About this document

This document is part of TrueConf Server video conferencing system documentation package and contains instructions on installation, setting up and use of the system's server part.

For effective work with the document basic level of IT and network literacy is required.

Contact Information

Telephone: +1 (347) 878-32-63
General inquiries: info@trueconf.com
Sales inquiries: sales@trueconf.com
Support inquiries: support@trueconf.com
# Table of Contents

1. **Server side**
   1.1. System requirements for TrueConf Server
   1.2. Installation
   1.3. Registration
   1.4. Offline registration
   1.5. Administering the server
   1.6. Changing the registration key
   1.7. Server status
   1.8. Server log
   1.9. Configuring preferences

2. **Client side**
   2.1. Where can I find client applications?
   2.2. Platforms supported by TrueConf client apps
   2.3. Client application features
   2.4. How to connect client app to your server
       2.4.1. Manual setup of the client app
       2.4.2. Connection using auto discovering
   2.5. How to update client apps?
   2.6. Call string formats
       2.6.1. Call string format for TrueConf Server users
       2.6.2. Call string format for TrueConf conferences
       2.6.3. Call string format for calling SIP endpoints
       2.6.4. Call string format for calling H.323 endpoints
       2.6.5. Call string format for calling RTSP endpoints

3. **Configuring server**
   3.1. "Dashboard" group of settings
       3.1.1. Summary
       3.1.2. Settings
   3.2. Network
       3.2.1. Network settings
       3.2.2. SMTP
       3.2.3. SIP gateway
           3.2.3.1. Invitation of the SIP terminal to the conference that is held on the TrueConf Server
           3.2.3.2. Connecting SIP endpoint to the conference via CID (conference ID)
       3.2.4. H.323 gateway
           3.2.4.1. How to call TrueConf users and conferences from H.323 devices
           3.2.4.2. How to register H.323 devices on TrueConf Server
           3.2.4.3. How can an H.323 endpoint user make a call to a TrueConf user?
       3.2.5. Federation
   3.3. "Web" group of settings
       3.3.1. Settings
       3.3.2. Web security
       3.3.3. HTTPS
   3.4. "Users" group of settings
       3.4.1. User accounts
           3.4.1.1. User accounts
           3.4.1.2. User profile
       3.4.2. Groups
           3.4.2.1. Editing group list
           3.4.2.2. Setting up address book for users of the group
3.4.2.3. Setting application settings for group users
3.4.3. Aliases
3.4.4. LDAP / Active Directory
   3.4.4.1. Registry mode
   3.4.4.2. LDAP mode
3.5. "Group conferences" group of section
   3.5.1. Conference list
      3.5.1.1. Creating video conference
      3.5.1.2. "General" tab
      3.5.1.3. "Participants" tab
      3.5.1.4. "Additional" tab
   3.5.2. Templates
   3.5.3. Streaming
3.6. API
   3.6.1. OAuth2
3.7. Reports
   3.7.1. Events
   3.7.2. Call history
      3.7.2.1. Call list
      3.7.2.2. Call or conference information
      3.7.2.3. Connection properties
   3.7.3. Chat messages
   3.7.4. Configuration changes
   3.7.5. Conference recordings
   3.7.6. Endpoints
      3.7.6.1. Events that update device information
3.8. File storage
3.9. Recordings
3.10. Manage add-ons
   3.10.1. TrueConf Directory
- 1. Server side

TrueConf Server consists of two components:
- TrueConf Server system services
- TrueConf Server control panel

**TrueConf Server system services**

This component is a video conferencing server itself. It gets installed as Windows operating system service and provides:
- Endpoints authentication and authorization
- Support for multi-point video conferences and point-to-point video calls
- Events logging (calls history, usage statistics and chat messages)
- Traverse NAT and proxy servers to connect endpoints
- Scalable video coding (SVC) manipulations to media streams
- Transcoding for third-party protocols and systems (SIP, H.323, RTSP, WebRTC and Skype for Business)
- Communication with remote federated servers

**Control panel TrueConf Server**

This component is used to control and manage TrueConf Server and provides:
- Interface to manage all settings described in this document
- Server state monitoring, start and stop controls
- Access to usage reports and recordings
- Users and groups management
- Conferences scheduling
- API access and more

### 1.1. System requirements for TrueConf Server

<table>
<thead>
<tr>
<th></th>
<th>Recommended configuration</th>
<th>Advanced configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Intel Core i5-2320 @ 3.00GHz&lt;br&gt;Intel Xeon E3-1220 @ 3.10GHz</td>
<td>Intel Core i7-3770 @ 3.40GHz+&lt;br&gt;Intel Xeon E5-1620 v3 @ 3.50GHz+</td>
</tr>
<tr>
<td>50 WebRTC users</td>
<td>50 WebRTC users&lt;br&gt;Recording a conference on server&lt;br&gt;100 SIP/H.323 non-transmitting connections or up to 1 conference with SIP/H.323 and with 3</td>
<td>50 WebRTC users&lt;br&gt;Recording a conference on server&lt;br&gt;RTSP/CDN Streaming&lt;br&gt;100 SIP/H.323 non-transmitting connections or up to 1 conference with SIP/H.323 and 8 broadcasting</td>
</tr>
</tbody>
</table>
1.2. 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 supported platforms are available on the TrueConf web-site. Run the installation package once downloaded to begin the installation. The installation process will take a couple of minutes.

During the installation you can specify:

- TCP port for accessing control panel over HTTP
- TCP port for server’s reports files database
- Installation directory

**Note:** The ports are selected during the installation and cannot be changed afterwards. To change them, you will need to reinstall TrueConf Server. By default the control panel is given port 80 or port 8080 if port 80 is not available. If both ports are unavailable you will be prompted to specify a different port number. You can later switch control panel to use HTTPS. If control panel port is not 80 (HTTP) or 443 (HTTPS), you have to specify the port number manually in URL to access the control panel (e.g. http://localhost:8080).
Can I install TrueConf Server on a PC with a web server already installed?

Yes. The installer will either auto-select available port, or give you the option to assign the port manually.

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

**Note:** If you are installing TrueConf Server 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.

Is it possible to change TrueConf Server control panel port number without having to re-install the server?

Yes. To do this, go to the server installation directory (by default C:\Program Files (x86)\TrueConf Server). Open httpconf\conf\listen.conf file there with a text editing app of your choice and change the port number in line containing "Listen <port number>" and save changes. Please restart the machine to apply changes.

1.3. Registration process

After the installation of your web browser will automatically start server setup interface. Register the server. To activate the server you have to get a registration key. Click on **Get FREE Key** to obtain one:
Click to open a page with application to TrueConf Server Free. Carefully fill all the fields and click on Submit & Download:

A registration key will be sent to the email address that you provided:
Note: The key should be delivered in 15 minutes maximum. If this did not happen, request a key via live chat, or check the SPAM folder in your email client.

Return to the page of TrueConf Server settings and enter the registration key you have just received by e-mail. Press Register to continue:

Once the server has been successfully registered, you will see "running, registered" at the top-right corner of the control panel window.
1.4. Offline registration

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 https://trueconf.com/server/trial/ and follow the instruction from the Registration section.

When you receive an email with the registration key you need to put it in the appropriate field “Registration key” in the control panel on a computer without internet connection and click Registration.

In the registration window a new button will appear, Create registration file. Clicking on it will generate a file that you will need to send:
The generated file **offlinereg.vrg** will be saved in the browser's default 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.

Click on **Select file** on your computer and select the file **offline.reg**. Then click **Continue**:

If registration has been successful control panel page opens to notify you that the server has been registered.

### 1.5. Administering the server

By default 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.* and 127.*. If the administrator wants to administer the server from a remote machine, he/she needs to make sure that the firewall allows incoming connections over TCP port chosen for control panel (80 by default).

To gain remote access, log in using your Windows account information from one of the following groups:
- **TrueConf Server Admin** — to administrate the server
- **TrueConf Server Security Admin** — to view logs and conference recordings

When the server is installed, the user’s current account is added to the first group. To make the control panel accessible to another user, the administrator should add this user’s account to one of the groups.
If Allow admin access from localhost without authentication option is checked in the Web > Security section, the control panel can be accessed directly without authorization from the machine where the server was installed via localhost or 127.0.0.1 host in any browser.

How to administer the TrueConf Server outside of LAN ->
How to connect external users ->

1.6. Changing the registration key

You can change the registration key by going to Dashboard > Summary and clicking Registration button.

Enter a new key and click Registration:

What you should do if you get the message "Computer change is not available for this server code"?
This means that your key is "bound" to the hardware on the machine where the server was installed.
To disable this bond please contact our support:
Telephone: sales@trueconf.com

If you get the message The registered server doesn't have valid licenses. Please contact technical support to do it manually upon entering the key, it means either that the key has expired or the time and date on your PC have busted. Make sure time and date on your PC are correct.

1.7. 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?

In this case the red massage Stopped will be displayed in the Server status line.

Possible reason #1: You have no valid licenses, or the license is expired.
Workaround: contact us or your reseller.
Possible reason #2: Some server files are missing or have been damaged.  
Workaround: reinstall TrueConf Server.

Possible reason #3: The hardware key is invalid.  
Workaround: check the manual to fix the hardware key.

1.8. Server log

If you encounter any issues with TrueConf Server, our support team will be able to help you troubleshoot them more efficiently if you provide server log files. To access the 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 start collect more details in server's log. Our technical support staff may ask you do this to ease troubleshooting process.

You can download the full log by clicking on the save button above the log:

1.9. Configuring preferences

There are preferences individual for every authenticated administrator, such as control panel interface language and time zone. You can access these settings in System > Preferences section.

There is also an Export to CSV section in the preferences which affects server's log export format. Default settings are most commonly used for .csv files, however you can select custom encoding and
field separator character.

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

1. Shortcut for **Preferences** section
2. Interface preference
3. Reports file export preferences
2. Client side

To be able to use video conferencing service provided by TrueConf Server the user must have a client application installed.

2.1. Where can I find client applications?

Just send out a link to the guest page to your users. Guest page allows users to download client applications for all supported platforms along with instructions on how to connect them to your server.

The guest page is available at: \text{http[s]}://<\text{server}>[:<\text{port}>]/guest/ where:

- \text{<server>} — address of the PC with TrueConf Server installed
- \text{<port>} — port used to access the control panel (optional)

2.2. Platforms supported by TrueConf client applications

The following platforms are natively supported. Please open a guest page to obtain a version for your operating system. Please note that WebRTC application is only available for users who access conference using a browser via conference invitation URL.

- Windows
- macOS
- Linux
- Android
- Android TV
- iOS
- watchOS
- WebRTC

2.3. Client applications features

Once installed on a PC or Mac, desktop application allow users to perform the following actions.
• Authorize and maintain connection through NAT and proxy to TrueConf Server
• Browse address book, groups and users
• Set personal preferences
• Make calls, create or join conferences
• Collaborate and vote during conferences
• Share desktop or application window
• Select video layouts
• Exchange files and text messages with other users.
• View chat and call history
• Select peripherals, such as mic or camera
• Enable echo cancellation, noise reduction and automatic gain control

The full list of features is much larger. Please follow our blog to be updated. Mobile application capabilities are fewer compared to desktop application, please refer to marketplaces descriptions for more details.

2.4. How to connect client application to TrueConf Server?

There are network settings in every client application where you can specify address and port of TrueConf Server instance you want this endpoint to connect to. You can either do it manually or let the client application locate TrueConf Server automatically via DNS. Once connected to the server user will be prompted to authenticate on this server using username and password.

2.4.1. Manual setup of the client app

To configure server connection manually, a user should go to the network settings menu and enter the server address and the connection port by hand, either when running the application for the first time or later. Detailed instructions for connecting each application to the server can be found on the guest page.

2.4.2. TrueConf Server auto discovering

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 list 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:
• Navigate to root of the desired domain.
• Choose «Other New Records…» in a right-click menu.
• Choose type «Service Location».
• Set the following parameters.
In this example server has address videoserver.your.domain.com and port 4307. Please make sure that protocol name (tcp) does not contain underscores.

2.5. How to update client apps?

Desktop application for Windows is bundled with TrueConf Server installation package and updated automatically when a new version of the server is released. To update other TrueConf applications you need to manually download the new version from our web site or get the updates from corresponding marketplace for Android/Android TV/iOS/macOS platforms.

2.6. Call string formats

TrueConf Server not only enables users to call each other or participate in group conferences, but also make possible to reach any SIP, H.323 or RTSP endpoint using built-in gateway. For each type of supported third-party protocols there is a specific call string format to be used.

Call string are very powerful and can be used in many different places:

- Pasted in search bar in the client applications
- Saved as a new contact in the address book
- Included into invitations list during conference scheduling
- Addressed via TrueConf Server API requests
- And much more

2.6.1. Call string format for TrueConf Server users

To call a regular user, just enter the user’s ID in the call-to field. You can also call remote users of federated TrueConf Server instance. To do so use the following call string format:

```
<TrueConf_ID>@<server>
```

where:
- `<server>` is an IP address or domain name of a remote TrueConf Server,
2.6.2. Call string format for TrueConf conferences

You can connect to a conference using the following call string: \c\<CID>@<server> where:
- \<CID> is the ID of a TrueConf conference,
- <server> is the IP address or the domain name of the server hosting the conference.

2.6.3. Call string format for calling SIP endpoints

One of the following formats can be used to address SIP endpoint:
- #sip:<user_id>@<server_name>, where:
  - <server_name> is a host name or IPv4 address of the SIP server,
  - <user_id> is the SIP user’s name.
- #sip:<user_id>@[<server_name>], where:
  - <server_name> is IPv6 address of the SIP server (please note that brackets are the part of the call string),
  - <user_id> is the SIP user’s name.
- #sip:<user_id>, where:
  - <user_id> is the SIP user’s name.
  
  **Note:** the call will be directed to the server that had been configured as Default SIP Proxy server by ticking a corresponding box (in the Network > SIP Gateway tab).
- #tel:<user_id>, where:
  - <user_id> is the SIP user’s name.
  
  **Note:** the call will be directed to the server that had been configured as Default VoIP server by ticking a corresponding box (in the Network > SIP Gateway tab).
  
  **Note:** #tel:<number> call string can be used to call regular phone numbers.
- #sip:@<endpoint_ip>, where:
  - <endpoint_ip> is IPv4 address of the SIP endpoint.
- #sip:@[<endpoint_ip>], where:
  - <endpoint_ip> is IPv6 address of the SIP endpoint.
- #sip:@<host_name>, where:
  - <host_name> is DNS name of the SIP endpoint.

Call string examples for SIP protocol:
#sip:james78@sip.company.com
#sip:james78
#sip:8001
#sip:@192.168.1.99
#sip:@[fe80::805a:1cf9:12f9:def7]
#tel:501
#tel:13478783263

2.6.4. Call string format for calling H.323 endpoints

The following call string formats can be used for calling an H.323 endpoint:
- #h323:@<IP>, where:
- `<IP>` is IP address of the H.323 endpoint.
- `#h323:@[<IP>]`, where:
  - `<IP>` is IPv6 address of the H.323 endpoint.
- `#h323:<user_id>@<IP>`, where:
  - `<IP>` is IP address of the H.323 gatekeeper or MCU,
  - `<user_id>` is ID of endpoint registered on the H.323 device.
- `#h323:<user_id>@[<IP>]`, where:
  - `<IP>` is IPv6 address of the H.323 gatekeeper or MCU,
  - `<user_id>` is ID of endpoint registered on the H.323 device.
- `#h323:\e<e164_id>@<IP>`, where:
  - `<IP>` is IP address of the H.323 gatekeeper or MCU,
  - `<e164_id>` is number in E.164 format of the endpoint registered on the H.323 device.

The following call string formats can only be used if there is H.323 rule with a role **Default H.323 gatekeeper** enabled for it:
- `#h323:<user_id>`, where
  - `<user_id>` is ID of the H.323 endpoint.
- `#h323:\e<e164_id>`, where
  - `<e164_id>` is the number of H.323 endpoint in E.164 format.

Call string examples for H.323 protocol:
- `#h323:@192.168.1.99`
- `#h323:hdx8000@192.168.1.99`
- `#h323:@[fe80::805a:1cf9:12f9:def7]`
- `#h323:james78`
- `#h323:\e8001`

### 2.6.5. Call string format for calling RTSP endpoints

To display a video from RTSP stream you need call it or invite into the conference using the following call string format `#rtsp:<address>`, where the `<address>` can be an HTTP, HTTPS, RTSP or an IP address of the stream (e.g. `#rtsp://192.168.1.99/axis-media/media.amp`).
- 3. Configuring server

3.1. "Dashboard" group of settings

3.1.1. Summary

Dashboard contains details about the license activated for this server, license’s owner contacts and features available for this server. You can also re-register the server from this page to obtain a new license.

![Dashboard summary](image)

**Note:** If you're using a free version of TrueConf Server and connection to our registration server (host is `reg.trueconf.com` and TCP port is 4310) is lost, your server will shut down in 12 hours. The expected shut down time will be displayed in the Summary tab. Full version of TrueConf Server doesn't have such limitation.

If the server is connected to the Internet, administrator from time to time will receive notifications in control panel about available TrueConf Server updates. A message with a link to a new version download will be displayed on top of this page.

3.1.2. Settings

This section allows to change a working directory for TrueConf Server and apply some other server wide settings. Please refer to a list below for more details. Working directory is used to store all log files and reports. Reports are stored in PostgreSQL database format.
1. A path to a working directory of TrueConf Server.
2. Enable extensive logging of server activities. Might be required by our technical support team for troubleshooting.
3. Create a backup file with server settings.
4. Restore your settings using a backup file.
5. Download links for client applications, which are published for your users on the guest page. We strongly advise you not to use the following settings, unless being told so by our tech. support team, as they might significantly decrease the quality of video conferences or put TrueConf Server security at risk. The ability of TrueConf Server to automatically and dynamically manage video streams encoding parameters is crucial for effective collaboration.
6. Special key used to sign authentication request from client authentication, eg. allows to sign in under some server's user credentials without password verification.
7. A key similar to the previous one and used to sign in using guest accounts.
8. Hard limit the output bitrate from client applications to TrueConf Server and other endpoints (in kbps).
9. Hard limit the maximum FPS rate transmitted from client applications to TrueConf Server and other endpoints.
10. Set exact video resolution client applications will use to capture and encode a video source.
11. Enable additional in-conference statuses for participants, eg. polling.
12. Save application settings.

Configuration back-up and restore

Backup allows you to export and save most of the server settings excluding HTTPS settings, log files and usage reports. Backup file is essential for TrueConf Server migration and re-installation tasks. You can find the full guide on making a backup copy of and restoring the settings after a server transfer on our website, in our Knowledge Base.

Applications update settings

You can use this settings to show notifications about new client application version availability to your users or to force the client applications to upgrade to the version you need. Click on the application name to open it's update settings.

**Note:** we don't allow to manage mobile applications update policies (for Android, Android TV and iOS) using these settings, please ask your users to stay up to date by installing new updates from Google Play and App Store correspondingly.

![Settings TrueConf Client](image)

1. Minimal version of the client application TrueConf Server will allow to connect from. If the user's version of the app is older than the one specified here, the app will pop up an update dialog with Setup URL linked to a new version. Close of this dialog will exit the application.
2. Current supported version of the client app. 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. Just a string used to label a new version in update dialogs.

3.2. Network

This section covers TrueConf Server settings for connectivity with other TrueConf Server instances, TrueConf client applications, third-party SIP or H.323 endpoints and email templates for notifications.
3.2.1. Network settings

Settings on this page are used by TrueConf client applications only.

Please note that our client applications communicate with TrueConf Server over 4307 TCP port. This single port is used for signalling, presence statuses, authentication, audio and video streams transmitting and messaging. During slide shows, files transfer and API calls HTTP or HTTPS port specified in Web / Settings / External address is also used. No UDP ports or other TCP ports are used for communication between TrueConf Server and our client applications.

The list of Internal addresses (and ports) are used by TrueConf Server to listen for incoming connections from TrueConf client applications. When "Listen on all IP addresses" checkbox is enabled (which is so by default) you can see the list of all IP addresses available for this machine in a list.

External addresses are used to help TrueConf client applications to find and connect to the server from outside the local network. TrueConf Server doesn't listen for incoming connections from these addresses as they are only used by client applications, eg. to reach external IP address of your NAT or address TrueConf Server by DNS name. After every successful connection to the server client applications automatically obtain and save the list of external addresses available for this server. If the list of external addresses is empty the internal addresses will be stored instead.

Note: we don't cover topics about TCP port forwarding or DNS names resolving in this manual please refer to your network equipment documentation.

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 list of external address beforehand. This will help client apps to store the new address right after the next connection to the server in advance. Once the server is switched to the new address, client apps will automatically connect to it too.

Network Settings

1. To specify an external addresses you have to enable Specify checkbox.
2. To change a list of internal addresses, uncheck "Listen on all IP addresses" checkbox.
3. To add a new internal or external IP address. Use the button Add and enter the necessary data in the Host and Port fields.
4. Return to previous settings.
5. Click to save the changes.

3.2.2. SMTP

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

In case of a missed call TrueConf Server will try to locate user's email address from E-mail field in Account information or corresponding field imported during LDAP synchronization. In case of recurrent conference scheduling, the invited users will receive invitation for the first event in a row only. In case the conference has been set up without start date and time, the invited users will receive a notification email without calendar invitation. If invited participant is offline when conference starts a notification about the conference he or she is expected to be in will be send. In case of a regular conference scheduling, all invited participants will receive an email with calendar invitation for date and time specified.
1. IP address or SMTP server host name.
2. Port used by SMTP server.
3. Select connection security method (STARTTLS, SSL or without encoding).
4. Select authorization type (with or without password).
5. If you have selected password authorization please specify a username used on the remote SMTP server for connections from TrueConf Server.
6. And it's password.
7. All emails will be delivered using this From: field address.
8. Shows SMTP server connection status: Successfully connected in case of successful
connection and authorization on external SMTP server and *invalid server* if the connection can not be established.

9. Update connection status.

10. Email address of TrueConf Server administrator. Enable the checkbox below if you'd like to receive notifications about unexpected TrueConf Server restart events.

11. Enables missed call notifications for users.

12. Restore all email templates to defaults.

13. Template of a missed call email send to registered users.

14. Template of a missed call email send to unregistered users, eg. if someone will try to call an email address from TrueConf client applications, the owner of this address will receive an invitation to register on this server.

15. Enables calendar invitations for invited group conferences participants.

16. Template of the invitation email.

17. Click here to save changes.

### 3.2.2.1. The list of substitutions used in email templates

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

- For notifying users about missed calls:
  - `%caller_display_name` — display name of the caller.
  - `%recipient_display_name` — display name of the caller (user who missed the call).
  - `%caller_call_id` — ID of the user who made the call. (eg. *user@server.trueconf.name*).
  - `%missed_call_time` — time and date of the call.

- For inviting to a conference:
  - `%conf_name` — name of the conference.
  - `%conf_id` — ID of the conference, eg. `\c\CID`.
  - `%user_display_name` — display name of the user who invited to the conference.
  - `%owner_name` — display name of the conference owner.
  - `%start_time` — time and date of the conference. Time is provided for UTC+00:00 time zone, be aware of your time zone difference
  - `%host` — TrueConf Server external web address.
  - `http[s]://host/c/%conf_id` — link to join the conference from PC, macOS devices, mobiles, SIP/H.323 endpoints and browsers, eg. `https://server.trueconf.name/c/CID`.

Server administrator contacts parameters:

- `%admin_name`
- `%admin_email`
- `%admin_phone`

### 3.2.3. SIP gateway

TrueConf Server has built-in gateway for SIP, H.323, and RTSP protocols interoperability. This section helps to configure TrueConf Server built-in SIP gateway parameters. Please note that TrueConf Server Free version supports only one active connection via gateway, while the number of rules created using these settings is unlimited. Calling up devices via SIP gateway requires specific *call string formats*. 
Network settings

This table contains address gateway used to listen for incoming SIP 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.

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 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 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 pre-selected, e.g. port, protocol, used video codec and registration mode.

New rule form
Name field is only displayed in the table for rules. Host and Port fields are more important and also mandatory. They are required to determine call direction applied to this rule. Please note that it isn't possible to set different rules for one host but different ports.

The following block of fields are designed to authorize on a SIP device for which the rule is created. If Authorization name is identical to login, you may leave this field blank. With International call prefix you can replace "+" symbol which is used in phone numbers with other value, e.g. "810". If you leave this field blank, "+" symbol will not be replaced in phone numbers your users call to.

Registration mode defines registration method for the rule:
- Off. REGISTER request is not sent, registration or authorization on 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.
- Off. REGISTER request is not sent, registration or authorization on 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.

Please note that each active gateway connection reserves one SIP/H.323 connection slot from your server's license.
Enable ICE support (Interactive Connectivity Establishment) checkbox makes TrueConf Server gateway available behind NAT.

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

Enable content sharing over 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.

Enable far end camera control checkbox enables support for far end camera control of SIP endpoints via FECC, H.224 and H.281 protocols from TrueConf client applications.

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, e.g. Lifesize endpoints. For more details please contact our technical support team.

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

- **Default SIP Proxy**. This role allows users to avoid to enter full SIP URI for calls with #sip: prefix. For example, all calls in the #sip:Endpoint@Host 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 used to treat SIP endpoint as a VoIP service or PBX. All calls made from dialers built-in into TrueConf client applications, as well as the calls dialed with #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 Default SIP Proxy or Default VoIP server roles can not be applied for multiple SIP connection rules.

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.

- Create a new account on Skype for Business server for TrueConf Server gateway.
- 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.
- Enter Skype for Business server IP address or domain name in the Host field.
- Check Default SIP Proxy checkbox.
- Save the rule and check if the connection status has changed to successful in the table for rules.

To call Skype for Business users from TrueConf client applications, use the following format: #sip:User, where User is Skype for Business username. This user will receive an incoming call from the step 1 TrueConf Server account created during step 1. 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 (on step 1): /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 call Skype for Business user and connect him/her to a TrueConf user or a conference. If you try to call this user directly, the call will be rejected and you will receive a help message with a list of available commands in chat. However, if default call destination is set in global SIP settings, you will be connected to this default destination address.

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

Global SIP settings section

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

- **SIP From domain.** It is used to generate a SIP URI for outgoing calls in the following format user@server, where server is the entered value and user stands for the user ID who initiated the call. It is usually displayed as caller address on SIP devices.
- **Default call destination.** Use this field to enter user ID or conference ID (CID) which will receive all incoming calls over SIP protocol where specific user wasn’t specified in SIP URI.
- **Reduce SIP messages size.** Use this option to reduce SIP messages size and avoid possible issues related to its maximum size (MTU).

### 3.2.3.1. Invitation of the SIP endpoint to the conference

There are multiple ways of inviting a SIP endpoint into a conference: conference owner can call a SIP endpoint using a specifically formatted call strings from TrueConf client application or administrator can do it from server’s control panel.

To add a 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.
3.2.3.2. Connecting SIP endpoint to the conference via CID (conference ID)

Proceed to Group conferences list and create a group conference. Take note of your Conference ID or CID (e.g., `c\e22a39ba2a`).

To connect to the conference from the endpoint registered on TrueConf Server, enter CID into the endpoint address string. Please note that you need to replace `\` in CID with 00 (two zeroes). In our case, you need to call 00e22a39ba2a.

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

- CID@<Server>, where CID is a conference ID with two leading zeroes and <Server> is an IP address of TrueConf Server gateway e.g., 00e22a39ba2a@192.168.1.99.
- CID@<Server>:<Port>;transport=<Protocol>. You can indicate non-standard port for SIP connection and choose a protocol (TCP or UDP) e.g., 00e22a39ba2a@192.168.1.99;5061;transport=TCP.

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

3.2.4. 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.

**Note:** TrueConf Server Free gateway supports only one connection for H.323/SIP endpoints.
H.323 interoperability is generally used to call legacy video conferencing endpoints. TrueConf Server gateway also provides integration with MCUs, H.323 gatekeepers and PBXs, which might be useful for addressing endpoints registered on these devices via H323-ID or E.164 names instead of direct IP address calls. Calling up H.323 devices from TrueConf applications is simple using call string formats.

**Network settings**

This table contains address gateway used to listen for incoming SIP 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.

**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. Each rule 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 Configuration button.

**New rule form**
Name field value is used only to distinguish one rule from another. Host and Port fields are more important and 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.

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 enable registration support using the corresponding drop-down menu.

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.

Please note that every active gateway connection reserves one SIP/H.323 connection from your 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 over 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.
Enable far end camera control 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.

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 used to take H.323 device as telephony service or PBX. All calls made from dialers built-in into TrueConf client applications, as well as the calls dialed with #tel: prefix will be automatically forwarded to this H.323 device. 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 Default H.323 gatekeeper or Default VoIP server roles can't be applied for multiples SIP connection rules.

Global H.323 settings

Most of the settings in this section are identical to the settings described above. However, they automatically apply for all H.323 connections for which there are no rules. Use Default call destination field to enter TrueConf user ID or conference ID (CID) which will receive all incoming calls over H.323 protocol in cases where destination user ID wasn't specified.

3.2.4.1. 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

©2019 TrueConf. All rights reserved.
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.
- **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.

For TrueConf Server versions older than 4.3.9 the following notation is used:

- **\c\CID@Server**, where *CID* is ID of the conference on TrueConf Server and *Server* is TrueConf Server IP address.
- **\\c\\CID@Server**, some endpoints require to escape back slashes in a call string.

### 3.2.4.2. How to register H.323 devices on TrueConf Server?

TrueConf Server can act as a H.323 gatekeeper or MCU for third-party H.323 devices and simplify their addressing. From the TrueConf user perspective an H.323 device registered on TrueConf 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 Server user ID equal 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 H.323 gatekeeper or MCU address and use username and password of any TrueConf Server account to authenticate.

### 3.2.4.3. How can an H.323 endpoint user make a call to a TrueConf user?

Registering H.323 devices on TrueConf Server is similar to the registration of other endpoints available on the market. At first, enter TrueConf Server address as the address of an H.323 gatekeeper or an MCU. After that provide the username and password of a TrueConf Server user account on whose behalf the device will make calls.

### 3.2.5. Federation

Federation allows TrueConf Server users to call and invite to conferences remote users of other TrueConf Server instances. Federation is available only in full version of TrueConf Server (e.g. - for every paid license). The number of servers involved in federation is unlimited. Group video conferences will be conducted with regard to the license limitations of the server initiating the connection.

The only requirement for federation to work between any two given TrueConf Server instances is that they shouldn’t blacklist each other or otherwise they have to be whitelisted for each other. Administrator can either disable federation on the server or select between blacklist and whitelist federation security approaches.

For example, by adding a `trueconf.com` Server Name to a whitelist you’ll allow all your users to call and
receive calls from cloud service users, whose IDs are written as follows ID@trueconf.com. Or by blacklisting videoserver.company.com Server Name you will disable federation for all remote users whose IDs are anything@videoserver.company.com.

**Note:** The server should be available to other servers by its FQDN Server Name indicated during registration. The server name can be registered for the existing DNS name, as well as be specified with the help of the SRV DNS records. Please refer for more details to Connection using auto discovering topic.

1. Allow connections from all servers except blacklisted ones.
2. Federation is disabled.
3. Allow connections with whitelisted servers only.
4. Click to add a remote server to the blacklist.
5. Click to add a remote server to the whitelist.
6. Click to save changes.

### 3.3. "Web" group of settings

This tab contains settings of external web pages that are available to unregistered users.

#### 3.3.1. Settings section
1. TrueConf Server address used to build guest page links and scheduled web conference links.
2. A link to the guest page which contains instructions on how to connect new users to TrueConf Server.
3. Server administrator contact details which are published on the guest page and web conference pages.
4. Links to client application for Windows and macOS which are displayed on the guest page.
5. Custom logo upload form for the guest page.

3.3.2. Web security
1. Select Windows users who will have administrative access.
   By default, members of the local administrators group have the ability to manage the server.

2. Accessing and managing the server from the IP addresses specified below does not require user authorization. Disabling this option will make authorization mandatory for all users.
   **Attention!** Before checking this box make sure you have a user on this computer that is in the security group - **TrueConf Server Admin**. Otherwise after applying the changes you will neither be able to authorize yourself nor enter the control panel. If that happened reinstall the server or contact our support team.

3. Check this box to limit access to your server to the IP addresses specified on the list.

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 – 4 octets in decimal representation without initial noughts from 0 to 255, separated by dots, eg. 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. The security key provides permanent access to your server’s API until the security key is changed. Hence we recommend using the secret key only for testing API, and using OAuth2 for regular work with it.

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.

### 3.3.3. HTTPS

In this control panel section you can configure the safety data transfer parameters between your browser and the TrueConf Server.
1. Select one of the three operating modes:
   - **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. Click here to go to the full user guide in our blog.

3. Set TCP port, which will for operating via HTTPS (use numbers) protocol. Port 443 is set by default.

4. Specify which protocol versions are supported by your server (select at least one version).

5. Click this button to verify the HTTPS configuration data without restarting the web server. This action does not change the configuration file of the Apache web server.

6. Click this button to save a web server configuration file and restart the server. Upon clicking on this button a dialogue box will appear, notifying the user that this action will lead to a reboot of the server. TrueConf and Apache reboot processes start up simultaneously because TrueConf Server uses the same certificate to run WebSockets WSS secure channel.

7. Generate a new certificate. The "Self-Signed Certificate" section will appear as shown on the picture only if this certificate type has not been issued before. If the certificate was issued before, this section will contain the main parameters of the root certificate and certificate which was used...
by the web server and the TrueConf Server (see Self-Signed Certificate section).

8. Select the appropriate certificate and key files and click Upload. The Custom certificate section looks like this only if this certificate type has not been issued before. If the certificate has already been downloaded, this section will contain the main certificate data (see Custom certificate segment below).

The existence of safe connection channel between browser and server is essential for in-browser media capture using WebRTC technology for Google Chrome (starting from version 47).

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. Press Test configuration for your server to check if your HTTPS port is available.

Self-signed and custom certificates

There are two certificate types available for use in TrueConf Server. If you are using a trusted certificate, no additional actions is 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 TrueConf Server 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.

However, self-signed certificates have their own peculiarities. For example, the root certificate installation process differs in Chrome and Firefox browsers.

Self-signed certificate
To create a new self-signed certificate for TrueConf Server, press Create 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.

**Custom certificate**

If the certificate has already been downloaded, this section will contain the basic parameters of the certificate.

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.

### 3.4. "Users" group of settings

#### 3.4.1. User accounts

#### 3.4.1.1. User accounts
In the User accounts section you can add and manage users.

The maximum number of accounts in the free version of TrueConf Server Free is 12.

1. Add a user
2. Search for users
3. View user groups available on the server
4. The list of users registered on the server. User icons on the left of user names indicate their status: green means online, red means offline, yellow means that the user is currently in the conference, yellow star means that the user is the owner of the running conference. If you want to change user personal data, press their name. If you want to remove a user, click the trash can icon.

**Note:** In **LDAP mode** user edit is not possible, edit users using your LDAP directory tools.

The list of users in group mode will be shown as:
3.4.1.2. User profile

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

1. Switching user to active or inactive status. If the status is inactive, the user account still exists, but the user cannot log-in to his/her TrueConf client application.
2. Disconnecting user from the network. You may use this option to allow another user to connect to your TrueConf Server, when the maximum number of connections in your license has been reached.
3. A unique name is used to sign into the client application and make calls. The server name is indicated next to the username (@<server> near the input box) to call other server users. The username is set when the user account is created and cannot be modified later.

4. User password. You can change your password anytime.

5. The email address to which user notifications will be sent. Please refer to the SMTP configuration of the TrueConf Server.

6. The entered name will be displayed in the address book of other users. This field is prefilled as <ID>@<server>, where <ID> is the username entered in step 3, and is your server name. However, the field value can be changed.

7. User's personal details. These fields are not required.

8. Defines user group. Click the arrow to view existing groups on the server. To add a user to the group, check the field to the left of the group name.

9. User’s mobile, work or home phone number.

10. Save changes in user account. Remove user account. Go back to the previous page.

At the bottom of the page you can select additional settings that will be activated in client application when the user signs in. These settings define input and output bitrate limits.

If such settings have not been configured, user group settings (if configured) are applied to the user. User group settings are displayed next to the user settings field. They are displayed for preview only and cannot be changed.

User application settings take precedence over user group settings. If the user has smaller limitations as compared to user group limitations, only user limitations will be applied.

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 user addresses to the address book of the user being edited. Please note that you can add not only TrueConf Server user, but also SIP/H.323 or RTSP users to the address book.
1. Adding user to the list. Start entering user’s name and select an appropriate option in the drop-down list to add a user quickly.
2. The list of groups where the user belongs, address books of which are included to the user address book and cannot be removed.
3. Search for users.
4. User profile from the address book.

3.4.2. 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.

To add a new group, enter its name and press Create.

The newly created group will appear in the list of groups.

At the group level you can allow or forbid:
- 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 the group’s address book. If the box is not checked, group users will not be able to perform the actions mentioned above.
In this case, all changes are performed by administrator in TrueConf Server control panel and extend to all address books of the users from this group.

- Making point-to-point calls.
- Content sharing and slide show.
- Creating group conferences.
- Operator Rights. Operator right enables a group participant to become a moderator of any conference he or she joins.

These settings allow to give server users different rights.

### 3.4.2.1. Editing group list

Click on the group name to open the page "User accounts". On this page you can rename a group and add users to any group. To add a user to the group, press **Add user**:

![User Accounts](image)

Select the users you wish to add to the group. After you have selected the users they will be checked. When you are done, press **Save**.
All selected users will appear on the group page:

To rename the group being edited, press **Rename**. The following window opens:

In the field **Group** enter a new group name and press **Save** (or **Cancel** if want to exit the window).
3.4.2.2. Setting up address book for users of the group

Click Customize in the Address Book column to open edit menu of the common address book for all users of the current group. Group members can add new contact in the address book if they have corresponding rights. To grant such rights, Address Book Editing box should be checked in the main table. In the address book menu you can add groups of all the users belonging to any other group to the address book of the group (i.e. to the address book of every member of this group).

Users of a specific group can search for other server users and add them to their address book (if editing address book is allowed).

3.4.2.3. Setting application settings for group users

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

3.4.3. Aliases

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

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

**Aliases**

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. TrueConf ID of a user or a call string. The calls to aliases will be redirected to this TrueConf ID. One user may have several aliases.
3. Press the button to add a new alias to the list.
4. To delete an alias from the list, check the box on the left and press the button.

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

### 3.4.4. LDAP / Active Directory

Syncing server with LDAP is unavailable in TrueConf Server Free version.

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.
3.4.4.1. 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.

3.4.4.2. LDAP mode

In this mode the server operates information about the users from removed or local LDAP directory. 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.

In LDAP mode, user rights correspond to the Active Directory group where users belong. To activate this mode, check LDAP > Enable mode and press Settings LDAP button at the bottom. LDAP settings window will open.
1. Following this link you will enter the Help section. (LDAP tab description).
2. LDAP Server type.
3. Connection to the LDAP in the safe mode. Only in this case safe transmission of the user information through the network is ensured.
4. Automatic choice of the LDAP server.
6. In the automode 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.
7. LDAP server address and port.
8. Core LDAP context.
10. Authorization parameters on the LDAP server.
11. After choosing this option the users can automatically get authorized in the system by using the current Windows user account. The option is available only for the systems working on the basis of Microsoft Active Directory. For NTLM authentication work it’s necessary that the server on which TrueConf Server software is installed is located in the same AD domain with the users.
12. For Active Directory in this field it’s possible to indicate LDAP - group of users, who can get authorized on the TrueConf Server. To choose a LDAP-group using the Browse button you need to fill in the spaces for connection to the LDAP server (Server Settings and Authentication), including Base DN field.
13. Additional LDAP parameters. Allow to adjust the parameters to other types of LDAP-servers.
14. Back on page "User storage".

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".

**Note:** The users’ passwords are not imported. After being imported the users’ accounts are marked as «inactive» (see description in the «User accounts» tab).

Directory of groups and users registered on the video-conferencing 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) of the created group. You can edit his/her attributes in the Edit user information window. In the LDAP mode this window allows to define rights for several LDAP groups. User attribute can be defined in the LDAP folder.

**Note:** On the server the `<Not in group>` is created by default.

### 3.5. "Group conferences" group of settings

This section allows you to manage group conferences created via TrueConf Server control panel.

#### 3.5.1. Conference list

![Conference list](image)

1. Add a group conference.
2. See the conference ID
3. Press the link to open widget menu designed to integrate video conferencing into third-party websites and systems.
4. Manual conference launch. Prior to the conference start you can select the users to be invited to the conference immediately after it has been launched: all participants added during scheduling or only selected users.
5. Go to the conference page.
7. Remove selected conference.

#### 3.5.1.1. Creating video conference

Press **Create** button in the **Conference List** menu to select conference type:

- **Private**. Such conferences are available for authorized TrueConf Server users and third party SIP/H.323/RTSP devices (only if they have conference ID). Unauthorized guests cannot join private conferences.
Public. External users or guests can join public conferences, and in this case user account is not required. If your license does not include corresponding extension, Public conference button will be unavailable.

3.5.1.2. "General" tab
1. Set conference name (e.g. Marketing Meeting).
2. Select conference owner.
   While scheduling the conference, the administrator appoints conference owner (who automatically becomes conference moderator) and other moderators. Other roles can be set for the conference participants during the meeting.
3. Choose your conference mode: symmetric, asymmetric or role-based.
   Maximum number of participants in a role-based conference depends on your license type. The maximum number of participants is 250.
   TrueConf Server Free version allows up to 12 participants for any conference type for free.
4. Choose conference start mode: room (without schedule) and conference (scheduled).
5. Set one-time conference date, time, duration or recurring conference schedule.
6. Save conference settings as a template to create conferences with the same settings in one click.

3.5.1.3. "Participants" tab

This tab shows the number of participants added to the conference depending on the conference mode. Participants can be added to the conference from the user list, by ID or by email (for public conferences).
Adding by ID

Enter user ID or call string for SIP/H.323/RTSP devices to the search field in the Contacts tab, to make the user conference participant.

Adding Email for Sending Invitations
To invite a user to the conference, proceed to Email tab fill in Name and E-mail fields, and press Add.

How to Add 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.
3.5.1.4. "Additional" tab

Private conference

1. Press to set up conference recording (see "Recording" section).
2. Press to enable streaming.
3. Select the streaming preset (see "Streaming" section).
4. Turn on UDP Multicast mode. With this mode you can distribute network resources more efficiently as streams are transmitted bypassing the server conference participants. Audio and video streams are transmitted within UDP Multicast domain. These domains can be used in the local network or VPN. UDP Multicast mode is regulated by the license.
   In UDP Multicast mode, the following features are unavailable: connecting to the conference via third-party protocols (WebRTC, RTSP, SIP, H.323, etc), recording video sessions on the server, and streaming.
   This mode is recommended only for those users who have sufficient qualification as a network administrator. Please make sure that your network supports this technology beforehand.

5. Enter IP address multicast/broadcast. By default this field is filled in with 224.0.1.224:4000-6000 value.

6. Enable email invitations for conference participants.
   This option is available only if SMTP server integration is set up.

7. Conference description (e.g., speaker list, etc). This text will appear on the conference page.

Public conference

1. Set up conference ID to make it easier for the users to connect to the conference.
2. Set up permissions for guest users.

WebRTC conferences are available for Chrome, Opera, Mozilla Firefox, Edge and Safari
browser users. Public web conferences and the number of guest accounts are regulated by the license.

### 3.5.2. Templates

This section allows server administrator to create new conference templates and edit saved ones. Templates can also be saved while editing conference (see "General" tab). Conference template includes information about conference mode, participant list, conference owner, as well as additional parameters. 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 templates.

### 3.5.3. Streaming

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

To create a new configuration, click Add configuration button.
Streaming through CDNvideo cloud service

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

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

Streaming via third-party services and products

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

**Wowza Streaming Engine**

1. Configuration name displayed in "Streaming configuration" list on the conference edit page.
2. Address of the Wowza Streaming Engine.
3. Wowza Streaming Engine accepts connections on this port (e.g. 1935 or 1940).
4. You can find necessary information in Wowza Streaming Engine user's guide.
5. Check "Authentication" to enter username and password to access Wowza Streaming Engine if required.
6. This section includes additional settings for current streaming configuration (see Additional streaming configuration settings in present user's guide).
Wowza Streaming Cloud

1. Link to the instruction on how to setup streaming through Wowza Streaming Cloud in our blog.
2. Configuration name displayed in "Streaming configuration" list on the conference edit page.
3, 5 and 6. You can find necessary information in Wowza Streaming Cloud user’s guide.
4. Wowza Streaming Cloud accepts connections on this port (e.g. 1935 or 1940).
7. This section includes additional settings for current streaming configuration (see Additional streaming configuration settings in present user’s guide).

YouTube

1. Link to the instruction on how to setup streaming via YouTube.
2. This section includes additional settings for current streaming configuration (see Additional streaming configuration settings in present user’s guide).

How to get a conference RTSP URL for YouTube streaming?
1. Proceed to the conference list page.
2. Select the conference you have previously set for streaming.
3. Click on Display conference details... in the side menu.
4. Follow Available options link.
5. Copy an RTSP link to the stream from the pop-up window.

You will also need this link for streaming in Pull mode, for example, on Facebook.

Manual settings

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

Publish manual setting
1. Configuration name displayed in "Streaming configuration" list on the conference edit page.
2. The address which will be used to notify about available stream via RTSP ANNOUNCE protocol.
3. Check **Authentication** to enter username and password and gain access to Wowza Streaming Engine.
4. This section includes additional settings for current streaming configuration (see **Additional streaming configuration settings** in present user’s guide).

**RTSP Pull manual settings**

1. Configuration name displayed in "Streaming configuration" list on the conference edit page.
2. This section includes additional settings for current streaming configuration (see "Additional streaming configuration settings" in present user’s guide).

**Additional streaming configuration settings**

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

3.6. API

3.6.1. OAuth2

This 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 frame below. Please note that it is no longer recommended to access API via Secret key in Web / Security section as this option will be deprecated in one of the following TrueConf Server versions.

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. Server administrator can manage third-party application permissions and access tokens obtained via this section.

Oauth 2.0 is used to authorize certain applications (clients) to access protected resources with limited scopes and rights. This method grants administrator a way to immediately block particular application or a user from accessing protected data without affecting other applications.

Using this protocol, third-party applications are authorized to access server’s API and perform actions on the server on behalf of the user. 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.

<table>
<thead>
<tr>
<th>OAuth 2.0 authorization method</th>
<th>Access token scope</th>
<th>Authorization result</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client Credentials</strong>&lt;br&gt;The client gets access token, the scope of which is server wide. User authorization is not performed. This method is recommended for trusted applications only.</td>
<td>Server wide</td>
<td>Access token valid for 24 hours is issued.</td>
</tr>
<tr>
<td><strong>User Credentials</strong>&lt;br&gt;(a.k.a. Resource Owner Password Credentials Grant)&lt;br&gt;<strong>To obtain access token, it is required to provide</strong></td>
<td>User’s scope</td>
<td>Access token valid for 24 hours and refresh token valid for 14</td>
</tr>
</tbody>
</table>

©2019 TrueConf. All rights reserved.
username and password received on the application side.

<table>
<thead>
<tr>
<th><strong>Authorization Code</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>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 also defines a set of permissions he or she grants to this application.</td>
</tr>
<tr>
<td><strong>Access token</strong></td>
</tr>
<tr>
<td>User's scope</td>
</tr>
<tr>
<td>Access token valid for 24 hours and refresh token valid for 14 days are issued.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Refresh Token</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>This method is used to obtain a new access token based on your existing refresh token.</td>
</tr>
<tr>
<td><strong>Equal to scope of the user who has received refresh token initially.</strong></td>
</tr>
<tr>
<td>Access token valid for 24 hours is issued. This method cannot be used to obtain new refresh token.</td>
</tr>
</tbody>
</table>

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.

Some applications cannot be removed from the list of existing apps, e.g. trueconf_slack_agent, which is created when connecting TrueConf Server to an existing Slack team. To remove it, you’ll need to disable this integration in the Manage add-ons section of TrueConf Server control panel.

### Permissions

Permission set given to a third-party application can be read differently depending on the access token scope obtained after OAuth 2.0 authorization.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Server wide scope</th>
<th>User's scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>conferences</td>
<td>Create, view, edit, delete, start and stop any conference on the server.</td>
<td>If the user is the conference owner, he/she can create, view, change, delete, start and stop the conference. If the user was listed among participants when conference was scheduled he/she can only view conference properties.</td>
</tr>
<tr>
<td>conferences.invitations</td>
<td>View, add, and remove any participants invited to the conference. For conference owners: view, add and remove participants invited to the conference. For listed participants: view the list</td>
<td></td>
</tr>
<tr>
<td>Module</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>conferences.participants</td>
<td>View the list of active participants that are currently in the conference;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>send a request to join the conference to other users or endpoints.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For conference owners: view the list of active conference participants.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For listed participants: view the list of active conference participants.</td>
<td></td>
</tr>
<tr>
<td>groups</td>
<td>Create, view and edit names and rights of any server group.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>View names and permissions of the server groups if the user is a member of</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the group.</td>
<td></td>
</tr>
<tr>
<td>groups.users</td>
<td>View, add and delete any server group users. Editing of group’s address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>book is forbidden.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>View group user lists if the user is a member of the group.</td>
<td></td>
</tr>
<tr>
<td>users</td>
<td>Create, view, change, and delete any server user. In LDAP mode only reading</td>
<td></td>
</tr>
<tr>
<td></td>
<td>mode is available.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>View and edit user profile on the server.</td>
<td></td>
</tr>
<tr>
<td>users.addressbook</td>
<td>View, add, and delete address book entries of any server user.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>View, add, and delete entries in user’s address book.</td>
<td></td>
</tr>
</tbody>
</table>

Creating new OAuth 2.0 application

1. **Application name.** Only displayed in the application list.
2. **URL redirect** field is only used for Authorization Code method. For other authorization methods please indicate the following address https://localhost/.
3. Permissions set which is described in the previous section.
4. Don’t forget to save the information to create new application.
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 TrueConf Server 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.

3.7. Reports

This 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.

On the right of some of the tables there’s a dashboard containing detailed information about an event reflected in a corresponding table. Dashboard content changes when you select a table row.

In the tables, time is displayed according to the time zone selected in the preferences menu.

These tables have common functions:

1. Filter entries
2. Save tables in CSV format
3. Sort entries by field values (click on any column name to change sorting order)

3.7.1. Events

“Events” section contains all changes of user states that are recorded sequentially: login, logout, etc. Click on an event in a table to check detailed information, e.g. client applications or IP address used to log in or user status changes.
1. General table interface (see the description above)
2. Event details
3. Link to an active user profile

3.7.2. Call history

This section contains history and detailed information about video calls and conferences on the server

3.7.2.1. Call list

You can find any calls you like in the table on the main page of the section. Along with call history, call list contains information about the current conference. End field remains blank for current conferences.

1. General table interface (see the description above)
2. Link to the page with detailed information about a call or conference
3. Link to a **profile** of the conference or call owner

### 3.7.2.2. Call or conference information

When you click on a call or conference ID in the general table, you proceed to the menu that displays information about the selected call. This information includes:

- Time and information about the conference owner
- List of the participants who attended the conference anytime
- History of conference invitations and reactions

#### 3.7.2.3. Connection properties

For each user of the conference, you may get the information about all the conference connection details — from the client application version to an operating system and CPU.
### 3.7.3. Chat messages

"Chat messages" section features all messages sent by server users to each other and during video conferences. Please note that one 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 common chat, you can filter by **Sender**, **Recipient**, **Conference 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 conference to the common chat of which a message was sent
3.7.4. Configuration changes

This section displays the history of server settings changes. Each table entry corresponds to a particular change. When you click on an entry, a panel on the right displays server settings before and after the changes have been made.

1. General table interface (see the description above)
2. Name of the modified parameter
3. Previous parameter value (before making changes)
4. New parameter value (after making changes)

3.7.5. Conference recordings

This section contains a list of recorded conferences. Conference records can be downloaded or deleted here.
1. General table interface (see the description above)
2. Link to the page with detailed information about a recorded conference or a call
3. Link to a user profile of the conference moderator or video call owner
4. Conference type: video call, symmetric, and asymmetric or role-based
5. Download button
6. Delete button

3.7.6. Endpoints

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

1. Unique connection ID.
2. Select the number of displayed connections in the table.
3. Trueconf ID of the users who are currently connected to the server.
4. Name of the user's client application and application version.
5. Field used to search for a connection. The system searches through all fields (once a table has been filtered, the system displays only those records that have at least one field with string entered).
6. User IP address.

By clicking on the table entry, you can see the pages containing information about a particular user connections. This page may include information about:
- Available playback and audio capture devices
- Available video capture devices
- Selected equipment settings
- The latest conference where a device participated
- DirectX properties
- Network connection
- Network test results
### 3.7.6.1. Events that update device information

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

#### 3.8. File storage

In this section you can setup storage settings for files your users are exchanging:
1. Select a location of the files directory. You can use network paths.
2. Available free space on logical drive used for storage.
3. File lifetime (in days) before the files are removed automatically. Start time is the first file upload. The files are stored for 7 days by default. Minimal value is one day, and maximal value is unlimited.
4, 5. Use the slider to set maximum upload and download speed limits to upload or download the files from the server.
6. Save changes.

3.9. Recordings

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

1. The path to the folder where all recordings are saved. Default recordings folder is located in the server working folder. The list of recorded conferences displays the videos from the specified folder. If the path is redefined, the list is re-formed respectively. In this field, you can also specify network path if TrueConf Server service has the rights to place recordings in this directory.
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 ("Upon Request" mode).
4. Video quality of conference recording.
5. Video format of conference recording.
6. 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).

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

Yes, but you will have to download and install a specific codec for that. Once the installation is complete, start encoder configuration procedure. Select "libavcodec" decoder in the VP8 video encoder configuration window.

You can also upload any of your recordings to Youtube to share with your colleagues.

**How to publish a conference recording on YouTube**

- Download the recording.
- Convert this file to .mp4 format using FFmpeg utility.
- Process it in any video editor available to you.
- Upload to YouTube.

3.10. Manage add-ons

3.10.1. TrueConf Directory

In this section, you can make your TrueConf Server instance available for integration with TrueConf Directory. To do it, please click on the **Activate** button. If you want to disable integration, click on the **Deactivate** button.

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

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

<table>
<thead>
<tr>
<th>Directory</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>3.0.0 or above</td>
</tr>
<tr>
<td>SSL (HTTPS)</td>
<td>enabled</td>
</tr>
</tbody>
</table>

To connect TrueConf Server Directory to TrueConf Directory, use the key as it is shown in our blog post.