TASSTA

ENGLISH

Document revision: **2407.01-1840**

T.Commander 3.5

Administrator's Guide

Last revised: July 1, 2024

This document is not warranted to be error-free. If you find any problems in the documentation, please report them to us in writing.

Due to ongoing product improvements and revisions, TASSTA GmbH cannot guarantee the accuracy of printed or soft material after the publishing nor can it accept responsibility for errors or omissions. Updates to this document and other documentation can be downloaded at TASSTA Documentation Center.

Contents

Introduction 10
Product overview 11
Signing in 12
Resetting the password 12
Editing profile 12
Changing password 12
Password best practices 13
User interface 14
Sorting and filtering 15
Sorting 15
Smart filtering 15
Filter by column 15
Navigating through options 16
Reviewing changes 16
Changing the interface language 16
Servers 17
Dashboard 17
Adding a server 17
Adding multiple servers 18
Cloning a server 18
License pool 19
Adding a map overlay 20
Issuing an access token 21
Reconfiguring a server 21
Restarting a server 22
Starting or stopping a server 22
To stop a server: 22
To start a server: 22
Exporting server settings 23
Exporting user provisioning information 23
Importing server settings 23
Resetting a server 24
Server properties 24

Main....24
Miscellaneous....25
Users....32
Adding a user....32
Adding multiple users....32
Cloning users....33
Copying users....34
Copying user settings....34
Working with templates....34
Editing a user....35
Generating QR code....36
Guest access....38
Editing lone worker protection settings....38
Checking effective privileges....39
Creating a rule....39
User role assignment....40
Deleting a user....40
User properties....40
Main....41
Client type....42
Codec....42
Common calls....42
Data calls and messaging....44
Emergency....45
Group calls....48
Guard tours....48
History....49
Individual calls....49
Lone worker protection....50
Map and tracking....50
Miscellaneous....53
Remote control....55
User authentication....57
Video....57
Channels....61

Adding a channel 61
Adding multiple channels 61
Editing a channel 62
Updating channel's ID 63
Deleting a channel 63
Organizing channels into zones 64
Adding a zone 64
Editing a zone 64
Deleting a zone 65
Channel properties 65
Main 66
Miscellaneous 66
Lone worker protection 68
Configuring lone worker profile 68
Copying profile properties 68
Working with templates 69
Applying a template 69
Managing templates 69
Lone worker properties 70
Main 70
Battery monitor 70
Connection 71
Emergency contact 71
Emergency timer 72
Impact 72
Info 72
Man down 73
Miscellaneous 73
Movement 73
Periodic check 73
Periodic Check U 74
Sensor check 74
Rules 75
General concepts 75
Scheduling 76

Inheritance ... 76
Inheriting rules for dynamic sub-channels ... 76
Inheriting rules from the Main channel ... 76
Access teams ... 76
Adding a team ... 77
Editing a team ... 77
Deleting a team ... 78
Creating a rule ... 78
Editing a rule ... 79
Reordering rules ... 80
Checking effective privileges ... 80
Enabling rules ... 80
Inheriting rules ... 81
Disabling rules ... 81
Turning off rules' inheritance ... 81
Deleting rules ... 81
Password protected channels ... 82
Task Manager ... 83
Customizing task fields ... 83
Adding Task Manager field ... 83
Editing Task Manager field ... 84
Deleting Task Manager fields ... 85
Customizing task priorities ... 85
Adding task priority ... 85
Editing task priority ... 86
Deleting task priority ... 86
Customizing task statuses ... 86
Adding task status ... 87
Editing task status ... 87
Deleting task status ... 87
Customizing Task Manager roles ... 88
Adding Task Manager role ... 88
Editing Task Manager role ... 88
Deleting Task Manager roles ... 88
User roles and statuses ... 90

Managing roles and statuses 90
User role assignment 90
Status messages 92
Adding status messages 92
Changing a status message 92
Deleting status messages 93
Workgroups 94
Adding a workgroup 94
Updating a workgroup 94
Deleting workgroups 94
Administering a platform 96
Server nodes 96
Adding a node 96
Editing a node 97
Deleting a node 97
T.Commander users 98
Adding a user 98
Editing a user profile 99
Deleting users 101
Backup and recovery 101
Creating a backup 101
Exporting and importing backups 101
Scheduling regular backups 102
Restoring settings 102
Deleting a backup 102
T.Commander logs 103
Recording configuration 104
Setting up recorder profiles 104
Configuring activity recording 105
Starting and stopping recording 107
Recording location history 107
Billing reports 108
Client updates 108
Important considerations 108
Adding an update 108

Managing updates 109
Cross-server communication 109
Key elements 110
Managing server connections 110
Managing multi-channel groups 111
Snapshots 113
Creating a snapshot 113
Restoring from a snapshot 114
Removing snapshots 114
Annex I: Isolated teams 115
Preconditions 115
Setting up rules in T.Commander 115
Configuring access to *Electrical* channel 115
Configuring access to *Rig* channel 116
Annex II: Client features 117
Server properties 117
Main 117
Miscellaneous 117
User properties 121
Main 121
Client Type 121
Codec 121
Common Calls 122
Data Calls And Messaging 123
Emergency 123
Group Calls 125
Guard Tours 125
History 126
Individual Calls 126
Lone Worker Protection 127
Map And Tracking 127
Miscellaneous 128
Remote Control 129
User Authentication 130
Video 131

Channel properties....132
Main....132
Miscellaneous....132
Lone worker protection properties....133
Main....133
Battery Monitor....133
Connection....133
Periodic Check U....134
Emergency Contact....134
Emergency Timer....135
Impact....135
Man Down....135
Miscellaneous....136
Movement....136
Periodic Check....136
Sensor Check....137
Annex III: Managing favorites....138

Introduction

This guide provides detailed instructions on using T.Commander for configuring TASSTA communication network. It is oriented towards system administrators possessing a good understanding of TASSTA solutions and services.

The instructions assume T.Lion and T.Commander are already deployed.

Product overview

T.Commander provides the convenient web interface for configuring and managing TASSTA solutions:

- T.Lion / T.Brother
- T.Flex
- T.Rodon
- T.Recorder
- TASSTA SDK

T.Commander can be accessed anywhere using only a web browser. No additional software is required - simply enter the address on your computer and start administering the network.

The product supports most modern browsers based on Chromium engine:

- Google Chrome;
- Microsoft Edge (Chromium).

> NOTE:
>
> It is recommended to update your web browser to the latest version.

Signing in

1. Provide the **login** and **password**.
2. Click **Log in**.

To avoid verifying your identity for the next thirty days on the current device and browser you are currently using, select **Remember me for 30 days**.

Resetting the password

If you forgot the password, follow these steps to recover access to your account:

1. Click **Forgot your password?**.
2. Provide the login or email address you are using to sign in to T.Commander.
3. Click **Send**.
4. Check your email. You should get a message with the password reset link.
5. Click **Reset password** button in the message.
   NOTE: The password reset link expires in *1 hour*. If the link has expired, repeat the steps 1-3.
6. Provide the new password and click **Reset**.

Editing profile

To customize the user's name and contact information:

1. Click the profile name in the top right corner.
2. Select **Edit profile** from the dropdown menu.
3. Update the required properties.
4. Click **Save**.

> NOTE:
>
> You should be signed in to edit the profile.

Changing password

If you feel the credentials might be compromised, update the password for your account immediately:

1. Click the profile name in the top right corner.
2. Select **Change password** from the dropdown menu.
3. Provide the new password in **New password** and **Confirm password** fields.

4. Click **Save**.

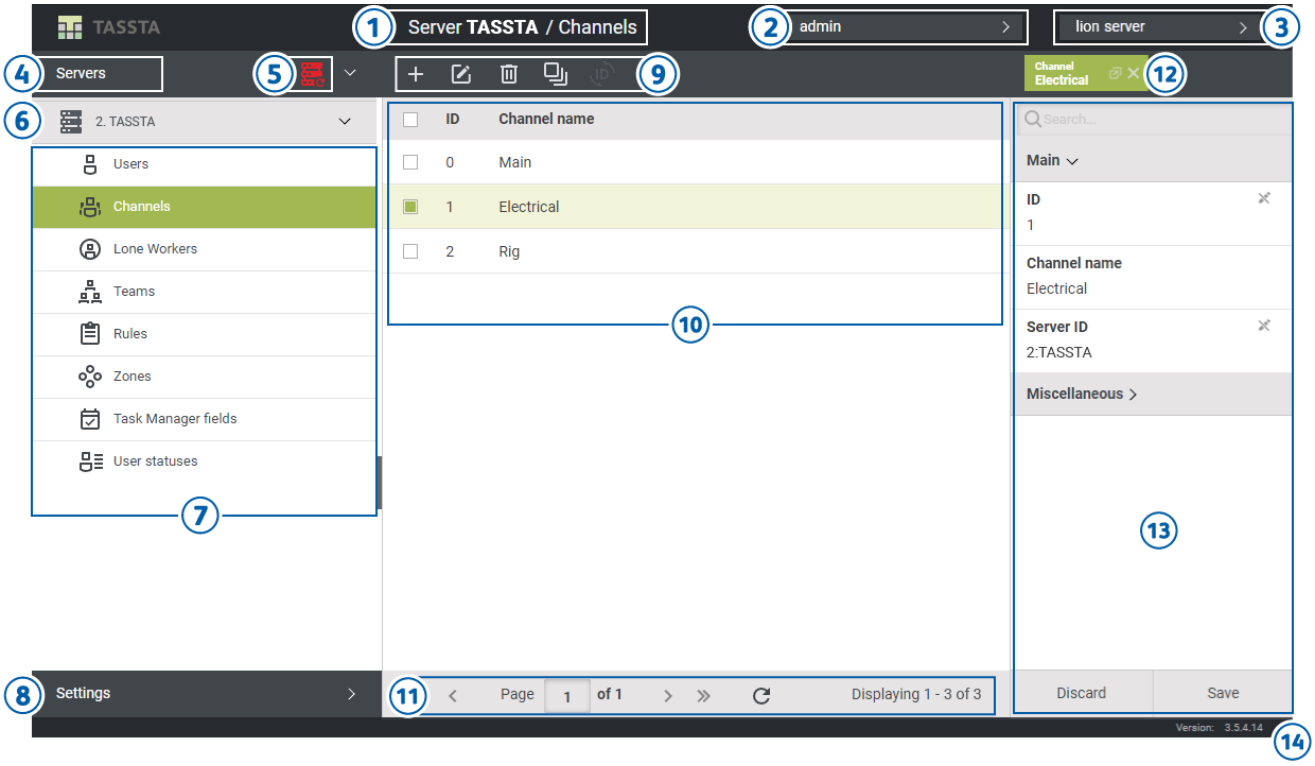
> NOTE:
>
> You should be signed in to change the password. Alternatively, you can reset the password directly from the login screen.

Password best practices

- Password length should be at least 8 characters.
- Make the password hard to guess, even by those who know a lot about you.
- Never re-use the password for multiple systems and for non-work related purposes.

User interface

T.Commander interface consists of the following areas:



1. **Breadcrumbs** - the section you are currently working with.
2. **Profile** - view the current user, change interface language, log off.
3. **Nodes** - switch between T.Lion nodes.
4. **Servers** - manage servers on the current node.
5. **Restart the server** - indicates that the server needs to be restarted to apply changes.
6. **Server** - expand this section to manage server properties.
7. **Navigation pane** - shows server properties or global settings, depending on the context.
8. **Settings** - administer the node.
9. **Toolbar** - perform common context-sensitive operations.
10. **Items** - the list of items (users, channels and so on) based on the current selection in the navigation pane.
11. **Pagination** - navigate through long lists of items.
12. **Sidebar tabs** - switch between currently opened sidebars.
13. **Sidebar** - view and modify the settings.
14. T.Commander version number.

Sorting and filtering

To ensure the interface responsiveness and performance, the list of items (servers, users, channels and so on) only shows a limited number of objects at a time. To quickly navigate to the required item, use sorting and filtering.

Sorting

- Click the column title to sort the list by that column.
- Click the column title again to toggle the sorting order (ascending or descending).

Smart filtering

1. Click icon in the toolbar.
2. Type in a property of the object (ID, any part of the name, and the like).
3. Press **Enter**.

The list will only show relevant objects.

To reset the filter and show all objects, click icon in the filter field.

Filter by column

To filter by a certain column:

1. Hover the column and click icon at the right.
2. Select **Filters** option and provide the filtering criteria. The filter depends on the column type:
   - For numeric columns (ID, port, and the like), you can specify *less than* (=), *greater than* (>), or *equal to* (=) criteria.
   - For text columns (name, alias, and the like), you can specify any part of the column value.
3. Press **Enter**.

To reset a filter by column:

1. Hover the column and click icon at the right.
2. Clear **Filters** option.

> NOTE:
>
> The sorting and filtering settings are not saved. When you switch to another list and back again, the sort order is reset to default and all filters are cleared.

Navigating through options

Some objects, such as servers or users might have dozens of configuration options. In order to quickly navigate to the required option:

1. Type in any part of the option name in **Search** field on top of the sidebar.
2. Press **Enter**. The list of related options is displayed.
3. Click the required option to navigate to it.

Reviewing changes

The option that has been changed from its default value is marked with icon.

This icon is also shown to the right of the sidebar section containing one or more modified options.

Changing the interface language

To change T.Commander interface language:

1. Click the profile name in the top right corner.
2. Select **Edit profile** from the dropdown menu.
3. Select a language from the dropdown menu.
4. Click **Save**.

The following languages are currently supported:

- English (default);
- Arabic;
- Chinese Traditional;
- French;
- German;
- Greek;
- Hungarian;
- Japanese;
- Portuguese;
- Russian;
- Spanish;
- Turkish.

The actual list of interface languages available for you is set in your profile's configuration.

Servers

A **server** is a "subnet" of the communication network with its own members, channels, policies and settings.

You can create more than one server on a single TASSTA system node (T.Lion and the related services). From a technical standpoint, a server is represented by a network port on T.Lion server.

Dashboard

To access the dashboard, click the server in the left pane.

The dashboard provides provides at-a-glance summary of key server configuration:

- Number of users that can connect through PTT clients.
- Total number of channels and zones.
- Total number of teams and rules set for them.
- Total number of lone workers.

To see detailed information, click the corresponding widget (box) on the dashboard.

You can also quickly start or stop the server by using the switch in the top-right corner of the dashboard.

Adding a server

To add a new server to the selected node:

1. Click **Servers** in the left pane.
2. Click  icon in the toolbar. A sidebar with server settings opens.
3. Provide server's display name in **Server name** field.
4. Click **Miscellaneous** and configure server properties.
5. Click **Save**.
6. To enable call recording for the server, click **Yes** in the popup.
   If you click **Cancel**, the server is created without activity recording. You can turn it on later.

> NOTE:
>
> Server ID and a port number are assigned automatically.

Adding multiple servers

To add several servers to the selected node:

1. Click **Servers** in the left pane.
2. Click  icon in the toolbar. A sidebar with server settings opens.
3. Specify the number of servers you want to create in **Amount** field.
4. Specify the starting index to be used for auto-generated server names in **Start from** field. This number is incremented by 1 for each created server.
5. Specify the optional server name mask under **Server name**.
   - **Prefix** string is prepended to the auto-generated index based on **Start from** field.
   - **Postfix** string is appended to the auto-generated index based on **Start from** field.
6. Click **Miscellaneous** and configure common server properties. You can customize them later for each created server.
7. Click **Save**.
8. To enable call recording for servers, click **Yes** in the popup.
   If you click **Cancel**, the servers are created without activity recording. You can turn it on later.

> NOTE:
>
> Unique ID and port number are assigned automatically to each server.

Cloning a server

To create a new server with the same settings, users and channels as the existing one:

1. Click **Servers** in the left pane.
2. Locate the server in the list.
3. Click  icon in the toolbar.
4. Provide a new server's display name in **Server тame** field.
5. Select **Include channels** option to create the same channels on a new server.
6. Select **Include users** option to create the same users on a new server.
7. Select **Init Recorder** option to enable call recording on a new server.
8. Click **OK**.

> NOTE:

A new server will have unique ID and port number, different from the original one. They are assigned automatically.

License pool

You can distribute the total amount of licenses between multiple servers. This gives you the flexibility to control license usage according to the needs of individual groups or clients, and ensure that one team does not block other groups from communicating by consuming all available licenses.

To limit the license usage per server, modify the following miscellaneous server properties:

License	Property	Description
TF.SMART	Maximum online Flex Smart clients	The maximum number of T.Flex Smart clients that can connect to the server at the same time.
TF.PTT	Maximum online Flex PTT clients	The maximum number of T.Flex PTT clients that can connect to the server at the same time.
TR.SMART	Maximum online Rodon Smart clients	The maximum number of T.Rodon Smart clients that can connect to the server at the same time.
TR.PTT	Maximum online Rodon PTT clients	The maximum number of T.Rodon PTT clients that can connect to the server at the same time.
TBR.API	Maximum online Bridge API clients	The maximum number of concurrent T.Bridge to DAMM TetraFlex®, T.Bridge Tier3, or T.Bridge to TeltronicPower users allowed on a server.
TBR.RADIO	Maximum online Bridge Radio clients	The maximum number of concurrent T.Bridge to Hytera DMR (Tier II), T.Bridge to Kenwood NEXEDGE®, T.Bridge to Kenwood P25, T.Bridge to MOTOTRBO™, or T.Bridge to Sepura users allowed on a server.
TBR.4WIRE	Maximum online Bridge 4Wire clients	The maximum number of concurrent T.Bridge 4wire or T.Bridge to Vocality users allowed on a server.
T.SDK	Maximum online SDK clients	The maximum number of concurrent TASSTA SDK client connections to a server.

License	Property	Description
E2EE	Maximum end-to-end encryption clients	The maximum number of clients allowed to use end-to-end encryption.
EMC	Maximum Task Manager clients	The maximum number of clients allowed to use Task Manager.
INDOOR	Maximum indoor clients	The maximum number of clients allowed to use indoor positioning.
LWP	Maximum lone worker clients	The maximum number of clients allowed to use lone worker protection features.
VIDEO	Maximum push-to-video clients	The maximum number of clients allowed to use video calls and push-to-video.

If one of the licensed features is enabled for a user, the corresponding license slot is used as soon as the user's client connects to the server, even if the user does not currently use the feature. The license is released when the user disconnects from the server, and the license slot can be used by other clients, including the clients from other servers.

> IMPORTANT:
>
> - The maximum number of licenses per server (second column) must not exceed the total amount of licenses (first column).
> - The grand total of all licenses for all servers may exceed the total of licenses in the first column. However, this may result in one team blocking other teams from communicating by consuming all available licenses.

Adding a map overlay

Map overlay is used to visualize some extra information that is not present on the geographical map, such as transport routes, tunnels, construction sites, and so on. The overlay is displayed in T.Flex and T.Rodon clients.

> IMPORTANT:
>
> Map overlay only works with Mapbox geodata provider.

The overlay is a GeoJSON file that can be created in an on-premise or online editor, for example, geojson.io.

To add a map overlay to the server:

1. Click **Servers** in the left pane.
2. Select a server from the list.
3. Click  icon in the toolbar.
4. Click **Browse…** button and select a GeoJSON file.
5. Click **Upload** button.

To replace the existing map overlay, simply upload another GeoJSON file to the server.

Issuing an access token

Third party location tracking systems require an access token for authorization in TASSTA services. To issue a token that opens access to location history of all users on the server:

1. Click **Servers** in the left pane.
2. Select a server from the list.
3. Click  icon in the toolbar.
4. Copy the token text by clicking the *Copy* button next to it.
5. Close the dialog.

> IMPORTANT:
>
> - The existing token stops working immediately after a new token is issued.
> - The token text is displayed only once. Be sure to copy it before closing the dialog.

Reconfiguring a server

To change the server's settings:

1. Click the server in **Servers** navigation pane.
2. Click  icon in the toolbar. A sidebar with server settings opens.
3. Modify the server display name in **Server name** field or change server properties under **Miscellaneous**.
4. Click **Save**.
5. In order to apply new settings, restart the server.

> NOTE:
>
> Server ID and port number cannot be changed.

Restarting a server

> WARNING:
>
> When the server is restarting, all related communication is suspended, including emergency calls. While the restart only takes a few seconds, it is recommended to do it during non-working hours.

If you have changed the server's settings or encounter problems with the server, restart it:

1. Click the server in **Servers** navigation pane.
2. Click  icon in the toolbar.
3. Confirm restarting.

> TIP:
>
> If any of the servers needs restarting,  icon is shown on top of the **Servers** navigation pane. Click the icon and then click the required server in the dropdown to restart it.

Starting or stopping a server

> WARNING:
>
> Stopping a server disconnects all clients and stops all related communication, including emergency calls!

To stop a server:

1. Click the server in **Servers** navigation pane.
2. Click  icon in the toolbar.
3. Confirm stopping a server.

To start a server:

1. Click the server in **Servers** navigation pane.
2. Click  icon in the toolbar.
3. Confirm starting a server.

Alternatively, you can use  switch to quickly start or stop the server.

Exporting server settings

You can export all server settings (including users and channels) to a file for backup or migration purposes:

1. Click the server in **Servers** navigation pane.
2. Click  icon in the toolbar.
3. Select **Export server configuration into file (.cfg)**. The file will be downloaded to your computer.

Exporting user provisioning information

You can generate an automated user provisioning script for mobile clients based on their IMEI and phone (SIM) number. It may be very useful for configuring radios without screen or automatically sign in users without need for login or password.

To export user provisioning script:

1. Click the server in **Servers** navigation pane.
2. Click  icon in the toolbar.
3. Select **Export user credentials into file (.csv)**. The file will be generated and downloaded to your computer.

Refer to T.Flex documentation for instructions on how to apply user provisioning information on end-user devices.

Importing server settings

To create a new server based on the exported settings:

1. Click **Servers** in the left pane.
2. Click  icon in the toolbar.
3. Provide server's display name in **Server Name** field.
4. Select **Include channels** option to import channels from the configuration file.
5. Select **Include users** option to import users from the configuration file.
6. Select **Initialize Recorder** option to enable call recording on a new server.
7. Click **Browse...** and select the server configuration file you have exported earlier.
8. Click **OK**.

> NOTE:
>
> Server ID and port number are assigned automatically.

Resetting a server

> WARNING:
>
> Resetting a server deletes all users and channels in it and resets all settings (except for ID and port number) to default values. Make sure to export server settings before resetting it.

To reset a server:

1. Click **Servers** in the left pane.
2. Locate the server in the list.
3. Click  icon in the toolbar.
4. Confirm server reset.

> NOTE:
>
> The server is not physically deleted. It is still available in T.Commander as a stopped unnamed server, so you can reconfigure and reuse it later on.

Server properties

T.Commander provides a number of configuration options that you can set for the server. To simplify navigation, options are organized in logical groups:

- Main
- Miscellaneous

Certain server options enable additional functionality or grant access to advanced configuration, such as individual calls, zones, lone worker protection and so on.

Main

Core properties of the server.

- **Server name** (required)
  Provide display name for the server.
- **Port** (automatically generated)
  Network port number.
- **ID** (automatically generated)
  Unique ID of the server.

Miscellaneous

Any of those options can be left at the default value. However, certain features of TASSTA network require customizing corresponding settings. For example, you should provide a non-zero number of **Maximum channels** if you want to create additional channels on the server.

Common settings

- **Maximum users**
  Set the total number of users that can be created on a server.
- **Maximum online users**
  Set the maximum number of concurrent users allowed on a server.
- **Maximum push-to-video clients**
  Set the maximum number of users allowed to use video calls and push-to-video.
- **PTT queue size**
  Limit the maximum number of waiting users in a PTT queue. Set the value to `0` for unlimited queue length.
- **PTT time limit (seconds)**
  Set the number of seconds after which a user's PTT session is automatically released, even if the user keeps holding PTT button. Use `0` to allow a user to speak as long as PTT button is pressed or toggled.
  Limiting the duration of user's PTT session might be very useful in conjunction with Toggle PTT Button setting, or certain equipment that uses toggle instead of holding down PTT button.
  This setting only applies to group calls, push-to-video calls, broadcast calls, and emergency calls (after emergency PTT timeout ends). It does not apply to users from external radio systems connected via T.Bridge.
  IMPORTANT: **When PTT time limit is provided, emergency recordings may be incomplete!**
- **Hide offline users**
  - *Show all offline users on the server* - show offline users in T.Flex and T.Rodon
  - *Hide all offline users on the server* - hide offline users in T.Flex and T.Rodon
  - *Show offline users from visible channels only* - show offline users who were last seen on channels that the current user can join.
    For example, the user *Rigger* disconnected while being a member of the channel *Construction-Site*. Other members of *Construction-Site* or members of other channels with access to *Construction-Site* will see him/her in the users list.
- **Maximum channels**
  Set the total number of channels that can be created on a server.
  NOTE: *Main* channel is created by default, regardless of the maximum number of channels.
- **Zones**
  Allow for organizing channels into zones.

- Comment
  Provide a verbose description for a server.

T.Flex settings

- Maximum online Flex Smart clients
  Set the maximum number of *T.Flex* clients that can connect to the server at the same time.
- Maximum online Flex PTT clients
  Set the maximum number of *T.Flex PTT* clients that can connect to the server at the same time.

T.Rodon settings

- Maximum Rodon Smart clients
  Set the total number of *T.Rodon* clients that can connect to a server.
- Maximum online Rodon Smart clients
  Set the maximum number of concurrent *T.Rodon Smart* users allowed on a server.
- Maximum online Rodon PTT clients
  Set the maximum number of concurrent *T.Rodon PTT* users allowed on a server.

Task Manager settings

- Task Manager
  Enable clients to use Task Manager.
- Maximum Task Manager clients
  Set the total number of clients allowed to use Task Manager.
- Task Manager project
  Provide a custom label assigned to all tasks created on this server.

T.Bridge settings

- Bridge
  Allow *T.Bridge* connections.
- Maximum online Bridge Radio clients
  Set the maximum number of concurrent T.Bridge users allowed on a server.
- Maximum online Bridge API clients
  Set the maximum number of concurrent T.Bridge API users allowed on a server.
- Maximum online Bridge 4Wire clients
  Set the maximum number of concurrent T.Bridge 4Wire users allowed on a server.
- Maximum online Bridge SIP clients
  Set the maximum number of concurrent T.Bridge SIP users allowed on a server.

Recording settings

These settings affect activity history access from *T.Rodon*, *T.Flex* and *T.Recorder*.

- Recorder server
  Recorder Server API endpoint. If you are using or planning to use the Google Play version of T.Flex, provide the domain name for which the SSL certificate is issued instead of the IP address.
  IMPORTANT: Do not modify the default value of this field. Contact TASSTA support if you encounter problems with recording.
- Recorder server key
  Recording profile access key for T.Flex and T.Rodon. If the server is assigned to multiple recording profiles, provide the key from the most suitable one.

SDK settings

- Maximum online SDK clients
  Set the maximum number of concurrent *TASSTA SDK* client connections to a server.

Lone worker protection settings

- Lone worker protection
  Enable lone worker protection feature on a server.
- Maximum lone worker clients
  Set the total number of clients allowed to use lone worker protection functionality.
- LWP dispatcher required
  Require T.Rodon operator to be online in order to use lone worker protection functionality on T.Flex clients.
- Sensor check validity period
  Specify how long lone worker protection remains active after the sensor check is passed. Applies to all users.

Indoor localization settings

> IMPORTANT:
>
> T.Flex for iOS only supports indoor positioning based on Bluetooth beacons.

- Indoor localization
  Enable indoor localization feature on a server.
- Resolve position based on fixed beacons
  Switch to alternative positioning mode, when signals from beacons with predefined coordinates are used to determine a client's location on map in areas where GPS lacks precision or does not work (tunnels, buildings).
  IMPORTANT: Turning this mode on disables *Indoor Localization* menu in client applications.
- Maximum indoor clients
  Set the total number of clients allowed to use indoor localization.
- Indoor localization share interval (milliseconds)
  Set the location sharing interval for indoor positioning, in milliseconds. Providing lower values may

improve location accuracy, but increase the server load.
Optimal value for most environments: 2-3 seconds (2000-3000 milliseconds).

- Indoor localization mode
  Choose indoor positioning technique. At the moment, it is only possible to resolve position based on fixed fixed anchor points - Bluetooth beacons with unique identifiers placed at predefined positions (*Based on Bluetooth signal*).
- Bluetooth UUID
  Specify UUID of Bluetooth beacons used for indoor positioning. Required for correct functioning of Indoor Localization feature in T.Flex iOS clients running under iOS 15.

  IMPORTANT: All beacons with other UUID's are ignored. After specifying or changing this value, the indoor positioning AI must be retrained.
- Infsoft indoor localization key
  Set the access token that allows clients to use indoor positioning solution provided by infsoft GmbH.

  NOTE: infsoft indoor positioning only works for users with Mapbox geodata provider.

MCGW configuration

Configure communication bridging via SMS and email messages (multi-communication gateway).

SMS

> NOTE:
>
> Sign up for Twilio account to use SMS services in TASSTA network.

- Phone number
  Provide preconfigured phone number from your Twilio account.
- Communication service ID
  Provide Twilio account SID.
- Communication service token
  Provide Twilio auth token.

Email

- Address
  Provide outgoing email address.
- Username
  Provide mail server login.
- Password
  Provide mail server password.
- SMTP server
  Provide SMTP server name or IP address.

- SMTP port
  Provide SMTP server port number.

End-to-end encryption settings

- End-to-end encryption
  Allow end-to-end encryption on clients.
- Maximum end-to-end encryption clients
  Set the total number of clients allowed to use end-to-end encryption.

Jitter buffer settings

Jitter buffer is a temporary storage for incoming data packets in voice over IP (VoIP) networks. It ensures the continuity of audio streams by smoothing out packet arrival times during periods of network congestion. Larger buffer size can smooth out the audio in unstable network conditions at the cost of adding more delay.

T.Commander allows you to configure the jitter buffer range:

- JB1 size (packets)
  Minimum number of data packets in the buffer.
- JB2 size (packets)
  Maximum amount of extra buffering (data packets). The playback is started when the number of packets in the jitter buffer achieves JB1 + JB2/2.

Recommended values:

Preset	JB1	JB2	Resulting delay (milliseconds)
Fastest	2	4	240
Optimal	6	8	600
Smooth	12	8	960

Map

TASSTA clients use Mapbox as the default map provider. To unlock the feature, sign up for a free Mapbox account and create an access token.
Learn more details at https://docs.mapbox.com/help/getting-started/access-tokens/.

You can either use a single token for all clients, or register a separate token for each client type. The latter offers you more flexible approach to monitoring the usage and managing the costs of the Mapbox subscription(s).

> IMPORTANT:

Mapbox is a paid service with a free tier. Additional charges may apply depending on your map usage profile. Check Mapbox pricing for details.

- Map
  Enable client access to maps and show extended **Map And Tracking** options for users on a server.
- Mapbox access token (Flex Android)
  Set the Mapbox service token for all T.Flex Android clients.
- Mapbox access token (Flex iOS)
  Set the Mapbox service token for all T.Flex iOS clients.
- Mapbox access token (Rodon)
  Set the Mapbox service token for all T.Rodon clients.
- Google Maps API key
  Set the Google authentication credentials (API key) that allows all clients to use Google Maps as a geodata provider.

Extended settings

- Individual calls
  Allow users on a server to make individual calls.
- History replay
  Show extended **History** options for users on a server.
- Priority
  Allow setting relative PTT priority level for users on a server.
- Remote control
  Enable remote control and show extended **Remote Control** options for users on a server.
- Transparent PTT
  Enable conferencing functionality for channels on a server.
- Call queue
  Allow T.Flex users to initiate "callback" requests to dispatchers (call queues). This setting also enables the corresponding functionality in T.Rodon.
- Maintenance
  Allow users to start, stop, and restart a server.
- Service gateway
  Provide the central endpoint for T.Lion services API. If you are using or planning to use the Google Play version of T.Flex, provide the domain name for which the SSL certificate is issued instead of the IP address.
  IMPORTANT: Do not modify the default value of this field. Contact TASSTA support if you encounter problems with your server configuration.
- Samsung hardware buttons license
  Provide a license key for compatible Samsung devices with hardware PTT buttons, such as Samsung Galaxy XCover FieldPro.
- Maximum online connectors
  Set the maximum number of concurrent Connectors allowed on a server.

- Force TCP
  Force all traffic, including video streams, to be transmitted over TCP/IP.

Users

A user is an operator of T.Flex/T.Rodon, or a service account for TASSTA SDK. To show and manage users, expand a server in navigation pane and click **Users**.

- To select a single user, click it.
- To select multiple users, select or clear the checkbox to the left of user's name.

Adding or updating users do not require restarting a server. The changes are applied immediately after saving.

Adding a user

> IMPORTANT:
>
> You should set non-zero **Maximum users** parameter in server settings in order to add users.

To add a new user to the selected server:

1. Expand the server in the left pane and click **Users**.
2. Click  icon in the toolbar. A sidebar with user settings opens.
3. Provide a login in **Name** field.
   IMPORTANT: Usernames `cpoint<number>` (for example, `cpoint20`) are reserved for the T.Qonnector service. You cannot create users with these names.
4. Provide a password in **Password** field.
   To generate a random strong password, click  icon in this field and select **Copy new password to clipboard**.
5. Configure user properties.
6. Click **Save**.

> NOTE:
>
> User ID and server ID are assigned automatically.

Adding multiple users

> IMPORTANT:
>
> You should set non-zero **Maximum users** parameter in server settings in order to add users.

To add several identical users to the selected server:

1. Expand the server in the left pane and click **Users**.

2. Click  icon in the toolbar. A sidebar with user settings opens.
3. Specify the number of users you want to create in **Amount** field.
4. Specify the starting index to be used for auto-generated logins in **Start from** field. This number is incremented by 1 for each created user.
5. Specify the optional login mask under **Name**.
   IMPORTANT: Usernames `cpoint<number>` (for example, `cpoint20`) are reserved for the T.Qonnector service. You cannot create users with these names.
   - **Prefix** string is prepended to the auto-generated login based on **Start from** field.
   - **Postfix** string is appended to the auto-generated login based on **Start from** field.
6. Specify the auto-generated password mask under **Password**.
   NOTE: Password complexity requirements are defined by T.Lion server policies. Make sure auto-generated passwords meet them.
   - **Prefix** string is prepended to the auto-generated password based on **Start from** field. To generate a random string of the required length, click  icon in this field.
   - **Postfix** string is appended to the auto-generated password based on **Start from** field.
7. Configure user properties. You can customize them later for each created user.
8. Click **Save**.
9. T.Commander generates QR codes for each user based on the automatically generated login and password.
   - To save all QR codes locally, click **Save** in **Generated QR codes** popup and choose whether you want to save all codes as a single PDF file (**All-In-One report**) or as a ZIP archive with individual PDF files for each user (**Package with multiple reports per user**).
   - To ignore automatically generated QR codes and simply create the users, click **Close**.

> NOTE:
>
> Unique ID is assigned automatically to each user.

Cloning users

You can create one or more users based on the existing users' settings:

- Copying users
- Copying user settings
- Working with templates

Copying users

To create new users based on the existing users:

1. Expand the server in the left pane and click Users.
2. Select one or more users from the list.
3. Click  icon in the toolbar.
4. Click  icon in the toolbar.

Copies of the selected users are created on a server. They retain the same settings as the original ones (including passwords), except for logins and IDs.

Copying user settings

To copy all settings from a user to other users:

1. Expand the server in the left pane and click Users.
2. Select a source user from the list.
3. Click  icon in the toolbar.
4. Select one or more target users from the list.
5. Click  icon in the toolbar.

All settings of the source user, except for the login and password, are applied to the selected users.

Working with templates

T.Commander supports saving common user settings as a template, so you can use them later to create new users or apply them to the existing users. The list of templates is common for the entire TASSTA system node, so you can apply them across multiple servers.

To create a template based on the existing user settings:

1. Expand the server in the left pane and click Users.
2. Select a user from the list.
3. Click  icon in the toolbar. A sidebar with user settings opens.
4. Provide the name of the template in Template name field.
5. Select settings you want to save as a template.

> IMPORTANT:
>
> Saved templates are specific to each user and are not shared across other node's users.

Creating new users based on the template

1. Expand the server in the left pane and click **Users**.
2. Click  icon in the toolbar. A sidebar with user settings opens.
3. Provide a login in **Name** field.
   IMPORTANT: Usernames `cpoint<number>` (for example, `cpoint20`) are reserved for the T.Qonnector service. You cannot create users with these names.
4. Provide a password in **Password** field.
   To generate a random strong password, click  icon in this field and select **Copy new password to clipboard**.
5. Right-click anywhere in the sidebar, select **Apply template** from the context menu.
6. Click  icon to the right of the template name.
7. Click **Save**.

Applying a template to existing users

1. Expand the server in the left pane and click **Users**.
2. Select one or more users from the list.
3. Right-click anywhere in the users list, select **Apply template** from the context menu.
4. Click  icon to the right of the template name.

Managing templates

To delete a template:

1. Expand the server in the left pane and click **Users**.
2. Right-click anywhere in the users list, select **Apply template** from the context menu.
3. Click  icon to the right of the template name.
4. Confirm the template removal.

> WARNING:
>
> **Deleted templates cannot be restored.**

Editing a user

> IMPORTANT:
>
> If you change the login or password, the user is immediately disconnected from the server. Only do it during non-working hours!

To change the user's settings:

1. Expand the server in the left pane and click **Users**.
2. Select a user from the list.
3. Click  icon in the toolbar. A sidebar with user settings opens.
4. Modify user properties.
5. Click **Save**.

> NOTE:
>
> User ID and a server cannot be changed.

To change settings of multiple users at once:

1. Expand the server in the left pane and click **Users**.
2. Select users from the list.
3. Click  icon in the toolbar. A sidebar with user settings opens.
4. Revise the list of users you want to apply new settings to under **Users**.
5. If you want to update users' passwords, provide the auto-generated password mask under **Password**. To keep individual passwords unchanged, do not modify this field.
   NOTE: Password complexity requirements are defined by T.Lion server policies. Make sure auto-generated passwords meet them.
   - **Prefix** string is prepended to the auto-generated number (starting from *1*). To generate a random string of the required length, click  icon in this field.
   - **Postfix** string is appended to the auto-generated number (starting from *1*).
6. Modify user properties.
   To apply the identical setting (regardless of whether it was changed or not) to *all* selected users, select a checkbox to the left of the option name. You can apply the configuration of entire option groups in the same manner.
7. Click **Save**.

Generating QR code

The users can sign in to T.Flex with QR codes as an alternative to providing login and password. To generate QR codes for users:

1. Expand the server in the left pane and click **Users**.
2. Select one or more users from the list.
3. Click  icon in the toolbar.

4. Provide a new password for users. This password replaces the existing user's password.
   NOTE: Password complexity requirements are defined by T.Lion server policies.
   - To set a common password for all selected users, select **The same password** and type in the password in **New password** field.
   - To auto-generate passwords, select **Use template** . This option is only available when you select multiple users.
     a. Specify the starting index to be used for auto-generated passwords in **Start from** field. This number is incremented by 1 for each user.
     b. **Prefix** string is prepended to auto-generated passwords based on **Start from** field.
     c. **Postfix** string is appended to auto-generated password based on **Start from** field.
   - Select **Use unique** and type in an individual password for every user.
     This option is only available when you select multiple users.
5. Click **OK**.
6. T.Commander generates QR codes for each selected user. To save all QR codes locally, click **Save** in **Generated QR codes** popup.
7. Choose whether you want to save all codes as a single PDF file (**All QR codes in one file**) or as a ZIP archive with individual PDF files for each user (**Each QR code as a separate file**).
8. In addition to QR codes in PDF format, you can save configuration files with connection parameters. These files can be imported to end-user devices, allowing them to automatically sign in without setting up a connection or providing access credentials. This can be very useful for devices without a screen or camera.
   To save configuration files along with QR codes, select **Include configuration files with connection parameters** option.
   NOTE: A separate configuration file is created for each user, even if you save all QR codes as one file. The files are named *\.usr*.

If the user's password does not meet the policy, a broken QR code is generated:

You should generate a new code for that user.

IMPORTANT:

- If you update QR code, the user is immediately disconnected from the server. Only do it during non-working hours!
- If you change the login or password, the existing QR code is deactivated and cannot be used for signing in. You should generate a new code after that.

Guest access

You can grant the user time-limited access to T.Mugen web client. No credentials are required - the user simply opens the provided URL in a web browser and communicates with other users on TASSTA network. When the link expires, access is automatically lost. This can be useful for temporarily adding volunteers, contractors, or external consultants to your team.

To allow guest access for a user:

1. Create a user or select the existing one.
2. Click  icon in the toolbar.
3. Specify **access expiry date** and **time**.
4. Click **Save** button to generate the guest access link.
5. Click **Click here to copy a guest access link** to copy the URL to the clipboard.
6. Send the link to the user.

> NOTE:
>
> If prompted, update the user's password.

If the access link is lost:

1. Select the user.
2. Click  icon in the toolbar.
3. Click **Click here to copy a guest access link** to copy the URL to the clipboard.

To renew the access link or change its duration:

1. Select the user.
2. Click  icon in the toolbar.
3. Specify new **access expiry date** and **time** (maximum 1 week from now).
4. Click **Save** button to generate the new access link.
5. Click **Click here to copy a guest access link** to copy the URL to the clipboard.

> IMPORTANT:
>
> The existing access link is automatically revoked and can no longer be used.

Editing lone worker protection settings

A new lone worker profile is automatically created when you add a user. To edit lone worker protection settings:

1. Expand the server in the left pane and click **Users**.

2. Select one or more users from the list.
3. Click  icon in the toolbar.
4. Configure lone worker profile.

Checking effective privileges

To check the resulting user's privileges based on all active rules:

1. Expand the server in the left pane and click **Users**.
2. Select a user from the list.
3. Click  icon in the toolbar.

You get the list of channels with effective privileges represented with icons:

- To enter and view a channel: 
- To listen to a channel: 
- To speak in a channel: 
- To move another user to a channel: 

Grey icon means the corresponding privilege is not defined by any rules. Such privileges are granted by default.

Green icon means the corresponding privilege is granted.

Red icon means the corresponding privilege is denied.

To get detailed information on the rules which define effective privileges for the channel, click the channel name in the popup. You can disable or edit a rule by clicking its name and selecting the corresponding option from the dropdown.

Creating a rule

To quickly define a rule for a group of users:

1. Expand the server in the left pane and click **Users**.
2. Select one or more users from the list.
3. Click  icon in the toolbar.
4. Provide a name of the access team in **Team name** field.
5. Select a channel to define the rule for.
6. Click **Create new**.
7. Proceed with the rule creation.

This operation automatically creates the team with all selected users and adds a rule for it, without having to do those operations separately.

User role assignment

To assign a role to one or more users:

1. Expand the server in the left pane and click **Users**.
2. Select one or more users from the list.
3. Click  icon in the toolbar.
4. Select a role from the popup and click **Save** button.

> NOTE:
>
> You can only assign one role to a user.

Current user roles are shown in **Assigned roles** column of the users list.

Deleting a user

> WARNING:
>
> - Deleted users cannot be restored. It is recommended to save user's settings as a template before deleting it.
> - Deleted users are immediately disconnected from the server.

To delete users from the server:

1. Expand the server in the left pane and click **Users**.
2. Select one or more users from the list.
3. Click  icon in the toolbar.
4. Confirm the removal of the selected users.

User properties

T.Commander provides a number of configuration options that you can set for the user. To simplify navigation, options are organized in logical groups.

- Main
- Client type
- Codec

- Common calls
- Data calls and messaging
- Emergency
- Group calls
- Guard tours
- History
- Individual calls
- Lone worker protection
- Map and tracking
- Miscellaneous
- Remote control
- User authentication
- Video

Most of the options can be left at the default value. However, certain features of TASSTA network require customizing corresponding settings.

> NOTE:
>
> The availability of certain options depends on the server settings. Check an option description for details.

Main

Core properties of the user.

- Name (required)
  Set user login. IMPORTANT: Usernames `cpoint<number>` (for example, `cpoint20`) are reserved for the T.Qonnector service. You cannot create users with these names.
- Password (required)
  Set password for the user. Password complexity requirements are defined by T.Lion server policies.
- Server (automatically assigned)
  Current server.
- ID (automatically generated)
  Unique ID of the user.

Client type

- Allow SDK
  Enable the user to programmatically interact with T.Lion server through TASSTA SDK.
  NOTE: Set a non-zero value for **Maximum online SDK clients** in the server settings to enable SDK access.
- Log in as dispatcher
  Allow the user to log into desktop and web clients with dispatcher rights.
  NOTE: Set a non-zero value for **Maximum Rodon Smart clients** in the server settings to enable dispatcher's access.
- Allow teams management
  Allow the user to create, edit and remove teams, as well as manage their participants.

Codec

A collection of settings to control the behaviour of a media encoding.

> IMPORTANT:
>
> The default settings provide good results for the most use cases. Contact TASSTA support if you encounter problems with media encoding.

- Variable bitrate
  Switch between variable bitrate (enabled) and constant bitrate (disabled). Default value: *variable bitrate*.
- Forward error correction
  Turn on forward error correction. Default value: forward error correction is *enabled*.
- Bitrate (bit/s)
  Set the bitrate for encoded media stream, from *6,000 bps* to *510,000 bps*. A higher bitrate improves the media quality at the cost of increasing network traffic. Default value: *10000 bps*.
- Packet loss (percent)
  Define acceptable percentage of packet loss. Default value: *20%*.
- Complexity
  Set media encoding complexity. Varies from *0* (low quality, least CPU utilization) to *10* (best quality, highest CPU utilization). Default value: *auto (-1)*.

Common calls

Generic call settings.

- Mute button
  Allow the user to temporary mute communications in T.Flex and T.Rodon.
- Disable PTT
  Completely disable push-to-talk (PTT) functionality in T.Flex.

  - *Enable*: Turn off PTT. Hardware PTT buttons are also disabled.
  - *Disable*: PTT is allowed (default).
- End-to-end encryption (disabled by default)
  Allow the user to activate end-to-end encryption.
  NOTE: Turn on **End-to-end encryption** in the server settings to configure this option. Make sure you have also provided the total number of clients allowed to use end-to-end encryption in **Maximum end-to-end encryption clients**.
  If you turn off **End-to-end encryption** in the server settings, the encryption is disabled for all users.
- Priority (default is 0)
  Set the user's relative priority (any number from 0 to 9,999). Use higher or lower numbers to increase or decrease the priority level correspondingly. See **User's priority** below for details.
  NOTE: Turn on **Priority** in the server settings to configure this option.
  If you turn off **Priority** in the server settings, the users' priorities are ignored.
- Broadcast calls
  Allow the user to make broadcast calls.
- Listen to multiple channels simultaneously from Rodon
  Allow the user to hear several channels at once in T.Rodon.
- Channel name on PTT button
  Show the last channel name on PTT button.
- On-screen PTT button toggle
  Switch the activation mode of PTT in T.Flex. This option only affects on-screen PTT button, hardware PTT buttons will work as usual.
  - *Enable*: Press on-screen PTT button once to start transmitting and then once again to stop transmission.
  - *Disable*: Press and hold on-screen PTT button as you speak. When you release the button, transmission stops.
- Disable on-screen PTT button
  - *Enable*: Disable on-screen PTT button in T.Flex. Hardware PTT buttons will work as usual.
  - *Disable*: On-screen PTT button is operational (default).
- Full-duplex calls
  Allow the user to make full-duplex calls in T.Flex for Android.
- Do not auto-close channels with members
  Prevent automatic closing of push-to-video and full-duplex call channels, even if the user is the last participant on the call, regardless of whether it was a call originator or a receiving party.
  This setting is required for simultaneous monitoring of multiple PTV calls from T.Rodon. It prevents automatic termination of PTV calls when the dispatcher switches to another call.

User's priority

The setting affects user's priority in group and one-to-one calls.

- A user with higher priority can get through group calls with important information, even if another user with a lower priority is currently talking.
- A user with higher priority cannot be muted by users with lower priority.
- A user with higher priority can interrupt individual calls of users with lower priority according to the following rules:
  - If the user's priority is higher than the priority of all users in the ongoing individual call, he/she takes the floor and may speak.
  - If a user's priority is lower than or equal to the priority of any of the users in an individual call, the ongoing individual call is not affected.

Data calls and messaging

Various settings related to messaging.

- Task Manager (disabled by default)
  Enable Task Manager functionality for the user.
  NOTE: Turn on Task Manager in the server settings to configure this option. Make sure you have also adjusted the related options in the server settings.
  If you turn off Task Manager in the server settings, the Task Manager is disabled for all users.
- Messaging
  Allow the user to send and receive messages.
- Share device info
  Allow the user to share device status information: signal level, remaining charge and so on.
- Email settings for MCGW
  Configure user-specific communication bridging via email messages.
  - Receive settings
    - Email address
      Provide email address for incoming messages.
  - Send settings
    - Address
      Provide outgoing email address.
    - Username
      Provide mail server login.
    - Password
      Provide mail server password.
    - SMTP server
      Provide SMTP server name or IP address.
    - SMTP port
      Provide SMTP server port number.

- Prefer user's email settings
  Override the server's communication bridging configuration with the user's settings defined in MCGW Configuration.
- SMS number
  Provide the user's phone number for receiving SMS messages.
- Continuous message alarm
  Turn on continuous notification tone for incoming messages.
- Message history capacity
  Define the maximum number of message history entries shown to the user, from 1 to 100,000.The actual number of records kept on the server may exceed this value.
- Message history retention
  Specify how far back in time (floating window) the message history is shown to the user. Older messages are kept on the server, but not shown.
  This setting can be configured with 30 minutes accuracy. The maximum value cannot exceed *90 days*.
- Missed call notification
  Set the duration of a missed call notification.
- Allow client delete own messages
  Allow mobile (T.Flex) users to delete their own messages from chats.
- Allow the dispatcher to delete messages
  Allow dispatchers (T.Rodon users) to delete their own messages from chats.
- Clear chats on switching channels or logging out
  Automatically clears the group chat history for the user when the user leaves the channel or logs out. The user can only see messages that arrive after joining the group - unless the multi-listening is enabled for that group. If multi-listening is enabled, the user can still see all of the messages for the group.
  If the connection is lost and then automatically, the history is not cleared.
  NOTE: Individual chats and recorded activity history are not affected.

Emergency

Emergency call settings.

- Make emergency calls
  Allow the user to make emergency calls.
- Prevent emergency cancellation
  Prevents the user from cancelling emergency calls.
  NOTE: Cancelling an emergency call requires dispatcher's approval.
- Emergency countdown (seconds)
  Set the countdown (in seconds) before initiating an emergency call in T.Flex. The emergency can be cancelled during that period.

- Receive emergency calls
  Allow the user to receive incoming emergency calls and notifications.
  - Receive Emergency Call (current channel only)
    The user only receives emergency calls from members of the channel where he/she is in. Emergency calls from other channels are ignored.
    This option is only available when Receive Emergency Call is enabled.
- Lost connection signal
  Determine how the user is notified when the server connection is lost.
  - *No not notify*: disable disconnect notifications.
  - *Audio alert*: play a notification sound.
  - *Voice notification*: read the notification aloud. Text-to-speech must be enabled and configured on the user's device.
  - *Audio alert with voice notification*: play notification sound and read the notification aloud. Text-to-speech must be enabled and configured on the user's device.
- Maximize sound volume for notifications
  Increase the sound volume to maximum when an emergency call is initiated or received in T.Flex. Overrides the current volume settings on a device.
- Acknowledge emergencies
  Force the user to manually acknowledge every emergency call before performing any other operation in T.Rodon.
- Emergency popup
  Show a popup in T.Rodon when an emergency call is received from another user. The current user must close the popup by pressing Acknowledge or Show on map button before performing any other operation in T.Rodon.
- Mute outgoing emergency
  Do not play notification sound when the user initiates an emergency.
  NOTE: Turning this setting off automatically disables Covert emergency.
- Incremental sound
  Gradually increase the sound volume for "Everything fine?" notification in T.Flex. Overrides the current volume settings on a device.
- Emergency PTT timeout (seconds)
  Set the number of seconds the user can talk after initiating an emergency call, as if PTT button is pressed. Once this timeout expires, the user should press PTT button to continue talking.
  NOTE: Setting this option to *0* allows the user to talk indefinitely without pressing PTT button until the emergency call is cancelled.
- Prevent emergency calls auto-listening
  - *Enabled*: The user does not hear emergency calls automatically. The user can still manually listen to the emergency channels.
  - *Disabled*: The user automatically hears all emergency calls.

- Release emergency calls from Flex
  Allow the user to release emergency calls from T.Flex.
- Fullscreen emergency notification
  Show fullscreen notification in T.Flex when receiving emergency call.
- Pre-alarm timer alert
  Set the notification mode for emergency pre-alarm timer in T.Flex:
  - *Silent*: no sound.
  - *Vibration*: vibration without sound. Only works for devices that support vibration.
  - *Sound*: play notification sound.
  - *Sound with vibration*: continuous notification sound accompanied by vibration.
- Incoming emergency notification
  Set the notification mode for incoming emergency calls in T.Flex.
  - *Silent*: no sound.
  - *Vibration*: vibration without sound. Only works for devices that support vibration.
  - *Beep 3 times*: 3 short beeps.
  - *Beep 3 times with vibration*: 3 short beeps accompanied by vibration.
  - *Continuous sound*: continuous beeps until the call is answered or rejected.
  - *Continuous vibration* until the call is answered or rejected.
  - *Continuous sound with vibration*: continuous beeps accompanied by vibration until the call is answered or rejected.
- Continuous alert on lost connection
  Enable a continuous audio notification in T.Flex when the connection to the server is lost.
  IMPORTANT: If Lost connection signal is set to *Do not notify*, audio notifications will not be played, even if this setting is enabled.
- Outgoing emergency alert
  Set the notification mode for outgoing emergency calls in T.Flex.
  - *Silent*: no sound.
  - *Vibration*: vibration without sound. Only works for devices that support vibration.
  - *Beep 3 times*: 3 short beeps.
  - *Beep 3 times with vibration*: 3 short beeps accompanied by vibration.
  - *Continuous sound*: continuous beeps until the call is answered or rejected.
  - *Continuous vibration* until the call is answered or rejected.
  - *Continuous sound with vibration*: continuous beeps accompanied by vibration until the call is answered or rejected.
- SOS key delay time (seconds)
  Specify the number of seconds the hardware SOS key should be held down before the emergency

countdown begins. 3-5 seconds delay prevents an emergency from being triggered when SOS key is accidentally pressed.

- Covert emergency
  Disables visual or audible indications for the user who initiates an audio or video emergency call. This affects manually initiated emergency calls, as well as emergency calls that are automatically started when a certain condition is met (for example, when a periodic lone worker check is ignored).
  The setting does not mute incoming audio from other users and does not affect emergency notifications on other users' devices.
  NOTE: When covert emergency is turned on, Mute outgoing emergency setting is automatically enabled.
- Vibrate on covert emergency
  Vibrate the user's device to notify when the covert emergency is activated.
  IMPORTANT: Vibration can be noticed by a criminal / suspect.

Group calls

Group call settings.

- Show channels
  Show the list of channels for T.Flex user.
- Default channel
  Select a channel that the user automatically joins after signing in.
- Listen to multiple channels simultaneously from Flex
  Allow the user to hear several channels at once in T.Flex.
- Play channel join sound upon connect
  Enable channel joining sound upon logging in or reconnecting.
- Listen to channels
  Specify the list of channels the user can listen to in T.Flex. This setting is useful for centralized management of mobile clients and for configuring radios without screen.

IMPORTANT:

- As long as the list of listened channels is configured, the user cannot change the list of channels he/she listens to from T.Flex.
- If a channel is added to the list of listened channels, the user will be able to listen to it, even if rules prohibit entry or listening. However, under these conditions, the user will not receive emergency calls if rules inheritance is enabled.

Guard tours

- Guard tours
  Enable guard tour functionality for the user.

- Allow Guard Tour Management
  Allow the user to create, edit and remove patrols.

History

Activity history tracking for the user.

- Show activity history
  Allow the user to access activity history from T.Flex and T.Rodon.
- History capacity (default is 100)
  Set the maximum number of records to show in history.
  NOTE: Turn on History Replay in the server settings to configure this option.
- Recording retention (unlimited by default)
  Specify the maxumum period of time call recordings are available for the user. Older recordings are kept on the server, but are only accessible with T.Recorder.
  Set the value to *0* to allow unlimited access to recordings.
  NOTE: Turn on History Replay in the server settings to configure this option.
- Use rules for activity history access control (disabled by default)
  Show activity history according to the active channel's rules.
  NOTE: Turn on History Replay in the server settings to configure this option.

Individual calls

Individual call settings.

- Show users
  Allow the user to access a list of users in T.Flex.
- Individual calls (disabled by default)
  Allow the user to make one-to-one calls to other users.
  NOTE: Turn on Individual calls in the server settings to configure this option.
  If you turn off Individual calls in the server settings, the users cannot make one-to-one calls.
  - Direct individual calls (disabled by default)
    Allow the user to make direct calls to other users. Direct calls are connected automatically, without confirmation from the person on the other end.
    NOTE: This option is only available if individual calls are enabled for the user.
- Inactivity timeout (seconds) (disabled by default)
  Set the inactivity timeout (in seconds) for individual calls. If no communication is detected within this time period, the individual call is automatically ended.
  NOTE: Use *0* to turn off the inactivity timeout and keep the call active until the user manually ends it.
- Direct call with PTT button
  Allow the user to initiate direct calls by pressing PTT button.

Lone worker protection

Lone worker protection settings.

> NOTE:
>
> Turn on **Lone worker protection** in the server settings to configure these options.
> If you turn off **Lone worker protection** in the server settings, lone worker protection is disabled for all users.

- **Lone worker protection** (disabled by default)
  Allow lone worker protection for the user.
- **Allow Emergency Journal** (disabled by default)
  Allow the user to work with Emergency Journal.
- **Continuous alert when dispatcher is offline** (disabled by default)
  Play a continuous audio notification in T.Flex when a dispatcher is unavailable.

Map and tracking

Geolocation and indoor positioning settings.

Geolocation

> NOTE:
>
> Turn on **Map** in the server settings to configure geolocation options.
> If you turn off **Map** in the server settings, access to maps is disabled for all users.

- **Map** (disabled by default)
  Allow the user to access a map in T.Flex and T.Rodon.
- **Maximum zoom level** (18 by default)
  Set the maximum zoom level for the map, from 1 to 22.
- **Geodata provider**
  Choose the geodata provider to be used for map and navigation. The following providers are supported:
  - Mapbox;
  - OpenStreetMap or Apple Maps (the latter only applies to iOS devices);
  - Google Maps.
- **Share location** (disabled by default)
  Send information about the user's location to the server.
- **Location sharing interval (seconds)** (default is every 30 seconds)
  Define an interval (in seconds) for periodically refreshing the user's position on a server. Lower

value improves the map accuracy, but slightly increases the network traffic.
NOTE: A location sharing interval of less than **10 seconds** greatly increases the traffic and server load, and may not be supported on all mobile devices. Do not use 1-9 second interval unless it is critical to tracking specific fast moving users.

- **Map Tools editor** (disabled by default)
  Allow the user edit data in T.Rodon Map Tool.
- **Share location upon PTT** (disabled by default)
  Always send information about the user's location to the server while the user pushes/holds PTT button in T.Flex.
- **Use local map server** (disabled by default)
  Allow for using the local server as a map tiles source.
- **Location clustering distance**
  Define a distance (in meters) for clustering locations of neighboring users into a single point on the map. If this value is set to `0`, the user is always displayed separately from others.
- **Focus map on PTT** (enabled by default)
  Enable this option to automatically center the map to the speaker's position.
- **Focus map on PTT settlement period**
  Timeout (in seconds) after which the map will be re-centered to the other speaker's position. Increase this value to avoid abrupt map switching between speakers; decrease it to improve the reaction time.
  NOTE: Only applicable when **Focus map on PTT** is enabled.

Indoor positioning

> NOTE:
>
> Enable **Indoor Localization** in the server settings to configure indoor positioning options.
> If you turn off **Indoor Localization** in the server settings, indoor positioning is disabled for all users.

- **Indoor localization**
  Allow indoor positioning for the user.
- **Share indoor position**
  Send information about the user's indoor position to the server.
- **Use GPS for indoor**
  Try calculating user's indoor position based on GPS data when the user's device is out of range of beacons / anchor nodes. Only works if GPS provides the acceptable accuracy (see **Indoor GPS accuracy threshold (meters)** below).
- **Indoor GPS accuracy threshold (meters)**
  This value determines the moment when the positioning is switched from indoor beacons to GPS if **GPS priority for indoor** is enabled. Once GPS provides better (smaller) accuracy, the positioning algorithm ignores beacon signals and starts using GPS coordinates.
  Lower values provide more accurate positioning, but may cause the system not switching to GPS if

buildings, bridges or terrain are obstructing signals. Higher values may cause the incorrect position detection when GPS data is inaccurate.

- Indoor localization permissions
  This setting works in alternate modes depending on whether internal localization artificial intelligence (AI) is enabled or disabled:
  - Indoor localization AI is active (Resolve position based on fixed beacons server setting is turned off).
    - Select *User* to ignore the user's activities when training the indoor localization AI.
    - Select *Deployer*, *Maintainer* or *Supervisor* to collect and analyze the user's activities for training indoor localization AI.
  - Indoor localization AI is disabled (Resolve position based on fixed beacons server setting is turned on).
    Determine whether the user can manage, place and maintain beacons. Possible values:
    - *User* - the user can access beacon data, but cannot manipulate beacons.
    - *Deployer* - the user can install (activate) beacons at designated locations.
    - *Maintainer* - the user can install, relocate, manage, and remove beacons.
    - *Supervisor* - the user can import beacons into a database and plan beacons' placements on the map.
- Bluetooth beacons type
  Set the type / format of Bluetooth beacons to be used for indoor positioning. Only applicable if Bluetooth beacons are enabled in IL Mode server setting.
  - *All / MAC Address* (default)
  - *iBeacon / UUID*
- Infsoft indoor localization
  Use indoor positioning provided by infsoft GmbH instead of the native TASSTA solution. Requires Infsoft indoor localization key to be specified in server setting.

  NOTE: Activating infsoft indoor positioning automatically switches the user to *Mapbox* geodata provider.

Location privacy

- Location privacy Show or hide the user's location from other users. This setting applies to both GPS and indoor positioning.
  - *Enable.* Only show the user's location during emergency calls. Otherwise, the user is not displayed on the map.
  - *Disable.* Always show the user's location.

If you enable Share location and / or Share indoor position, the user's location is always sent to the server, regardless of the privacy setting. This setting only determines whether to display the user on the map.

> NOTE:
>
> TASSTA SDK always receives location data for all users, regardless of their privacy settings. Data privacy should me maintained by the custom application logic.

Miscellaneous

Miscellaneous user settings.

- Comment
  Provide a verbose description for the user.
- Last channel
  Name of the last channel the user has accessed. This is a read-only field for information purposes.
- Network usage
  Allow the user to access network usage statistics in T.Flex.
- Show features
  Allow the user to check features availability in T.Flex.
- Self-manage settings
  Allow the user to self-manage T.Flex settings:
  - *Allowed all*: Allow changing all settings.
  - *You are only allowed to modify credentials*: Only allow to log in using any username and password.
  - *Block access to settings and prevent URLs to be opened from Flex*: Prevent the user from changing settings and do not open web links when the user taps an URL in T.Flex. This setting prevents the user from switching to another app by tapping the Privacy Policy or another element that opens the URL in the default browser.
  - *Allow to change credentials and to pair Bluetooth devices*: Allow the user to log in using any username and password and to pair wireless headsets and other Bluetooth devices.
  - *Allow pairing of Bluetooth devices*: Allow the user to pair wireless headsets and other Bluetooth devices.
  - *Changing the settings is not allowed*: Prevent the user from changing settings.
- Flex home screen
  T.Flex automatically switches to the selected screen after the user signs in.
  - *PTT screen* - full-screen push-to-talk button.
  - *Shortcut view* - My TASSTA view. Selecting this option automatically enables Shortcut view.
  - *User list* - the list of users.
  - *Group list* - the list of channels.

  - *Map* - map view.
    IMPORTANT: Map must be enabled in server settings and allowed for the user. Otherwise, the user will be automatically redirected to *PTT screen*.

- Shortcut view
  Enable My TASSTA view in T.Flex.
- Home screen on channel selection
  Automatically redirect the user to home screen after selecting a channel.
- Use Apple Push Notification Service
  Send push notifications from T.Lion server to T.Flex iOS through Apple.
- Sound scheme (Android)
  Set the sound scheme for T.Flex Android client app. IMPORTANT: This setting does not apply to T.Flex iOS and T.Rodon.
- Text-to-speech
  Enable text-to-speech conversion in T.Flex. Text-to-speech service must be enabled and configured on the user's device.
- Connection quality
  Show the connection quality indicator in T.Flex.
- Share detailed app statistics
  Allow for collecting and sharing detailed logs in client applications.
- Favorite PTT view
  Show Favorite PTT screen in T.Rodon.
- Manage Favorites configuration on server
  - *Disabled*: The contents of My TASSTA screen in in T.Flex and Favorite PTT plugin in T.Rodon can be customized by the user from the client application.
    If a user logs into the client application from a another device, he/she will have to reconfigure the favorites from scratch.
  - *Enabled*: The user is not allowed to change the contents of My TASSTA screen in in T.Flex and Favorite PTT plugin in T.Rodon.
    When the setting is turned on, all tiles, their settings and layout are saved on the server. The user will see the same favorites no matter what device he/she is logged in.
- Rodon Favorite PTT configuration
  The contents of Favorite PTT plugin in T.Rodon. This field is automatically updated when the user changes the tiles in T.Rodon and is used when Manage Favorites configuration on server is enabled.
  HINT: See Managing favorites for usage example.
- Flex Android My TASSTA configuration
  The contents of My TASSTA screen in in T.Flex Android. This field is automatically updated when the user changes the tiles in T.Flex app and is used when Manage Favorites configuration on server is enabled.
  HINT: See Managing favorites for usage example.

- Flex iOS My TASSTA configuration
  The contents of My TASSTA screen in in T.Flex iOS. This field is automatically updated when the user changes the tiles in T.Flex app and is used when Manage Favorites configuration on server is enabled.
  HINT: See Managing favorites for usage example.
- Auto-mute Flex on external calls
  Enable this feature to automatically mute voice and notifications in T.Flex, except for emergency, if there is an active call in another communication app. If this setting is disabled, T.Flex will always play all sounds.
- Mute button in Flex
  Allow the user to add and use Mute button on the T.Flex shortcut screen.
- Mute interval
  Set the number of seconds for muting the sound when the user taps the Mute button on an T.Flex shortcut screen.
- Mute button notification
  Set the notification mode when the user taps Mute button on the T.Flex shortcut screen.
  - *None*: no notification.
  - *Audio*: play a notification sound.
  - *Vibration*: vibration without sound. Only works for devices that support vibration.
  - *Audio and vibration*: play a notification sound accompanied by vibration.

Remote control

Remote control settings.

- Imprint metadata in camera snapshots
  Append a timestamp and geolocation coordinates to the remotely captured photos.
- Remote control privacy
  Configure remote control privacy for the user.
  - *Enable*: only allow remote audio listening and remote camera access during emergency calls.
  - *Disable*: allow remote audio listening and remote camera access.

> NOTE:
>
> Turn on Remote Control in the server settings to configure the below listed options.
> If you turn off Remote Control in the server settings, remote listening is disabled for all users.

Monitored user

- Ambient sound sharing (disabled by default)
  Enable remote audio listening for the user's device.

- Notify on remote listening (disabled by default)
  Show a notification to the user when remote audio listening is activated on his/her device. Disable this option to activate remote audio listening without notifying the user.
- Share camera snapshots (disabled by default)
  Enable remotely taking photograph from the user's camera.
- Remote video sharing (disabled by default)
  Enable remotely capturing video from the user's camera.
- Remote video quality
  Set the quality of remotely captured video:
  - *Profile*: select one of the predefined video quality profiles:
    - *Low*: guarantees an uninterrupted video for a large number of simultaneous video streams or a low-performance hardware;
    - *Optimal*: default setting;
    - *High*: guarantees an uninterrupted video for a small number of simultaneous video streams or a high-end hardware;
    - *Custom*: fine-tune individual settings.
  - *Resolution*: choose the video resolution:
    - *320*: 320x240 pixels;
    - *720*: 720x480 pixels;
    - *1280*: 1280x720 pixels (720p).
  - *Framerate*: choose the frame rate (frames per second).
  - *Bitrate*: choose the bit rate (kilobits per second).
  - *Use front camera by default*: turn on to use a front-facing camera as a default video source.
  - *Display video info*: show an overlay with video parameters.
  - *Avoid mirroring front camera*:
    - *Enabled*: turn off "mirror reflection" effect for the front-facing camera;
    - *Disabled*: use the image from the front-facing camera as provided by the device.
- Notify on remote camera access (disabled by default)
  Show a notification to the user when someone remotely accesses the camera on his/her device. Disable this option to activate remote camera access without notifying the user.

Observer

- Ambient listener (disabled by default)
  Allow the user to remotely listen to the other's device surroundings.
- Take camera snapshots remotely (disabled by default)
  Allow the user to remotely take photographs from the other's camera.

- Remote video monitoring (disabled by default)
  Allow the user to remotely capture video from the other's camera.

User authentication

User identity management.

- Alias
  Provide the alternative name for the user.
  NOTE: You can assign the same alias to multiple users, and then use it to quickly select multiple users in client applications. Refer to the corresponding client documentation for details.
- Lock user to device
  Prevent the user from signing in with the other device by binding it to the device ID (such as IMEI).
- Device ID
  Provide the device ID (such as IMEI) for locking the user to the certain device.
- Logout with password
  Request the user to provide logout password for signing out from T.Flex.
- Logout password
  Provide the password for signing out from T.Flex when logout lock is active.
- Use external user's ID
  Substitute the user's ID with the external user's ID for custom clients based on TASSTA SDK.
- External user's ID
  Provide the external user's ID for Use External User Id option. You can use any number of any characters except for the white space.

Video

Video call settings.

- Video Calls
  Allow the user to make one-to-one video calls to other users.
- Push-to-video
  Allow the user to make push-to-video calls.
- Video emergency
  Allow the user to use video in emergency calls.
- Push-to-video quality
  Set the quality of push-to-video calls:
  - *Profile*: select one of the predefined video quality profiles:
    - *Low*: guarantees an uninterrupted video for a large number of simultaneous video calls or a low-performance hardware;
    - *Optimal*: default setting;

    - *High*: guarantees an uninterrupted video for a small number of simultaneous push-to-video calls or a high-end hardware;
    - *Custom*: tune individual settings. See Important considerations below.
  - *Resolution*: choose the video resolution:
    - *320*: 320x240 pixels;
    - *720*: 720x480 pixels;
    - *1280*: 1280x720 pixels (720p).
  - *Framerate*: choose the frame rate (frames per second).
  - *Bitrate*: choose the bit rate (kilobits per second).
  - *Use front camera by default*: turn on to use a front-facing camera as a default video source.
  - *Display video info*: show an overlay with video parameters.
  - *Avoid mirroring front camera*:
    - *Enabled*: turn off "mirror reflection" effect for the front-facing camera;
    - *Disabled*: use the image from the front-facing camera as provided by the device.
- Video calls quality
  Set the quality of one-to-one video calls:
  - *Profile*: select one of the predefined video quality profiles:
    - *Low*: guarantees an uninterrupted video for a large number of simultaneous video calls or a low-performance hardware;
    - *Optimal*: default setting;
    - *High*: guarantees an uninterrupted video for a small number of simultaneous push-to-video calls or a high-end hardware;
    - *Custom*: fine-tune individual settings. See Important considerations below.
  - *Resolution*: choose the video resolution:
    - *320*: 320x240 pixels
    - *720*: 720x480 pixels
    - *1280*: 1280x720 pixels (720p)
  - *Framerate*: choose the frame rate (frames per second).
  - *Bitrate*: choose the bit rate (kilobits per second).
  - *Use front camera by default*: turn on to use a front-facing camera as a default video source.
  - *Display video info*: show an overlay with video parameters.
  - *Avoid mirroring front camera*:
    - *Enabled*: turn off "mirror reflection" effect for the front-facing camera.
    - *Disabled*: use the image from the front-facing camera as provided by the device.

- Emergency video quality
  Set the quality of emergency video calls:
  - *Profile*: select one of the predefined video quality profiles:
    - *Low*: guarantees an uninterrupted video for a large number of simultaneous video calls or a a low-performance hardware;
    - *Optimal*: default setting;
    - *High*: guarantees an uninterrupted video for a small number of simultaneous push-to-video calls or a high-end hardware;
    - *Custom*: tune individual settings. See Important considerations below.
  - *Resolution*: choose the video resolution:
    - *320*: 320x240 pixels;
    - *720*: 720x480 pixels;
    - *1280*: 1280x720 pixels (720p).
  - *Framerate*: choose the frame rate (frames per second).
  - *Bitrate*: choose the bit rate (kilobits per second).
  - *Use front camera by default*: turn on to use a front-facing camera as a default video source.
  - *Display video info*: show an overlay with video parameters.
  - *Avoid mirroring front camera*:
    - *Enabled*: turn off "mirror reflection" effect for the front-facing camera;
    - *Disabled*: use the image from the front-facing camera as provided by the device.
- Video streams
  Allow the user to initiate video calls with optional participants. Participants are notified and can join the call at any time.
- Video streams quality
  Set the quality of video streams:
  - *Profile*: select one of the predefined video quality profiles:
    - *Low*: guarantees an uninterrupted video for a large number of simultaneous video calls or a a low-performance hardware;
    - *Optimal*: default setting;
    - *High*: guarantees an uninterrupted video for a small number of simultaneous push-to-video calls or a high-end hardware;
    - *Custom*: tune individual settings. See Important considerations below.
  - *Resolution*: choose the video resolution:
    - *320*: 320x240 pixels;
    - *720*: 720x480 pixels;

    - *1280*: 1280x720 pixels (720p).
  - *Framerate*: choose the frame rate (frames per second).
  - *Bitrate*: choose the bit rate (kilobits per second).
  - *Use front camera by default*: turn on to use a front-facing camera as a default video source.
  - *Display video info*: show an overlay with video parameters.
  - *Avoid mirroring front camera*:
    - *Enabled*: turn off "mirror reflection" effect for the front-facing camera;
    - *Disabled*: use the image from the front-facing camera as provided by the device.
- Conference push-to-video calls
  Allow the user to initiate or participate in push-to-video communication when multiple users can press PTT button and speak at the same time.
  The quality of PTV conference calls is determined by the Push-to-video setting.

Important considerations

All predefined video profiles are configured for a low resolution (320x240 pixels) and a low bitrate to guarantee the smooth video streaming, even with poor connection quality or high server load.
To increase the resolution, select *custom* profile. We suggest using the following custom settings depending on your hardware performance, load and network quality:

- Average, suitable for most cases: video resolution 720x480 pixels, bitrate 1,500 kbps, 20 frames per second.
- Low, suitable for a large number of simultaneous video calls or a low-performance hardware: video resolution 320x240 pixels, bitrate 500 kbps, 10 frames per second.
- Best, suitable for a small number of simultaneous video calls or a high-end hardware: video resolution 1280x720 pixels, bitrate 3,000 kbps, 30 frames per second.

You can fine-tune the settings based on the specifics of your environment:

- Higher resolution requires greater processing power. Setting too high a resolution with insufficient processing power and / or too many simultaneous video calls can lead to interrupted / unstable video stream.
- Higher level of motion in your video requires a higher bitrate at the same resolution.
  For typical T.Flex usage scenarios, the actual bitrate will be around 20% of the provided value.
- Higher framerate greatly impacts the look and feel of a video, making it more smooth and realistic. However, high framerates use up quite a lot of bandwidth.

Channels

A channel is a virtual lobby that allows a group of users to communicate. It is similar to a portable radio frequency band.
To show and manage channels, expand a server in navigation pane and click **Channels**.

- To select a single channel, click it.
- To select multiple channels, select or clear the checkbox to the left of channel's name.

By default, the channel *Main* is automatically added when you create a server. The ID of this channel is always *0*.

> IMPORTANT:
>
> Adding or updating channels require restarting a server.

Adding a channel

> IMPORTANT:
>
> You should set non-zero **Maximum channels** parameter in server settings in order to add channels.

To add a new channel to the selected server:

1. Expand the server in the left pane and click **Channels**.
2. Click  icon in the toolbar. A sidebar with channel settings opens.
3. Provide a channel name in **Channel name** field.
4. Configure channel properties.
5. Click **Save**.
6. Restart the server.

> NOTE:
>
> Channel ID and server ID are assigned automatically.

Adding multiple channels

> IMPORTANT:
>
> You should set non-zero **Maximum channels** parameter in server settings in order to add channels.

To add several identical channels to the selected server:

1. Expand the server in the left pane and click **Channels**.
2. Click  icon in the toolbar. A sidebar with channel settings opens.
3. Specify the number of channels you want to create in **Amount** field.
4. Specify the starting index to be used for auto-generated channel names in **Start from** field. This number is incremented by 1 for each created channel.
5. Specify the optional channel name mask under **Channel name**.
   - **Prefix** string is prepended to the auto-generated number based on **Start from** field.
   - **Postfix** string is appended to the auto-generated number based on **Start from** field.
6. Configure channel properties.
7. Restart the server.

> NOTE:
>
> Unique ID is assigned automatically to each channel.

Editing a channel

To change channel settings:

1. Expand the server in the left pane and click **Channels**.
2. Select a channel from the list.
3. Click  icon in the toolbar. A sidebar with channel settings opens.
4. Modify channel properties.
5. Click **Save**.
6. Restart the server.

> NOTE:
>
> Channel ID and server ID cannot be changed.

To change settings of multiple channels at once:

1. Expand the server in the left pane and click **Channels**.
2. Select channels from the list.
3. Click  icon in the toolbar. A sidebar with channel settings opens.
4. Revise the list of channels you want to apply new settings to under **Channels**.
5. Modify channel properties.
   To apply the identical setting (regardless of whether it was changed or not) to *all* selected

channels, select a checkbox to the left of the option name. You can apply the configuration of entire option groups in the same manner.

6. Click **Save**.
7. Restart the server.

Updating channel's ID

> IMPORTANT:
>
> Changing the ID is only possible for newly created channels until the server is restarted. This limitation is imposed to mitigate potential issues with channel's history.

To change the ID of the existing channel:

1. Expand the server in the left pane and click **Channels**.
2. Select a channel from the list.
3. Click  icon in the toolbar.
4. Provide a new ID for the channel, from 1 to 2,147,483,647. The identifier should be unique across the entire server.
5. Click **Change ID**.
6. Restart the server.

> NOTES:
>
> - ID of the Main (default) channel is always `0` and cannot be changed.
> - When the channel is created, the system automatically assigns a unique ID to it. You cannot customize the channel ID upon creation.

Deleting a channel

> WARNING:
>
> **Deleted channels cannot be restored.**

To delete channels from the server:

1. Expand the server in the left pane and click **Channels**.
2. Select one or more channels from the list.
3. Click  icon in the toolbar.
4. Confirm the removal of the selected channels.

5. Restart the server.

> NOTE:
>
> The default channel (with ID equals to 0) cannot be deleted.

Organizing channels into zones

Zones are predefined groups of channels. They streamline the navigation by allowing users to work with a few relevant channels rather than searching for a channel in a long list.

To use zones, enable **Zones** in server settings.

To show and manage zones, expand a server in navigation pane and click **Zones**.

- To select a single zone, click it.
- To select multiple zones, select or clear the checkbox to the left of the zone name.

> IMPORTANT:
>
> Adding or updating zones require restarting a server.

Adding a zone

To add a new zone to the selected server:

1. Expand the server in the left pane and click **Zones**.
2. Click  icon in the toolbar. A sidebar with zone settings opens.
3. Provide a zone name in **Zone name** field.
4. Select channels to be included in the zone under **Channels**.
   TIP: You can add a channel to multiple zones.
5. Click **Save**.
6. Restart the server.

> NOTE:
>
> Zone ID and server ID are assigned automatically.

Editing a zone

To modify a zone:

1. Expand the server in the left pane and click **Zones**.
2. Select a zone from the list.

3. Click  icon in the toolbar. A sidebar with zone settings opens.
4. Rename the zone (**Zone name**) or revise the list of channels in it (**Channels**).
5. Click **Save**.
6. Restart the server.

> NOTE:
>
> Zone ID and server ID cannot be changed.

Deleting a zone

> WARNING:
>
> Deleted zones cannot be restored.
> To temporary hide all zones on a server without deleting them, turn off **Zones** in server settings.

To delete zones from the server:

1. Expand the server in the left pane and click **Zones**.
2. Select one or more zones from the list.
3. Click  icon in the toolbar.
4. Confirm the removal of the selected zones.
5. Restart the server.

Channel properties

T.Commander provides a number of configuration options that you can set for the channel. To simplify navigation, options are organized in logical groups.

- Main
- Miscellaneous

Most of the options can be left at the default value. However, certain features of TASSTA network require customizing corresponding settings.

> NOTE:
>
> The availability of certain options depends on the server settings. Check an option description for details.

Main

Core properties of the channel.

- Channel name (required)
  Provide display name for the channel.
- Server ID (automatically assigned)
  Current server.
- ID (automatically generated)
  Unique ID of the channel.

Miscellaneous

Miscellaneous channel settings.

- Channel maximum users quantity
  Highlight the channel in T.Rodon if the maximum number of channel members exceeds the provided value.
- Conference (disabled by default)
  Enable channel members to participate in conference calls. Conference participants can simultaneously press PTT button and speak rather than waiting until the current speaker releases the button.
  Note, that cross-server communication does not work with conference channels.
  NOTE: Turn on Transparent PTT in the server settings to configure this option.
- Inherit access control
  Inherit the rules defined for the *Main* channel. See Rules inheritance for more information.
  NOTE: This option is not available for the *Main* channel.
- Select channel to use PTT
  Automatically disable PTT button in a certain period of time after selecting a channel. The timeframe is defined in Channel selection timeout.
- Channel selection timeout (seconds)
  Set the timeout (in seconds) after which PTT button is automatically disabled in a channel. Only works if Select channel to use PTT is turned on.
  NOTE: If PTT button is pushed during this time frame, the timeout is automatically extended for the number of seconds provided in this field.
- SMS
  Provide the phone number for receiving SMS messages from the channel. The phone should be provided in international format, including `+` symbol and the country code; for example `+4951172752021`.
- Email
  Provide the email address for receiving incoming messages from the channel as emails.

- Protect channel from deletion
  Prevent accidental deletion of the channel when the flag is enabled. Can only be turned on or off by users with *Administrator* rights.
  NOTE: While this flag is enabled, the channel cannot be deleted by anyone, including *Administrators*.
- Index
  Provide a unique sequence number that is used for manual sorting of channels in client applications. If this property is not specified, the channel ID will be used for sorting.
- Bridge profile
  If you plan to integrate the bridged network into this channel, select the type of the connected T.Bridge service in this field. Refer to T.Bridge documentation for details (Integrating T.Bridge as a static channel article).
  The following T.Bridge types are supported:
  - *DAMM* - T.Bridge to DAMM TetraFlex®
  - *TIER3* - T.Bridge to Hytera DMR Tier III
  - *HYTERA* - T.Bridge to Hytera DMR Tier II
  - *KENWOOD* - T.Bridge to Kenwood NEXEDGE®
  - *MOTOTRBO* - Motorola MOTOTRBO™
  - *SEPURA* - T.Bridge to Sepura
  - *P25* - T.Bridge to Kenwood P25
  - *TAIT* - T.Bridge to TAIT
  - *JPS* - T.Bridge to JPS RSP-Z2™
  - *4WIRE* - T.Bridge 4wire
  - *IMTRADEX* - T.Bridge to Imtradex
  - *TELTRONIC* - T.Bridge to Teltronic PowerTrunk
  - *VOCALITY* - T.Bridge to Vocality

Lone worker protection

Lone workers are employees who carry out the work in isolation from others, without close or direct supervision. They are often exposed to increased risks and require an immediate assistance in case of emergency: work-related accidents, sudden illnesses, and the like.

TASSTA provides certified lone worker protection functionality for client devices. To activate lone worker protection for a user of TASSTA network:

- Enable **Lone worker protection** in server settings.
- Turn on **Lone worker protection** in user settings.

To configure lone worker protection settings, expand a server in navigation pane and click **Lone Workers**.

- To select a single user, click it.
- To select multiple users, select or clear the checkbox to the left of user's name.

The changes are applied immediately after saving.

> NOTES:
>
> The dispatcher can enable or disable lone worker protection as well as customize some of the settings from T.Rodon.

Configuring lone worker profile

A new lone worker profile is automatically created when you add a user. To edit profile properties:

1. Expand the server in the left pane and click **Lone Workers**.
2. Select a user from the list.
3. Click  icon in the toolbar. A sidebar with lone worker protection settings opens.
4. Configure lone worker protection properties.
5. Click **Save**.

Copying profile properties

To copy all settings from a lone worker profile to other profiles:

1. Expand the server in the left pane and click **Lone Workers**.
2. Select a user from the list.
3. Click  icon in the toolbar.

4. Select one or more target users from the list.
5. Click  icon in the toolbar.

All settings of the source lone worker profile are applied to the selected profiles.

Working with templates

T.Commander supports saving lone worker profile settings as a template, so you can apply them to other users.

To create a template based on the existing lone worker profile settings:

1. Expand the server in the left pane and click **Lone Workers**.
2. Select a user from the list.
3. Click  icon in the toolbar. A sidebar with lone worker profile settings opens.
4. Provide the name of the template in **Template name** field.
5. Select settings you want to save as a template.

> NOTE:
>
> The list of templates is common for the entire TASSTA system node, so you can apply them across multiple servers.

Applying a template

1. Expand the server in the left pane and click **Lone Workers**.
2. Select one or more users from the list.
3. Right-click anywhere in the list, select **Apply template** from the context menu.
4. Click  icon to the right of the template name.

Managing templates

To delete a template:

1. Expand the server in the left pane and click **Lone Workers**.
2. Right-click anywhere in the list, select **Apply template** from the context menu.
3. Click  icon to the right of the template name.
4. Confirm the template removal.

> WARNING:

Deleted templates cannot be restored.

Lone worker properties

T.Commander provides a number of protection options that you can set for the user. To simplify navigation, options are organized in logical groups.

- Main
- Battery monitor
- Connection
- Distress signal
- Emergency contact
- Emergency timer
- Impact
- Info
- Man down
- Miscellaneous
- Movement
- Periodic check
- Sensor check

Main

Core properties of the lone worker profile.

NOTE:

This section is for information purposes only. Do not modify any of its values.

- ID
  Unique ID of the lone worker profile.
- User ID
  Unique ID of the user.
- Server ID
  Current server.

Battery monitor

Battery level monitoring and alerting.

- Battery level monitor
  Turn on monitoring of battery charge level for a client device.
- Low battery warning level (percent)
  Send an emergency warning when the battery charge reaches this level (percentage). This value should be well above **Low battery alarm level**.
  This value also defines a minimum battery charge level to pass sensor checks in T.Flex.
- Low battery emergency call
  Automatically initiate an emergency call when battery charge level reaches the critical (**Low battery alarm level**) value.
- Low battery alarm level
  Set the critical battery charge level (percentage). When the battery charge level reaches this value, an alarm is raised.
  This value should be less than **Low battery warning level**.

Connection

Connection monitoring and alerting.

- Disconnect monitor
  Send a notification when a lone worker is disconnected from the network.
- Connect monitor
  Send a notification when a lone worker is connected to the network.

> NOTE:
>
> Connections and disconnections are registered in the journal regardless of whether lone worker protection is enabled or disabled for a user.

Emergency contact

Alternative communication channels for emergency notifications.

> NOTES:
>
> - Configure communication bridging (**MCGW**) in server settings or user settings to send emergency notifications via email.
> - GSM calls are made through the mobile operator and require a dedicated software (such as Phone) to be installed and configured on the device.
> - SMS messages are sent through the mobile operator and require a dedicated software (such as Messages) to be installed and configured on the device.

- Emergency email
  Send an email message to the designated address in case of emergency.
- Emergency email address
  Provide the target email address for emergency notifications.

- Emergency GSM call
  Call the designated phone number in case of emergency.
  IMPORTANT: This setting takes precedence over standard emergency calls from T.Flex (lone worker protection only). A call is always performed through the mobile operator.
- Emergency phone number
  Provide the phone number to called in case of emergency.
- Emergency SMS
  Send SMS message to the designated phone number in case of emergency.
- Emergency SMS Number
  Provide the phone number to receive emergency SMS messages.

Emergency timer

- Warning timer (seconds)
  Set the timeout (in seconds) during which the user should acknowledge his/her status. If the user has not reacted, an emergency is raised.
  Unlike periodic check, emergency check is turned on or off by the user at any moment.

Impact

Fall detection by recognizing the quick motion of the device followed by an impact.

- Impact detection
  Enable impact detection.
- Impact limit (G)
  Set the minimum threshold for an accelerometer to identify an impact. Baseline value: *2.3*.
- Impact time (milliseconds)
  Set minimum the time frame (in milliseconds) for an accelerometer to identify an impact based on **Impact limit** value.

> NOTE:
>
> Impact detection settings may vary depending on the device model/manufacturer. It is recommended to test the thresholds before using them in production.

Info

Lone worker protection status for the user. This section is read-only.

- State
  Current state of a lone worker protection.
  NOTE: You can enable **Lone worker protection** in user settings.
- Date created
  A date and time when the lone worker protection profile was created.

- Date updated
  A date and time when the lone worker protection profile was modified.

Man down

Detect whether a user suffers a fall and is knocked unconscious by checking the device orientation.

- Man Down
  Turn on Man Down detection.
- Tilt (degrees)
  Set the device orientation (in degrees) to activate Man Down alert.
- Tilt timer (seconds)
  Set the period of time (in seconds) during which the device should remain at the angle set in Tilt to activate Man Down alert. Increasing this value might prevent false positives.

Miscellaneous

Miscellaneous lone worker protection settings.

- Not active when charging
  Temporary disable lone worker protection when the device is being charged.

Movement

User's movement tracking.

- Track movement
  Detect the user's movement.
- Inactivity timer (seconds)
  Maximum period of time (in seconds) for the user to stay motionless. If no movement is detected during this period, the alert is raised.

Periodic check

Periodic acknowledgement of the user's status.

- Periodic check
  Force the user to periodically acknowledge his/her status in an given interval. If the user has not reacted, an emergency is raised.
  Unlike emergency timer, periodic check is enforced by the dispatcher.
- Periodic check countdown (seconds)
  Set the timeout (in seconds) during which the user should acknowledge his/her status.

Periodic Check U

- Periodic Check U timer (seconds)
  Set the timeout (in seconds) for a distress state initiated by the user. If the user does not cancel the countdown during that period, the signal is sent.

Sensor check

Configure the periodic device check-ups. If the required checks are not passed, lone worker protection for the user is disabled and the alert is raised.

- GSM call sensor check
  Check the ability to perform GSM calls.
- GPS sensor check
  Check location services availability for the device.
- Last sensor check (read-only)
  The date and time when the last check-up was performed.
- Wi-Fi connection sensor check
  Check Wi-Fi connectivity for the device.
- Bluetooth connection sensor check
  Check Bluetooth connectivity for the device.
- Sensor check validator period
  Set the interval to notify the user about periodic sensor checks.
  NOTE: To specify how long lone worker protection remains active after the sensor check is passed, use Sensor check validity period server setting.
- Vehicle mode
  Automatically activate lone worker protection on a device without passing periodic check-ups. This might be useful for stationary devices, such as in-vehicle panel computers or mobile devices without required sensors.

Rules

T.Commander allows for configuring flexible access policies (**rules**) for channels. Rules control all aspects of channel access, user behavior, and membership.

To show and manage rules, expand a server in navigation pane and click **Rules**.

- To select a single rule, click it.
- To select multiple rules, select or clear the checkbox to the left of the rule name.

> IMPORTANT:
>
> Adding or updating rules require restarting a server.

General concepts

A rule controls what a group of users can do in a channel. It can either allow or deny the following activities:

- To enter and view a channel
  - *Not set*: A user can see the channel in a client application and is able to switch to it.
  - *Allow*: A user can see the channel in a client application and is able to switch to it.
  - *Deny*: A user does not see the channel and cannot access it by any means (neither interactively nor programmatically).
    IMPORTANT: A user will not receive emergencies from the denied channel.
- To listen to a channel
  - *Not set*: A user can hear what others are speaking in the channel.
  - *Allow*: A user can hear what others are speaking in the channel.
    IMPORTANT: This permission does not guarantee the ability to speak in the channel.
  - *Deny*: A user does not hear channel's participants.
- To speak in a channel
  - *Not set*: A user can speak in the channel.
  - *Allow*: A user can speak in the channel.
    IMPORTANT: This permission does not guarantee the ability to hear channel's participants.
  - *Deny*: A user cannot speak in the channel.
- To move another user to a channel (only affects T.Rodon):
  - *Not set*: A user can add other users to a channel.
  - *Allow*: A user can add other users to a channel.
  - *Deny*: A user cannot add others to a channel.

You can combine several privileges within a single rule. For example, to make a team of "observers": *allow* users to *enter* and *listen* for a channel, but *deny* the ability to *speak* and *add members*.

> IMPORTANT:
>
> Conflicting rules override each other in the order they are shown under a channel.

Scheduling

The rules can be time-bound. For example, you can grant access to certain channels according to scheduled work shifts or temporary deny access from private devices during non-working hours.

Inheritance

Rules can be propagated to underlying channels. The effective privileges will vary based on the channel's type.

Inheriting rules for dynamic sub-channels

Turn on **Apply to inherited channels** switch in the channel's rule. The rule will be applied to all *dynamic* channels under this channel, regardless of whether they are created manually or automatically.

Inheriting rules from the Main channel

The rule from the *Main* channel can be propagated to another channel and all dynamic channels under it:

- Turn on **Apply to inherited channels** switch in the *Main* channel's rule.
  While you can rename *Main* channel to anything you want, it can always be identified by ID equals to *0*.
- Turn on **Inherit access control** switch in the target channel's properties.

> IMPORTANT:
>
> If the target channel already has its own rules, they take precedence over the rules derived from the *Main* channel.

Access teams

The rules are applied to **access teams** - groups of users. A user can be included in several teams.

When a server is created, *admin* access team is automatically added to it. This team is is reserved for system purposes. It cannot be edited or deleted.

T.Commander also offers a number of virtual access teams, dynamically changed based on the server configuration:

- All users - all users created on a server.
- All who is authenticated - all users signed in to T.Flex/T.Rodon.
- All who is in this channel - all users in a channel, for which the rule is applied.
- All who is out of this channel - all users who are *not* in a channel, for which the rule is applied.
- No one - empty team for creating exclusions.

To show and manage access teams, expand a server in navigation pane and click Access teams. To select a team, click it.

> IMPORTANT:
>
> Adding or updating access teams require restarting a server.

Adding a team

To add a new team to the selected server:

1. Expand the server in the left pane and click Teams.
2. Click  icon in the toolbar. A sidebar with team settings opens.
3. Provide a team name in Name field.
   IMPORTANT: Do not create a team called *admin*. This name is reserved for system purposes.
4. Select team members under Users.
5. Specify the password that members of the team must enter before joining the channels to which the rules with this team apply.
6. Click Save.
7. Restart the server.

> NOTE:
>
> Team ID and server ID are assigned automatically.

Editing a team

To modify a team:

1. Expand the server in the left pane and click Teams.
2. Select a team from the list.
3. Click  icon in the toolbar. A sidebar with team settings opens.

4. Rename the team (**Name**) or revise its members (**Users**).
5. Specify the password that members of the team must enter before joining the channels to which the rules with this team apply.
6. Click **Save**.
7. Restart the server.

> NOTE:
>
> *admin* team is reserved for system purposes. It cannot be edited.

Deleting a team

> WARNING:
>
> Deleted teams cannot be restored.

To delete a team from the server:

1. Expand the server in the left pane and click **Teams**.
2. Select a team from the list.
3. Click  icon in the toolbar.
4. Confirm the removal of the selected team.
5. Restart the server.

> NOTE:
>
> *admin* team is reserved for system purposes. It cannot be deleted.

Creating a rule

To add a new rule:

1. Expand the server in the left pane and click **Rules**.
2. Click  icon in the toolbar. A sidebar with rule configuration opens.
3. Select a channel under **Channel**.
4. Select a team under **Apply to**. To apply the rule to all users who are *not* included in the team (invert the choice), turn on **All who is in** switch.
5. Grant privileges under **Allow**. Click  to grant a privilege or  to remove a previously granted privilege.

6. Deny privileges under **Deny**. Click  to deny a privilege or  to remove a previously denied privilege.
7. Specify a schedule during which the rule will be active under **Schedule**.
8. To enable a rule, turn on **Apply to this channel** switch.
9. To propagate a rule to all underlying channels, turn on **Apply to inherited channels** switch.
10. Click **Save**.
11. Restart the server.

> IMPORTANT:
>
> Be very careful when defining rules. If you configure a rule like "**All users** are **Denied to enter and view a channel**", the channel will become inaccessible for everyone.

Editing a rule

To edit the existing rule:

1. Expand the server in the left pane and click **Rules**.
2. Select a rule from the list.
3. Click  icon in the toolbar. A sidebar with rule configuration opens.
4. Select another channel under **Channel**.
5. Select a different team under **Apply to**. To apply the rule to all users who are *not* included in the team (invert the choice), turn on **All who is in** switch.
6. Grant privileges under **Allow**. Click  to grant a privilege or  to remove a previously granted privilege.
7. Deny privileges under **Deny**. Click  to deny a privilege or  to remove a previously denied privilege.
8. Specify a schedule during which the rule will be active under **Schedule**.
9. To enable a rule, turn on **Apply to this channel** switch.
10. To propagate a rule to all underlying channels, turn on **Apply to inherited channels** switch.
11. Click **Save**.
12. Restart the server.

> IMPORTANT:
>
> Be very careful when editing rules. A rule like "**All users** are **Denied to enter and view a channel**" will result in the channel to be inaccessible.

Reordering rules

Expand the server in the left pane and click **Rules**. You should see a list of rules grouped by channels.

The rules are applied according to their order within a channel. Rules at the top have lower priority, while rules at the bottom have higher priority.

To reorder rules, simply drag and drop them.

Restart the server to apply the updated order of rules.

Checking effective privileges

To check the resulting user's privileges based on all active rules:

1. Expand the server in the left pane and click **Users**.
2. Select a user from the list.
3. Click  icon in the toolbar.

You get the list of channels with effective privileges represented with icons:

- To enter and view a channel: 
- To listen to a channel: 
- To speak in a channel: 
- To move another user to a channel: 

Grey icon means the corresponding privilege is not defined by any rules. Such privileges are granted by default.

Green icon means the corresponding privilege is granted.

Red icon means the corresponding privilege is denied.

To get detailed information on the rules which define effective privileges for the channel, click the channel name in the popup. You can disable or edit a rule by clicking its name and selecting the corresponding option from the dropdown.

Enabling rules

To quickly enable rules without editing them one-by-one:

1. Expand the server in the left pane and click **Rules**.
2. Select one or more rules from the list.
3. Click  icon in the toolbar.

4. Restart the server.

Inheriting rules

To quickly propagate rules to underlying channels without editing them one-by-one:

1. Expand the server in the left pane and click **Rules**.
2. Select one or more rules from the list.
3. Click  icon in the toolbar.
4. Restart the server.

Disabling rules

To quickly disable rules without editing them one-by-one:

1. Expand the server in the left pane and click **Rules**.
2. Select one or more rules from the list.
3. Click  icon in the toolbar.
4. Restart the server.

Turning off rules' inheritance

To quickly remove the propagation rules to underlying channels without editing them one-by-one:

1. Expand the server in the left pane and click **Rules**.
2. Select one or more rules from the list.
3. Click  icon in the toolbar.
4. Restart the server.

Deleting rules

> WARNING:
>
> Deleted rules cannot be restored. It is recommended to disable them instead of deletion.

To delete rules from the server:

1. Expand the server in the left pane and click **Rules**.
2. Select one or more rules from the list.

3. Click  icon in the toolbar.
4. Confirm the removal of the selected rules.
5. Restart the server.

> NOTE:
>
> Deleting a rule does not delete the corresponding team or channel.

Password protected channels

The rules allow you to add an extra layer of security to the system. It will require certain users to enter the predefined password before joining certain channels.

To protect a channel with a password:

1. Expand the server in the left pane and click Access teams.
2. Create a new team or open the existing one.
3. Specify the password in Channels access password field.
4. Save the changes.
5. Expand Rules in the left pane.
6. Create a new rule or open the existing one.
7. Select the channel to be protected with password in Channel ID field.
8. Select the team for which you have specified a password in Apply to field.
9. Allow *To enter and view channel* or higher level privilege. Otherwise, the users will not be able to join the channel, even with the password.
10. Save the changes.
11. Restart the server.

Now all users in the team will be asked for a password every time before joining the channel to which the rule applies.

Task Manager

TASSTA Task Manager is an advanced tracking system for orders, deliveries, service requests and related activities. T.Commander allows you to enhance and customize preconfigured tasks by adding a server-specific set of fields, priorities, statuses, and roles to a standard task/issue.

- Customizing task fields
- Customizing task priorities
- Customizing task statuses
- Customizing Task Manager roles

> NOTE:
>
> To enable clients using Task Manager and perform its basic configuration, check the server settings.

Customizing task fields

To show and manage custom fields, expand a server in navigation pane and click **Task Manager fields**.

- To select a single field, click it.
- To select multiple fields, select or clear the checkbox to the left of field's name.

Adding or updating fields do not require restarting a server. The changes are applied immediately after saving.

> NOTE:
>
> To enable clients using Task Manager and perform its basic configuration, check the server settings.

Adding Task Manager field

To add a custom field for Task Manager issues:

1. Expand the server in the left pane and click **Task Manager fields**.
2. Click  icon in the toolbar. A sidebar with field settings opens.
3. Provide a field name in **Name** field.
4. Select a field format under **Format**:
   - *Text*: Standard text field.
   - *Boolean*: "Yes/No" switch.

5. Provide a default value for the field under **Default value**. The value depends on the field **format**.
6. Provide all allowed values for the field under **Values**. This option is only available for *text* fields.
   - Click  to append a value.
   - To edit a value, select it, click  and provide a new value.
   - To remove a value, select it and click  .
7. Specify whether the field is accessible in the Task Manager with **Visible** switch.
8. To allow T.Flex operator updating the field's value in tasks, turn on **Editable (Flex)** switch. If this option is disabled, the field value can only be changed by T.Rodon dispatcher.
9. Click **Save**.

Editing Task Manager field

To edit a custom field:

1. Expand the server in the left pane and click **Task Manager Fields**.
2. Select a field from the list.
3. Click  icon in the toolbar. A sidebar with field settings opens.
4. Change the field name in **Name** field.
5. Update a default value for the field under **Default value**. The value depends on the field **format**.
6. Change allowed values for the field under **Values**. This option is only available for *text* fields.
   - Click  to append a value.
   - To edit a value, select it, click  and provide a new value.
   - To remove a value, select it and click  .
7. Specify whether the field is accessible in the Task Manager with **Visible** switch.
8. To allow T.Flex operator updating the field's value in tasks, turn on **Editable (Flex)** switch. If this option is disabled, the field value can only be changed by T.Rodon dispatcher.
9. Click **Save**.

> NOTE:
>
> Field format cannot be changed.

Deleting Task Manager fields

WARNING:

- Deleted fields cannot be restored.
- If you delete the field, it disappears from all existing tasks and all corresponding values are removed.

To delete Task Manager fields from the server:

1. Expand the server in the left pane and click **Task Manager fields**.
2. Select one or more fields from the list.
3. Click  icon in the toolbar.
4. Confirm the removal of the selected fields.

Customizing task priorities

To show and manage custom priorities, expand a server in navigation pane and click **Task Manager Priorities**.

- To select a single priority, click it.
- To select multiple priorities, select or clear the checkbox to the left of the priority's name.

Adding or updating priorities do not require restarting a server. The changes are applied immediately after saving.

NOTE:

To enable clients using Task Manager and perform its basic configuration, check the server settings.

Adding task priority

To add a custom priority for Task Manager issues:

1. Expand the server in the left pane and click **Task Manager Priorities**.
2. Click  icon in the toolbar. A sidebar with priority settings opens.
3. Provide a priority title in **Name** field.
4. To force the priority to be set by default for all tasks, turn on **Default** switch.
5. Click **Save**.

Editing task priority

To edit a custom priority:

1. Expand the server in the left pane and click **Task Manager Priorities**.
2. Select a priority from the list.
3. Click  icon in the toolbar. A sidebar with priority settings opens.
4. Change the priority title in **Name** field.
5. To force the priority to be set by default for all tasks, turn on **Default** switch.
6. Click **Save**.

Deleting task priority

> WARNING:
>
> Deleted priorities cannot be restored.

To delete task priorities from the server:

1. Expand the server in the left pane and click **Task Manager Priorities**.
2. Select one or more priorities from the list.
3. Click  icon in the toolbar.
4. Confirm the removal of the selected priorities.

Customizing task statuses

To show and manage custom statuses, expand a server in navigation pane and click **Task Manager Statuses**.

- To select a single status, click it.
- To select multiple statuses, select or clear the checkbox to the left of the status name.

Adding or updating statuses do not require restarting a server. The changes are applied immediately after saving.

> NOTE:
>
> To enable clients using Task Manager and perform its basic configuration, check the server settings.

Adding task status

To add a custom status for Task Manager issues:

1. Expand the server in the left pane and click **Task Manager Statuses**.
2. Click  icon in the toolbar. A sidebar with status settings opens.
3. Provide a status title in **Name** field.
4. To force the status to be set by default for all tasks, turn on **Default** switch.
5. To make the status a trigger for closing a task, select the **Closed** checkbox.
6. Select the status color code.
7. Click **Save**.

Editing task status

To edit a custom status:

1. Expand the server in the left pane and click **Task Manager Statuses**.
2. Select a status from the list.
3. Click  icon in the toolbar. A sidebar with status settings opens.
4. Change a status title in **Name** field.
5. To force the status to be set by default for all tasks, turn on **Default** switch.
6. To make the status a trigger for closing a task, select the **Closed** checkbox.
7. Change the status color code.
8. Click **Save**.

Deleting task status

> WARNING:
>
> Deleted statuses cannot be restored.

To delete task statuses from the server:

1. Expand the server in the left pane and click **Task Manager Statuses**.
2. Select one or more statuses from the list.
3. Click  icon in the toolbar.
4. Confirm the removal of the selected statuses.

Customizing Task Manager roles

To show and manage Task Manager roles, expand a server in navigation pane and click **Task Manager Roles**.

- To select a single role, click it.
- To select multiple roles, select or clear the checkbox to the left of the role name.

Adding or updating roles do not require restarting a server. The changes are applied immediately after saving.

> NOTE:
>
> To enable clients using Task Manager and perform its basic configuration, check the server settings.

Adding Task Manager role

To add a custom role for Task Manager:

1. Expand the server in the left pane and click **Task Manager Roles**.
2. Click  icon in the toolbar. A sidebar with role settings opens.
3. Provide a role title in **Name** field.
4. Click **Save**.

Editing Task Manager role

To edit a Task Manager role:

1. Expand the server in the left pane and click **Task Manager Roles**.
2. Select a role from the list.
3. Click  icon in the toolbar. A sidebar with role settings opens.
4. Change a role title in **Name** field.
5. Click **Save**.

Deleting Task Manager roles

> WARNING:
>
> Deleted roles cannot be restored.

To delete Task Manager roles from the server:

1. Expand the server in the left pane and click Task Manager Roles.
2. Select one or more roles from the list.
3. Click  icon in the toolbar.
4. Confirm the removal of the selected roles.

User roles and statuses

Status is a predefined text message that shows the user's availability or activity to others. A list of available statuses depends on the user's role. For example, *Security Guard* can have the following statuses:

- On post;
- Patrolling;
- Investigating an incident;
- Taking a break.

Managing roles and statuses

Roles are server-specific. To manage roles and statuses:

1. Expand the server in the left pane and click **User statuses**. **Edit roles and statuses** popup is opened.
2. Click **+** to add a new role.
3. Click the default role name ("*Role*") and provide a unique name for the role.
   IMPORTANT: Roles with duplicate names are removed on save.
4. Click the line with the role name (outside of the name field) to select a role.
5. Click **+** under **Statuses for the selected role** to add a status:
   - Click the default status text ("*Status*") and provide a unique status message.
   - Pick the status color.
6. To remove a role or a status, select it and click **-** on top of the corresponding section.
7. Click **Save** button to save roles and statuses.

User role assignment

To assign a role to one or more users:

1. Expand the server in the left pane and click **Users**.
2. Select one or more users from the list.
3. Click  icon in the toolbar.
4. Select a role from the popup and click **Save** button.

> NOTE:
>
> You can only assign one role to a user.

Current user roles are shown in Assigned roles column of the users list.

Status messages

A status message is a predefined text message that you can send with a couple of clicks, rather than typing the same text every time.

Status messages are configured for the server.

Adding status messages

To add a status message:

1. Expand the server in the left pane and click **Status messages**.
2. Click  icon in the toolbar. A sidebar with status message properties opens.
3. Provide the message text in **Message** field. This text will be shown in chat when the status message is sent or received.
4. Provide the message description for informational purposes in **Comment** field.
5. Pick the message highlighting **color**.
6. Specify the type of the communication client that can send the message in **Available to**:
   - *No one* - the message cannot be sent.
   - *Everyone* - the message can be sent from any client and TASSTA SDK.
   - *Clients only* - the message can be sent from T.Flex only.
   - *Dispatchers only* - the message can be sent from T.Rodon and TASSTA SDK only.
7. Provide a unique numeric **code** for quick-sending the message with `#<code>` shorthand (from 0 to 2,147,483,647).
8. Provide a short **title** of the message which is shown in communication clients.
9. Click **Save** button.

Changing a status message

To update a status message:

1. Expand the server in the left pane and click **Status messages**.
2. Select a status message from the list.
3. Click  icon in the toolbar. A sidebar with status message properties opens.
4. Modify the message text in **Message** field. This text will be shown in chat when the status message is sent or received.

5. Modify the message description for informational purposes in **Comment** field.
6. Pick another highlighting **color** for the message.
7. Specify the type of the communication client that can send the message in **Available to**:
   - *No one* - the message cannot be sent.
   - *Everyone* - the message can be sent from any client and TASSTA SDK.
   - *Clients only* - the message can be sent from T.Flex only.
   - *Dispatchers only* - the message can be sent from T.Rodon and TASSTA SDK only.

> NOTE:
>
> If the message availability is changed to the value that prevents sending it from the current client, all previously sent messages remain in chat history and the related channel status is displayed in T.Rodon.

8. Modify a unique numeric **code** for quick-sending the message with `#<code>` shorthand (from 0 to 2,147,483,647).
9. Modify a short **title** of the message which is shown in communication clients.
10. Click **Save** button.

Deleting status messages

To remove status messages:

1. Expand the server in the left pane and click **Status messages**.
2. Select one or more status messages from the list.
3. Click  icon in the toolbar.
4. Confirm the removal of the selected messages.

> NOTE:
>
> All previously sent messages remain in chat history, even if the status message is deleted.

Workgroups

A workgroup is a predefined group of users to which geofence triggers are applied.

Workgroups are configured for the server.

Adding a workgroup

To add a workgroup:

1. Expand the server in the left pane and click **Workgroups**.
2. Click  icon in the toolbar. A sidebar with workgroup properties opens.
3. Provide the **workgroup name**.
4. Select the users to be included in the workgroup in **Members** field. Move a user to **Selected users** list to make it the member of the workgroup.
5. Click **Save** button.

Updating a workgroup

To rename a workgroup or revise its members:

1. Expand the server in the left pane and click **Workgroups**.
2. Select a workgroup from the list.
3. Click  icon in the toolbar. A sidebar with workgroup properties opens.
4. Change the **workgroup name**.
5. Expand **Members** field and add or remove users from the workgroup.
   - Move a user to **Selected users** list to make it the member of the workgroup.
   - Move a user to **Available users** list to remove it from the workgroup.
6. Click **Save** button.

Deleting workgroups

To remove workgroups:

1. Expand the server in the left pane and click **Workgroups**.
2. Select one or more workgroups from the list.
3. Click  icon in the toolbar.

4. Confirm the removal of the selected workgroups.

> WARNING:
>
> If you delete a workgroup, the corresponding geofence trigger will stop working immediately!

Administering a platform

This chapter describes common administrative tasks that affect the entire T.Lion server node:

- Managing T.Lion server nodes
- Managing T.Commander users
- Backup and recovery
- Configuring call recording and activity history
- Deploying client updates
- Getting billing information

Server nodes

A *node* is a physical machine or a cloud instance running T.Lion server.

Normally, you have a single node pre-configured during T.Lion deployment; however, T.Commander can manage multiple T.Lion servers from a single administrative console.

To switch between nodes, use the corresponding dropdown in the top-right corner.

To see all nodes, click **Settings** in the left pane, expand **Tools**, and click **Nodes**.

Adding a node

> IMPORTANT:
>
> Before adding a node, it is strongly recommended to clarify its properties with TASSTA service team.
> Setting incorrect values might cause errors in T.Commander and client applications.

To add a node:

1. Click **Settings** in the left pane, expand **Tools**, and click **Nodes**.
2. Click  icon in the toolbar. A sidebar with node settings opens.
3. Provide node properties:
   - **Name** - node name.
   - **Title** - node alias.
   - **Node address** - Address of the node. This value is used for generating QR codes for client access.
   - **Number of servers** - the maximum number of servers on the node.
   - **Recorder API URL** - URL of the Recorder server, including the protocol and the port.

- Recorder API key - access key for authorizing requests to the Recorder server.
- Service API URL - T.Lion proxy URL, including the protocol and the port.
- Service key - access key for authorizing service requests.
- Record geolocation - turn on location history recording, if necessary.

4. Click Save.

Editing a node

> IMPORTANT:
>
> Contact TASSTA service team before changing node properties.
> Setting incorrect values might cause errors in T.Commander and client applications.

To change node settings:

1. Click Settings in the left pane, expand Tools, and click Nodes.
2. Select a node from the list.
3. Click  icon in the toolbar. A sidebar with node settings opens.
4. Modify node properties:
   - Name - node name.
   - Title - node alias.
   - Node address - Address of the node. This value is used for generating QR codes for client access.
   - Number of servers - the maximum number of servers on the node.
   - Recorder API URL - URL of the Recorder Server, including the protocol and the port.
   - Recorder API key - access key for authorizing requests to the Recorder Server.
   - Service API URL - T.Lion proxy URL, including the protocol and the port.
   - Service key - access key for authorizing service requests.
   - Record geolocation - turn on location history recording, if necessary.
5. Click Save.

Deleting a node

> IMPORTANT:
>
> Write down all properties before deleting a node, so you can restore it if necessary.

To delete a node:

1. Click **Settings** in the left pane, expand **Tools**, and click **Nodes**.
2. Select a node from the list.
3. Click  icon in the toolbar.
4. Confirm node removal.

T.Commander users

You can set up multiple user accounts with different roles who can access T.Commander. It allows you to assign several administrators and implement the segregation of duties.

To see all T.Commander users, click **Settings** in the left pane, expand **Tools**, and click **Profiles**.

To sign in as a different user:

1. Expand the profile dropdown in the top-right corner.
2. Click **Log out**.
3. Sign in under another account.

Adding a user

To add T.Commander user:

1. Click **Settings** in the left pane, expand **Tools**, and click **Profiles**.
2. Click  icon in the toolbar. A sidebar with user settings opens.
3. Fill in user profile information:
   - Provide a **login**.
   - Provide a **password**.
     To generate a random strong password, click  icon in this field and select **Copy new password to clipboard**.
   - Provide user's **first** and **last** name.
   - Select user's role:

Permission	Viewer	Performer	Master	Administrator
View server configuration	+	+	+	+
Start, stop, and restart servers		+	+	+
Create and edit users		+	+	+

Permission	Viewer	Performer	Master	Administrator
Create and edit channels		+	+	+
Create and edit zones		+	+	+
Configure lone workers		+	+	+
Configure access policies (rules)		+	+	+
Configure access policies (rules)		+	+	+
Define user roles			+	+
Assign user roles		+	+	+
Create and edit status messages		+	+	+
Edit T.Commander users			+	+
Edit server nodes				+
Backup and recovery				+
Configure recording profiles				+

- To create an account without activating it, turn off **Active** switch.
- Provide user's **email**.
- Select nodes and servers the user can access under **Allowed**.
- Choose the interface **language**.

4. Click **Save**.

Editing a user profile

To change user's profile:

1. Click **Settings** in the left pane, expand **Tools**, and click **Profiles**.
2. Select a user from the list.
3. Click  icon in the toolbar. A sidebar with user settings opens.
4. Modify user profile:
   - Change a **login**.

- Change a **password**.
  To generate a random strong password, click  icon in this field and select **Copy new password to clipboard**.
- Change user's **first** and **last** name.
- Select user's role:

Permission	Viewer	Performer	Master	Administrator
View server configuration	+	+	+	+
Start, stop, and restart servers		+	+	+
Create and edit users		+	+	+
Create and edit channels		+	+	+
Create and edit zones		+	+	+
Configure lone workers		+	+	+
Configure access policies (rules)		+	+	+
Configure access policies (rules)		+	+	+
Define user roles			+	+
Assign user roles		+	+	+
Create and edit status messages		+	+	+
Edit T.Commander users			+	+
Edit server nodes				+
Backup and recovery				+
Configure recording profiles				+

- Activate or disable an account using **Active** switch.
- Change user's **email**.
- Select nodes and servers the user can access under **Allowed**.
- Choose the interface **language**.

5. Click **Save**.

Deleting users

> IMPORTANT:
>
> Deleted users cannot be restored.

To delete users:

1. Click **Settings** in the left pane, expand **Tools**, and click **Profiles**.
2. Select one or more users from the list.
3. Click  icon in the toolbar.
4. Confirm the profile removal.

Backup and recovery

T.Commander administrators can take backups of server settings and restore them in case of misconfiguration or problems.

Creating a backup

> IMPORTANT:
>
> Only the last backup is saved.

To take a snapshot of the current node settings:

1. Click **Settings** in the left pane, expand **Tools**, and click **System backups**.
2. Click  icon in the toolbar. A backup is started immediately. It can take quite a long time, depending on the amount information on the server.

Exporting and importing backups

To download a backup file:

1. Click **Settings** in the left pane, expand **Tools**, and click **System backups**.
2. Select a backup file. You can check the file size in **Size** column.
3. Click  icon in the toolbar.

To import a previously downloaded backup file:

1. Click **Settings** in the left pane, expand **Tools**, and click **System backups**.

2. Click  icon in the toolbar.
3. Select a backup file you have previously downloaded.
4. Click **OK**.

Scheduling regular backups

> IMPORTANT:
>
> **Only the last backup is saved.**

To schedule regular backups:

1. Click **Settings** in the left pane, expand **Tools**, and click **System backups**.
2. Click  icon in the toolbar.
3. Specify backup frequency.
4. Select **Enabled** option to turn on automatic backups.

Restoring settings

To restore a backup:

1. Click **Settings** in the left pane, expand **Tools**, and click **System backups**.
2. Select a backup.
3. Click  icon in the toolbar. The restore is started immediately. It can take quite a long time, depending on the backup size.

Deleting a backup

> IMPORTANT:
>
> **Deleted backups cannot be restored. Download the required backup files before deleting them.**

To delete a backup:

1. Click **Settings** in the left pane, expand **Tools**, and click **System backups**.
2. Click  icon in the toolbar.
3. Confirm backup removal.

T.Commander logs

All configuration changes performed from T.Commander administrative interface are sent to syslog and logged into the database:

- Logging in and logging out of the administrative console.
- Creating, configuring and managing servers.
- Creating, configuring and managing users.
- Creating, configuring and managing channels.
- Managing lone worker protection settings.
- Configuring access policies.
- Customizing Task Manager fields.
- Creating and managing status messages.
- Switching between nodes.
- Creating, configuring and managing T.Commander users (TASSTA network administrators).
- Creating and managing activity recording settings.
- Adding and deleting client application updates.
- Unblocking clients.

The log includes the following details:

Category	Logged data
WHEN	Date and time the configuration change was made with millisecond precision, server time.
WHERE	• Host name of the T.Lion node. • The unique identifier of the created/updated object (where applicable).
WHO	ID, username, first and last name, and role of the user who made the change.
WHAT	• Verbose operation description (for example, “The user updated”). • The list of updated field names along with their original values and new values.

You can view administrative operation logs directly from T.Commander web interface. Click Settings in the left pane, expand Tools, and click Commander logs.

To change logging severity level, click  and select one of the following values from the list:

- *WARN* (default) - log T.Commander exceptions and non-critical errors.
- *INFO* - in addition to *WARN* events, log details about background services and user requests.

- *DEBUG* - in addition to *WARN* and *INFO* events, log in-depth technical information that may be necessary for Support and Professional Services.
- *ALL* - log all events.

> NOTE:
>
> The changes are logged when the user clicks **Save** button in T.Commander. If the change affects multiple fields, all of them are written to a single log entry.

Recording configuration

TASSTA communication network supports detailed activity logging, including calls and messages recording, location history, and user activity reports.

To configure the recording, click **Settings** in the left pane, expand **Tools**, and click **Recorder settings**. You will see a list of recorder profiles and servers, assigned to them.

Setting up recorder profiles

Recorder profile controls access to calls and messages history on a single server or a group of servers. You should have at least one profile to enable recording.

Adding a recorder profile

1. Click **Settings** in the left pane, expand **Tools**, and click **Recorder settings**.
2. Click  icon in the toolbar.
3. Click **Add** button.

> NOTE:
>
> Profile name and access key are generated automatically.

Renaming a recorder profile

1. Click **Settings** in the left pane, expand **Tools**, and click **Recorder settings**.
2. Click  icon in the toolbar.
3. Click **Edit** button.
4. Change the profile name in the **Profile info** field and click **Save** button.

Getting a profile key

Profile key is a unique token that authenticates access to activity recordings from client applications. It is automatically generated when a profile is created.

> IMPORTANT:
>
> Make sure it is always well-protected and is only known to a limited number of people inside the company. If you feel the profile key is compromised, re-assign all servers to another profile and delete the profile in question.

To get a profile key:

1. Click **Settings** in the left pane, expand **Tools**, and click **Recorder settings**.
2. Right-click any server under a profile (a key is common for all servers).
3. Click **Copy profile key to clipboard**. The key is put to the clipboard so you can communicate it to the operator.

Deleting a recorder profile

> NOTE:
>
> Before deleting a recorder profile, remove all server assignments from it.

1. Click **Settings** in the left pane, expand **Tools**, and click **Recorder settings**.
2. Click  icon in the toolbar.
3. Select a profile that is not marked as *Assigned*.
4. Click **Delete** button.

Configuring activity recording

By default, recording is turned off for all servers (unless directly enabled during the server creation). To enable activity history tracking for a server:

1. Click **Settings** in the left pane, expand **Tools**, and click **Recorder settings**.
2. Make sure at least one recorder profile exists.
3. Click  icon in the toolbar. A sidebar with recording settings opens.
4. Select a server for which you want to enable activity history tracking.
5. Click **Recording mode**. There are 3 recording options:
   a. **Recording is disabled** - simply assign a server to the profile without activating recording. You can turn it on later.
   b. **Record Call History only** - only record call statistics (timestamp, participants).
   c. **Record Call History and Media** - record everything, including audio and video streams.
6. Click **Recorder profiles** and select one or more profiles to assign the server to. The recordings can be accessed using the access key of any profile with which the server is assigned.

NOTE: The history is recorded only once for each server, regardless of the number of profiles the server is assigned to.

7. Click **Save**.
8. Restart the server. If **Record Call History only** or **Record Call History and Media** is selected, the recording will be activated immediately after restarting.

> TIP:
>
> You can assign a server to multiple recorder profiles. It allows you creating a "master key" for system administrators or T.Recorder operators while keeping individual keys for each server.

To change the recording mode

1. Click **Settings** in the left pane, expand **Tools**, and click **Recorder settings**.
2. Select a server under any profile it is assigned to.
3. Click  icon in the toolbar.
4. Select another **recording mode**.
5. Click **Save**.
6. Restart the server.

To re-assign a server to another profile:

1. Click **Settings** in the left pane, expand **Tools**, and click **Recorder settings**.
2. Select a server under any profile it is assigned to.
3. Click  icon in the toolbar.
4. Select other profile(s) under **Recorder profiles**.
5. Click **Save**.
6. Restart the server.

To unassign a server from the profile:

1. Click **Settings** in the left pane, expand **Tools**, and click **Recorder settings**.
2. Select a server under a profile from which you want to unassign it.
3. Click  icon in the toolbar.
4. Confirm server unassignment.

> NOTE:
>
> Unassigning a server from one profile does not affect its assignments with other profiles.

Starting and stopping recording

By default, recording is automatically activated after the server is assigned to the recorder profile.

To temporary pause recording for the server:

1. Click **Settings** in the left pane, expand **Tools**, and click **Recorder settings**.
2. Select a server.
   NOTE: If the server is assigned to multiple profiles, select any assignment. The recording will be paused for the server in all profiles to which it is assigned.
3. Click  icon in the toolbar.
4. Confirm recording deactivation.

To resume recording for the server:

1. Click **Settings** in the left pane, expand **Tools**, and click **Recorder settings**.
2. Select a server.
   NOTE: If the server is assigned to multiple profiles, select any assignment. The recording will be activated for the server in all profiles to which it is assigned.
3. Click  icon in the toolbar.
4. Confirm recording activation.

To permanently stop recording for the server:

1. Click **Settings** in the left pane, expand **Tools**, and click **Recorder settings**.
2. Unassign the server from *all* profiles it is assigned to.
3. Restart the server.

Recording location history

> IMPORTANT:
>
> Location history recording is enabled or disabled for all servers on the node.

1. Click **Settings** in the left pane, expand **Tools**, and click **Nodes**.
2. Select a node from the list.
3. Click  icon in the toolbar. A sidebar with node settings opens.
4. Switch **Record geolocation** to turn location history recording on or off.
5. Click **Save**.

Billing reports

To get a detailed billing report:

1. Click **Settings** in the left pane, expand **Tools**, and click **Billing**.
2. Choose the billing month.
3. Click **Download** to get a report in Microsoft Excel format (.XLS).

Client updates

TASSTA communication network supports automatic updates of mobile clients and dispatcher consoles. T.Commander offers a fast and easy way to distribute client updates all over the network.

Important considerations

You can only automatically update mobile clients installed from a downloadable package.

T.Flex Android client installed from Google Play is updated only using standard Google Play procedures. Automatic update settings configured via T.Commander are ignored. If you need to keep a specific version, turn off automatic updates in the Google Play console, or uninstall the app and re-install it from the downloaded APK.

T.Flex iOS client can only be updated through Apple App Store.

Adding an update

To publish the updated version of an application on the server:

1. Check for updates on TASSTA website and download the latest versions.
2. Click **Settings** in the left pane, expand **Tools**, and click **Version management**.
3. Click  icon in the toolbar.
4. Click **Browse…** button and search for the new installation file you have previously downloaded.
5. Select **Latest version** option.
6. To make the update mandatory for users, select **Force install** option.
7. Choose the correct application type for the update under **Application name**.
8. Enter the port number of the server to which the update applies. If you skip this parameter, the update will apply to all servers.
   IMPORTANT: The port number can only be specified at the time the update is uploaded. It cannot be changed in the future.
9. Type in the full version of the application. Check the downloaded file name for details.
10. Click **OK**.

The users will be notified about an available update as soon as they start the client.

Managing updates

To change parameters of the published update:

1. Check for updates on TASSTA website and download the latest versions.
2. Click **Settings** in the left pane, expand **Tools**, and click **Version management**.
3. Select an update from the list.
4. Click  icon in the toolbar.
5. To mark update as the latest, select **Latest version** option.
6. To make the update mandatory for users, select **Force install** option.
7. Change the application type for the update under **Application name**.
8. Modify the full version of the application. Check the update file name for details.
9. Change the update file name, if necessary.
10. Click **OK**.

> IMPORTANT:
>
> The server port number cannot be changed after the update is published. Delete the update and re-upload it to change or specify the port.

To delete a published update:

1. Check for updates on TASSTA website and download the latest versions.
2. Click **Settings** in the left pane, expand **Tools**, and click **Version management**.
3. Select an update from the list.
4. Click  icon in the toolbar.
5. Confirm the update removal.

> IMPORTANT:
>
> Users who have already installed the update will continue using it, even if the distributive is removed from the server.
> Use **Force install** option on one of the existing updates to replace all clients.

Cross-server communication

Group communication within a single channel is well-suited for the majority of business cases. However, there are some specific scenarios that require cross-channel communication:

- Communication of users from multiple bridged radio systems.

- Situational merging of several channels within a single server when users cannot leave their current channels due to access rules or corporate policies. For example, temporary direct communication between several ambulance brigades in case of mass emergency.
- Cross-communication between channels from different TASSTA servers. For example, direct communication between fire brigades and ambulance without involving dispatchers and operational headquarters.

TASSTA has cross-channel communication functionality which allows to combine up multiple channels into a single communication unit. Any combination of channels is possible: from the same server, from different servers or nodes or from bridged systems.

Cross-server connections are created and managed through T.Commander. Click **Settings** in the left pane, expand **Tools**, and click **Cross server communication**. Access to cross-server communication interface requires **Administrator** permissions.

> IMPORTANT:
>
> For cross-channel communication to work, the T.Qonnector service must be installed and configured on the T.Lion server.

Key elements

Cross-server communication works with the following objects:

- **Server connection** - the endpoint for joining the server channels to the cross-channel communication unit (multi-channel group).
- **Multi-channel group** - a group of channels from multiple servers joined into a single voice communication unit. Members of these channels will hear each other in group calls.

Managing server connections

Server connection is an endpoint for joining the server to the cross-channel communication unit. Creating a connection is a prerequisite for adding server's channels to a multi-channel group.

To manage server connections, go to **Cross server communication** and click  icon in the toolbar.

Adding a server connection

To create a new server connection:

1. Add a user which will be used for connecting to the server. You should only set the user **name** and **password**, all other properties can be left with default values.
2. Go to **Cross server communication** and click  icon in the toolbar.
3. Click **plus** icon in the **Server connections** popup. A new connection is added to the bottom of the table.
4. Click the value in **Host address** column and provide the IP address or DNS name of T.Lion node.

5. Click the value in **Port** column and provide the server's port number.
6. Click the value in **Login** column and provide the name of the user created on the first step.
7. Click the value in **Password** column and provide the password of the user created on the first step.

> IMPORTANT:
>
> Once the connection is added, T.Qonnector service is automatically restarted to apply the changes. All ongoing cross-server communication will be temporary suspended.

Modifying a server connection

To modify an existing server connection:

1. Go to **Cross server communication** and click  icon in the toolbar.
2. Click the value in **Host address** column and provide the IP address or DNS name of T.Lion node.
3. Click the value in **Port** column and provide the server's port number.
4. Click the value in **Login** column and provide the name of the user created on the first step.
5. Click the value in **Password** column and provide the password of the user created on the first step.

> IMPORTANT:
>
> Once the connection is modified, T.Qonnector service is automatically restarted to apply the changes. All ongoing cross-server communication will be temporary suspended.

Deleting a server connection

To remove a server connection:

1. Go to **Cross server communication** and click  icon in the toolbar.
2. Click the connection's row.
3. Click **minus** icon in the **Server connections** popup and confirm the removal.

> IMPORTANT:
>
> - Removing the connection also removes all related channels from multi-channel groups.
> - Once the connection is removed, T.Qonnector service is automatically restarted to apply the changes. All ongoing cross-server communication will be temporary suspended.

Managing multi-channel groups

Once one or more cross-server connections are created, you can join channels from those servers into a single voice communication unit. Members of these channels will hear each other in group calls.

To manage multi-channel groups, go to **Cross server communication**.

IMPORTANT:

Cross-channel communication does not support conference channels.

Adding a multi-channel group

To allow users from multiple channels to hear each other in group calls:

1. Add server connections for each server whose channels will be joined to the group.
2. Go to **Cross server communication** and click  icon in the toolbar.
3. Provide the group name.
4. Specify a relative group priority. This value is only used when a very large number of concurrent connections start to conflict.
   Multi-channel groups with lower priority will be automatically suspended. Users from different groups will not be able to hear each other, but communication within each channel will work as usual.
5. Join channels to the group:
   a. Click **plus** icon.
   b. Select the previously created server connection.
   c. Specify the ID of the server's channel to be added to the group.
6. Click **Save** button.

IMPORTANT:

- Once the multi-channel group is added, T.Qonnector service is automatically restarted to apply the changes. All ongoing cross-server communication will be temporary suspended.
- Cross-channel communication does not support conference channels.

Modifying a multi-channel group

To modify a multi-channel group:

1. Go to **Cross server communication** and click  icon in the toolbar.
2. Change the group name.
3. Update a relative group priority. This value is only used when a very large number of concurrent connections start to conflict.
   Multi-channel groups with lower priority will be automatically suspended. Users from different groups will not be able to hear each other, but communication within each channel will work as usual.
4. Add or remove channels from the group:

- Click plus icon to add a new channel. Select the previously created server connection and specify the ID of the server's channel to be added to the group.
- Select a channel and click minus icon to remove the channel from the group.

5. Click Save button.

IMPORTANT:

- Once the multi-channel group is added, T.Qonnector service is automatically restarted to apply the changes. All ongoing cross-server communication will be temporary suspended.
- Cross-channel communication does not support conference channels.

Deleting a multi-channel group

To remove a multi-channel group:

1. Go to Cross server communication and select a group.
2. Click  icon in the toolbar.
3. Confirm the removal.

IMPORTANT:

Once the multi-channel group is deleted, T.Qonnector service is automatically restarted to apply the changes. All ongoing cross-server communication will be temporary suspended.

Removing a group only prevents users from its channels from hearing each other. Communication between users of individual channels is not affected.

Snapshots

T.Commander administrators can take snapshots of node settings and quickly restore them in case of misconfiguration.

Unlike full backups, snapshots cannot be used to restore data, but only revert configuration fields to their previous values. It is recommended to make a snapshot every time before applying significant configuration changes so you can restore the system to the operational state as fast as possible in case of problems.

To create, restore and manage snapshots, click Settings in the left pane, expand Tools, and click Snapshots.

Creating a snapshot

To take a snapshot of the node configuration, simply click  icon in the toolbar and provide the snapshot name.

Restoring from a snapshot

To recover node configuration to the snapshot state, select a snapshot and click  icon in the toolbar.

Important considerations

- To maintain uninterrupted client workflow, restoring from snapshots preserves current user passwords. This means that even if a user's password has been changed since the snapshot was created, they can still log in using their current credentials.
- For security, user passwords are excluded from snapshots. Restoring a deleted user from a snapshot will not bring back the original password. You will have to set the new password for that user.

Removing snapshots

To delete snapshots, select them from the list and click  icon in the toolbar.

Annex I: Isolated teams

Rules and teams are very flexible and powerful instruments for fine-tuning access to channels and establishing a segregation of duties.

This scenario demonstrates how to use rules to eliminate the interference between dispersed teams while coordinating common operations through a central dispatcher. For example:

- Isolate internal communication of geographically distributed police departments, but handle all distress calls from a single dispatch center.
- Ensure clear coordination and safety at the construction site by providing a dedicated communication channel for each team, with the ability to broadcast emergency messages to every worker from the dispatcher console.
- And similar use cases.

Preconditions

Let's consider a simple construction site with 2 teams: electricians and riggers. To make sure the workers clearly understand each other and to avoid misunderstanding or errors, a dedicated channel is created for each construction team:

- *Electrical*,
- *Rig*.

A central dispatcher makes announcements to all on-site personnel and coordinates the work across teams.

Setting up rules in T.Commander

Add 3 teams corresponding to job responsibilities. Each team should include all users with the corresponding role.

- *Electricians*,
- *Riggers*,
- *Dispatchers*.

Configuring access to *Electrical* channel

1. Create a rule to **deny** access to the *Electrical* channel for all workers who are not specifically designated for this job.
   IMPORTANT: This must be the topmost rule for this channel.
   a. Select *Electrical* under **Channel**.

b. Select *Electricians* team under **Apply to** and turn on **All who is in** switch. This selects all users who are **not** members of *Electricians* team.

c. Add *To enter and view a channel* under **Deny**.

2. Create a rule to allow dispatchers to communicate in the *Electrical* channel.

a. Select *Electrical* under **Channel**.

b. Select *Dispatchers* team under **Apply to**.

c. Add *To enter and view a channel*, *To listen to a channel*, *To speak in a channel*, and *To move another user to a channel* under **Allow**.

Configuring access to *Rig* channel

1. Create a rule to **deny** access to the *Rig* channel for all workers who are not specifically designated for this job.
IMPORTANT: This must be the topmost rule for this channel.

a. Select *Rig* under **Channel**.

b. Select *Riggers* team under **Apply to** and turn on **All who is in** switch. This selects all users who are **not** members of *Riggers* team.

c. Add *To enter and view a channel* under **Deny**.

2. Create a rule to allow dispatchers to communicate in the *Rig* channel.

a. Select *Rig* under **Channel**.

b. Select *Dispatchers* team under **Apply to**.

c. Add *To enter and view a channel*, *To listen to a channel*, *To speak in a channel*, and *To move another user to a channel* under **Allow**.

As a result, you should get the following set of rules:

Apply rule to	Allowed	Denied	Applied	Applied for inherited
Electrical Channel				
All who are NOT in 'Electricians' team		Enter		
All who are in 'Dispatchers' team	Speak, Listen, Enter, Move			
Rig Channel				
All who are in 'Dispatchers' team	Speak, Listen, Enter, Move			
All who are NOT in 'Riggers' team		Enter		

> TIP:
>
> You can configure the isolation for more than 3 teams in a similar manner.

Annex II: Client features

This chapter provides a mapping of T.Commander settings to TASSTA clients.

Server properties

Main

Check Main server properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
Server name					
Server port	+	+	+	+	+
ID	+	+	+	+	+

Miscellaneous

Check Miscellaneous server properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
Face Recognition server IP address					
Maximum online Flex Smart clients	+				
Maximum online Flex PTT clients		+			
Maximum online Rodon Smart clients				+	

Maximum online Rodon PTT clients					+
Maximum online Bridge API clients					
Maximum online Bridge Radio clients					
Maximum online Bridge 4Wire clients					
Maximum online SDK clients					
Maximum online connectors					
Maximum users	+	+	+	+	+
Maximum online users	+	+	+	+	+
Maximum channels					
Maximum Rodon Smart clients				+	
Maintenance					
Map	+				
Individual calls	+	+			
History replay	+		+		
Priority	+	+	+	+	+
Task Manager	+		+		
Lone worker protection	+				
Remote control	+	+		+	+

Transparent PTT					
End-to-end encryption	+		+		
Force TCP	+	+	+	+	+
JB1 size (packets)	+	+		+	+
JB2 size (packets)	+	+		+	+
Task Manager project	+		+	+	
Comment					
MCGW configuration	+	+		+	
Bridge					
Indoor localization share interval (milliseconds)	+		+		
Recorder server	+	+	+	+	+
Recorder server key	+	+	+	+	+
Service gateway	+	+	+	+	+
Indoor localization mode	+		+	+	
Indoor localization	+		+		
Resolve position based on fixed beacons	+				
Zones	+	+	+	+	+
Call queue	+		+	+	

LWP dispatcher required	+			+	
Maximum lone worker clients					
Maximum indoor clients					
Maximum end-to-end encryption clients					
Maximum Task Manager clients					
Maximum push-to-video clients					
Samsung hardware buttons license	+	+			
Hide offline users	+	+	+	+	+
PTT queue size	+	+	+	+	+
Mapbox access token (Flex Android)	+				
PTT time limit (seconds)	+	+	+	+	+
Mapbox access token (Flex iOS)			+		
Mapbox access token (Rodon)				+	+
Sensor check validity period	+		+		
Bluetooth UUID			+		

User properties

Main

Check Main user properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
ID	+	+	+	+	+
Name	+	+	+	+	+
Server	+	+	+	+	+
Password	+	+	+	+	+

Client Type

Check Client type properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
Allow Rodon				+	+
Allow SDK					

Codec

Check Codec properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
Variable bitrate	+	+		+	+
Forward error correction	+	+		+	+

Bitrate (bit/s)	+	+	+	+
Packet loss (percent)	+	+	+	+
Complexity	+	+	+	+

Common Calls

Check Common call properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
Mute button	+	+	+	+	+
Disable PTT	+	+	+	+	+
End-to-end encryption	+		+	+	
Priority	+	+	+	+	+
Broadcast calls	+		+	+	
Listen to multiple channels simultaneously from Rodon				+	+
Channel name on PTT button	+	+	+	+	+
On-screen PTT button toggle	+		+		
Disable on-screen PTT button	+	+	+		
Full-duplex calls	+				

Data Calls And Messaging

Check Data calls and messaging properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
Task Manager	+		+	+	
Messaging	+	+	+	+	+
Share device info	+	+	+	+	
Email settings for MCGW	+			+	
Prefer user's email settings	+			+	
SMS number				+	
Continuous message alarm	+	+	+		
Message history capacity	+	+	+	+	+
Message history retention (days)	+	+	+	+	+
Missed call notification	+	+	+		

Emergency

Check Emergency properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT

Make emergency calls	+	+	+	+	+
Prevent emergency cancellation/td>	+		+	+	
Emergency countdown (seconds)	+	+	+		
Receive emergency calls	+	+	+	+	+
Lost connection signal	+	+			
Maximize sound volume for notifications	+	+			
Acknowledge emergencies				+	
Emergency popup				+	
Mute outgoing emergency	+				
Incremental sound	+				
Emergency PTT timeout (seconds)	+	+	+		
Prevent emergency calls auto-listening	+	+	+	+	+
Release emergency calls from Flex	+				
Fullscreen emergency notification	+				
Pre-alarm timer alert	+				

Incoming emergency notification	+				
Continuous alert on lost connection	+				
Outgoing emergency alert	+				
SOS key delay time (seconds)	+				

Group Calls

Check Group call properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
Show channels	+	+	+		
Default channel	+	+	+		
Listen to multiple channels simultaneously from Flex	+	+	+		
Play channel join sound upon connect	+	+	+		

Guard Tours

Check Guard tour properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
Guard tours	+				

History

Check History properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
Show activity history	+	+	+	+	+
History capacity	+	+	+	+	+
Recording retention	+	+	+	+	+
Use rules for activity history access control					

Individual Calls

Check Individual call properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
Show users	+	+	+		
Individual calls	+	+	+	+	+
Inactivity timeout (seconds)	+	+		+	+
Direct individual calls	+	+	+	+	+
Direct call with PTT button	+				

Lone Worker Protection

Check Lone worker protection properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
Lone worker protection	+		+	+	
Allow Emergency Journal	+		+	+	
Continuous alert when dispatcher is offline	+		+		

Map And Tracking

Check Map and tracking properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
Map	+		+	+	+
Share location	+	+	+	+	
Location sharing interval (seconds)	+	+	+	+	
Map Tools editor				+	
Indoor localization	+		+	+	
Location privacy	+	+	+	+	+
Share indoor position	+		+		

Share location upon PTT	+	+	+		
Use GPS for indoor	+				
Geodata provider	+	+	+		
Maximum zoom level	+	+	+		
Use local map server	+	+	+		
Indoor localization permissions	+		+		
3D indoor map	+		+		
GPS priority for indoor	+				
GPS priority accuracy threshold	+				
3D DeepMap demo mode	+				
Bluetooth beacons type	+		+		

Miscellaneous

Check Miscellaneous user properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
Comment					
Network usage	+	+			

Show features	+	+			
Self-manage settings	+	+		+	+
Shortcut view	+		+		
Flex home screen	+		+		
Home screen on channel selection	+		+		
Use Apple Push Notification Service			+		
Sound scheme	+	+	+		
Text-to-speech	+	+			
Connection quality	+	+	+		
Share detailed app statistics	+	+	+		
Favorite PTT view				+	+

Remote Control

Check Remote control properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
Ambient sound sharing	+	+	+	+	+
Ambient listener	+		+	+	

Notify on remote listening	+	+		+	+
Share camera snapshots	+	+	+	+	+
Take camera snapshots remotely	+		+	+	
Notify on remote camera access	+	+			
Imprint metadata in camera snapshots	+		+		
Remote control privacy	+	+	+	+	+
Remote video monitoring	+				
Remote video sharing	+				
Remote video quality	+				

User Authentication

Check User authentication properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
Alias	+	+	+	+	+
Lock user to device	+	+	+		
Device ID	+	+	+		

Logout with password	+		+		
Logout password	+		+		
Use external user's ID					
External user's ID					

Video

Check Video properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
Video calls	+		+	+	
Push-to-video	+		+	+	
Video emergency	+		+		
Push-to-video quality	+				
Video calls quality	+				
Emergency video quality	+				
Video streams	+				
Video streams quality	+				

Channel properties

Main

Check Main channel properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
ID	+	+	+	+	+
Channel name	+	+	+	+	+

Miscellaneous

Check Miscellaneous channel properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
Conference	+	+	+	+	+
Channel maximum users quantity				+	+
Inherit access control					
Select channel to use PTT	+	+	+	+	+
Channel selection timeout (seconds)	+	+	+	+	+
SMS				+	
Email				+	

Lone worker protection properties

Main

Check Main LWP properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
ID	+		+	+	
User ID	+		+	+	

Battery Monitor

Check Battery monitor properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
Battery level monitor	+		+	+	
Low battery warning level (percent)	+		+	+	
Low battery emergency call	+		+	+	
Low battery alarm level	+		+	+	

Connection

Check Connection properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT

Disconnect monitor				+	
Connect monitor				+	

Periodic Check U

See Periodic Check U properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
Periodic Check U timer (seconds)	+		+	+	

Emergency Contact

Check Emergency contact properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
Emergency email	+			+	
Emergency email address	+			+	
Emergency GSM call	+			+	
Emergency phone number	+			+	
Emergency SMS	+			+	
Emergency SMS number	+			+	

Emergency Timer

Check Emergency timer properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
Warning timer (seconds)	+			+	

Impact

Check Impact properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
Impact detection	+		+	+	
Impact limit (G)	+		+	+	
Impact time (milliseconds)	+		+	+	

Man Down

Check Man Down properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
Man Down	+		+	+	
Tilt (degrees)	+		+	+	
Tilt timer (seconds)	+		+	+	

Miscellaneous

Check Miscellaneous LWP properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
Not active when charging	+				

Movement

Check Movement properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
Track movement	+		+	+	
Inactivity timer (seconds)	+		+	+	

Periodic Check

Check Periodic check properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
Periodic check	+		+	+	
Periodic check countdown (seconds)	+		+	+	

Sensor Check

Check Sensor check properties for details.

Setting	T.Flex for Android Smart	T.Flex for Android PTT	T.Flex for iOS	T.Rodon Smart	T.Rodon PTT
GSM call sensors check	+				
GPS sensors check	+		+		
WI-FI connection sensor check	+				
Bluetooth connection sensor check	+		+		
Sensor check validator period	+		+		
Vehicle mode	+		+		

Annex III: Managing favorites

By default, the contents of My TASSTA screen in in T.Flex and Favorite PTT plugin in T.Rodon are device-specific. If a user logs into the client application from another device, he/she gets a blank favorites screen that needs to be completely reconfigured.

We offer a centralized approach to storing and managing favorites on the server side. It is configured individually for each user:

1. Open the user settings.
2. Expand Miscellaneous section.
3. Turn on Manage Favorites configuration on server.

Once the setting is enabled, layout, contents and customization of My TASSTA screen in in T.Flex and Favorite PTT plugin in T.Rodon are stored on the server. The user will no longer be able to change the contents of the screen, including re-ordering the tiles. In return, he/she will see the same favorite tiles no matter what device they are logged in on.

> NOTE:
>
> The content of My TASSTA screen is platform-specific.The tiles under T.Flex Android and T.Flex iOS are configured and saved separately, even if favorites are managed on the server side.

Additionally, this functionality allows you to apply the same favorites screen layout to multiple users:

1. Identify the user who will be used as an "exemplar" for favorite screens. It can be one of the existing users or specifically created account.
2. Log in to client applications under that user account.
3. Configure My TASSTA / Favorite PTT screens in client applications.
4. Lock the user's favorites by enabling Manage Favorites configuration on server setting.
5. Check whether the favorites were saved. For each favorites screen saved on the server, the unique identifier should appear as the value of the following fields corresponding to each client app (refresh the page if necessary):
   - T.Rodon - Miscellaneous\Rodon Favorite PTT configuration
   - T.Flex Android - Miscellaneous\Flex Android My TASSTA configuration
   - T.Flex iOS - Miscellaneous\Flex iOS My TASSTA configuration
6. Right-click the user in the list and select Manage favorites.
7. Click Copy Rodon Favorite PTT configuration/Copy Flex Android favorites (My TASSTA)/Copy Flex iOS favorites (My TASSTA) depending on the client you want to apply favorites to.
8. Right-click the user you want to apply saved favorites to.

9. Select Manage favorites and click Apply Rodon Favorite PTT configuration/Apply Flex Android favorites (My TASSTA)/Apply Flex iOS favorites (My TASSTA) depending on the client for which you copied the favorites on *Step 7*.

TASSTA

All-in.

+49 30 57710674
hello@tassta.com
tassta.com

tasstaworld
t-a-s-s-t-a
TASSTAGmbHHannover
tassta_now
tassta_gmbh