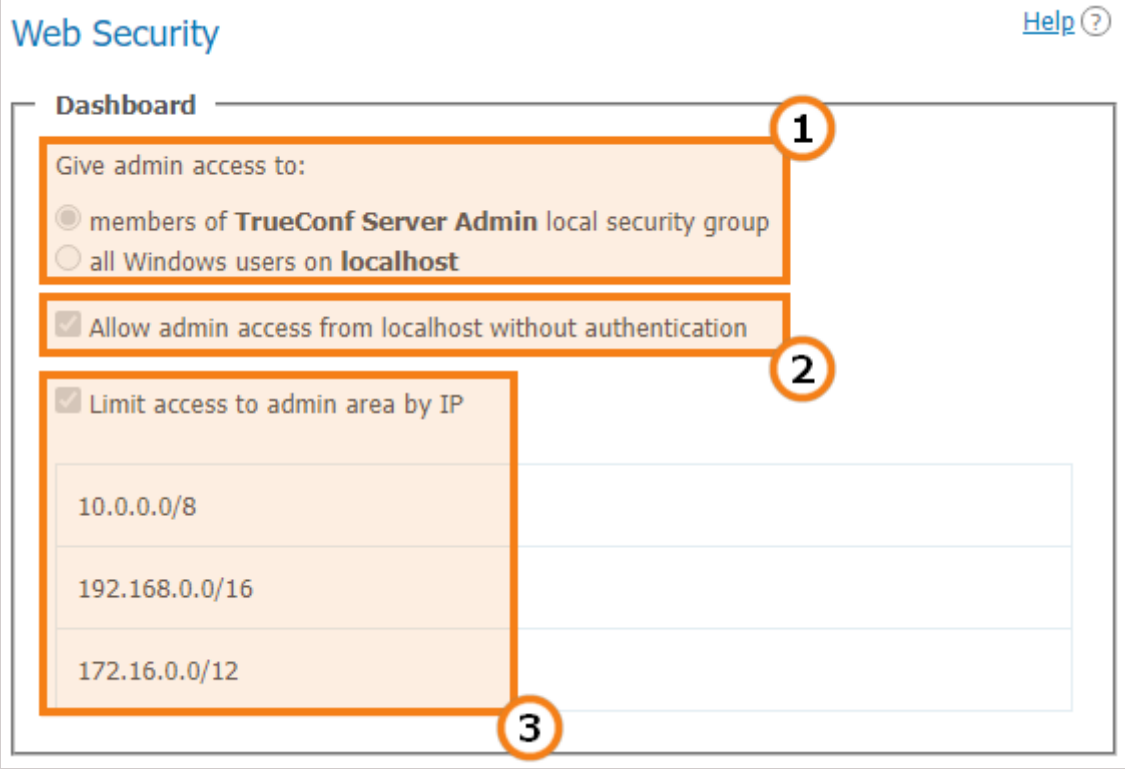
22.7. Server log

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.

22.8. Access settings

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



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.

i Security Admins are not allowed to change the settings described above; only TrueConf Server admins with full access rights can manage these settings.

22.9. 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.

22.9.1. 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.

22.9.2. 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.

22.9.3. Chat Messages

The **Chat Messages** section displays the history of all messages between TrueConf Server users, including group chat history.

22.9.4. 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.

22.9.5. 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.

22.9.6. 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.